Computer Hackers and Hacking: Exploring Those Lurking Behind the Screen

Michael Nycyk
MICHAEL NYCYK
COMPUTER HACKERS AND HACKING: EXPLORING THOSE LURKING BEHIND THE SCREEN
Computer Hackers and Hacking:
Exploring Those Lurking Behind the Screen

Author: Michael Nycyk

Design: Michael Nycyk
Front Cover Images:
Hacker– Anonymous Hacker Behind PC – Designer Credit: elconomeno@email.com
https://openclipart.org/detail/288357/anonymous-hacker-behind-pc
Used by permission from Open Clip Art https://openclipart.org
Publisher: Michael Nycyk, Brisbane, Australia
ISBN: 978-1-68454-806-4
©2018

Contact

The author at michael.nycyk@gmail.com

This publication is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia (CC BY-NC-ND 3.0 AU)

See https://creativecommons.org/licenses/by-nc-nd/3.0/au/ and https://creativecommons.org/licenses/by-nc-nd/3.0/au/legalcode

No article in this book may be reproduced in any form by any electronic or mechanical means without permission in writing from the author.
## CONTENTS

**Acknowledgements**  
1

**Chapter One - Introduction**  
2
Definitions of Hackers, Hacking and Cybercrime  
3
Types of Hacking  
6
Understanding Computer Virus Transmission  
10
Frederick Cohen and the Computer Virus: A Defining Moment in Virus History  
11
Malware, Worms and Trojan Horses  
13
Major Hacker Attacks on Systems  
19
Why Do Hackers Hack?  
23
Classification of Hackers and Hacking Activity  
26
The Main Types of Hackers and Hacking  
27
What do Hackers Use to Hack?  
30
Legal Consequences of Hacking  
33
Chapter Summary  
36
This Book’s Exploration of Hackers and Hacking  
36
Chapter Contents  
36
Potentially Offensive Material in Book Alert and Use of Technical Terms  
37

**Chapter Two – History of Hackers and Hacking**  
41
1903 – The First Recognised and Recorded Hacker Incident  
41
Hacking to keep Populations Safe: the Enigma Machine  
43
The First Ethical Hacker? René Carmille and the Register  
44
First Accounts of Hacker Viruses in the Computer Age  
45
Chapter Three – A Case Study of Hackers: Anonymous 78
Part 1: Formation, Structure, History and Ethos of Anonymous 79
A History of Anonymous 86
Controversies and Divisions in Anonymous: Arrests and Legal Trials 87
Part 2: Targets and Causes: Documenting Anonymous Attacks 92
Operation MegaUpload 92
Operation Chanology: The Church of Scientology Protest 94
The Westboro Baptist Church and the Newtown Sandy Hook Protest 98
The WikiLeaks and Anonymous Conflict 100
Other Anonymous Attacks and Causes 102
Conclusions and Summary 108

Chapter Four – An Example Study of Hacker Behaviours 113
The Study’s Theoretical Framework: Power and Capital Concepts 114
The Study 116
Conclusions and Summary 135

Chapter Five – Hacking and Gender, Hacking and Cinema Portrayals 137
Woman Hackers 138
Ten Women Hackers 139
Conclusion of Women Hackers’ Profiles Samples 142
Computer Hacker’s Representations in Cinema 143
List of Figures

Figure 1. Flame virus as computer virus example (Tracy, 2012) 7
Figure 2. Unaffected DOS computer screen (danooct1, 2012) 8
Figure 3. Affected DOS computer screen with letters falling to bottom of screen (danooct1, 2012) 9
Figure 4. Virus transmission from email attachments 11
Figure 5. Cohen’s example of computer virus presented in Maryland (Cohen, 1984, p. 242) 12
Figure 6. Adware example (Valeros, 2016) 13
Figure 7. Ransomware attack screen message demanding payment (Caldwell, 2017) 15
Figure 8. Common message sign of a DOS attack (Thatcher Development Software, 2013) 17
Figure 9. Christmas Tree virus/work 1987 (Brown, 2018) 20
Figure 10. All in One Keylogger software (TechTarget, n.d.) 31
Figure 11. Marconi’s machine and the projector that was hacked (Smithsonian Channel, 2013) 42
Figure 12. The Enigma Machine (BBC, 2018) 43
Figure 13. Message from Brain virus creators for people to contact them for inoculation (Radeska, 2016) 48
Figure 14. Morris worm code (Kelty, 2018) 49
Figure 15. AOHell picture on startup of toolkit (Breakingvc, 2014) 58
Figure 16. FloodNet screen inviting people to send messages (Griffis, 2014) 62
Figure 17. The Melissa Virus in an email (Panda Security, 2017) 63
Figure 18. BSNL (2018) website before hacker defacement 70
Figure 19. BSNL website after defacement showing who did it (Chronicle & Suares, 2018) 70
Figure 20. Anonymous member reading a news announcement (Smith, 2015) 80
Figure 21. Anonymous member in mask (Strevo, 2008) 81
Figure 22. Anonymous rare public protest (Galloway, n.d.)
Figure 23. March with Anonymous marcher asked why they are there (Sevenblade, 2015)
Figure 24. Million Mask March Anonymous (van Nispen, n.d.)
Figure 25. Anonymous Scotland Million Mask March Brian McNeil (McNeil, 2014)
Figure 26. LulzSec tweet forthcoming hacking activity (Brenner, 2012)
Figure 27. Anonymous logo for Operation MegaUpload (Know Your Meme, 2012)
Figure 28. Tweet from Anonymous Twitter account celebrating victory
Figure 29. Feature that caused WikiLeaks Anonymous conflict (Kerr, 2012)
Figure 30. HAL from 2001: A Space Odyssey (Racatumba, 2006)
Figure 31. Hackers manually hack Turin Traffic Control system (Stack Exchange, 2015)
Figure 32. NORAD challenge text on computer from War Games (Ion Music, 2014)
Figure 33. Dennis Nedry computer hack screen as appears in Jurassic Park (BJ22CS, 2011)
Figure 34. An antivirus interface with choices for actions (Auslogics, 2017)
Figure 35. Example of virus warning (tothepc.com, 2010)
Figure 36. Scareware message on computer screen (Fraud Watch International, 2017b)
Figure 37. Ransomware message (Suberg, 2012)
Figure 38. Clear cookies (The Windows Club, 2018)
Figure 39. Possible threats to passwords
Figure 40. Password manager that stores multiple passwords (Snap Files, 2018)
Figure 41. Warning of possible untrusted website certificate (BT, 2018)
Figure 42. SSL https shown in browser bar
Figure 43. Scam email using eBay (SiteMinder, 2018)
List of Tables

Table 1: Examples of hacking events over the decades since hackers have attacked computer systems 20

Table 2: Why hackers hack explanations 25

Table 3: Hacker and hacking terms 28

Table 4: Anonymous attacks and causes 103

Extra Table in Chapter Four within Research Article

Table 1: Capital Type, Theme Names and Theme Elements 122
Acknowledgments

This is the third book in a series exploring Internet issues. The first was called *Adult-to-Adult Cyberbullying: An Exploration of a Dark Side of the Internet*, published in 2015, while the second was called *Trolls and Trolling: An Exploration of Those That Live Under The Internet Bridge*, published in 2017.

Hackers are a major concern as we move towards more use of information technology and artificial intelligence. Although alarming, understanding hackers and how to prevent hacking is valuable. This book raises awareness of this issue. Like the first two books, it is a mixture of practical and academic material. While not totally conclusive and recognising not all material can be covered in this type of book, it still functions as a reference guide.

I would like to thank:

Again, like the first two books, Dr Thomas Apperley of Deakin University Melbourne for advice on book layout.

Professor Tara Brabazon, Dean of Graduate Research and Professor of Cultural Studies at Flinders University, Adelaide for incredible encouragement especially confirming that any form of research and writing offered up for public scrutiny is still worth doing. Thank you.

Cybersecurity and hacking is important. In exploring those that are lurking behind the screen, I want to again thank the vast numbers of people from the first hacker to current hackers, and to those who have written and published about them.

PLEASE BE AWARE THIS BOOK CONTAINS MATURE CONTENT WHICH SOME MAY FIND OFFENSIVE
CHAPTER ONE
INTRODUCTION

What hackers do is figure out technology and experiment with it in ways many people never imagined. They also have a strong desire to share this information with others and to explain it to people whose only qualification may be the desire to learn. – Emmanuel Goldstein, pen name of Eric Corley

It is a fairly open secret that almost all systems can be hacked, somehow. It is a less spoken of secret that such hacking has actually gone quite mainstream. Everybody hacks … sometimes. – Dan Kaminsky, American Security Expert 2013

We now see hacking taking place by foreign governments and by private individuals all around the world. – Michael Pompeo, Director of the Central Intelligence Agency in 2017

At the end of a long working week you look forward to being paid on Friday. You go to the Automatic Teller Machine after work to get some cash for a dinner and drinks evening with friends. Your account balance is zero. What happened? You ring your bank’s emergency number and ask why the money is not there. They claim the money went in your account but was withdrawn immediately. There is nothing they can do. You have become a victim of a computer hacker.

These scenarios have become common as our reliance on the Internet increases. We have many passwords for many accounts that are not unique and often not changed. We place our trust in websites and phone applications (apps) to do financial transactions. We often buy goods and services using our credit cards. We visit web sites without updating our firewalls and anti-virus software. Our personal data, especially our names, addresses and electronic mail (email) addresses, are stolen. The constant battle of banks, governments and businesses to protect your data is growing. Hackers have a long history of causing disruption and mayhem. Now, in this online age, the potential for catastrophic damage is on a global scale as electricity grids are shutdown and money can disappear from bank accounts instantly.

Hacking has gone from an underground to a mainstream practice. Plenty of online public tutorials, hacker forums and social media groups offer advice on how to hack. Yet not all hackers are criminals; some are considered heroes and some have turned from malicious hacking to helping the companies they hacked to stop other attacks. It has become a complex issue for our society to manage and prevent.

This book aims to inform the reader about hackers, hacking and the types of cybercrime that raises concerns and anxieties about one’s online safety. There are many books about hacking, its history and its consequences. A World Wide Web search can yield many alarming stories about hackers. This book will discuss a selection of hacking issues designed to create an awareness of the depth of these issues and an appreciation of the hacker ethos and mindset.

To begin, a framework of who, what and how of hackers is presented in this chapter. It serves to show what will be discussed in this book and define the terms that are used.
Definitions of Hackers, Hacking and Cybercrime

The terms ‘hacker’, ‘hacking’ and ‘cybercrime’ strike fear into people based on past perceptions and knowledge, combined with the panic of media reporting, that such people are out to cause harm. In this book these will be defined to create an understanding of whom they are, what they are and what they do. These are general definitions based on a collective and common understanding of them.

Hackers

Hackers are people who share an appreciation of technology, how it can be turned into new and unexpected uses, and have a low-level familiarity with the operation of it, being capable of devising technically elegant software solutions.

The key part of this definition, based on Jordan and Taylor’s (1998) and Levy’s (1984) descriptions of hackers, is the ability of a person to change technology and design a new way of using it. Hackers use skills to change a system often, but not always, for a criminal or mischievous cause. This is the main point to remember; for whatever reason a hacker tries to take what is and change it to extract something from it and turn it into something it is not. This view will become clearer as more examples of hacking are discussed.

Scholars and media reports have over time added several views on hackers that convolute understandings of them as good or bad people. Negative views of hackers are generally culturally accepted as true. These reports and opinions are significant to be considered in understanding the nature of hackers:

1. Hacker, as a label, has acquired a negative connotation of computer criminal and electronic vandal (Chandler, 1996).

2. The public tends to stereotype hackers as clever, yet sinister computer criminals who essentially live in cyberspace where they go on thrill-inducing missions to exploit vulnerabilities in other networks and systems (Bachmann, 2010).

3. There exists an informal hacker community where collegial groups share information (Holt, Strumsky, Smirnova & Kilger, 2011) and virtual communities and social media teach new hackers (newbies) ethical and non-ethical hacking techniques (Nycyk, 2016).

4. Hackers within such communities or meritocracies\(^5\) as they are also called, are judged based on their skill and abilities to hack then self-promote on social media and virtual community forums (Holt, Strumsky, Smirnova & Kilger, 2011; Jordan & Taylor 1998; Holt, 2007). However, such communities are often collegial with much information sharing on how to hack taking place, but also experienced hackers sometimes admonishing newbies when they post requests for illegal activity hacking (Nycyk, 2016).

5. Hackers still maintain a culture of being secretive (Holt, Strumsky, Smirnova & Kilger, 2011) despite posting online public postings on how to hack.
6. Males may still be the dominant gender in the hacking community, but the number of female hackers has grown over time. Four examples include: Natasha Grigori who used her hacking skills to uncover those involved in children pornography, Kim Vanvaeck who created viruses to destroy information, Krisina Svechinskaya who attacked bank accounts with Trojan horses (a type of malware) and Chinese hacker Ying Cracker who offers her hacking knowledge services for a fee to prevent hackers accessing systems (TechLog 360, 2017).

7. Hackers are labelled deviants based on their social group membership, accepting themselves as being apart from mainstream society (Turgeman-Goldschmidt, 2008; Becker, 1963).

8. Hackers range extremely broadly in their activities from script kiddies who only copy code to international cyberterrorists who seek to destroy banking, infrastructure and warfare hardware and software to create chaos and anarchy in nations.

9. Hackers are classified according to three hat colours: black, white and grey. Xu, Hu, and Zhang (2013, p. 66) describe these as:

   Computer hackers gradually separated into two camps – white hats and black hats – depending on motivation and objective. White hats are on a quest for knowledge, discovering and alerting security weaknesses in organizational systems and developing better, more secure computer systems; black hats go for revenge, sabotage, or outright criminal gain (such as to steal money, products, or services). In between are gray hats who hack for curiosity, fun, notoriety, or self-fulfillment but usually do not intend to harm their targets.

In summary, the hacker has common characteristics that define what they are and what they do. Turning a computer system into something new or unexpected through devising solutions to problems by changing how software and hardware operates is a broad and appropriate definition.

**Hacking**

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator’s original objective (Laws, 2007) and is broadly defined as intentionally accesses a computer without authorization or exceeds authorized access (USLegal Inc, 2016).

In this definition, the key terms are accessing, modifying (altering) and achieving a goal. This is the process of hacking that applies to all hacking activity.
Cybercrime

Cybercrimes are defined as those:

1. Directed at computers or other devices.
2. Where computers or other devices are integral to the offence (for example, online fraud, identity theft and the distribution of child exploitation material) (Australian Cybercrime Online Reporting Network (ACORN), n.d.a).

Cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences (Australian Institute of Criminology, 2011). Hacking can be a form of cybercrime, although examples of what are called cybercrimes are broad such as:

- Identity Theft and Forgery
- Credit Card Theft and Scamming
- Child Exploitation Material
- Copyright Infringements as represented by the famous case of Napster in the 1990’s
- Computer Viruses
- Email Spam and Scams
- Online Piracy such as Bit Torrents where movies and music can be downloaded for free
- Steganography which is concealing information within files

Controlling hacking and cybercrime is very difficult as it takes place across transnational boarders making prosecution difficult. Attempts have been made to standardise hacking laws across the world, such as that which took place in 2001 by the Conseil De L’Europe (Council of Europe) with the creation of a treaty called the ETS NO. 185 Convention on Cybercrime (Conseil De L’Europe, n.d.). Although it was primarily for use of the member States of the Council of Europe and associates it assisted other countries to formally recognise the growing problems of hacking and cybercrime.

This treaty was heavily criticised by security experts as to its validity to force governments to take action with quick formation of hacking and cybercrime laws. The problem of controlling computer crimes is reported by Weber (2003, p. 426) as:

The jurisdictional problem of cybercrime manifests itself in three ways: lack of criminal statutes; lack of procedural powers; and lack of enforceable mutual assistance provisions with foreign states. Because international cooperation on cybercrime has traditionally been the exception rather than the rule, these requirements are frequently an insurmountable barrier to the successful prosecution of cyber criminals.
This is the main problem that hinders progress on catching hackers. In a later chapter I will discuss some ways of protecting home computers and devices against cybercrime, but it is of great concern that daily attacks occur on large-scale computer systems that go unpunished.

Types of Hacking

This section has a substantial discussion of types of hacking to give an indication of how it appears and what it consists of. The discussion in this section is not exhaustive and focuses on common types of hacking and hacker techniques. It will attempt to avoid as much jargon as possible, but will need to explain technical terms.

Computer Viruses

A computer virus is defined as:

A program that can replicated itself and infect a computer, spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive (Khan, 2012, p. 8).

A computer virus is often compared to a human biological virus and certain terms used to describe how they work. They can be broadly defined as an infection that attacks the very basics of the global order (Parikka, 2005). Metaphors such as ‘infected’, ‘spread’ and ‘epidemic’ are often used when talking about computer viruses in the same way to describe biological viruses (Buiani, 2005).

Hacker viruses are feared by personal and business computer users. A business has reputation and monetary values it wants to keep, but if their data is hacked or destroyed it can be devastating for them. These fears are accurate as there are destructive, polymorphic and increasingly unpredictable, self-replicating, viruses that are causing more issues as they are transmitted across the Internet (Gan, Yang, Liu, Zhu & Zhang, 2012; Serazzi & Zanero, 2004). Computer viruses appear as code where instructions to execute (that is open or start) the virus are embedded amongst correct code. Figure 1 is an example The Flame Virus code that affected the running of computer systems in Iran in 2012. Note the highlighted section displaying the instruction InstallFlame which causes the computer systems to become infected:
Figure 1. Flame virus as computer virus example (Tracy, 2012)

Also notable are the names hackers give viruses that they create. On The World Wide Web a wiki site called *The Virus Encyclopedia* keeps track of these names. Five examples of such virus names that were well-known are:

1. **The Melissa Virus:**

   This virus was created by David L. Smith in 1999 which was based on what is still a common problem; putting a virus into a Microsoft Word macro and sending a Word attachment in an email with the message “Here is that document you asked for, don’t show it to anybody else” (Strickland, 2017). It was one of the first email viruses to become known to the public. The main thing it did that caused concern was it disabled corporate and mail servers causing slow receiving of email, which at that time was disastrous (Rouse, n.d.).

2. **ILOVEYOU Virus - also called The LoveBug:**

   In 2000 24 year old Pilipino hacker, Onel De Guzman, created a virus by sending it through emails with the subject ILOVEYOU and in the body of the text “kindly check the attached LOVELETTER coming from me”. When opened it added a file to the user’s computer registry, corrupted files on the hard drive, and then went into the user’s address book and sent the email to others. The virus spread quickly because the email came from people the user trusted (Brodie, n.d.). With companies, it was reported that they were hit hard with corrupted files and anti-virus companies could not control it due to the sheer number of people downloading it. The LoveBug showed how to get spam to send itself and how, with a cleverly designed virus that preyed on human psychology and technical failings, it could affect enormous numbers of computer users (Ward, 2010).
3. CIH Virus – also called by the mass media The Chernobyl Virus

In 1998 Taiwanese student, named Chen In-hau, created a virus that attacked hardware wiping data from hard drives and overwriting the Basic Input/Output System (BIOS) chip that then had to be replaced. In some cases the entire computer’s motherboard also had to be replaced. What is unique about this virus is how it was programmed to activate on the anniversary of the Chernobyl reactor meltdown, the 26th of April 1986 (Cluley, 2011). It is an example of the power of a destructive computer virus because it left some computers unusable.

4. The Cascade Virus

An early virus created in the 1980’s, Cascade was notable as a prankster virus having the effect of making the computer screen’s characters fall to the bottom of the screen when a .com (containing commands for the computer) was executed. It was also called ‘Fallen Tears’ and ‘Autumn Leaves’ and was considered an insidious virus because it was one of the first that could camouflage itself using an encryption algorithm (Ferbrache, 1992). To illustrate the operation of this virus, Figure 2 shows a Disk Operating System (DOS) command screen before the virus is executed:

![Figure 2. Unaffected DOS computer screen (danooct1, 2012)](image)

By contrast, Figure 3 shows the screen’s text missing characters because the virus has given the computer a command to drop the letters at random to the bottom of the screen:
5. Shamoon Virus

This virus appeared in 2012 and attacked the NT Kernel\textsuperscript{10} bit-based Microsoft Windows, a part of the Windows operating system that controls hardware and systems resources. Its power was that as a virus it could shut down computers and destroy data. It was identified in the cyber attacks on RasGas Qatar in 2012 (Zetter, 2012) and Saudi Arabia’s Aramco, shutting down computers and deleting files (Pagliery, 2015).

Shamoon, executed by an employee opening a link in an email, is worth describing to appreciate the procedure a virus does to gain a hold into a computer system. As this description by Symantec Security Response (2016) highlights, one insidious part of hacker created viruses is the overwriting of the computer’s normal instructions that results in deletion of files:

Shamoon can spread from an infected machine to other computers on the network. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, upload them to the attacker, and erase them. Finally, the virus overwrites the master boot record of the infected computer, making it unusable.

These five examples of hacker viruses show the creativity and destruction hackers can do when creating them. Many others have been created and been given names that have become well-known and infamous. Anti-Virus companies, such as Norton, Symantec and AVG, face a constant daily battle to update their anti-virus definitions to combat such attacks. However, hackers are sophisticated and the growth in scale of attacks can be attributed to the ability to hide viruses within the computer codes that cannot always be detected by anti-virus software.
Understanding Computer Virus Transmission

A simple concept of understanding how a virus works is to visualise the virus code piggybacking onto other programs and documents which is necessary for the virus to be executed, that is, it runs and infects the computer. Brain (n.d.) describes how this works:

The virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies it to add the virus's code to the unsuspecting program. Then the virus launches the “real program”. The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time either of those programs gets executed, they infect other programs, and the cycle continues.

Although viruses are changing with technological developments, there are two recognised types of viruses (Horton & Seberry, 1997):

1. The Direct-Action Virus – Initially executed in the course of the daily use of a computer system as it identifies executable objects for infection, but in an interesting hacker move to cover their tracks, will exit the system after infection.

2. The Resident Virus – Installs itself in computer’s memory and lies there until it is executed at some future time infecting files.

The operation of both types of viruses is of concern because of their mutability and their inability to always be picked up by anti-virus software.

Ferbrache (1992, p. 31) offers this technical explanation of how viruses get into computer system, arguing that there are four methods of inserting code into the host’s system:

The first question is: How can a virus insert its code into the host system? This can be achieved in a variety of ways - there are four primary methods of inserting a block of viral code into a host executable program, namely:

1. Prepending: moving the original host's code (or part of the code) to a later memory or disk location, leaving a gap into which the virus can insert its code.

2. Appending: simply adding the virus' code to the end of the host program.

3. Shell: embedding the host's original code within the virus as a subroutine.

4. Overwriting or injective: the host is destroyed by being overwritten by virus code.

Company workers can also be virus carriers by inserting USB keys, DVD’s or CD’s, and in the past floppy disks, into their computers, not checking them for viruses and running them. As stated before, files from the Internet and World Wide Web can carry viruses that attach themselves to the system, but email attachments and links are still primary carriers of viruses.
An example of a virus transmission through email is shown in Figure 2 which occurs when a person opens an email attachment. Note the circular grey part of the diagram; this represents if the virus has not stopped and how it can start again:

![Virus Transmission in Email](image)

*Figure 4. Virus transmission from email attachments*

On a personal home computer it can find a user’s email address book and send automatic emails to everyone in it. This can be embarrassing as pornographic and abusive messages have been sent by hackers using a virus that then sends them on to everyone on the address list.

As Horton and Seberry (1997) state, the virus infectors, the parts of the code that infect the files, are activated by attachment of code to other executable files and in a boot sector where many commands are embedded that run the computer. Hackers have done these using other computers within the organisation which are termed zombie computers. This type of computer is one that hides, aids and abets viruses in the absence of the owner’s or user’s awareness, as the computer is being remotely controlled by a hacker (Muller, 2011). As Erickson (2008) states, computer networking in organisations and in people’s homes, is taken for granted and many do not realise the vulnerabilities that exist in the networked applications such as email, the Web and instant messages.

**Frederick Cohen and the Computer Virus: A Defining Moment in Virus History**

The work of Dr Frederick Cohen was considered a defining moment in computer virus history. This was because although computer viruses had previously existed, Cohen is credited with defining what a virus is and how it worked as an infection. He studied at the University of Southern California and in 1983 demonstrated at a computer security seminar how a virus implanted in a Trojan program called ‘vd’ as part of his experimentation with the
VAX virus resulted in his gaining full system permissions to a mainframe computer system (Ferbrache, 1992). He also continued to experiment infecting other systems to prove how computer viruses could propagate in military security systems. After publication of this thesis, he did research over the decades recognising the growing threats of virus that were fast emerging.

Cohen produced a simple but comprehensive theory of computer viruses that he discussed in his thesis. In 1984 at the 7th Conference on Computer Security, he published a conference paper that laid the foundation for understanding what a virus is that, although not always universally agreed upon (Highland, 1997), is reproduced here to show the beginning of the public understanding of them (Cohen, 1984):

We define a computer ‘virus’ as a program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows.

Although there were criticisms of his work, such as it being not practical enough for industry (Highland, 1997), over time his research was influential in suggesting ways of protecting systems from computer virus attacks. Among the features of the paper was an example of a simple virus code that alerted his audience what to look for and what a virus code looks like. Figure 5 reproduces this exact code showing how a simple set of instructions Cohen provides can put into motion a virus attack on a computer system:

```
program virus :=
{1234567;
 subroutine infect-executable :=
 {loop: file = random-executable;
 if first-line-of-file = 1234567
 then goto loop;
 prepend virus to file;
 }
 subroutine do-damage :=
 {whatever damage is desired}
 subroutine trigger-pulled :=
 {return true on desired conditions}
 main-program :=
 {infect-executable;
 if trigger-pulled then do-damage;
 goto next;
 }
 next:;}
```

*Figure 5. Cohen’s example of computer virus presented in Maryland (Cohen, 1984, p. 242)*

The current hacker created viruses are unlikely to contain the word ‘virus’ in them, hence they can be more difficult to find. Cohen’s contribution in the early 80’s was significant in terms of alerting industry, government and the public on what is a virus and how they work, but also on how to prevent them. As at the time of writing he is still working in this area.
After his discoveries, and over time, more types of hacker attacks began occurring, aided by the invention and use of the Internet.

**Malware, Worms and Trojan Horses**

Malware is short for malicious software that can alter systems, destroy data and uncover private files. Viruses are considered malware, but in this section other types of it are discussed.

1. **Adware**

Adware is a program that installs an additional component that causes unwanted advertising to appear on the computer screen, often by delivering pop-up ads or by installing a toolbar in your browser. This malware can introduce system anomalies or incompatibilities that cause problems with other programs and can disrupt the functioning of the operating system as well as making it difficult to reconfigure a start page or toolbar back to its original setting (Landesman, 2017). Figure 6 is an example of adware:

![Adware Example](image)

*Figure 6. Adware example (Valeros, 2016)*

To appreciate the scope of the worldwide cost of malware attacks, Computer Economics Online (2007) and Distler (2007) estimated malware infections in 2006 cost $13.3 billion dollars. Argued over time is that anti-malware software has reduced this spread, but the cost is still large to users and a problem is that installing patches to stop this malware still requires human intervention (Provos, McNamee, Mavrommatis, Wang & Modadugu, 2007).

2. **Spyware**

This is software designed to covertly collect information from a computer system without the permission or knowledge of the computer user (Interhack Corporation, 2018). When it is installed it will transmit information through the Internet connections and networks. Common types of spyware include:
- Keylogging Software
- Form Fillers
- Trackware
- Cookies
- Rootkits - This is a computer program designed to provide continued privileged access to a computer while actively hiding its presence
- Web Beacons - a transparent graphic image placed on a website that monitors the computer user’s behaviour

3. Worms

A worm is a small piece of software that uses computer networks and security holes to replicate itself (Brain, n.d.). A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

4. Trojan Horses

A Trojan Horse program has the appearance of having a useful and desired function. Secretly, the program will perform other undesired functions. These may cause data destruction or compromise a system by providing a means for another computer to gain access, thus bypassing normal access controls, such as Firewalls. Trojan horse attacks are one of the most serious threats to computer security as they can be spread in the guise of literally anything, which makes it difficult to notice them (Khan, 2012, p. 9).

5. Ransomware

Ransomware is a piece of pernicious software that exploits a user’s computer vulnerabilities to sneak into the victim’s computer and encrypt all his/her files (Liao, 2017; Unitrends, n.d.). The key point with this hacker attack is the locking of the files with strong unbreakable encryption11 that usually cannot be unlocked by computer users. The attacker keeps the files locked unless the victim agrees to pay a ransom or the price of giving a key or code to unlock the computer increase. It results in data loss and is a form of blackmail. It is wasteful for large organisations in terms of time lost and money paid out to hackers, can be critically devastating if crucial data, such as patient health records, is locked and is personally distressing to the user who loses data such as personal photos. As such it is considered the most insidious of malware, especially as the payment usually needs to be made by cryptocurrency12 Bitcoin13, which home computer users may not have.

Unitrends (n.d.) identified the software program LataRebo Lock as one example of ransomware software giving this technical explanation:
LataRebo Locker prevents its victims from using their computers by using a large image containing the ransom note. It adds entries to the Windows Registry to enable activation whenever the user’s operating system starts up. It will also add additional registry entries that disable the task manager, preventing users from terminating its process.

Figure 7 shows a message which appears on the screen when your computer is infected with ransomware malware:

Figure 7. Ransomware attack screen message demanding payment (Caldwell, 2017)

There is also a dilemma for companies who have to pay the hackers because they may pay the ransom without consulting law officials so the company’s reputation remains intact (Axelsen, 2017).

The list of high-profile companies damaged by ransomware attacks has grown. Two high profile attacks were on pharmaceutical company Merck and global freight company Fed Ex, causing data loss and negative impacts on their financial performance (Braue, 2017). To date, the worst attack occurred in 2017 when Britain’s health system had a ransomware attack that had consequences such as the cancellation of patient operations (ABC News, 2017). In an Australian study, Osterman Research (2017) found from a survey that another identified problem with ransomware were the detrimental effects on work productivity with no access to computer systems for long periods of time. Ransomware is clearly one of the most negative creations hackers and cyber criminals have created to date.
Summary

These examples of malware are a sample of what computer user’s face from hackers. There are solutions to minimising, and preventing, such attacks in the form of anti-virus and anti-malware software. Suggestions on these will be discussed in a later chapter. Other types of hacker attacks are now discussed.

Logic Bombs

The logic bomb is considered a malware Trojan Horse, not a virus, which causes widespread computer system destruction. They are camouflaged segments of code embedded in the computer program, mostly used to destroy data once a certain condition is met (Khan, 2012). Although code can be searched, if a computer code has thousands of lines of code it can be difficult to find a logic bomb. For example, in the code below the letters cmd stand for execute a command, or tell the computer to do something, dstr meaning destroy data and to execute data destruction at midday on the 13th of May 2018.

<cmd>s dstr 13-05-2018_12:00<cmd>

Simple commands like this can cause data loss and also be passed onto other computer systems by email or the Internet.

Denial of Service (DOS)

A Denial of Service attack stops people from using someone’s website and is a common hacking strategy. This denies the user the opportunity to use the web site that can cause the owner to lose business. A technical explanation is offered by Schuba, Krsul, Kuhn, Spafford, Sundaram and Zamboni (1996) as to how the DOS attack works:

It works by an attacker sending many TCP (Transmission Control Protocol) connection requests with spoofed source addresses to a victim's machine. Each single request causes the targeted host to instantiate data structures out of a limited pool of resources. Once the target host's resources are exhausted, no more incoming TCP connections can be established, thus denying further legitimate access.

These are network based attacks occurring through the business’s computer networks, although it can be also done through exploiting vulnerabilities on the host’s computers own computer internal computer system (Gu & Liu, 2007). Hackers doing this may be people within a business’s own organisation. Another term seen in this type of attack is the hacker’s use of what are termed zombie computers where they contact the server where the website is hosted, causing the website to be slow to reach and even be shut down. To illustrate these actions, Figure 8 shows a DOS attack by a simple message that confronts the user when they try to reach the site they want to view:
The DOS attack is also reasonably easy to do as there are online hacker tools that can be downloaded to undertake this type of attack.

**Structured Query Language (SQL) Injections**

Our personal details are now contained in countless databases across the world, filled with information hackers would like to obtain. When obtaining information from a database, programmers use a programming language to manage data in a relational database system called Structured Query Language. It operates across many database management systems, especially on commonly used databases such as Oracle and Microsoft SQL Server Access. As databases contain much sensitive data, particularly financial, health and police record data, organisations struggle to keep SQL Injections from happening. There are legal consequences as people have taking out class actions against organisations that did not take steps to protect client or patient data from these attacks.

An SQL Injection Attack is code injection technique that is used on database where crafted SQL statements are inserted into database fields that trick the system into doing something it should not (Rapid 7, n.d.). Although many types of injections have been identified, the piggyback injection is a fairly common and harmful SQL statement that can extract data and send it to the hacker. Randive, Khatke and Reddi (2014) demonstrate an example of a piggyback SQL injection by querying a database. The first is a legitimate query asking the data to be returned with details only that would go to the client. In this case, it is finding out how much is owed on the client’s bank loan:

```sql
SELECT name FROM bank WHERE userid='prerna' AND pswrd=''; drop table Loans
```

This means select client name from the bank where the user id and password returns loan amount the customer owes.

Randive et al. (2014) then show this SQL injected statement that piggybacks on the above statement which runs after the above query. The database treats it as two queries but deletes the client information or sends it to a hacker:

```sql
SELECT name FROM bank WHERE userid='prerna' AND pswrd=' '; drop table Loans –
AND pin='123'
```
This statement can be inserted in SQL based databases, be executed and result in data loss or the passing on of information to hackers. Considering the millions of databases that exist, the potential for hackers to externally or internally write statements that can destroy data or collect information attests to the depth of the problem of SQL Injections.

**Network Hacking and the use of Cloud Computing**

As the size of computer-based data grows, a problem has been how to store data so it can be retrieved later. The solution was the invention of the computer cloud, or the cloud as it is known as. Cloud computing is (Woodford, 2017):

> Cloud computing means that instead of all the computer hardware and software you’re using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user - it's just somewhere up in the nebulous “cloud” that the Internet represents

However, it is no longer just for business; personal computer users can use cloud services for their data. Examples of cloud services that are free or cost include: Google Drive, Amazon Cloud, Apple iCloud Drive, Dropbox and Mega. It is tempting to use such services because computer hardware devices can break down and data can be lost. The decision to store data on a cloud server is influenced by convenience and ease of mind that important photos are somewhere that can be accessed should they be lost.

These cloud services are very susceptible to hackers; although much work is done to protect data, but it is alarming to consider that banks, for example, store details and money on cloud servers. Hacking a cloud server is considered a challenge by hackers. For example, celebrity photos, especially of naked female singers and actors, have been stolen from the cloud and posted online. Examples include: Sienna Miller, Kim Kardashian, Mischa Barton, Scarlett Johansson, Jennifer Lawrence, Selena Gomez and Hillary Duff. Cloud data storage is being used more frequently, therefore it is a hacker’s challenge to crack into such servers and steal data.

**Identity Theft**

A second fear computer users have is their personal details and bank account/credit card details being stolen and used by others. Identity theft is defined as the unlawful use of another’s personal information including: date of birth, name, address, email account and other details to secure credit, buy goods and services unlawfully, obtain employment or evade a criminal investigation (Hanel, 2011; Bellah, 2001). Unlawful in the context of identity theft is understood as constituting the unauthorised use of another’s personal information with intent to do criminal acts for personal gain (Allison, Schuck & Lersch, 2005).

Some types of identity theft are: phishing hacking into online accounts and hacking into business databases that one’s information may be stored on (Australian Cybercrime Online Reporting Network (ACORN), n.d.b). A common area of identity theft that has grown has been on social media, especially Facebook and professional networking site LinkedIn. Hackers take photos of existing user profiles and then send friend request to fool others
which, although normally these can be found out by users to be fake, have caused distress to the person whose identity was stolen (Bilge, Strufe, Balzarotti & Kirda, 2009).

A common hacker strategy is called synthetic identity fraud where information is picked from various sources, combined and then accounts opened in the name of someone who is fictitious (Kshetri, 2010). Identity theft can have legal and personal consequences that can have permanent devastating effects on those who experience it.

**Summary**

This section presented a sample of the types of hacker and cyber crime attacks that happen to computer users. Although many new types of hacker attacks are being identified, this section gave an overall appreciation of what types of hacking attacks are possible. Stopping these attacks is a multi-million dollar industry, with such attacks growing in scale with widespread serious consequences for society.

**Major Hacker Attacks on Systems**

Large-scale cyber criminal and cyber terrorist attacks are almost a daily occurrence. Although not an exhaustive list, this section lists a selection of hacker attacks that have taken place since the invention of networked computer system. Notable in these attacks are their scale and their worldwide effects on financial systems, infrastructure and on the privacy of those affected by such attacks.

These attacks demonstrate the potential of disruption to organisations and peoples’ lives, but also display the difficulties of putting into place strategies to manage them. Other attacks not in this table were significant in alerting the public to hackers and especially viruses. Additionally, Hollywood movies such as ‘Sneakers’, ‘The Net’, ‘Blackhat’ but especially the 1983 film ‘War Games’, have changed perceptions of hackers and showed the public it was a serious social problem (Robertson, 2017; Skibell, 2002).

Table 1 displays the selection of hacker and cyber incidents over time that was well-reported in the media and has become part of hacker history:
Table 1
Examples of hacking events over the decades since hackers have attacked computer systems

<table>
<thead>
<tr>
<th>Year</th>
<th>Hacking Attack Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1903</td>
<td>Inventor Nevil Maskelyne disrupted a public demonstration by John Fleming who was using Marconi’s secure wireless telegraphy system by sending various insults through Morse Code from the auditorium projector.</td>
</tr>
<tr>
<td>1940</td>
<td>Rene Carmille was a double agent in World War Two and convinced the Nazi’s to be in charge of a punched card system that was set up to find out Jewish French citizens, but hacked the system so the Nazi’s could not easily, or at all, find Jewish citizens.</td>
</tr>
<tr>
<td>1976</td>
<td>Famous hacker Kevin Mitnick gained access through a phone number for a system called the Ark, run by Digital Equipment Corporation, copying their software.</td>
</tr>
<tr>
<td>1986</td>
<td>The 414 computer hacker group hacked into several computer systems in the United States, of which the hackers were aged 15 to 22 years old.</td>
</tr>
<tr>
<td>1987</td>
<td>A hacker inserts worm malware into IBM mainframe automatically drawing a green Christmas Tree on the screen as Figure 9 shows:</td>
</tr>
</tbody>
</table>

![Figure 9. Christmas Tree virus/work 1987 (Brown, 2018)](image)

<p>| 1988 | Release of the Morris Worm created by Robert Morris interrupted and slowed down computer systems. |</p>
<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>A Russian hacker in St Petersburg hacks into a major United States bank and steals money.</td>
</tr>
<tr>
<td>2000</td>
<td>Russian Natural Gas Company Gazprom had a Trojan Horse try to gain access to control the gas pipeline system.</td>
</tr>
<tr>
<td>2001</td>
<td>California Power distribution centre is attacked by hackers on 2 web servers due to poor information technology security.</td>
</tr>
<tr>
<td>2003</td>
<td>Worm malware used on an Ohio nuclear power plant.</td>
</tr>
<tr>
<td>2009</td>
<td>Night Dragon cyber attack on global oil companies.</td>
</tr>
<tr>
<td>2012</td>
<td>The Saudi Arabia Shamoon Disttrack viruses released.</td>
</tr>
<tr>
<td>2012</td>
<td>Virus attacks in United States on power companies.</td>
</tr>
<tr>
<td>2013</td>
<td>Power grid attacks in Austria and Germany resulting in deliberate breakdowns of power systems.</td>
</tr>
<tr>
<td>2013/15</td>
<td>Hacking of power plant designs and system passwords on power plants in the United States and Canada.</td>
</tr>
<tr>
<td>2015</td>
<td>South Korean nuclear power plant hack.</td>
</tr>
<tr>
<td>2015</td>
<td>Department of Resources and Energy in Australia’s computer systems hacked.</td>
</tr>
<tr>
<td>2016</td>
<td>Israel malware attacks in electricity systems.</td>
</tr>
<tr>
<td>2016</td>
<td>Hacker steals patient data and offers for sale on the dark web or dark net.</td>
</tr>
<tr>
<td>2017</td>
<td>British health system ransomware attack.</td>
</tr>
<tr>
<td>2017</td>
<td>Cloudflare, a cloud storage provider, did not respond to a cloud leakage from a bug which resulted in data being able to be obtained from accounts.</td>
</tr>
<tr>
<td>2017</td>
<td>Ride sharing company Uber pays ransomware hackers when up to 57 million customer names, account details, email and phone numbers were hacked.</td>
</tr>
</tbody>
</table>

As this table shows, it is only a fraction of the reported cyber attacks and hacking activities that have occurred over a long period in time. They display how they have grown in depth and scale. There are other dimensions to these attacks in that some of these have resulted in distress to customers. Two examples of this are the hacks and service outages seen with the companies, dating site Ashley Madison’s data breach in 2015 and Sony’s PlayStation network outage in 2011. These company’s responses from these companies in managing the public’s angry responses to private details being obtained by hackers is considered just as bad as the hack itself.
In Sony’s case, the security breach attacks on the Sony PlayStation network in April 2011 caused them to turn off the network on April 20 for 23 days. The hacker group Anonymous claimed responsibility for the attacks but then withdrew attacks as the group felt they were hurting Sony’s customers. Yet within days a group called OurMine took control of the Twitter and Facebook social media accounts of PlayStation customers, with an estimated 77 million registered PlayStation Network accounts having their details leaked. The problem of this hack is how Sony that let down those who had PlayStation network accounts. Phillips (2016) wrote on Eurogamer’s site how Sony failed:

It was the first day of the PSN outage. The network would not come online again for another three weeks, until 14th May.

As the first day wore on, Sony warned customers it might take up to 48 hours before they could log in again.

The following day, Sony confessed - there had been an “external intrusion” and it was now conducting a "thorough investigation to verify the smooth and secure operation of our network services going forward".

But, so far, there had been no warning anyone's personal details were at risk. That news would not be confirmed by Sony for another four days.

A week into the outage, and Sony had remained silent on the exact cause. Speculation centred on Sony pulling the plug on PSN to thwart further attempts at its systems. But the updates from Sony itself remained positive, if slightly evasive. Sony engineers were "working around the clock" to restore services, PSN users were repeatedly reassured.

It was the evening of 26th April when Sony finally broke the bad news: the personal details of millions had been compromised.

This incident highlights the fragility of personal data but also the moral and ethical behaviours of a corporation. It does make the computer user weary to join sites and give their information online, but attacks like these will only increase.

A second major data leakage attack that caused embarrassment to millions of online customers was the data breach of online dating site Ashley Madison in July 2015. The name of the hacking group was The Impact Team who copied customer data and threatened to release it online. The hackers wanted the site shut down because it was a site where people could meet up online and have extramarital affairs. Ashley Madison had a policy of, if the client stopped using it the data would remain on their site. Lord (2017b) reproduced an interview extract which is claimed to be from The Impact Team where the hackers state it was easy to hack the site:
In an interview with Vice, Impact Team claims to have over 300 gigabytes of hacked Ashley Madison data. When asked to provide details about their attack, Impact Team claims that it was easy: “We worked hard to make fully undetectable attack, then got in and found nothing to bypass.” As for Avid Life Media's security, “Bad. Nobody was watching. No security.”

What compounded this problem was that people created websites where the email addresses and names of clients could be searched to find out the names of those who joined the site. This was called the Cheater’s List as reported by Dewey (2015) of The Washington Post. These websites consisted of search boxes where details were typed in to see if they matched the Ashley Madison member database. The issue with this is, regardless of one’s moral views about adultery, Ashley Madison’s data hack was a violation of trust between them and their clients.

These major hacker attacks over time demonstrated the depth and seriousness of a growing problem in society. It is concerning that as we put more of our private lives on the Internet and give details to companies, such as our credit cards and dates of birth, that we have to consider this; how safe is our data from hackers?

Why Do Hackers Hack?

Hacking is considered a criminal and deviant act by the law, psychologists and sociologists. There has been over time the persistent belief that hacking is a criminal act to be feared, a form of social deviance and poses a serious worldwide threat to information systems security (Nycyk, 2016; Dremliuiga, 2014; Taylor, Fritsch, Liederbach & Holt, 2011; Kshetri, 2010; Warren & Leitch, 2009; Flowers, 2008). This has been re-enforced by the mass media and entertainment industries portraying hackers as mostly criminals with negative childhoods, being loners and have vengeful, vindictive personalities. The majority of research focuses on males as hackers, but females and other genders have also become major hacker figures.

There is a body of sociological and psychological research asking why people become computer hackers, either for amusement or for criminal purposes. A number of reasons will be listed and discussed in this section. Four metrics are suggested by Atkinson (2015, p. 5) that suggests an overall technical and psychological skill set hackers acquire that motivates them to hack:

- **Persistence** – taking time and effort to understand a system and compromise it using attention to detail and resources to do so, including taking time to gather information to do so.

- **Skill** – the technical skills that the hacker possesses developed over time, such as programming, network hacking skills and systems administration.

- **Greed** – The amount or need to acquire information or compromise numerous systems define the greed that a hacker possesses in order to get the most out of their ill-gotten gains.

- **Stealth** – The ability to manipulate and exfiltrate data without being detected, compromise a system and alter system logs without raising alarms which makes for causing much destruction. This is a key skill in doing the act of hacking.
Bachmann (2010, p. 652) in his study offers this explanation of illicit hacker behaviours:

Hackers do in fact have a considerably higher need for cognition and higher risk propensity than the general public. They tend to prefer rational thinking styles over intuitive approaches and they demonstrate a particularly high confidence in their ability to reach optimal decisions through a rational deliberation process. They prefer complex problems over simple ones and they enjoy solving problems that require hard thinking more than the average person. Second, they are also more prone to engage in potentially risky behaviors than members of the broader population.

Xu, Hu and Zhang (2013, p. 64) also provide some insights into why hackers hack and how this develops over time:

- Computer hackers start out not as delinquents or as social outcasts but often as talented students, curious, exploratory, respected, and, most important, fascinated by computers.

- Associating with like-minded individuals make for a fertile ground in transforming young talents into hackers.

In a study by Young, Zhang and Prybutok (2007) they found across many other studies; that hackers considered their hacking to be morally right. Punishments are not always seen as a deterrent. Another commonly mentioned motivation is that hacking is a form of intrinsic motivation; engaging in hacking tasks purely for challenge and interest (Voiskounsky & Smyslova, 2003). Despite differences in research approaches, surveying the hacker motivation literature and asking why hackers hack has resulted in a common set of findings. These findings are also accepted by law enforcement that uses such information to understand the motivations for hacking attacks.

Table 2 displays a list of reasons from different sources about why people become hackers. The work of Kirwan and Power (2011) was consulted when compiling this table. They argue that hacker motivation research is divided into theoretical and empirical studies. The following ten examples are representational of the findings of computer hackers’ motivations to hack computer systems.
<table>
<thead>
<tr>
<th>Researcher Names and Publication Year</th>
<th>Reason for Hacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chandler (1996)</td>
<td>Imitate behaviours of others, model behaviour on other hackers</td>
</tr>
<tr>
<td>Taylor (1999)</td>
<td>Curiosity, boredom, enjoyment, feeling powerful, peer acceptance</td>
</tr>
<tr>
<td>Spitzner (2002)</td>
<td>Entertainment, peer acceptance and social group membership</td>
</tr>
<tr>
<td>Dreyfus (2002)</td>
<td>Look at success of hack not consequences</td>
</tr>
<tr>
<td>Fötinger &amp; Ziegler (2004)</td>
<td>Feeling inferior leading to hacking providing a feeling of power</td>
</tr>
<tr>
<td>Rennie &amp; Shore (2007)</td>
<td>Hacker experiences sense of flow(^1) – concentration, interest and control</td>
</tr>
<tr>
<td>Sharma (2007)</td>
<td>Desire for fame and money outweigh fear of criminal consequences</td>
</tr>
<tr>
<td>Chiesa, Ducci &amp; Ciappi (2009)</td>
<td>Intellectual curiosity, making the personal computer safer, conflict with authority, boredom, seeking fame, anger, political reasons, escaping from responsibilities</td>
</tr>
<tr>
<td>Ledingham &amp; Mills (2015)</td>
<td>Regarding self as a hero (especially extremist hacker groups)</td>
</tr>
</tbody>
</table>

Money and fame, or notoriety, are proven to be part of some hackers’ motivations, but the other human emotions of curiosity, alleviating boredom, being angry or desiring peer group acceptance are also high motivators for hacking.

A concerning trend is the idea that hackers have reputations to uphold, either positive or negative, and as such are moving quickly into hacking bigger targets and challenges. The Internet has provided this futile ground by hacking large-scale sites, such as social media, Ashley Madison or financial institutions, to do so. Computer hacker researchers Décary-Hétu and Dupont (2013, p. 2) articulate this problem well in their study of reputation amongst what are called botmasters who not only hack for material gain but also for reputational gain:
More recently, hackers have come to realise the extent of their power and rather than show off to their peers, they have been taking more and more advantage of the criminal opportunities that the Internet provides. This is reflected in a recent research which shows that criminals now use the cyberspace to commit banking fraud, extortion through denial of service attacks, intellectual property fraud as well as identity fraud. This transition has been facilitated by the diffusion of technical knowledge and tools that are required to commit these types of crimes. The Internet has always been celebrated for its ability to foster discussions and exchanges; it is therefore not surprising to see that criminals are also taking advantage of these features to maximise their criminal opportunities.

A motivation is that of gaining a reputation amongst other hacking groups and cyber criminals (Décary-Hétu & Dupont, 2013). Motivations for hacking still needs much work to understand trends and reasons for hacking, but this section demonstrated some examples of reasons why hackers do hack.

**Classification of Hackers and Hacking Activity**

Classification of hackers consists of terms used in their culture that have become widely used. To compile this list and their definitions, several sources were consulted to find commonly used terms. Table 3 gives terms and definitions of the main terms used to describe hackers and hacking activities.

An important point of this list is that it is free of gender titles and references to the physical characteristics of hackers and their societal status. Over time hackers were assumed to be mostly young Caucasian males, but this has proven not to be true with female hackers becoming well-known for their illegal and ethical activities. Kirwan and Power (2011) argued that much research supports the young male as the stereotype and whilst likely still the majority, this is changing. They also argue that many hackers have some type of formal education.

There are four main terms used to describe hackers and hacking used by society, the law and researchers use to differentiate between positive and negative hacking. These terms are: black hacker, white hacker, grey hacker, ethical hacker, as well as the practice of Hacktivism. They are known by the term ‘hat’ and are discussed first. Table 3 lists and explains several terms. Kirwan and Power’s (2011) work is again drawn upon for the table, with other sources included.
The Main Types of Hackers and Hacking

Black Hats:

The common characteristic of black hat hackers is that they are usually malicious. They are hacking computer systems for personal and selfish gain. Best (2003) makes a claim that the black hats are ‘new school’ hackers motivated by greed, political ideas or other negative motivations such as desire for becoming notorious. This does seem at odds though with the motivations of many hackers who are white or grey that actually fight with black hackers trying to stop the black hats from destroying computer systems. However, the black hat has become the cultural term accepted for those who are hacking for purposes that are criminal.

White Hats:

The white hat hacker is also called an ‘ethical’ hacker because they use their hacking knowledge for motivation to help individuals and companies be protected from black hat hackers. Often they are hired by corporations performing computer system activities such as penetration testing, test in-place security systems and perform vulnerability assessments for companies, often paid large salaries to do so (Symantec, 2017). They are not criminals and are said to be working within the law of where they are operating from. Crawley (2016) from a network security and company position, such hackers possess qualities, such as not backing down from hacking challenges, which makes them valuable to the data protection process and makes the risk of hiring them a wise corporate strategy.

Grey Hats:

The term for this type of hacker arose in 1999 in The New York Times to describe those who hack, fitting in between the black and white hacker spectrum (Kirsch, 2014). This intersection of hackers is called grey because they can undertake illegal activities, but also have prevented black hat hackers from carrying out hacks. An effective description is given by Aggarwal, Arora, Neha and Poonam (2014):

A Grey Hat in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits

It is reported that grey hats exploit computer system vulnerabilities but do little to no damage other than access (Hald & Pedersen, 2012), although the same authors suggest grey hacker, United States Private Bradley Manning who downloaded 700,000 classified documents from the United States military and passed them to WikiLeaks^{18}, is an example of a grey hat hacker being labelled by the media as a criminal.
Hacktivism:

This has become a popular term widely used in the media, often associated with WikiLeaks and hacker group Anonymous that has become a hacking practice as a form of protest against powerful agents, such as governments. A definition found of the term is by Sorell, (2015, p. 391):

Hacktivism is a form of political activism in which computer hacking skills are heavily employed against powerful commercial institutions and governments, among other targets.

It has various negative connotations and can be mischievous. Yet it can be positive because it fights for the rights of individuals. Anonymous, for example, received praise for its hacking of the conservative American Westboro Baptist Church, governments and political leaders. While demonised by the media, Anonymous has received much support for their actions.

Taxonomy and Definitions:

Table 3 lists and defines a selection of hacker and hacking terms, although it should be stated that new terms to describe hackers and their activities will arise in the future. Again, Kirwan and Power (2011) are mainly drawn on due to their expertise in naming types of hackers. Any others sources are listed in the table.

Table 3

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition/Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat (APT) Agents</td>
<td>This group is responsible for highly targeted attacks carried out by extremely organized state-sponsored groups. Their technical skills are deep and they have access to vast computing resources. It refers to a group, such as a government, with both the capability and the intent to persistently and effectively target a specific entity (Aggarwal, et al., 2014, p. 49)</td>
</tr>
<tr>
<td>Casual Hacker</td>
<td>Less active hackers, may not hack much but keeps up-to-date with what other hackers are doing (Zhang, Tsang, Yue, &amp; Chau, 2015)</td>
</tr>
<tr>
<td>Coders</td>
<td>Hackers with high level skills who hack in white or black ways</td>
</tr>
<tr>
<td>Crackers</td>
<td>Violent attackers who cause serious damage to an organisation such as delete data or releasing personal details</td>
</tr>
<tr>
<td>Cyber-Punks</td>
<td>Capable skilled hackers who intentionally engage in malicious hacking acts like defacing web pages</td>
</tr>
<tr>
<td>Cyberterrorist</td>
<td>Carries out acts of terrorism by hacking computer systems</td>
</tr>
</tbody>
</table>
Cyber-Warrior | Hack more for monetary reasons
Ethical Hacker | Another name associated with the White Hat Hacker
Guru | Guru hackers have reputations through the media or the Internet that make them sort after by other hackers (Zhang et al., 2015)
Industrial Spy | A hacker who is motivated by money, including employees who work for an organisation
Information Warriors | Another name for hackers who commit acts of industrial espionage (Hald & Pedersen, 2012)
Internals | Disgruntled employees in an organisation who deliberately hack a system or destroy data
Learning Hackers | These hackers may not always maliciously hack, but rather are constantly for their own reasons learning how to hack and will share knowledge with others in Internet forums and social media (Zhang et al., 2015)
Newbie | A beginner hacker who usually join Internet virtual communities and forums, constantly asking questions. They have also been called Green Hats and their title is abbreviated as nOObz
Novice Hacker | These hackers are still learning but tend not to share their knowledge with others (Zhang et al., 2015)
Quiet, Paranoid and Skilled Hacker | A hacker who is paranoid and covers their tracks with incredible skill
Phreaker | Phreaker is a telecom network hacker who hacks a telephone system illegally to make calls without paying for them (OmniSecu.com, 2018)
Script Kiddies | Use others’ hacking tools to hack and then boast to others especially on social media and virtual forums, often treated with contempt by established hackers like newbies are. However, these hackers have gotten angry against those that make fun of them and if they take revenge they can be labelled Blue Hats (GrayHat4Life, 2015)
Social Engineer | In hacking terms these use deception to persuade people to, mostly unknowing, give information about the organisation they are hacking, phishing through email is part of this engineering
The ‘37337 K-rAd iRC #hack 0-day exploitz guy | Kirwan & Power (2011, p. 57) state these are ‘Characters who would do anything to become “famous”...they are willing to use “brutal methods” to get where they want to be’ and they have
This sample of hacker types demonstrates not just the wide range of definitions and labels, but also the activities they do.

**What do Hackers Use to Hack?**

Although an in-depth technical discussion of the vast array of hacking tools hackers use in their activities is beyond this book’s scope, naming and brief explanations of some of them give an appreciation of hacking. Some of these tools are reasonably easy to learn and use. These software tools are in the public domain of the World Wide Web, so although many are illegal they are easy to find and download. Using them with criminal intent is illegal but also those who use them do need to learn them, often turning to public or private hacking forums, social media and the Dark Web to find experienced hackers to mentor them (Nycyk, 2016).

These five examples of hacking tools and were found on web searches, representing a sample of what hackers use. They were chosen based on their reputation as key instruments of hacking and to illustrate the relative ease of what hackers can use to access a computer system.

1. **Keylogging Software**

   A keylogger is a hardware device or a software program that records the real time activity of a computer user including the keyboard keys they press (Mitchell, 2017). This is a concern because passwords and banking details are entered as keystrokes and can be detected and recorded. They can also be remotely used on computer networks. Although they can be removed by anti-virus and anti-hacker detection programs, they can be effectively hidden on computer systems. Money stealing has occurred because of this. As Mitchell (2017) further explains these can:

   - capture any passwords entered by users on the device
   - take screen captures of the device at periodic intervals
   - record the URLs that were visited via Web browsers, and possibly also take screen captures of the Web pages viewed
   - record a list of the applications run by users on the device
   - capture logs of all instant messaging (IM) sessions
   - capture copies of sent emails
   - automatically send the reports containing stored logs and emails to a remote location (by email, FTP or HTTP)

   Figure 10 shows an example of hidden keylogging software. Note how so much private information is recorded on the screen:
Examples of known and publically downloadable keylogging include: Trojanspy.Win32.Brisse.d, KeySnatch, NetSpy KeyLogger, KeyLogger Pro and Remote KeyLogger 1.01.0. It does take skill for a hacker to place one on a network or personal computer, and sometimes keylogging software is used for legitimate reasons.

2. Remote Administration Tools

A remote administration tool (RAT) is a programmed tool that allows a remote device to control a system as if they have physical access to that system. While desktop sharing and remote administration have many legal uses, RAT software is usually associated with unauthorized or malicious activity (Ethical Hacking Tutorials.com, 2017). Examples include: ScreenConnect, AnyDesk, GoToMyPC, TeamViewer and Chrome (Google) Remote Desktop.

Many people have been victims of hackers that have scammed them through convincing the person, usually someone who has a home computer, that their software contains many viruses. By complying and agreeing to let the hacker access the computer remotely, it is possible to scam the person of money as the confused person gives the hacker their credit card number. The RAT is able to access the home computer and find out file names and personal details from visited web sites such as online banking.
As this is an important issue, RAT hacker tools and the scams they allow are briefly explained to show how insidious they can be (Thompson, 2018; Cormack, 2017; Australian Competition and Consumer Commission, n.d.):

- The scammer or hacker phones the customer usually pretending to be a staff member from a company such as a telecommunications one like Telstra in Australia, from Microsoft or even just claim to be a technical support staff member that they claim you ask for.

- One example of what they may say is that the computer has been sending error message or has told their computer system it has virus as well as they can say the Internet connection is affecting the computer’s performance. It has also been reported that they can claim the broadband connection has been hacked.

- Granting them access means the scammer or hacker can install malicious software such as spyware, Trojans or keyloggers that steal personal data. If personal information is given out or on the computer, especially bank account and credit card details, these can be exploited by the person controlling the remote access to the computer. Another strategy is to get the person to pay for software that may not be necessary for the person to have.

- If the scammer does get a Remote Access connection to a computer, the potential for harm increases. With full control of your computer, the installation of viruses or other malicious software (malware) on your computer can do the following:

  ‘Ransomware’ which will freeze up your computer’s other functions until you make a payment.

  ‘Spyware’ which will keep track of everything you do and send it to third parties without your knowledge.

  More Remote Access software which will allow them to maintain control of your computer even after it appears that the Remote Access connection is finished.

It is crucial to appreciate the magnitude of this problem. Many people unintentionally trust the person on the phone, judge them as credible and give them the information that is private.

3. Spyware

As previously mentioned, spyware becomes embedded into a computer system working in the background to collect and record remotely, information that is on the computer. Examples include: GAIN, Cydoor, WeatherCast, Ezula and Hotbar.

4. Trojans

Trojans that are implanted by a hacker remotely gives control to them over the person’s computer. Five examples include: Coulomb Diale, Trojan.Win32.Revop.c, Dropper, MoneyTree and Unknown Dialer.
5. Worms

The worm is code that when introduced into the personal computer can spread to other parts of the computer and external drives. Examples include: Tofger, Locksky, MSBlast.b and I-Worm.NetSky.q, Nyxem/.

Although writing computer code is the main entry into hacking, these tools are used on people who own home computers, laptops, smart phones and tablets. Hackers continuously find ways to use these tools and develop new ones to infiltrate personal and organisational computer systems.

Legal Consequences of Hacking

Punishments for hacking and cybercrimes vary worldwide, but legislation exists in many countries which show the legal consequences of hacking. In this section the Australian laws on hacking and punishments under those laws will be discussed. Five short examples of the crime and punishment will also be discussed.

The Australian Act that covers cybercrimes is the Cybercrime Act 2001\(^\text{19}\) which was tabled in October 2001 and came into law in April 2002. A serious of definitions of data and electronic communication are useful as they frame what are subject to criminal tampering. It covers the nature of computer-based offences and the punishments the law courts have in making decisions to place monetary, community service or incarceration sentences on the offender. Although it is a lengthy document, for this book two areas will be taken from the legislation to show the seriousness of hacking crimes. They are: the crimes themselves and the intention to commit crimes that are proven that the person intended to hack.

The Act does raise concerns about the powers legal and policing authorities have to access computer systems. In another section the key logging and other invasive software was mentioned. Sometimes this software is used for legitimate reasons and not hacking, hence why the organisation Electronic Frontiers Australia (2001) expressed concerns about the Act before it was passed. They also had other concerns about how much power police and others would have to access individual and organisational computer system. Boulton (2004), of the organisation GIAC Certifications in Australia, also argued the investigation powers were invasive. However, the Act is in force as at today and despite concerns has not been challenged by the public.

In the Act, Division 477 which is numbered 477.1 to 478.4 lists the crimes and penalties in the act. This division lists what are called ‘Serious computer offences’. The criterion that has to be proven in a court of law is that the person causes unauthorised access to data and modification of that data. However, 477.1 (d) states that aiding another person or intending to participate in this but not doing so also is considered under the Act a crime. In this next section, a sample of crimes and penalties are shown to demonstrate the Act’s powers in Australia (Federal Register of Legislation, n.d.).
Crimes and Penalties:

The following are four examples of crimes and punishments related to hacking from the Act:

1. The person causes any unauthorised impairment of electronic communication to or from a computer - Penalty: 10 years imprisonment

2. The access to, or modification of, the restricted data is caused by means of a telecommunications service - Penalty: 2 years imprisonment

3. The person has that possession or control with the intention that the data be used, by the person or another person, in: committing an offence - Penalty: 3 years imprisonment

4. Producing, supplying or obtaining data with intent to commit a computer offence - Penalty: 3 years imprisonment

The commonality in these examples is that both committing a hacking offence and intending to commit one will subject the hacker to the maximum imprisonment terms listed in the Act.

Example Australian Cases:

There have been many cases of hacking activities brought before the courts for judgement, sentencing and monetary compensation punishments. Six of these cases are presented here that show the crime and the punishment. Some occurred before the implementation of the Act. These all took place in Australia and illustrate that over time Australian courts have taken hacking activity seriously:

1. Skeeve Stevens:

   **Activity:** In 1995 he broke into the computer system of Internet Service Provider AUSNet causing actual and potential commercial harm, by stealing and publishing the credit card numbers of 1200 AUSNet subscribers that was considered at that time a major and serious violation of privacy (AustLii, 1998).

   **Punishment:** Three years jail.

2. Vitek Boden:

   **Activity:** Hacked into a Maroochy Shire Council in Queensland waste management system causing raw sewerage to spill into marine life habitats, rivers and a luxury resort.

   **Punishment:** Two years jail.

3. David McIntosh

   **Activity:** Hacked into a Northern Territory government network causing computers to crash including deleting public service user accounts, including the Royal Darwin Hospital.

   **Punishment:** Three years jail.
4. David Cecil

**Activity:** Hacked into telecommunication wholesaler Platform Networks, a website defacing at the University of Sydney and data erasing at Distribute .IT.

**Punishment:** 2 and a half year’s jail but also restricted computer access.

5. Nahshon Even-Chaim

**Activity:** An early Australian hacker with several overseas hack targets but most notable the Australian organisation Commonwealth Scientific and Industrial Research Organisation (CSIRO), caught in 1990 by Australian Federal Police.

**Punishment:** 500 hours community service and a 12-month suspended jail sentence.

6. Julian Assange

**Activity:** Assange was charged with various hacking offences overseas and several Australian universities. He was arrested and charged in 1994 in Melbourne for hacking into a company called Nortel. His later career was founding WikiLeaks and at the time of writing this book has been living in the Ecuadorian embassy in London since 2012.

**Punishment:** A fine of $2100 and a good behaviour bond.

In January 2018, Chau and Calderwood (2018) reported the following case which is still in court. However, the following public information is lifted from this story from the ABC Australia news site that shows hacking cases are increasing:

> NSW Police arrested 37-year-old Illawarra man Nikola Cubrilovic for allegedly hacking into the database of GoGet.21

> Police allege the man illegally accessed and downloaded customer information on two occasions, and used it to steal access to vehicles 33 times between May and July last year.

These examples of computer hacking show that they are not new in Australia and the Cybercrime Act 2001, despite criticisms, is being used to prosecute hackers. As these crimes grow, the Australian Government will need to balance preventing these crimes with not violating an individual’s privacy. Additionally, it is likely that technology will grow further, such as Artificial Intelligence and Virtual Reality, presenting new challenges when these are eventually hacked.
Chapter Summary

This chapter has been an extensive introduction to hacking and hackers. The issues that this chapter have introduced have been:

- Defining hackers, hacking and cybercrime
- What hacking looked like and its types, including in-depth descriptions of the range of hacking activities that confront society
- Descriptions of some major hacker attacks and cyber terrorism
- Presented ideas as to why hackers hack systems
- Classifying hackers and hacking activity
- Some examples of the tools hackers use to hack computer networks and systems
- Legal consequences of hacking using Australian examples of the current Federal Act and hacker cases

The key message in this introduction is that hacking is a serious criminal and societal problem. Not all hackers do harm, which is an important point to consider when reading this book, challenging as that point-of-view may be. However, there is ample evidence to suggest that hacking is increasing as our reliance on computer networks and the Internet continues.

This Book’s Exploration of Hackers and Hacking

The book takes an exploratory approach using a combination of academic and anecdotal material to examine what hacking is, why it is done and what can be done to address it. It does view hacking as a criminal activity, but takes as much as possible an objective and informative approach to it. Each chapter is written in an academic manner, but uses many sources to explore several hacking topics. The chapters may also challenge a stereotype as there are beliefs that hacking can be positive for society and actually be a way of improving software and computer system design.

Chapter Contents

This chapter was a broad introduction to who, what, why and how of hackers and their behaviours.

Chapter Two is an account of the history of computer hacking and hackers. It is not meant to be complete but will give an appreciation of the development of hacking over time.

Chapter Three is a case study of the group Anonymous, their history and their role in many online hacking incidents. It also questions their activities as good or bad as some of their victims were not ethical themselves, so the dilemma of deciding if their motives are desirable can be difficult to assess as positive or not.
Chapter Four is a reproduction of article on beginning hackers that was originally published in 2016 (Nycyk, 2016) that serves as an example of a study into the online activities of an ethical hacker virtual community. There is also a brief discussion of the operation of power relations using the work of French sociologist Pierre Bourdieu. This is because his theoretical work was used in the study and is important as a guide to understanding how established hackers try to influence and control new hackers as the newer ones try to learn hacking.

Chapter Five lists and discusses gender in hacking and cinema portrayals of human and non-human hacking.

Chapter Six looks at the options and choices the individual computer user can employ to minimise and prevent many forms of hacking.

Chapter Seven are closing thoughts and conclusions of this book.

**Potentially Offensive Material in Book Alert and Use of Technical Terms**

Be advised that there is explicit language and photo images used in this book as well as descriptions of situations and events that may cause offence or distress. These included use of racist, sexist, homophobic, religious and culturally insensitive words and other types of offensive statements. This book does not show how to hack, but there may be descriptions of hacking techniques used, such as malicious code, to illustrate what hackers use to obtain their goals. Technical language will be explained in the text and notes, but will be kept to a minimum as much as possible. This is not a technical account, though terms will need to be used to describe hacker activities.
Notes

1 Quote from Emmanuel Goldstein the pen name of author Eric Corley from the book *Dear Hacker: Letters to the Editor of 2600.*

2 Dan Kaminsky is Chief Scientist of American security firm White Ops, sourced from an article in Business Insider Australia.

3 Quote by Michael Pompeo, director of the CIA in the United States since January 2017, obtained from https://www.brainyquote.com/quotes/mike_pompeo_794720

4 The term ‘online’ refers to the person using the Internet or a smart phone interacting with the software or phone app that is on the computer or phone.

5 A meritocracy is a society governed by people according to merit, hence why hackers get credibility. In a study I did (Nycyk, 2016) I found that new hackers called newbies are treated badly until they prove their hacker skills. They earn merit by paying attention to, and praising, the experienced hackers that are giving the newbies advice.

6 Napster is not considered strictly a hacking activity, but was included as such because there are authors, musicians and social commentators who do label the file sharing service has hacking. A 2013 comprehensive story on Napster in *Fortune* is worth reading and can be found currently at http://fortune.com/2013/09/05/ashes-to-ashes-peer-to-peer-an-oral-history-of-napster/

7 Polymorphic or polymorphism is a computer science term meaning the computer code’s operations can also be applied to values of some other type or types; that is, in object-oriented programming, such as Java, objects are processed depending on their data type or class.

8 The Virus Encyclopeida can be located at http://virus.wikidot.com/start. It is a wiki which means anyone can edit it and the goal of the Virus Encyclopedia is to gather all information possible about self-replicating programs (The Virus Encyclopedia, n.d.).

9 A Microsoft Word macro is a technical term meaning ‘macroinstruction’, which is a feature of Word where a macro can be created and the user clicks on it when typing to eliminate a repetitive task, for example, automate putting in your address into a Word document by just clicking on the Macro button (Computer Hope, 2017).

10 A simple explanation of what is an NT Kernel in Windows is that it is part of the architecture of Windows NT Operating System. The Kernel is one component of this system that has access to the hardware and system resources of the computer, hence why hackers create viruses to attack it.

11 A concise definition of encryption is offered by Lord (2017a) from the Digital Guardian blog:

   Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.
Encryption is very important to data protection, although home computer users are less likely to encrypt their data.

12 Cryptocurrency is a form of encrypted digital currency where users are able to transfer money across the world to anyone with Internet access without transaction fees and no intervention of banks or financial institutions (Finder.com, 2018).

13 Bitcoin is the name of a cryptocurrency. A guide to what it is, as at 2018, is located at the Bitcoin (2017) site located at https://bitcoin.org/en/how-it-works. What is of interest to this discussion of ransomware is that to someone who has not brought Bitcoin, there are many terms and procedures to learn as seen on this site such as: block chain, private keys, mining and wallets. The procedures must be learned quickly by the user and this can be stressful for someone who has never purchased Bitcoin.

14 Phishing is defined as an online scam where an email appears to be from a legitimate company, such as the Commonwealth Bank, asking the recipient to provide sensitive private information, usually by a link that takes the user to a fake, but legitimate looking, company or bank website (Webroot, n.d.).

15 Dark web and dark net are parts of the Internet which cannot be found by Google and other search engines, but is also associated with illegal material and criminal activity. A more technical description is offered by Walsh (2016) as:

   …a small portion of the deep web that is intentionally hidden and made inaccessible via search engines (the Tor network, only accessible via Tor browser)

Tor is a software browser that allows anonymous browsing of the Internet.

16 Empirical means the research is based on observation and experience not on theory.

17 Flow theory, where the person feels, according to Mihaly Csikszentmihalyi (1990, p. 4) “A state in which people are so involved in an activity that nothing else seems to matter; the experience is so enjoyable that people will continue to do it even at great cost, for the sheer sake of doing it.”

Flow theory is not about hacker behaviour, but human behaviour when activities undertaken are so absorbing the experience overtakes the person and they continue. Kirwan and Power (2011) suggest that it is a good indicator in early hackers of how far they will go in learning to hack and carrying out attacks, therefore it may be able to be stopped.

The website, Positive Psychology Program (2016) has simple explanations of this learning theory that is worth consulting if wanting to know more about his flow theories.
WikiLeaks may not be hackers as such but requires an explanation as it will be mentioned in this book. It is located at https://wikileaks.org. The following information accuracy describes what WikiLeaks is (WikiLeaks, n.d.):

WikiLeaks is a multi-national media organization and associated library. It was founded by its publisher Julian Assange in 2006.

WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption. It has so far published more than 10 million documents and associated analyses.

“WikiLeaks is a giant library of the world’s most persecuted documents. We give asylum to these documents, we analyze them, we promote them and we obtain more.” - Julian Assange, Der Spiegel Interview.

As at the time of writing this book the Act is available on the World Wide Web at this address: https://www.legislation.gov.au/Details/C2004C01213

It should be noted that although Google searches were done to find the six hacker cases, the information was fact. However, some of the text needs to be attributed to a Sydney Morning Article written in 2015 by journalist Keegan Thomson (2015) and is referenced in the works cited section of this book.

GoGet is an Australian ride-sharing transport company.
CHAPTER TWO
HISTORY OF HACKERS AND HACKING

In its original technological sense, the word ‘hacker’, coined at MIT in the 1960s, simply connoted a computer virtuoso. – Roush, 1995 on the term hacker

The first intentional artifacts of the hacker culture - the first slang lists, the first satires, the first self-conscious discussions of the hacker ethic - all propagated on the ARPAnet in its early years. – Eric Raymond, A Brief History of Hackerdom

“The hackers have accomplished such things as tying up all the tie-lines between Harvard and MIT, or making long-distance calls by charging them to a local radar installation. One method involved connecting the PDP-1 computer to the phone system to search the lines until a dial tone, indicating an outside line, was found.... To quote one accomplished hacker, “the field is always open for experimentation.”” – An incident at Massachusetts Institute of Technology (MIT) reported in an article in The Tech in 1963

This chapter discusses the history of computer hackers and hacking. Like all accounts of history, it draws on many sources to create a picture of where hacking has originated from. As with other literature on hacker history, such accounts are selective and omissions of events and people may occur. It aims to give a comprehensive account of hacker history, leading to appreciate why it has become a societal concern.

The chapter begins with the first reported hacking to the large-scale hacking occurring in 2018. Quotes from famous and infamous hackers will also form part of this account. This historical account will discuss several decades with descriptions of many hacking incidents. Most of these occurred in the United States because it was the centre of the growth of computer technology with companies like Microsoft and Apple. Sources for this account range from books and journal articles, although some websites were consulted to check facts and information.

1903 - The First Recognised and Recorded Hacker Incident

The first accepted known hack occurred in London at the Royal Institution in 1903. Physicist, John Fleming, was to demonstrate Italian inventor Guglielmo Marconi’s sending of messages over long distance by Morse code. This was a radical communication invention at that time. Marconi was in Cornwell, 300 miles away from the Institution, ready to receive the code. At the event the first recorded, and labelled as, hacking incident occurred to the machine where human interference caused the demonstration to go wrong. Figure 11 shows Marconi at this machine:
Minutes before Fleming was due to receive Marconi’s Morse messages from Cornwall, the hush was broken by a rhythmic ticking noise sputtering from the theatre’s brass projection lantern, used to display the lecturer’s slides. To the untrained ear, it sounded like a projector on the blink. But Arthur Blok, Fleming’s assistant, quickly recognised the tippity-tap of a human hand keying a message in Morse. Someone, Blok reasoned, was beaming powerful wireless pulses into the theatre and they were strong enough to interfere with the projector’s electric arc discharge lamp.

“The hush was broken by a ticking noise, the sound of a Morse code message. Then it got personal”

Mentally decoding the missive, Blok realised it was spelling one facetious word, over and over: “Rats”. A glance at the output of the nearby Morse printer confirmed this. The incoming Morse then got more personal, mocking Marconi: “There was a young fellow of Italy, who diddled the public quite prettily,” it trilled. Further rude epithets – apposite lines from Shakespeare – followed.

The person who did this was magician and inventor Nevil Maskelyne, who wanted to prove he could eavesdrop on the messages. In reporting that he could do so my means of a radio mast, it was shown technology could be hacked. Marconi and Fleming were said to have ‘damaged egos’ (Marks, 2011) because their credibility was damaged as their code machine was shown to be not secure. The wireless technology was new and assured as secure. Maskelyne proved it was not so and as such this was called one of history’s first hackers, although his actions were not judged as malevolent but rather a prank.
Hacking to keep Populations Safe: the Enigma Machine

During the first half of the 20th Century, conflicts in Europe meant new technologies had be invented to gain advantages in warfare. The problem in the pre-Internet age, even though radio signal transmission existed, was that sending confidential messages was difficult. These included the location of the enemy or sending information obtained from spying. German engineer Arthur Sherbius originally created the Enigma machine just before World War One ended, where the German military would use an encryption code, called Enigma. It was a machine that could encrypt messages to be transmitted, preventing others from reading them. Cryptography was essential for the Germans to continue their occupation of Europe\(^5\). It was an efficient way of sending confidential messages.

Figure 12 shows the Enigma Machine’s appearance:

![Figure 12. The Enigma Machine (BBC, 2018)](image)

The code was difficult to break. Codebreakers at London’s Bletchley Park, including computer scientist Alan Turing, used linguistic techniques to find a flaw in the Enigma. This lead to an eventual victory over the Germans and although Turing and others were not specifically labelled hackers, hacker history counts this achievement as such an act but for the good of humankind. Not acknowledged for decades were the Polish codebreakers assisting Turing with mathematical formulas to break more of the code and intercept German transmissions of codes and messages.

As Knapton (2016) reports, the Polish Government in 2016 called for greater recognition of these codebreakers after Turing’s biographical film *The Imitation Game* was released:

Poland’s main codebreakers were Jerzy Rozycki, Henryk Zygalski and Marian Rejewski who joined the Polish General Staff's Cipher Bureau in Warsaw.

While Britain still used linguists to break codes, the Poles had understood that it was necessary to use mathematics to look for patterns and had broken some of the early pre-war German codes.

They had then taken a further step by building electro-mechanical machines to search for solutions, which they called “bombes”.
The Germans consistently worked to make the Enigma almost invulnerable with constant sophisticated and ever-changing code alterations to improve its security (Winston, 2016). Gladwin (1997, p. 204) describes how messages were transmitted between Enigma machines, illustrating how encryption would become important in future computer communications:

To read a message enciphered by Enigma required the recipient to calibrate his (sic) machine in exactly the same way as the sender, following the same codebook instructions. He then typed in the ciphertext. As each corresponding key was pressed, a letter lit up on the lamp-board, revealing the original clear or plaintext.

Turing, along with Gordon Welchman and Harold Keen, worked using hacking type methods to find the Enigma’s code vulnerabilities. Although a technical description of this is out of the scope of this section, it is worth reproducing this extract from the Crypto Museum (2012) to illustrate an early way of hacking:

The Bomba is based on the principle that the random 3-letter message key is sent twice at the beginning of each message and that every now and then, a particular plaintext letter, yields the same ciphertext letter three positions further on.

The Enigma machine was considered an early form of hacking. Some of the principles involved, such as cryptography and figuring out vulnerabilities, have carried over into modern day hacking.

**The First Ethical Hacker? René Carmille and the Register**

Wills (2017) argues that Frenchman René Carmille was the first recorded ethical hacker for his actions in saving the lives of Jewish citizens living in German occupied France. Herman Hollerith’s electronic tabulating machine and the use of punch cards to record and collect data had been used worldwide since the late 1800’s. This was used in France during the war with the German government demanding that French citizens indicate their religion. This meant the person had to disclose that they were Jewish.

Carmille specialised in punched card technology being the comptroller general of the French Army and running the National Statistics Service. He was also a double agent for the French Resistance. In this capacity, he sabotaged the Nazi census of France, saving unknown numbers of Jewish people from concentration camps.

Over the two years of the census data collection, he and his group continuously, and often without detection until 1944 mishandled the punch cards the data was on and reprogramming the punch card machines. Column 11, that showed who was Jewish, was never punched into the computer (Davis, 2015). When asked to produce a list of all the Jewish people living in France to be sent to concentration camps, Carmille successfully stalled that assignment for two years (Murphy, 2017).

Carmille’s achievement saved many lives but did result in him being found out, tortured and murdered by the Nazi’s just before the Liberation of France. Wills (2017) sums up why Carmille has a place in hacker history:
While Carmille didn’t re-write code or introduce a bug in the system, his “hacking” was akin to sabotage, throwing a bureaucratic wrench into the machine. Heide calls Carmille’s initial form of resistance passive, a serious “departure from the loyal public servant he had been.”

Carmille is seen as an ethical hacker, and as such it can be contemplated that perhaps some types of computer and technology hacking may be a desirable action to take.

First Accounts of Hacker Viruses in the Computer Age

In Chapter One the first accounts of the computer virus were discussed and described in Table 1. Although hacking continued after World War 2 as society shifted towards using computers it was in the 1970’s that it became more visible to the public. Hacking also grew more sophisticated as the technology became more widespread and the paper-based society moved towards computerisation of data, information records became electronic and databases more used by business and government.

Particular hackers are noted during this time as their activities gained a permanent place in history. What follows is an account of those regarded as making significant contributions to understanding hacker and hacker behaviours.

Kevin Mitnick: Fame and Notoriety

Kevin Mitnick, as at 2018, is a United States security expert specialising in managing hacking prevention for organisations (Mitnick Security, 2018)⁸, cybersecurity speaker, an author and poster on Social Media and blogs. He has been the subject of documentaries, inspiration for films and widely written about. As an author, he was warned the public about the insidious nature of hackers, their mindsets and ideologies, referring to them as social engineers. These engineers can deceive people in what he describes as the use of knowledge about a system or organisation to exploit victims and achieved their own hacking goals (Mitnick & Simon, 2002),

His first hack was reported as invading a system at US Leasing in 1980 as a teenager, influenced by the use of the electronic system Usenet. Information about hacking was easily obtainable through this early type of communication system. Mitnick was arrested and put on probation for the act, though law enforcement was aware of other hackers with Ian Murphy, known as Captain Zap, becoming in 1981 the first official hacker charged with a felony for a hack on AT&T’s computer system (Ciment, 2006).

Mitnick’s most famous hacking attempt was gaining access through a phone number and copying their software. This system was named the Ark run by a famous technological company called Digital Equipment Corporation (DEC). He did not do this for financial gain. He was caught and convicted on charges of wire fraud and a given 12 months prison sentence, but during his supervised release he committed a second hacking of voicemail on the telecommunications company, Pacific Bell.

In his book Ghosts in the Wires, Mitnick offers an insight by reflecting on his behaviours and thoughts as hacker while he was involved in his activities. The DEC incident was considered
a brazen act, but over time has been debated if it functioned as a warning for the future. Mitnick offers this overview of the incident (Mitnick & Simon, 2011):

DEC’s network engineers could see all along that lots of large files were being transferred, but they couldn’t figure out how to stop it. Our unrelenting assault had them convinced that they were under some kind of corporate espionage attack by international mercenaries who’d been hired to steal their flagship technology. We read their theories about us in their emails. It was clearly driving them crazy. I could always log on to see how far they were getting and what they were going to try next. We did our best to keep them chasing red herrings along the way. Because we had full access to Easynet, we could dial in from the United Kingdom, and other countries throughout the world. They couldn’t identify our entry points because we were constantly changing them.

In 1982 he was reported to have been arrested for breaking into computers at the University of Southern California (Brenner, 2010). Later in 1988, Mitnick, with Lenny DiCicca, infiltrated the company Jet Propulsion Laboratory (JPL) in Pasadena, California. By 1986, the United States Congress passed the 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, called the Computer Fraud and Abuse Act (CFAA). Halbert (1997) views the reporting of the JPL incident as finally raising in the media the vulnerability of technology beyond the United States as hackers from other countries were involved in this incident.

There is much written on Mitnick’s hacking career. One website, Takedown.com (1995) has an extensive archive of incidents regarding Mitnick’s career from an outsider’s perspective. In terms of being a cultural hacking figure his public persona and activities were widespread. They struck fear into companies and the public about what was becoming possible with hackers and technology. His place in hacker history is important for the raising of this awareness.

There are debates over the severity of his crimes. Brenner (2010) argues that Mitnick was demonised by the media and the police force, with paranoia about hackers in the United States continuing even when he was arrested. His place in history according to Brenner is of being the poster boy for the realisation computers were vulnerable to hackers. Heusser (2014) is sympatric towards Mitnick with this quote:

The first bit of insight here is that Mitnick wasn’t a technical hacker; he didn’t cause a buffer overflow or SQL injection or upload an image that was really javascript. Instead he pretended to be someone who should have access and politely asked for a password reset, something that today we might call social engineering.

The abundance of literature, analysis, information and opinion on Mitnick illustrates a major historical event in hacker history and his influence on future hackers. Yet he was not the only hacker becoming a part of history.
Richard Skrenta and the Alvi Brothers

The spread of early viruses was attributed to the sharing of floppy disks rather than transmission through computer networks even in the early days of the Internet. The first recognised account of this transmission came from 15 year old Richard Skrenta who created the Elk Cloner in 1982. This was a boot sector virus created as a prank on the Apple II computer. He did this to his friends initially but moved on to creating the Cloner that after the disc was placed into the computer would secretly infect the operating system’s boot sector subtly. After the 50th insertion into the disc drive, it would boot up with a poem (Skrenta, n.d.):

Elk Cloner: The program with a personality

It will get on all your disks
It will infiltrate your chips
Yes it’s Cloner!

It will stick to you like glue
It will modify ram too
Send in the Cloner!

The significance to hacking history is that it was a virus that spread beyond his own friends to businesses. Skrenta is now at the time of writing a Silicon Valley entrepreneur. In 2007 he reflects on his memories of his contribution to hacker history (Skrenta, 2007):

“Why did I do it”, she asked. “Was it malicious?”

No, not malicious. It was a practical joke combined with a hack. A wonderful hack.

Back then nothing was networked. We had these computers in a lab, and there was software for them on floppy disks. You stick in the disk and run the software. Simple.

The essence of the hack isn’t just realizing you can use a system in a new, unexpected way. It's getting a disproportionate effect from your effort. It's catalyzing potential energy stored in the system.

And the hack often changes the whole world. The user-generated content model we developed with NewHoo is ubiquitous now; it was the main inspiration behind Wikipedia. Viruses and exploits are of course all too common. You can't put the genie back in the bottle.

The only consolation is that the genie would have gotten out anyway. But it's fun to be the first to let it out

Skrenta was not the first to contribute to hacker history for this activity. In Pakistan in 1986, brothers Basit Farooq Alvi and Amjad Farooq Alvi created the Brain computer virus. The virus was not created for malicious purposes, but to protect the custom medical software the brothers were working on which were being illegally copied. Creating a virus was to prevent
this happening and the customers were able to call the brothers who would provide antivirus software. They provided their phone numbers for people to call them for the code to inoculate the Brain virus, as Radeska (2016) reported, that appeared as message:

![Welcome to the Dungeon © 1986 Brain & Amjads (pvt). BRAIN COMPUTER SERVICES 730 IZANAMI BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...](image)

Figure 13. Message from Brain virus creators for people to contact them for inoculation (Radeska, 2016)

However, the bothers denied it was a malicious virus as it was for the protection of the copying of the software Radeska (2016):

The brothers stressed in interviews that they created the virus only for the illegal copies of the software, putting their names, phone numbers, and their shop’s address in the virus code. Basit and Amjad never thought of the virus growing into a global-sized monster, with powers beyond their capacities to control it.

The virus was called a stealth virus, paving the way for hackers to use, and improve upon, the virus’s capabilities to infect systems. Basit and Amjad’s virus received so much attention, including articles in *Time Magazine* (Priceconomics, 2015). The brothers and Skrenta were counted in hacking history because they brought attention to what was then a little known issue. They did not do their hacking for sinister purposes, yet went beyond their locality to become well-known historical events. They brought public attention to the potentials of boot sector viruses.

**Robert Morris: The First Recorded use of Worm Malware**

Another hacker earning a place in hacker history was Robert Morris. A piece of code was released in 1988 from an MIT computer at Cornell University by Morris, which was not meant to spread outside MIT. However, a design flaw made it spread further than expected. Morris was, like Basit and Amjad, not considered a hacker, yet the incident in terms of public awareness of network security was a significant hacker history event. In 2013, journalist Timothy Lee (2013) wrote in *The Washington Post* an assessment of why Morris was important to the hacker movement and to network security:

But the most significant effect of the worm was how it permanently changed the culture of the Internet. Before Morris unleashed his worm, the Internet was like a small town where people thought little of leaving their doors unlocked. Internet security was seen as a mostly theoretical problem, and software vendors treated security flaws as a low priority.

The Morris Worm destroyed that complacency. It forced software vendors to take security flaws in their products seriously. It invigorated the field of computer
security, creating a demand for such experts in both academia and industry. Today, the Internet is infested with malware that works a lot like the software Morris set out to build a quarter-century ago. And the community of Internet security professionals who fight these infections can trace the roots of their profession back to the events of November 1988.

The code Morris created has become a standard syntax for worms that continues today. Kelty (2018) provides an illustration of what a worm code looks like:

```
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>

#define PORT 5000

int main(int argc, char *argv[]) {
    struct sockaddr_in sin;
    char msg[] = "Hello, world!
    /* Some port number */
    bzero(&sin, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = htons(PORT);
    sin.sin_addr.s_addr = inet_addr("128.32.137.13");
    /* Open socket */
    s = socket(AF_INET, SOCK_STREAM, 0);
    if (s < 0) {
        perror("socket error");
    } else {
        /* Send data */
        if (sendto(s, msg, 1, 0, &sin, sizeof(sin))) {
            perror("sendto error");
        } else {
            /* Close socket */
            close(s);
        }
    }
    return 0;
}
```

*Figure 14. Morris worm code (Kelty, 2018)*

Morris was tried and convicted under the United States new Computer Fraud and Abuse Act of 1986, 18 U.S.C. Section 1030(a)(5)(A), and put on probation, community service and received a fine (Kelty, 2018). He became a Professor at the MIT Computer Science and Artificial Intelligence Lab where he is at time of writing this book, teaching and researching computer security. In terms of hacker history, it is widely debated how serious this issue was. Spafford (1988) stated the effects could have been worse had it been developed further and caused more destruction. Orman (2003) viewed the Morris Worm’s notoriety as not a security wake-up call, but that its legacy being it spawned imitators who created viruses based on the Worm’s code. Morris, though, has a place in hacker history for making this worm and the subsequent cultural place it earned in hacker history.
Peter Samson: The Grandfather of Hacking

MIT was considered a hub where hacking originated influencing generations of hackers. It was considered that his work started the hacking global culture in the 1960’s (Vilbig, 2013). The hacker philosophy grew during this period especially in the United States at Stanford, Berkeley and other universities aided by the electronic ARPANET campus networks growing across the States, in turn fostering a ‘hacking culture’ (Gupta & Manhas, 2017). Peter Samson was referred to as a ‘grandfather’ of hacking but was not a malicious hacker. His computer work is substantive, including creating computer waveforms to synthesize music, a large-scale computer war card game, a Chinese computer character digital communication and a Formula Translation (FORTRAN) compiler program which went on to be widely used. He also worked with John McCarthy who was a computer scientist that was said to have developed the term Artificial Intelligence (AI).

His activities also brought hacking to a new level of public awareness of it. Samson was credited as in 1959 as writing in the Tech Model Railroad Club Dictionary a first formal definition of the term hack as reproduced here (Norman, 2018):

1) An article or project without constructive end
2) A project undertaken on bad self-advice
3) An entropy booster
4) To produce, or attempt to produce, a hack.
5) Samson defined hacker as "one who hacks, or makes them.

Samson in 1966 famously attempted to ride the lines of New York City’s Subway System in as little time as possible. This he called Subway Riding, which later inspired other people to try to ride the whole subway system in as little time as possible. What was unique was his using a computer to give information to make the run as fast as possible. Samson later published a guide on how he achieved this. This extract from Samson (1980) showed how this hack worked:

At last the big day came: April 19, 1967. (There had been a brief dress rehearsal one week earlier.) A party of two - George Mitchell and Andy Jennings - were to make the run. Three persons, including myself, were at the Data Center. It was arranged that someone would be on hand at the computer at M.I.T. at all times during the run. And to convey information to and from the party were various volunteers; their number fluctuated between four and eight depending on the time of day or night. All was in readiness; the telephones, Teletype, maps, and clocks were in place at the Data Center; messengers were positioned at key nodes ahead of the run; and at 2:43 p.m. the party set off from 168th Street station on the Jamaica El and the run was on.

Vilbig (2013) describes how the culture of hackers operated during the early years that were occurring within universities that Samson was a part of:
This began a culture of computing where hacking into the late hours of the morning was necessary, because the more normal working hours were filled up with graduate students or professors working on their projects. The original generation of hackers were making sure that the computing resources available were used constantly. So they would end up hanging out by the machine, waiting, just in case one of the scheduled users failed to show. This practice created a culture of hanging around the machine while also fueling their obsession.

Samson’s place in the history of hacking was important because it contributed to defining the cultural boundaries of future hacking. Brunvand (1996) describes Samson and others during the 1950’s and 60’s as the golden age of the computer hacker.

Hacking Increases in the 1980’s

So far, the explanations of hacking history has involved individuals, most of who were either not malicious or went from black hat hacking to grey and white hat activities. Computer technology was developing; becoming more affordable for the home, more sophisticated for business to invest in and fostered the development of the networked society. During the 1980’s not only did hacking start to become serious, but also governments, especially the United States government, were forced to respond to this growing problem. Moral panic about hackers became widespread and with it the pressure to stop this activity and deal out punishments to hackers. Yet hackers began being treated as celebrities in the hacker community and a view developed that not all hacking was considered bad for society (Young, et. al, 2007; Skurodomova, 2004).

The 1980’s were considered revolutionary because of the invention of the personal computer, such as the first Apple computers, combined with modems to network with others across the world, making computing within anyone’s reach. However, some hackers began to explore computer systems for sinister purposes (Clarke, Clawson & Cordell, 2003. p. 1):

Although hacking expanded and enjoyed glorification during its golden years, a divide was forming within the hacking community by the late 1980s. An increasing number of hackers were no longer satisfied with benign exploration of systems merely to learn how they worked. The hacker principle of “freedom of technology” as described by Levy was changing, and a younger generation interested in individual gain emerged.

Halbert (1997) suggests that during the 1980’s the image of hackers as nerds and geeks, as well as threats to society, emerged, where also myths of hackers as a stereotype began. Thomas (2005) reviewed others’ research finding that demonising hackers was common in the media with labels such as: evil-doers, morally bankrupt, electronic trespassers, electronic vandals, saboteurs, a new or global threat and high-tech street kids. Strongly condemning hackers also emerged during the 1980’s.

Hacking increased because of better access to technology and media attention, but also began to spread beyond the United States. A number of hackers and organisations emerged and countries began drafting laws to punish hackers. Two phenomena also emerged: hackers became sophisticated in their activities and became more organised. Commonly, hackers would be working alone, but the emergence in the 1980’s of hackers as co-operating and
sharing knowledge, even before the emergence of the commercial Internet, began. Some significant examples of hacking from the 1980’s are now discussed.

**Hacking of the National CSS Inc United States 1981**

In 1981, the National CSS, a timesharing company, had stolen from their computer system an information file called at that time a customer password directory. It was considered a serious and criminal theft, hence the involvement of the Federal Bureau of Investigation (F.B.I). This was despite the crime not resulting in data loss or any cash being lost or paid as ransom. As reported in the *New York Times* (McLellan, 1981) at that time such a hacking case was rare; federal agents who were being trained in, and gaining knowledge about, hackers considered this a historical event which would benefit future investigations.

**The Chaos Computer Club e. V. (CCC) 1981**

Wau Holland in 1981 founded what was Europe’s largest association of hackers that still exists as at 2018, called The Chaos Computer Club. Holland was an activist who claimed he could see the coming issues of computer security that eventually arose. The organisation was not set up to be black hat hackers. However, as Silver (2017) reported, in 1984 an incident with the German Postal Service brought hacking to the attention of Europeans. The club’s members found an issue with an early Internet-based pay service where customers could access primitive information services electronically. It was found that small but significant amounts of money were being electronically stolen from a bank account associated with the service. The club went to the press and organised a televised conference to return the money. This publicity alerted the European people to the potential dangers of computer hacking.

**Captain Zap**

Another significant hacker was Ian Murphy who called himself Captain Zap. His inclusion in hacker history is for several reasons. First he hacked, with three others, the company AT&T’s network changing the internal metering clocks, meaning the customer billing system was interfered with charging customers excessive costs. The intent seemed to be a prank but the second reason for this being significant was that he was charged and convicted under new United States computer crime laws. For his part in the crime, Murphy was greeted with 1,000 hours of community service and 2 1/2 years probation which is considerably less than what hackers would receive today (Hack Story, 2011). Thirdly, his story was the inspiration for the 1992 hacker movie *Sneakers*.

**Conclusions of 1980’s Hacking**

The 1980’s brought many hackers to public notice, resulted in the first types of laws to prosecute them and made personalities out of hackers. Many of those that committed hacking moved from pranksters and black hats to white hats, such as security experts or helping law enforcement to stop new hackers. There was a celebrity and heroic status to some hackers. They did influence future hackers to be more daring in the scale of hacks. The growing computer communication networks during the 1980’s meant anyone could potentially become a hacker.
The 1990’s to 2018: Hackers and Hacking Increases

In examining the past 29 years of hacking history, there emerged sinister motives as well as easier access to sophisticated but simple to use hacking tools that characterise this period of hacker history. Hacking also became a collective, but there also developed rivalry between hackers. Law enforcement worldwide began waging wars on hackers and countries such as Russia and China began to employ hackers to interfere in other countries political systems. Scams and hacking of personal computers and devices also became more sophisticated with emails looking like those you would receive from your bank.

Once again, it needs to be stated that as growth accelerated in the hacking community, not all hackers were causing anarchy and destruction. This has, however in our age of relying on computer networks for almost every facet of life, made us vulnerable to cyberterrorism and invasion of our privacy. The potential for large-scale, even global, harm hackers can do is enormous. In this section it will be necessary to demonstrate the severity of hacking in the 2000’s era by providing definitions of cyberterrorism and warfare that has been provided by the work of Janczewski and Colarik (2008) and other authors.

Government Laws to Control Hacking: United States and United Kingdom

Law enforcement became determined to catch hackers and assure the public hacking was under control. In 1990 one operation in the United States was called Operation Sundevil. This was conducted by the United States Secret Service to crack down on illegal hacking and appease the public’s fears. In hacker history it is seen as a publicity stunt and in general an early example of how futile such raids could be. The raids also motivated the establishment in the United States of the Electronic Frontier Foundation (EFF), aiming to minimise the erosion of rights and freedoms in using technology (EFF, n.d.).

The operation was considered a failure by the United States media and public. There was more of a concentration of stopping hackers meeting and exchanging information on Electronic Bulletin Boards and confiscating equipment. It was not a simple operation with only four arrests and it proceeded too slowly (Computer Fraud and Security Bulletin, 1991). It also was claimed by the EFF and others that the conduct of the investigation team across many states and cities in the United States violated the First and Fourth Amendments (Alexander, 1992).

On an anonymous website written by a pseudonym named Shredder (1993), an assessment of the failed Operation that was shared by media and hackers was:

The outcome of Operation Sundevil was a let down for the Feds. They had sent their “message”, but only one indictment was served as a result of the arrests. Prosecutors involved in the case say chances are “extremely high” that all charges will be dropped. In the end, this two year, expensive operation resulted in not much of a real prize for the Feds, and shows that even if you do get arrested, the Feds don’t really have much of a case against you, even if they do take all your stuff.

In a document posted from MIT a claim is that Operation Sundevil represented that law enforcement and government was recognising hacking as an anti-social, deviant and criminal act (Massachusetts Institute of Technology, n.d):
The final message of Sundevil was intended for internal consumption by law enforcement. Sundevil was offered as proof that the community of American computer-crime police had come of age. Sundevil was proof that enormous things like Sundevil itself could now be accomplished. Sundevil was proof that the Secret Service and its local law-enforcement allies could act like a well oiled machine -- (despite the hampering use of those scrambled phones).

The lesson of Operation Sundevil in hacker history was that it was becoming clear the depth of the hacking problem with laws across the world mainly slow to react to making appropriate punishments. Geers (2010, p. 301) states hacking has become more difficult to manage as hacking becomes a world-wide problem:

In cyberwarfare, the attacker enjoys a formidable advantage: anonymity. Proof in cyberspace is hard to come by. Smart hackers hide within the maze-like architecture of the Internet. They route attacks through countries with which the target’s government has poor diplomatic relations or no law enforcement cooperation, and exploit unwitting, third-party networks. Cyberinvestigations typically end at a hacked, abandoned computer, where the trail goes cold.

As the previous section on 1980’s hacking showed, hackers do get caught but it is challenging to try to catch them and continuously change laws to suit developing and emerging technologies.

While Operation Sundevil in the United States was a response to hacking, during the 1990’s the United Kingdom government also struggled with the public’s demands to do something about hackers. In 1990 the Parliament of the United Kingdom introduced an act called The Computer Misuse Act 1990. It contains penalties for hackers that have become a part of many governments’ agendas to stop it. The three main parts of this act are about intent and access, and are (Legislation.gov.uk, n.d.):

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer (includes subsections for creating risk of serious damage and making, supplying or obtaining articles).

This meant that hacking was now a criminal act in the United Kingdom. At that time, the creation of the act was in response to a judge’s ruling in the case of Regina v Gold and Schifreen: HL 21 Apr 1988. Two hackers gained access to British Telecom’s UK Post Office’s videotex system in 1985, being caught and charged as the crime was a form of forgery. However, despite a small fine, the defendants’ decided to appeal the fine as the then Counterfeiting Act could not be applied to their case. The ruling in favour of the defendants and not the prosecution meant that new legislation had to be introduced to protect people from hackers, hence the Computer Misuse Act 1990 coming into legislation and has been a part of UK law since (Murray, 2016).

Laws to deter and punish hackers have been met with amusement by many hackers and frustration from the public that they were not strict enough. In Europe Dutch hackers were
amused by attempts to thwart their activities when in 1993 the Dutch government passed laws making hacking a criminal activity. The government called it a form of breaking and entering calling the hacking crime “huisvredebreuk” (literally “disturbing the peace of a home”) (Nevejan & Badenoch, 2014). However, across the world hackers or those that did any type of hacking were being pursued and prosecuted. For example, Bruce Esquibel, called Dr Ripco, managed the RIPCO bulletin board system. By merely running it, in 1992 he was arrested by the United States Secret Service because of the publication on his system of a how to hack manual (Charles, 1992; Thomas, 1992).

The Dark Avenger and 1260: New Star Hacker

The 1990’s saw more hackers emerge with sophisticated hacking skills and the ability to avoid in many cases being caught by the law. A notable hacker in 1992 was from Bulgaria called Dark Avenger. The virus Dark Avenger created was malicious, capable of destroying data and infecting systems from a host computer’s memory. Szor (n.d.) stated that the reason why Dark Avenger and the 1260 Virus was significant in hacker history is that it was a polymorphic virus that could fool the growing antivirus software that was emerging to protect computer users. Describing the Dark Avenger, Belsie (1992) stated:

> While the other Bulgarian virus writers seem to be just irresponsible or with childish mentality, the Dark Avenger can be classified as a ‘techno-path,’ writes Vesselin Bontchev, former director of a Sofia anti-virus lab and now doing doctoral work in Hamburg, Germany. “When asked why his viruses are destructive, he replied that ‘destroying data is a pleasure’ and that he ‘just loves to destroy other people's work.'

The worms, viruses and other hacking codes were increasing in their ability to cause widespread significant damage to computer networks. Dark Avenger was a new hacker star whose place in hacker history was how someone was able to make new types of code to destroy computer systems and exert an influence on future hackers to hack larger targets.

The First Public Hacker Gathering: Def Con 1993

Def Con is significant in hacker history because it was one of the world’s first Hacker Conventions, it was first held in 1993. Jeff Moss founded it in Las Vegas after organising a party for a friend that had left the country, so he invited his other friends to attend. The name came from two sources: Defense Condition (DEF CON) and from the movie War Games (DEF CON Communications, 2018). The first event was so popular it was repeated in 1994 and to the present day as at writing this book.

People who come to the event generally feel safe from law enforcement. The event has a mix of people from cyber security to white and grey hackers. The prize that is sought after is the Black Badge award for winning certain events including hacking games and challenges, especially the popular game Capture the Flag. Although there have been some controversies over the years, it is generally a welcoming hacker conference to all. The presence of computer security experts and white hat hackers mean that it leans towards being a conference for hacking protection, but black hat hackers have frequently attended it was well.
Although hackers have a reputation for working alone, hacker conferences do provide connection and solidarity. Hacker researcher Coleman (2010, p. 67) provides an ideal view of hacker conferences, which have grown in number worldwide, that celebrate hacking culture:

Despite the differences in the moral economy of conferences, they tend to be the basis for intense social solidarity that sustain relationships among people who are otherwise scattered across vast distances. For hackers, given the fierce celebration of some of their cons, they feel entropy - a cathartic release of laughter and pleasure, in which the daily rhythms and trouble of life can be placed aside. Yet these events work against entropy, sustaining unity all the while engendering new possibilities.

These conferences are now a part of hacker history and continue being held. How people view them is mixed; they can be endorsement of crime but also assist in stopping malicious hacking. Other conferences that occur are: The Chaos Communication Congress, Black Hat Briefings and Hackers on Planet Earth.

**The 1994 Citibank Hacking Incident**

Russia has had a history of organised hacking activities that continues in 2018. In 1994 Citibank was hacked with 10 million dollars sent to a hacker named Vladimir Levin through accounts in Finland and Israel. Citibank did recover most of the money and Levin was arrested and convicted in the United States. But at the time it was considered a major wide-scale hacking event unmatched by previous crimes. Gourley (2012) commented on the American FBI’s view of the case:

> The global dimensions of cyber crime, though, became apparent as early as 1994. That summer, from deep inside the heart of Russia, a young computer wiz named Vladimir Levin robbed a bank in the U.S. without ever leaving his chair. Over a two-month period, Levin - with the help of several conspirators - hacked into Citibank computers and transferred more than $10 million to accounts around the world using a dial-up wire transfer service. Working with Citibank and Russian authorities, FBI agents helped trace the theft back to Levin in St. Petersburg. Levin was soon lured to London and arrested.

What can be concluded is that it reflected the growing transnational nature of hacking crimes that although existed before, became widespread in the 1990’s. Levin was sentenced to three years jail. The FBI has since claimed that the case getting a lot of publicity was good because it made organisations, especially in the United States, more conscious of their network security (FBI, 2014). In hacker history it still, however, remains a widely discussed case and example of how hacking was, as a crime, growing.

**Making Hacking and Cracking Easier: AOHell**

During the 1990’s in the race to provide more Internet features, America Online (AOL) became a much used service and has an extensive and controversial history. It has also been a target for hackers, especially in the 1990’s. Customers’ accounts and details were often hacked. To reiterate, phishing is (Phishing.org, n.d.):
Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

In 1994 Koceilah Rekouche, a 17 year old hacker from Pittsburgh, called himself Da Chronic. His hacker toolkit was substantive in the access it could provide through what was then not as common programs such as credit card number generators. It was also notable for its unauthorised use of a rap track by Dr. Dre and Snoop Dog called *Nothin’ But a G Thang*. As other hackers obtained the toolkit, they began targeting AOL.

The toolkit’s name was AOHell, which being what was described as the first occurrences of phishing, would obtained customer’s credit card numbers. In an online document which was claimed to be written by Da Chronic (n.d.) tells why it was created:

AOHell is a Windows add-on program for the Windows America Online software. AOHell has many purposes. Basically, it is used to annoy others, get free service, and other things. You can knock people offline with it, you can Email bomb someone with it, and many other things. You can use it to automatically reply to IMs that you receive, ignore IMs from certain, but not all people, and much more. You can use the Artificial Intelligence bot to greet people who enter the room, and send other messages when certain things happen in the chat room.

You can also use the AOHell Fake Account Creator to make fake AOL accounts quickly. You can also use it to get other people's passwords and credit card information. If you're an anarchist, or just hate AOL and want to fuck them over, or if you just want to use the handy utilities mentioned above this is the tool for you!

Information sharing between hackers occurred on the AOL in the Warez chat rooms. The hackers had an issue with AOL’s Chairman Stephen Case and the way AOL were running their services to customers. Annoying them by distributing the hacker toolkit was Da Chronic’s way of becoming known in hacker history. As well as Dr. Dre’s rap song appearing when the toolkit was loaded, an image of the devil and Steve Case appeared as Figure 15 shows (Breakingvc, 2014):
AOHell was significant in terms of the technology used and the pranking/cracking/hacker culture that was reported arose from it. In 2018, attesting to its importance in hacker history, Velzian (2018) of Quadrotech used the case as a warning of phishing as a cybercrime documenting in simple language how the components of AOHell worked. This demonstrates the importance of phishing as a serious crime. AOL did try to take action against the hackers in 1995, though it proved difficult to catch them.

However, another online document claiming to be written by Rekouche (n.d.) reflects on why AOHell has a significant place in hacker history:

Unlike today’s phishing schemes which operate in an environment that has over fifteen years of phishing history, these early attacks had a very good success rate against their unsuspecting targets. The high success rate was also due to the unique operation of the New Member Lounge areas, as previously mentioned. On busy nights, and on occasions when AOL staff were not so diligent, many passwords or credit cards could be phished in a single session.

Because the phishing was done on fake or stolen accounts, there was no substantial risk to the attacker of being caught by AOL or the police. AOL relied on outside networks such as SprintNet for their telephone-modem connectivity, and these networks did not provide AOL with the incoming telephone number of the person logging in, say, through Caller ID. AOL later created or purchased its own modem network called AOLNet, but apparently it too did not retrieve the incoming telephone number.

This significant hacking event that occurred in the 1990’s, and as Velzian’s (2018) blog post shows, is still a benchmark for how hackers can cause widespread damage to computer networks, business and all those customers and others using online systems.
1996 and 1997: Hackers Gain and Lose Ground

From 1996 to the end of 1997, it was becoming obvious that computer security companies, the public and governments were well aware of hackers. For example, in 1997 a hacking group called the Brotherhood of Warez broke into the Canadian Broadcasting Corporation (CBC) after, it is claimed, the broadcaster presented unflattering reports about a hack on a hacker who pranked a family’s house and phone line (Jackson, 2014). It turned out to be the family’s 15 year old son who used the name Sommy who was the hacker, and was the subject of a documentary that caused moral panic in Canada who realised hacking was becoming a serious issue in their country.

The Brotherhood hacker group took action against the CBC by taking down their transmission and replacing it with a slogan “The Media Are Liars”. Middleton (2017) notes that the group only wanted to be heard and did not actually destroy data or take money from CBC; it was merely hackers getting a message across in ways that currently Anonymous do. Yet the case still worried computer users, bringing about a time in the 1990’s where the scope of the damage of hacking was being recognised as criminal and deviant behaviour.

In reviewing hacking history between 1996 and 1997, laws and law enforcement was having an effect on hacker activities. These, despite not keeping pace with fast growing technology, were being used across the world to prosecute hackers. New computer operating systems like Microsoft were too tempting not to hack. Credit cards and other data were being stored in databases that were becoming networked, that could be reached all over the world. Hackers saw these as challenges, hence why a race between hackers and the public emerged in the 1990’s. Files and data became digitised, with sound files being converted and shared using the MPEG-1 Audio Layer 3 (MP3), creating file sharing networks such as the controversial music file sharing client Napster. With less storage constraints, MP3 files were freely available to store and share (Carter & Rogers, 2014). Hackers were also developing sophisticated ways to hide their tracks as improvements in finding them were created by network security experts. Information on how to hack became shared on programs such as Internet Relay Chat and Usenet.

During this time Cryptovirology was invented. The explanation for this is complex but is significant in terms of hacker history. A protection for preventing the reading of data is cryptography, it arose as a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel (Bellare & Rogaway, 2005). Cryptovirology is studying cryptography to develop malicious attacks against it (Young, 2004) but also to find vulnerabilities and failures in an effort to improve it (Anandrao, 2011).

What is interesting about this was that this was developed out of academia as Young and Yung reported (2017):

It started at Columbia University as a natural by-product of an unnatural union: a former hacker placed in a room with a cryptographer, both given ample time with which to contemplate the dystopia of tomorrow. Collectively, given our backgrounds, we had amassed a body of highly unconventional scientific problems that hackers face when infiltrating computer systems as well as the foundational cryptography with which to solve those problems.
Yet later, hackers would use these same types of principles and codes to create ransomware.

While more hacking attacks grew, there was an increase of hacking on defence installations and networks, as well as the Central Intelligence Agency (CIA). Altering and defacing websites were particularly popular with hackers. In one example, hackers replaced the words of the CIA with ‘Central Stupidity Agency’ (Drash & Morris, 1996). In 1997 a Croatian youth hacked a system at the Guam U.S. Air Force base, while in 1996 a Swedish hacker had jammed the 911 emergency call system in Florida.

Yet despite these attacks growing in seriousness and scale, hackers were experiencing more publicity, hostility and were on notice they were being hunted. As crime and other academic discipline researchers’ suggest, hackers have viewed their activities as creative problem-solving not crimes (Nikitina, 2012), but they were still being feared and loathed by the public.

**Increased Hacking: 1998 and 1999**

The 1990’s saw the beginnings of, and rise of, the World Wide Web and companies such as Apple, Microsoft, Linux and web portal and search engines like Google and Yahoo. Hackers disliked these and saw them as challenges to hack. Additionally, attacks on infrastructure and law enforcements continued. An older web browser called Netscape was especially a target. Hackers began to threaten organisations and individuals at an increased rate.

Two examples that brought awareness of the expanding problem of hacking were a group of hackers wanting Kevin Mitnick to be freed and the youngest juvenile hacker, Jonathan James, being jailed for cybercrimes in the United States. Both cases are unique for the new ways hackers had become more open and brazen in their attacks:

**Case One: Yahoo! Hackers**

In January 1998 hackers, calling themselves PANTS/HAGIS left an online ransom note demanding Mitnick be freed from jail. Computer security experts were skeptical, but it was taken seriously by Yahoo. The *Los Angeles Times* reported (1997):

 Calling themselves PANTS/HAGIS, the hackers got into Yahoo’s Web site at about 7 p.m. Monday, leaving a digital ransom note. “For the past month, anyone who has viewed Yahoo's page and used their search engine now has a logic bomb/worm implanted deep within their computer,” it read. “On Christmas Day, 1998, the logic bomb part of this ‘virus’ will become active, wreaking havoc upon the entire planet's networks. The virus can be stopped. But not by mortals.” The note said an “antidote” program will be made available if hacker Kevin Mitnick is released.

**Case Two: Jonathan James**

James hacked into the United States Department of Defense systems such as NASA at age 15. Operating under the pseudonym of ‘C0mrade’, he stole source code which was needed on the International Space Station. He also become the first person in the world to crack the DOD by entering the Defense Threat Reduction Agency (DTRA) system and could view DOD staff messages (Emma, n.d.). He was caught and tried.
Kao, Huang and Wang (2009) in their study of young juvenile hackers stated that youths committing cybercrimes were misunderstood as they were often just after passwords to games and websites for fun. They did not need shaming but guidance as is the practice for juveniles. Yet under United States Law there was an expectation hackers of all ages would be severely punished. James was but in an unrelated hacking incident in the 2000’s he committed suicide for fear of being punished for a hack he did not do (Emma, n.d.).

These cases demonstrated how in the late 1990’s hacking was diversifying. In another example of how creative hackers were becoming, groups began to use hacktivism to conduct online attacks against governments and individuals. This was either done as pranks, but increasingly this saw groups using hacking against corporations and governments for protest. For example, a group called the Electronic Disturbance Theater claimed to be an online political performance and art group. They called their hacking conceptual art done to support the Zapatista movement in Mexico (Cultural Hijack, 2017).

This hack was also notable the group attempting to get the public to support their cause. Their varied hacks were on the Frankfurt Stock Exchange, defenselink.mil in the United States, the Pentagon and the then Mexican President Ernesto Zedillo. Lecher (2017) describes how a program called FloodNet was created to create a form of a hack on these organisations:

That year, members of an art group called the Electronic Disturbance Theater were invited to demonstrate a program called FloodNet. Billed as a “virtual sit-in,” users navigated to the FloodNet website at a predetermined time, and through a simple Java tool, were directed to a targeted website that would reload constantly, every few seconds. With enough people — perhaps thousands - the sit-in caused targeted websites to slow or maybe even crash, rendering them intermittently inaccessible.

Griffis (2014)\textsuperscript{21} preserved snap shots of FloodNet in an online article. Figure 16 shows a simple FloodNet screen for people to send messages to targets in a protest the group called Electronic Civil Disobedience:
Hackers can mostly work alone when causing disruption and harm, but during this period of hacker history, individuals working in groups increased from previous decades. As Julian (1999) described this form of hacking, to him it is a low-level of information warfare and an early example of cyberterrorism.

By contrast to the Electronic Disturbance Theater, the Level Seven crew in 1999 was notable for being earlier hacktivism incarnations of attacking information systems on large-scale attacks. Their hacking information was shared on IRC channels, but also notable was that although as stated hackers like to work on their own, they combined their hacking skills with other groups such as Global Hell and Hacking for Girliez. Initially their targets were The First American National Bank, NASA, the .ma Moroccan Internet domain name system server and Sheraton Hotel’s Group. But it was their September 1999 defacement of the United States U.S Embassy in China’s website that was significant in showing what hackers could do to what were thought of as unhackable web sites. A comment about the group appears online that reflects not only this group, but also a direction hacking was heading in the 1990’s (Revolvy, n.d.)

Level Seven typify a group of hackers who exploit or attack computers and networks for more than just the thrill and challenge, and for reasons other than money. During their era, they were activists, and they used their computer skills to make political statements and protest actions by government and industry. Thus, they bridged the realms of hacking and activism, operating in a domain that is now called “hacktivism”.

As being a precursor to the practice of hacktivism, Level Seven demonstrated what was going to become common practice; hacking for social and political reasons.
In Chapter One a Worm was defined as standalone malware programs that is self-replicating and spreads to other computers. Although worms were common hacker practice, it was the 1999 Melissa Worm that created at that time the worst damage as email had become so commonly used. David L Smith created it as a Microsoft Word file attached to an email. Opening the document that is infected with Melissa.A caused a mass-mailing macro\textsuperscript{24} which was also passed on to up to 50 people in the recipient’s email client contacts list in Microsoft Word. It especially slowed down computer network traffic, causing damage to reputations and costs of many companies. Figure 17 illustrates the type of email message people were receiving (Panda Security, 2017):

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{melissa_virus_email.png}
\caption{The Melissa Virus in an email (Panda Security, 2017)}
\end{figure}

During this time hackers became more hostile towards the growing power of Microsoft and targeted their operating systems. Windows New Technology (NT) was seen as a challenge to hack. The first reported attacks on the MS-DOS Microsoft based NT operating systems became well-known in the media and a source of public panic.

In 1998 Cnet (1998) reported that the shared file abilities of the Windows 98 system made systems vulnerable to hacking. What this mean was, you were able to share files and download files from the growing sophisticated World Wide Web sites as well as other types of sites such as ICQ chat programs, newsgroups or public open file sharing sites. Hacking types of this and previous versions of Windows was explicitly found on the web in sites such as Reddit where a user named BTORogers (2013) demonstrated the ease at which hacking such systems and denying users access was common place\textsuperscript{25}. During this period of hacker history, the rise of software security had begun and was quickly commercialised to capitalise on the public’s fears of hacking. Examples included Norton’s Anti Virus and Microsoft making users download security program patches to minimise hacker damage to home computers.

During 1999, governments committed to fighting hackers through funding security measures at all levels. Most notable was United States President Bill Clinton announcing in 1999 a $1.46 billion initiative to improve government computer security and implement what was
then seen as needed, expenditure on intrusion detection monitors (Hamblen, 1999). Doman (2016) reported how in March 1998 Operation Moonlight Maze was an inquiry into cyber attacks on the United States. He also reported that Newsweek had labelled it the first major co-ordinated hacking attack (Doman, 2016):

In 1998 a technician at a specialist materials company “ATI-Corp” identified a connection from their network to Wright Patterson Air Force Base. He noticed the user was connecting at 3 AM on a Sunday, and the owner of the account confirmed that they weren’t using the account at that time. He raised the alarm to a number of CERTs (Computer Emergency Response Teams) - the Air Force were the first to respond.

They identified it was an attacker, and found they had made further connections to Wright Patterson Air Force Base from the University of South Carolina, Wright University and the University of Cincinnati. In one instance it appeared the attackers had made a mistake - they had connected (possibly directly) from a machine in Moscow.

As the FBI commenced an investigation, code named “Moonlight Maze”, it became clear that this wasn’t an isolated case. It was a coordinated attack on an unprecedented scale.

As the United States continued to become involved in more conflicts in other countries, more cyberwarfare grew in response to United States having a role in many conflicts. The United States Department of Defence launched cyberattacks against Serbia’s computer networks during the Croatian War of Independence (Yugoslavian conflict 1991 to 1995). The North Atlantic Treaty Organisation (NATO) had also bombed by accident the Chinese embassy in Belgrade, Yugoslavia, causing the Chinese to launch cyber attacks against the United States. These incidents during the 1990’s demonstrated that hackers were no longer just targeting local or state computer systems, but could possibly from anywhere launch hacking attacks internationally against nations.

**Conclusions of 1990’s Hacking**

The sample of 1990’s hacking history illustrated the race between hackers and governments to destroy and protect data. Public alarm was growing, hence why computer protection for personal computers became an industry. What was seen during this period was the scale and types of hacking were becoming larger and continued to move from local hacking to hacking performed by hackers not in the country under attack. Hacking for social and political gain moved from performance to a design to destroy companies and government’s systems. Sharing of malicious hacking information and techniques was still mostly public in virtual communities and online chatting programs like ICQ and IRC. Hackers continued to work alone, but also organise groups. There was also the challenge of creating laws that kept pace with new technologies and increasing penalties for hackers. What occurred next were more sinister hacking activities on a global scale.
The Growth of Sophisticated Hacking and Cyberterrorism: 2000 to 2018

In Chapter One, a brief introduction to the seriousness of hacking in terms of how it can affect infrastructure, transport, utilities and financial data by disabling systems humans rely on was discussed. Additionally, as the Ashley Madison data attacked on accounts of those having affairs when partnered or married demonstrated, there can be serious consequences for personal relationships and social reputations. The sophistication of hacker skills combined with more people wanting to hack caused further concern about what was to occur in the future. There was not a long wait to see the potential harm hacking could do in the 21st Century.

Cyberterrorism: Hackers at their Most Dangerous

Although a definition amongst scholars is not always agreed upon (Bruce, 2013), terrorism does have specific characteristics that define it. The appropriate technical definition that suits is by Denning (2000) presented at a testimony at Georgetown University in the United States, and supported by Curran, Concannon and McKeever (2008, p. 1) is:

Terrorism can be defined as “The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons.”

Other scholars similarly define it in such term. For example: illegitimate force and political objectives (Laqueur, 1977), psychological fear production on others not always the immediate targets (Bjørgo, 2005) and violence and force (Schwenkenbecher, 2012). Government definitions of it often reflect the political situation of the country and its leaders (Badey, 2007). In one American survey, Huff and Kertzer (2018) stated that one result was that the respondents felt politicians can potentially manipulate perceptions of terrorism by framing violent incidents in certain ways through the use of political spin. Nevertheless, terrorism has horrific consequences not just in the events themselves, but how they change the way people view the world as a place where people want to harm others.

Cyberterrorism is defined by Curran, Concannon and McKeever (2008, p. 6), as:

Any premeditated, politically motivated attack against information and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.

These attacks are often in two forms: against data and against the controlling systems that have the data (Lemos, 2002). Colarik and Janczewski (2008, xv) describe the typical pattern of a hacker (or cyberterrorist as they became termed) attack ins five phases:

1. The first phase of an attack is reconnaissance of the intended victim. By observing the normal operations of a target, useful information can be ascertained and accumulated such as hardware and software used, regular and periodic communications, and the formatting of said correspondences.
2. The second phase of an attack is penetration. Until an attacker is inside a system, there is little that can be done to the target except to disrupt the availability or access to a given service provided by the target.

3. The third phase is identifying and expanding the internal capabilities by viewing resources and increasing access rights to more restricted, higher-value areas of a given system.

4. The forth stage is where the intruder does the damage to a system or confiscates selected data and/or information.

5. The last phase can include the removal of any evidence of a penetration, theft, and so forth by covering the intruder’s electronic trail by editing or deleting log files.

Ultimately, an intruder wants to complete all five stages successfully. However, this is entirely dependent on the type of attack method utilized, the desired end result, and the target’s individual defensive and/or monitoring capabilities.

Cyberwar or cyberwarfare is also a term used to describe the practice of cyberterrorism. It is also known as information warfare which means the same practice, with terms such as digital warfare, netwar or information terrorism (Cronin, 2001).

Yet there is a conflict amongst commentators in two ways: does Cyberwar actually exist and that has been a part of hacker history well before the 2000’s, or even the 1970’s? Retired Brigadier General John Brown of the United States Army wrote that computer scientist Willis Ware warned about large-scale hacking in 1967 and that forms of Cyberwar were occurring in the United States since the invention of the network system Advanced Research Projects Agency Network (ARPANET) (Brown, 2017). Arquilla and Ronfeldt (1993, p. 27) believe that such hacking is a form of war where the goal is obtaining knowledge about a country:

While both netwar and cyberwar revolve around information and communications matters, at a deeper level they are forms of war about “knowledge” - about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries.

Arquilla (2011) has continually argued that cyberattacks have continued on defence and infrastructure targets, and that the United States has done such acts on other nations to resolve and defuse international crises negating the need for military warfare.

Despite many strong arguments, some believe that cyberwarfare is media hype. Rid (2012) has the view that cyberattacks do not meet the criteria of what a war is. Being critical of Arquilla and Ronfeldt’s views, Rid stated that a hacking attack in June 1982 on the Siberian pipeline where the CIA implemented a logic bomb into the system was not a hacking attack. He also further writes that cyberweapons are unlikely to create massive collateral damage on people and nations. Others dispute this and argue that many nations and organisations are still not doing enough to protect computer systems from attacks (Lenzner & Vardi, 2004).

Cyberwarfare is not limited to defence or infrastructure. Hackers can gain access to commercial inventions and plans and use them to create something before other nations do.
This is termed Cyberespionage. For example, Chinese President Xi Jinping in 2005 agreed to a bilateral agreement with the United States not to carry out such acts. This did not get adhered to. Segal (2018) reported that 50-80% of cyberattacks on intellectual property (IP) were recorded as being from China, with energy, pharmaceutical and law companies targeted. The financial consequences are high, such as Segal stating in 2013 it was $300US billion dollars, but there is also the problem that inventions having their plans stolen and used by another country stifle the innovation process. This can damage a country’s economy.

China has over time been named as perpetrators of cyberwarfare despite the slow but noticeable opening up of that nation to tourism, foreign investment and trade with others. Schapp (2009, p. 132) in 2009 described the growing power that China gained which effectively illustrates the depth of that country’s influence in hacking history:

China currently possesses a significant cyber weapons and intelligence infrastructure, and their cyber warfare doctrine is designed to achieve global “electronic dominance” by 2050. This includes the capability of disrupting the information infrastructure of their enemies. In 1999, the PLA Daily, the official media outlet for the People’s Liberation Army (PLA) of the, stated, “Internet warfare is of equal significance to land, sea, and air power and requires its own military branch.” According to military and intelligence sources, Chinese cyber forces have developed detailed plans for cyber attacks against the United States and others. A 2007 Department of Defense report indicated the PLA had established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks.

Professor Greg Austin, an Australian cyber security scholar, provides insightful reasons behind the thinking of China in its quest for cyber dominance. To an extent, China may have more sophisticated hacking ability than the United States. Austin (2014, p. 144) explains this as:

In this regard, it is important to understand that China (like the United States) does not see cyber military power as a question of computer versus computer, network versus network, or hacker versus hacker. China sees cyber military power as the leveraged relationship between military cyber assets and other forms of military power. This approach is described well in the following definition of ‘cyber conflict’: “broader than cyber warfare, including all conflicts and coercion between nations and groups for strategic purposes utilizing cyberspace where software, computers, and networks are both the means and the targets”.

Austin reflects the ideology of Western countries that the cyberwarfare ability to use against nations is something China values.

The criticisms of China and Russia as the main protagonists of cyberwarfare have been ongoing despite nations, such as Australia, forging new levels of relationships and trust with them. There are other nations that may be also engaging in such warfare, North Korea being named although their expertise in unclear, with Kim (2018) reporting that the country’s hackers are rapidly improving with their skill level to attack large computer systems.
Yet the level of threat and potential harm is still not clear as at 2018. For example, Thompson (2012) argued that threats from Jihadist groups is often more in terms of urging people to conduct attacks especially on company or business websites, but are not always carried out on large-scales. However, in Australia, the establishment of the University of New South Wales Canberra Cyber Research Centre assists Australian government, business, defence and home computer users to prevent hacking. This certainly is useful and remedies Lenzner & Vardi’s (2004) view that countries are not doing enough to prevent cyber attacks.

At the stage of hacker history in the 2000’s, the potential exists for worldwide and catastrophic consequences of hacking. Yet like Rid (2012) stated, such attacks can be overestimated and even not possible. The doomsday scenarios reported online written by media, bloggers or even security experts need to be read critically. There does, however, need to be acknowledgement of cyberwarfare’s potential. These three examples show what has been or are possible:

**Scenario 1:**

According to Inglis (2018) The U.S. Department of Homeland Security has revealed that Russian government hackers have gained deep access to hundreds of U.S. electrical utility companies, gaining far more access to the operations of many more companies than previously disclosed by federal officials. One problem of this is that such attacks can cause electrical surges, capable of destroying electrical equipment on a mass scale. If essential equipment is destroyed on a large scale, such as a system of street lights or hospital equipment, this can cause damage to property and life.

**Scenario 2:**

Credit card details stealing by hackers has obviously been a large theme during this chapter, with hackers doing this behaviour for decades. The difference is the scale. It is possible that billions of credit card holders can be affected. Wiping out someone’s bank account is a major fear of people who invest all their money into banks. A large hack of credit cards was by the group FIN7 who stole credit card details from restaurants across the United States through email attachments in phishing attacks. But the amount of those affected can, at this point in hacker history, be considered significant at approximately 15 million credit card holders (Ng, 2018). The scenario of larger scale attacks is now more than possible, but perhaps inevitable.
Scenario 3:

Although this has been greeted with scepticism from plane manufacturers (Gibbs, 2015), a terrifying scenario is the idea that a hacker can gain control of any type of aircraft and crash it. It is comforting that the current thought is that hacking by taking direct control of a pilot’s network and the plane is difficult through the plane’s Wi-Fi or entertainment systems (Yu & Smith, 2015). Thomson (2014), however, stated that aircraft flying systems were very unlikely to be hacked due to the design of the systems and the judgement of pilots who can sense something may be wrong in flight. Yet it was reported that a United States Homeland security expert was able in 2016 to remotely hack and take control of a Boeing 757 (Murphy, 2017) and at a Black Hat conference a claim was made that there are weaknesses in satellite communications that control aircraft functions (The Courier Mail, 2018).

The mass media and law enforcement have continuously reported such terrifying scenarios after the major crackdowns of the 1980’s and 1990’s on hackers (Thomas, 2005). A good and evil scenario has intensified in the 2000’s as hacker attacks continued. The major emerging concern, as at this time of writing, is the Advanced Persistent (APT) which can be undetectable. This type of attack can consistently steal intellectual property and sensitive information from the web browsers used in a company system (Shaji, Dev & Brindha, 2018).

Major Hacking Incidents and Issues in the 2000’s

The types of hacking incidents over the 2000’s were sophisticated and widespread, but similar to those in previous decades. A point with hacker history during the 2000’s is how hackers would draw on past hacker exploits, share information openly on and offline, as well as continue to ignore growing laws making penalties harsher. Another factor is the increased security on many levels across the world after the terrorist attacks on the United States on September 11 2001. Cyberwarfare and attacks were taken far more seriously with the assumptions that they were done to disrupt democratic societies with fear. A final factor is the increased access to the Internet, with more people willing to be black, grey or white hackers and learn how to hack. Anyone who becomes skilled in hacking and in covering their activities can potentially learn to hack larger computer system targets.

Shutting down websites in DoS attacks is still a powerful way of disrupting commerce and information finding. Microsoft in 2001 was one of the first companies to experience this now common hacking activity. Various attacks on websites were now a challenge for hackers. For example a Turkish Hacker, Kerem125 attacked the United Nations website in 2007. Defacing occurred on government websites, such as the hacktivists BlackMas in 2004 attacking the New Zealand government website. It was also a concern when security company Trend Micro was hacked in 2008 by a Turkish hacker named Utku. These issues do erode consumer confidence in companies, hence why those who have websites try to prevent website defacement. Later in the decade social media was hacked with Sesame Street’s YouTube channel hacked and replaced with a pornographic film for 22 minutes in 2011 (Schwartz, 2011).

To illustrate hacker web defacement, in 2018 the Indian telecommunications company Bharat Sanchar Nigam Limited’s website was hacked. As the company had a large customer base in a developing country it needed to not lose contact with their customers. Figure 18 shows
how, as at 2018, their corporate website appears while Figure 19 shows how it looked when hacked and defaced:

Figure 18. BSNL (2018) website before hacker defacement

Figure 19: BSNL website after defacement showing who did it (Chronicle & Suares, 2018)
These types of attacks grew in popularity with hackers. The issues these cause is that the functionality of the website becomes impossible to use, such as the customer in the case of BSNL cannot log in and find out details about the firm’s telecommunication offerings.

Worms, malware and viruses also became more widespread. Although antivirus and malware detection did work, they did disrupt and destroy computer systems and data. The famous ones during the 2000’s made global headlines as they spread across international borders. Examples were:

- **2000:** ILOVEYOU worm, originating in the Philippines created by a student.
- **2001:** Dutch hacker released a virus called Anna Kournikova, a tennis player, by an email with an attachment claiming it contained provocative photos of her.
- **2001:** The Code Red worm infected tens of thousands of networks and was said to have cost $1.1 billion dollars to repair computer systems (Rossi, 2002).
- **2002:** Klez.H virus, which was considered the worst malware attack that although did not cause financial losses, was said to have infected at 2002 the most number of computer systems.
- **2009:** Continuing attacks on the vulnerable developing Microsoft Windows operating system, the Conficker worm infiltrated millions of business and personal computer systems worldwide, including defence systems such as the United Kingdom Ministry of Defence and Germany’s unified armed forces (We Live Security, 2016).
- **2010:** Hackers will invent new ways of spreading malware and viruses, with Stuxnet being spread by the growing use of USB drives on Windows computers, but some security experts believe it could have been more malicious (O’Murchu, n.d.) possibly made to launch a cyberattack on Iran’s nuclear weapons system.
- **2012:** Shamoon virus was extremely costly and destructive, being carried out by Iranian hacker group Cutter Sword of Justice, with energy company Saudi Aramco sustaining much damage to their computer systems.
- **2017:** The WannaCry ransomware attack was seen as unprecedented in the scale of damage it caused as it spread across 150 countries which exploited the Windows SMB and Microsoft’s use of it allowed executable code to be spread on systems (Fruhlinger, 2018).

These examples demonstrate the evolving nature of malware and viruses in terms of the reach and spread of them combined with the damage they can do to government, business and personal computer systems.

Hacker groups were formed during the 2000’s that were more high profile than previous groups with larger group memberships. For example, Anonymous in 2003/04, Lulz Security in 2011 and UGNazi in 2012 were three who began high profile attacks. Yet individual hackers refusing to join these groups mounted their own large-scale hacking attacks on systems, but law enforcement agencies targeted the hacker groups more as these were seen to
be more dangerous than individuals (Hollinger, 1991). Examples of hackers committing such acts were:

- 2011: Bank of America website hacked by Turkish hacker, 85,000 credit card numbers stolen.
- 2011: Play Station Network hacked and 77 million accounts had details published in the data breach.
- 2011: A computer hacker obtains electronically information from the United States various agencies, namely Department of Defense, NASA, NSA, US Military and, alarmingly, the Pentagon, as well as United Kingdom websites.
- 2012: In contrast to the mostly United States reports of hacking, Norwegian hackers in a group called Team Appunity hacked a user database of Norway’s prostitution website in a data breach.
- 2012: More, and frequent, hacks occurred including on the Marriott hotel group, Foxconn in Taiwan, WHMCS a web hosting platform and the online professional network platform LinkedIn.
- 2015: The two publicised data breach hacks were The United States Office of Personnel Management and the Ashley Madison breach of personal information incident.
- 2016: Russian intelligence hackers published online emails from the United States 2016 Democratic National Committee’s email leak.
- 2017: The hacker group The Dark Overlord showed that it was not always financial or terrorism motives for hacking when they obtained through networks unreleased episodes of the television series Orange is the New Black online.
- 2018: Two major data breaches occurred that contributed to a loss of trust in security from the public: Chinese hackers identified as hacking the Australian National University in Canberra that continuously compromised their research systems, and TicketFly a ticket event service that holds many credit card details.

Clearly during the 2000’s there has been a momentum of group and individual hackers committing acts which can involve the whole world.

### Identity Theft

A major part of hacker history has been the practice of identity theft. This is defined as the theft of a human’s identity information including a name, birth date, Centrelink (Social Security) number or a credit card number (Hoar, 2001). Hackers have made this practice a staple of their activities and it is usually malicious and for personal gain. It has also grown to be an industry with people’s personal information used for monetary and other gains.

The problem with identity theft is how it can become part of transnational crimes. An Australian report (The Australasian Centre for Policing Research & The Australian
Transaction Reports and Analysis Centre, 2006) reported that false identities from stolen
details is linked to fraud, drug trafficking, terrorism and human trafficking. Computer
security experts consistently warn the public to protect their documents, such as passports and
driver’s licences, as well as their online data.

**Mobile (Cell) Phone Hacking**

Another part of hacker history is that that attacks occur on mobile computing devices. The
mobile phone is underestimated by many as something that can be hacked. Why it is a
concern is that phone apps have access to personal information. These include banking,
Apple pay on the Iphone, emails, text messages and social media apps such as Facebook. It is
advised to use encryption on the phone and avoiding public Wi-Fi networks, but hackers can
obtain simple programs to hack phones. This issue will become more problematic in the
future as the mobile phone is relied upon and other devices such as the Apple Watch.

**The Dark Web**

The final part of the history of hacking that is important to acknowledge is that hackers have
sought to find larger targets to hack. Over the decades sharing hacking information was done
in chat programs such as ICQ and IRC, message boards, online chat and virtual communities.
Law enforcement has stopped some of these, so hackers have sought to create new virtual
channels to communicate information. As hackers use this, it is important to discuss its
importance in hacker history.

The definition of the Dark Web is simply described by Greenberg (2014) as a collection of
thousands of websites that use anonymity tools (web browsers) like Tor and I2P to hide a
users IP address. What has become concerning is how hackers can now pay through
cryptocurrency for hacking tools and advice, as well as mostly safely receiving payments
from victims of their ransomware attacks (Kirkpatrick, 2017). The Infosec Institute (2018)
have also reported that hackers can be found and be paid to hack others’ Facebook or social
media accounts. Hurlburt (2017) states that the Dark Web represents one of the biggest
threats to Cybersecurity worldwide and that the cybersafety methods, such as antivirus
programs, are not going to be sufficient in the future to protect individuals, business,
government and others from hacker harm. Yet scholar Eric Jardine, who acknowledges the
Dark Web’s nest of hackers and the damage they can do from it, states that the global nature
of it will be difficult to shut down and taking away Tor and other browsers can interfere with
peoples’ human rights to a free Internet (Jardine, 2015).

**Conclusions of 2000’s Hacking**

The 2000 to 2018 decades marked the evolution of hacking from individuals and groups to
ations who possess the power to inflict cyberwarfare on others. Individual hackers and
hacker groups built on the past achievements of hackers to conduct larger-scale attacks across
the world. The trajectory of hacking to such large scale hacks such as data breaches and
access to intellectual property and military data has been supported by the ability to access
information on the Dark Web combined with some countries, and businesses,
underestimating hacking attack potential. Overall, although law enforcement and security
experts, some of them former hackers, are battling hackers and cyberterrorist, this decade
showed how hacking has evolved to a sophisticated level that has shown the world what
hackers are capable of.
Conclusions and Summary

This has been a substantive chapter about the history of hacking and hackers. From the first recorded incident of hacking to the sophisticated, widespread hacking of today, it is stated that although the size of hacking is global, hackers still have a cultural and technical history influenced by previous hackers. The chapter could only sample the key hacking incidents over the decades, for there are many more that have been reported. Concerning is, despite reassurances from some security experts, that in the future hacker history may be filled with more apocalyptic incidents or potential new threats.

The next chapter is an in-depth look at one hacking group called Anonymous.
Notes


2 Appears on page three of Raymond’s PDF book A brief history of hackerdom.

3 Although this appears in The Tech, this quote was obtained from a blog called The Story of Information.

4 Figure 11’s image was obtained from a YouTube video from the Smithsonian Channel.

5 A straightforward short guide to the operation of the Enigma machine can be found at https://learnencrypt.org/history/the-enigma-machine (Learn Cryptography, 2018).

6 An in-depth technical and history account by Lee Gladwin, Alan Turing, Enigma and the Breaking of German Machine Ciphers in World War II is an excellent source for reading about the British and Polish work on this project. It can be found as at the time of writing this book at https://www.archives.gov/files/publications/prologue/1997/fall/turing.pdf

7 A more technical description of the Bombe machine can be found at http://www.cryptomuseum.com/crypto/bombe/

8 Mitnick’s computer security organisation can be found at https://mitnicksecurity.com/

9 The book Ghosts in the Wires has a full title of Ghosts in the Wires: My Adventures As The World’s Most Wanted Hacker, and as it lacks page numbers, the quote from Mitnick cannot be referenced correctly.

10 http://www.takedown.com/ has an archive of newspaper articles and much more information on Mitnick, but also at http://www.takedown.com/coverage/mitnick-timeline.html is a concise but detailed account of his life and activities.

11 Boot sector viruses, despite the phasing out of the floppy disc, were, and still are to an extent, a hacker’s entry point into systems. To appreciate this, an explanation from the Indiana University (2018) explains what is and why it is serious:

Boot sector viruses infect or substitute their own code for either the DOS boot sector or the Master Boot Record (MBR) of a PC. The MBR is a small program that runs every time the computer starts up. It controls the boot sequence and determines which partition the computer boots from. The MBR generally resides on the first sector of the hard disk. Since the MBR executes every time a computer is started, a boot sector virus is extremely dangerous. Once the boot code on the drive is infected, the virus will be loaded into memory on
every startup. From memory, the boot virus can spread to every disk
that the system reads.

The full transcript of Skrenta’s 2007 blog post reflecting on the 1982 prank can be
found at http://www.skrenta.com/2007/01/the_joy_of_the_hack.html

12 Peter Samson documents how he and his team achieved this at
http://www.gricer.com/anysrc/anysrc.html

13 This document is available at http://www.mit.edu/hacker/part3.html and is fairly long
to read. It is unclear who wrote it and it represents a view of only one person.
However, in terms of dealing with hackers in the timeline of hacker history,
Operation Sundevil represents what has become a major problem for law
enforcement; catching and prosecuting hackers.

14 Szor presents a technical explanation of polymorphic viruses at
http://computervirus.uw.hu/ch07lev1sec5.html

15 A brief scope of the problems America Online (AOL) have had can be found at the
Fast Company website article by Lumb (2015)
https://www.fastcompany.com/3046194/a-brief-history-of-aol

16 The 2012 BVMUndergroundHipHop video for Dr. Dre and Snoop Dog’s track that
played at the beginning of Da Chronic’s toolkit is at
https://www.youtube.com/watch?v=l4E4XC7qOfk

17 IM means Instant Messaging.

18 Velzian’s (2018) explanations of AOHell can be found at https://www.quadrotech-
it.com/blog/hacking-horror-stories-vol-1-aohell/

19 The Canadian documentary is, as at 2018, available on YouTube at
https://www.youtube.com/watch?v=qFlFIWghwwc&feature=youtu.be

20 A complex and informative website written by Young which explains Cryptovirology
is at https://www.cryptovirology.com/cryptovfiles/cryptovirologyfaqver1.html

21 Griffis excellent visual story of the Electronic Disturbance Theater is located at
https://iprh.wordpress.com/2014/09/17/electronic-civil-disobedience-and-collective-
interruption-online/

22 The .ma is part of the Internet domain name system in Morocco which is shown in the
URL’s of web addresses, for example, the English version of the Ministry of Culture
and Communication is http://www.maroc.ma/en.

23 Quote from Revolvy was lifted by that site from Wikipedia.
24 A Microsoft Word macro is a procedure in word processing where frequent and sometimes complex tasks are automated by the click of a button (Microsoft, 2018) such as repeating words that are so frequent the macro button in Word can be clicked to save typing it out continuously.

25 The Reddit demonstration of Windows operating system hacking can be found at https://www.reddit.com/r/hacking/comments/17kp3h/an_easy_way_to_bypass_the_windows_95_login/

26 The web address of the University of New South Wales Canberra Cyber Research Centre as at September 2018 is https://www.unsw.adfa.edu.au/unsw-canberra-cyber/

27 The Server Message Block (SMB) is a crucial part of the operation of the computer that is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers (Sharpe, 2002), a technical paper on which can be found at Sharpe’s page https://www.samba.org/cifs/docs/what-is-smb.html
CHAPTER THREE
A CASE STUDY OF HACKERS: ANONYMOUS

We are Anonymous.
We are Legion.
We do not Forgive.
We do not Forget.
Expect US.
– (me.me. n.d.)

By sacrificing the public self, by shunning leaders, and especially by refusing to play the game of self-promotion, Anonymous ensures mystery; this in itself is a radical political act, given a social order based on ubiquitous monitoring and the celebration of runaway individualism and selfishness. – Gabriella Coleman 2018

Hacker groups and hactivists engage in negative and positive computer security activities across the world. Many groups have caused great harm to individuals, business and government computer systems. They do this for many reasons. In Chapter Two, it was shown that over time hacking groups would hack for fun or challenge, but also political and personal reasons. Some hacking groups have become championed by the public while others are feared. People joining together for a common cause to hack has been a part of hacker behaviour for decades.

This chapter focuses on hacker group Anonymous. Part 1 will concentrate on the formation, structure and ethos of Anonymous. Part 2 will focus on some incidents and conflicts the group has been involved in. The case study’s aim is to present an example of how a hacker group operates in the increasingly reliant technological world and to examine a hacker culture. It is important to disclose that getting information on Anonymous relies heavily on media, academic articles and social media posts. Therefore, the material presented and analysed in this chapter should be read as informative and not reflective of Anonymous members’ views.
Part 1: Formation, Structure, History and Ethos of Anonymous

Formal Explanation of Anonymous: Characteristics of the Group

The literature and studies about Anonymous have developed a common set of characteristics to describe the group. Based on a wide reading of the group, these characteristics were found to give the best explanation of what Anonymous is (Brad, 2016; Stanek, 2015; Woods, 2013):

- They are a group composed of a loosely organised but powerful international network of hactivists
- Their hierarchy is almost non-existent except for some running their social media and there is no formal leadership or head of the organisation
- No absolute conditions or rules exist to become a member, it is open to almost anyone of any age with some form of hacker knowledge and identification with the group’s ethos and beliefs, including being against all forms of censorship and government surveillance
- Anonymous produces and disseminates much of its rhetoric on the Internet and uses Internet sites to call members to action

Serracino-Inglott (2013), who quotes Coleman (n.d.), further states about the group:

Anonymous includes hard-core hackers as well as people who contribute by editing videos, penning manifestos, or publicizing actions. Then there are myriad sympathizers who may not spend hours in chat rooms but will heed commands to join DDoS attacks and repost messages sent by Anonymous Twitter accounts, acting as both mercenary army and street team. Anonymous has developed a loose structure, with technical resources such as Internet Relay Chat (IRC) being run and controlled by a handful of elites, but these elites have erected no formal barriers to participation like initiation guidelines or screening processes, and ethical norms tend to be established consensually and enforced by all.

Mikhaylova (2014), in a study of Anonymous observed:

- There is agreement amongst members that certain core issues, such as social justice, are important to adhere to, but members have very diverse issues and opinions, with some calling the group an idea not a group.
- As a result, Anonymous can have subsets within the group who will have different targets and causes.
- Anonymous use propaganda slogans such as being a legion of gatherers to evoke fear.
- Anyone who is truly part of Anonymous use the nickname Anonymous in public or online so that people do not know the status of that person in the group.

Wong and Brown (2013, p. 1024) labelled Anonymous ‘e-banditry’ and, as happens in any group, believe that they can be fractured and adversarial within:
In one sense, the open and leaderless nature of Anonymous makes it susceptible to problems of incoherence and a lack of directed action. Sometimes Anons are interested in “hacking as a form of protest,” other times however, Anons are subject to internal strife and in-fighting. Indeed, some former participants have become vigilantes who seek to expose and bring down other Anons.

Therefore, the characteristic that defines Anonymous is that despite its loose connections and splits in ranks, it is a hacktivist organisation with a social justice ideology that use hacking methods to cause disruption

**Where Anonymous Exists**

Anonymous only operates only: there is no physical place existing where they are headquartered. They exist on the Internet and Dark Web in many forms such as:

- Their website Anonymous Official
- Social media including Facebook, Twitter and YouTube
- A 2014 document called *The Story of the Anonymous Hacktivists Full Documentary*
- Online updates and major announcements in a news bulletin format style as Figure 20 shows:

![Image](image.png)

*Figure 20. Anonymous member reading a news announcement (Smith, 2015)*

Anonymous are the subject of documentaries, books, scholarly research and media attention that all contribute to understanding who they are, what they do, why they hack and how they achieve their aims.
The Anonymous Mask

Anonymous are publicly identified by the symbolic Guy Fawkes mask they wear at protests and that appears in their videos and other publicity material. The members will further disguise their voices when talking to the media or appearing in videos, using a Vocoder\textsuperscript{8} robot type sound. Figure 21 shows an example of a member’s mask:

![Anonymous member in mask (Strevo, 2008)](image)

_Guy Fawkes\textsuperscript{9} was an Englishman born in 1570, who converted to being a Catholic, joining a Roman Catholic group to assassinate King James I who was a Protestant. This occurred on what is now known in the United Kingdom as Guy Fawkes Day on the 4\textsuperscript{th} of November 1605. The plot was also to destroy by blowing up the House of Lords. This was the ‘Gunpowder Plot’ which failed as Fawkes was caught trying to light the fuse to the barrels under the House of Lords. However, the wearing of the mask by Anonymous was also inspired by a book written by Alan Moore called _V for Vendetta_, where a character, an anarchist named V, wears a Guy Fawkes mask as a disguise while trying to influence people to give up democracy._

Nicksburg (2015) reported a story behind Anonymous making the decision to wear the masks as a result of a conflict with the Church of Scientology\textsuperscript{10}:

_The hacktivist collective Anonymous popularized these masks in 2008 when it launched Project Chanology, a movement targeting the Church of Scientology after the church tried to censor an interview with Tom Cruise on the web. Members of the collective agreed to come out from behind their computer screens to protest the Church of Scientology, but needed a way to conceal their identities. The Guy Fawkes mask was their chosen disguise. Although the collective has never officially stated the reasoning behind this choice, it’s likely an homage to an eerie scene in _V for Vendetta_ in which a group of masked protesters marches on the British Parliament._
Figure 22 shows a public protest held in Los Angeles where many Anonymous members are wearing the Guy Fawkes mask:

![Figure 22. Anonymous rare public protest (Galloway, n.d.)](image)

Garrison (2015) argues that the masks have a deeper meaning embedded in a culture where hackers are social justice driven, but by wearing the Guy Fawkes mask are in some way protected by those forces who seek to shut them down:

Anonymous - themselves accused of being cyberterrorists - turns this narrative on its head with their ubiquitous use of the Guy Fawkes mask.

The state cannot “read” or “infer” anything from the mask. The mask hides the identity of all its many wearers from the law. But it does more than that. The mask creates a place where the law is suspended so that a community can voice their demands.

Overall, the mask acts as a disguise but also as a promotional symbol that is recognisable to all in society and is a protest symbol against those Anonymous seeks to deliver justice to.
A History of Anonymous

Beginning Attacks and Message Boards

The officially reported origins of Anonymous are that it began on the bulletin board called 4chan (http://www.4chan.org/). As the 4chan (n.d.) site states, it is a simple image-based bulletin board where anyone can post comments and share images, with a variety of topics discussed and no need to register an account to post on it. This was estimated to have started around 2003 (National Cybersecurity and Communications Integration Center, n.d.), but that is not clear. Hackers who posted on 4chan also began posting on other Internet and World Wide Web message boards.

There were two reported incidents before 2008 that suggested Anonymous were serious about targeting people or organisation. Anonymous hackers mostly did hacking for the LULZ. This term means to have fun, laughter, or amusement that is derived at another’s expense (Oxford Living Dictionaries, 2018). The first was in December 2006 on Hal Turner, who according to the website Hacktivism (n.d.) was a Neo-Nazi who espoused the views of the Nazi Party on his website and on podcasts. He upset 4chan members in a podcast by making negative comments about the board. It is an interesting story because it showed the beginnings of Anonymous becoming a loosely united band to cause someone issues. The extract from Olszewski (2010) shows what happened between Turner and Anonymous:

In December 2006, a band of Internet vigilantes (reportedly based in 4chan.org and 7chan.org) attacked Hal Turner’s ‘net audio broadcasts and Web Site.

The initial foray consisted of a coordinated series of prank calls to Hal Turner’s Internet talk show. Mr. Turner retaliated by posting the callers’ phone numbers at his Web Site.

The ePosse escalated the attack over a wider front. The pranksters posted the personal phone numbers of Hal Turner and his parents. Included in the message were allegations of domestic abuse and cruelty to animals, which Mr. Turner has denied.

Turner’s website became a target of a Denial of Service Attack, which prevented people from accessing his site due to huge amounts of traffic being directed to it. He also had to pay a large Internet bill for this attack. The attackers posted their pride in the attacks Olszewski (2010). Turner tried to sue 4chan and others for copyright infringement in a United States court, but lost. A student by the name of Christina Snyder (2014) wrote an analysis on her blog post of this war which illustrates well an overview of the incident:

The reason for attacking Turner had transformed from retaliation for fellow 4chan members, to winning a war. The group needed to prove to Turner that they were a force to be reckoned with. This can be seen in most other initiatives led by Anonymous. The focus is to offend people simply because they can. They do not care who they are offending or why, but only that they are doing it.

Yet it was the second incident that formed the idea that perhaps Anonymous were not always a villainous group. It concerned their Internet vigilantly activities to expose and stop child pornography sites. In 2007 Chris Forcand was charged by the Toronto (Canada) Police
Service luring a child under 14, other attempted acts, exposure and touching, as well as weapon offences. Members of Anonymous interacted with him and were sent naked photos by Forcand. The police were alerted and decided to take the evidence sent by Anonymous and use it to implicate Forcand. However, the media found out and made public that this happened. Later, the International Business Times (2011) reported Anonymous and their anti-child pornography activities, including attacking a hosting service of such material, would become a staple hacker attack that still continues.

Anonymous also began using a still in existence as at 2018 parody of Wikipedia site called Encyclopedia Dramatica to post images and text to make fun of their targets.

**2008: Anonymous Raises its Public Profile**

The main incident that brought Anonymous to worldwide notice was a response to the Church of Scientology’s attempt to remove their materials such as beliefs and practices from website and YouTube. In Part Two of this chapter, this will be explored further. In a study by Earl and Beyer (2014, p. 216) the authors show the difference between pre 2008 Anonymous and post 2008, and their new status as hacktivists, in this extract:

In early 2008, the Church of Scientology attempted to force websites such as YouTube to remove Church related materials from the Internet. In response, Anonymous mobilized against the Church of Scientology - an action that included Anonymous protesting in the streets for the first time. Anonymous mobilized because it viewed the Church’s behavior as an attack on information freedom. Since 2008, Anonymous messages have become increasingly framed in normative and explicitly political terms, rather than focused on a nihilistic pursuit of entertainment for entertainment’s sake. This turn toward activism also changed the meaning of membership.

Prior to 2008, Anonymous could refer to anyone who posted on 4chan, but usually referred to someone who posted on 4chan’s general topic (/b/) board, or on any of the other online locations Anonymous communities occupied. After 2008, Anonymous referred to both pre-2008 Anonymous communities as well as new members who were involved in online and offline activism but may never have used 4chan or any other posting board system associated with Anonymous.

There also grew splits in the Anonymous ranks with some members unhappy at its direction. Yet the number of targets Anonymous used hacking on continued to grow, as did their reputation. The initial communication between members was through IRC chat and 4chan, but social media was used as such platforms began to become available.

Between 2011 and 2012, Anonymous’ hacking targets became diversified. Some were still done for LULZ or for fun, but Anonymous continued to bigger, more political targets and corporations. There was involvement with the Arab Springs Campaigns, known as Operation Tunisia that aimed to continue to spread information to the world about what was happening there. A further operation in Egypt to do the same by hacking Internet browsers to bypass security restrictions was viewed by Anonymous as a success (Ryan, 2011). This demonstrated that they were now global and could influence world events. Being political began to override the need to hack just for the fun of it.
The Million Mask March 2013

This annual march is an important part of Anonymous history. As at 2018 it still occurs on Guy Fawkes Day in the United Kingdom, 5th of November, but is held worldwide. It takes place in many parts of the world, increasingly in countries where the march was either banned or discouraged, but mostly in urban areas such as: London, New York, Amsterdam, Berlin, Rome and Paris. Over 650 cities participated in 2015. The march also reminds the public that Anonymous is still in existence.

The original organiser of this march was John Fairhurst. There have been clashes across various cities between the marchers and police, especially in London and to an extent Los Angeles. Marchers wear the mask or paint on a mask with face paint, carry various placards with messages and carry Anonymous flags. Many of the marches begin at city halls, parliament buildings, capital buildings and law enforcement buildings such as FBI, CIA and Scotland Yard.

Figures 23 to 25 are random examples of photographs of various Million Mask Marches over time:

![Image](Figure 23. March with Anonymous marcher asked why they are there (Sevenblade, 2015))
As at October 2018 the next Million Mask March will be occurring in November. Australia does participate with Melbourne the most active with the most marchers to date, although Sydney, Brisbane and other capital cities have marches.
Controversies and Divisions in Anonymous, Arrests and Legal Trials

Anonymous has not been without its difficulties within the group and law enforcement. Some members became unhappy with the group’s direction, too radical or too soft, or clashes with other hacktivists and organisations such as the Pirate Party (Coleman, 2014) which caused splinter groups and causes to occur. Anonymous still played a part in these newer and different types of groups with two high profile ones: the now defunct Lulz Security (LulzSec) and AntiSec. These are discussed to show how divisions and issue can cause disunity.

Lulz Security

LulzSec were a black hat hacker group arising from Anonymous but were not representative of Anonymous members’ behaviours. The online chat rooms of Anonymous was where LulzSec formed and although its rise was fast, it did experience a demise due to a number of factors, including pressures from the FBI with arrests and other hackers with grudges who attacked LulzSec. Members viewed Anonymous as rivals. LulzSec became well-known for an attack on the user accounts of American entertainment group Sony Pictures and taking down the CIA website. They also employed humour and pre-warned on social media some attacks. For example, one of their social media accounts was The Lulz Boat named after 1970s American television show The Love Boat. Figure 26 shows an announcement on social media of a forthcoming hacking activity against Sony Pictures:

![Figure 26. LulzSec tweet forthcoming hacking activity (Brenner, 2012)](image)

They also attacked in 2011 American broadcaster Fox.com as a joke, but were offended by comments presenters had made against American rapper and musician Common when he was called ‘vile’ (Arthur, 2013). This resulted in a leak of thousands of United States talent show The X Factor contestants’ profiles and names. They also attacked Sony Playstation in a famous hack where 24.6 (approximately) million account holders’ private data was stolen, as was discussed in Chapter One. It was significant in terms of LulzSec destroying customer trust in organisations having the ability to protect online private data.
**Operation Anti-Security (AntiSec)**

AntiSec is a global hacktivist campaign beginning around 2011 that still exists as at 2018. The launch of AntiSec was done by Anonymous hackers within the organisation protesting Internet censorship, especially by governments which grew during the mid 2000s, and the monitoring of the Internet by commercial organisations and law enforcement. LulzSec former members also joined the operation as well as hackers from a group called BlackSec. Another issue AntiSec has are disagreements with worldwide copyright laws which they claim stifle freedom of expression and file sharing.

To get their message out into the public, in 2009 the image hosting service ImageShack (https://imageshack.us/) was hacked by AntiSec with millions of images on the site redirected to an image posted by the group. This image is important to consider for two reasons. First, in bringing the image into public awareness, the ability to take over customer’s photos and embed code into ImageShack’s system is a significant, anarchistic statement. Second, the manifesto speech is significant to read because it shows how the security and law enforcement agencies are to the disdain of the hackers. In a reproduction of an image that was posted online, it shows how AntiSec thinks in its quest against the global computer security industry is a necessity and is for the good of freedom of expression (Atalaya, 2009):

> We're a movement dedicated to the eradication of full-disclosure. We wanted to give everyone an image of what we're all about.

> Full-disclosure is the disclosure of exploits publicly - anywhere. The security industry uses full-disclosure to profit and develops scare-tactics to convince people into buying their firewalls, anti-virus software, and auditing services.

> Meanwhile, script kiddies copy and paste these exploits and compile them, ready to strike any and all vulnerable servers they can get a hold of. If whitehats were truly about security this stuff would not be published, not even exploits with silly edits to make them slightly unusable.

> As an added bonus, if publication wasn't enough, these exploits are mirrored and distributed widely across the Internet with a nice little advertisement embedded in them for the crew or website which first exposed the vulnerability to the public.

> It's about money. While the world is difficult to change, and money will certainly continue to be a very important in the eyes of many, our battle is that of the removal of full-disclosure for the purpose of making it harder for the security industry to exploit its consequences.

> It is our goal that, through mayhem and the destruction of all exploitive and detrimental communities, companies, and individuals, full-disclosure will be abandoned and the security industry will be forced to reform.

> How do we plan to achieve this? Through the full and unrelenting, unmerciful elimination of all supporters of full-disclosure and the security industry in its present form. If you own a security blog, an exploit publication website or you distribute any exploits... “you are a target and you will be rm'd. Only a matter of time.”
This isn't like before. This time everyone and everything is getting owned.

Signed: The Anti-sec Movement

“No images were harmed in the making of this... image.””

Of note is the humour at the end of the message that is indicative of AntiSec, that is, saying no images were harmed in the making of the image that appeared on ImageShack.

Some initial attacks the group did included those on the now disbanded United Kingdom Serious Organised Crime Agency, the Arizona Department of Public Safety, the Brazilian Government and the famous hacking of an online United Kingdom newspapers saying its owner, Rupert Murdoch, was no longer alive. Other larger targets over time included NATO, Homeland Security United States, Fox News Twitter accounts and various governments such as Zimbabwe and Tunisia. This resulted in law enforcement all over the world, the USA and UK especially, sort to find members of AntiSec, arrest and convict them, as well as trying to stop future attacks.

Company private documents and emails were especially targets. It also made people concerned that such hacks by Anonymous and AntiSec were spectacular in their size and scope. For example, in 2011 the Vanguard Defense Industries hack in Texas, USA, was an attack done because Vanguard was associated with the FBI, U.S. Marshall Service and the Department of Homeland Security. This was clearly an attempt to highlight that after the September 11 Attacks on the United States, security on citizens had gone too far and the power such agencies had was an invasion of peoples’ privacy.

Not all attacks were considered to be useful to public awareness of government surveillance. One hack that was done in response to arrests of other hackers by AntiSec was in August 2011 called Shooting Sheriffs Saturday. The leaked information compromised the security of law enforcement with many U.S. sheriffs’ offices and law enforcement agencies hacked. The information included private details of officers’ data, including home addresses and the identities of those who anonymously gave information as informants to law enforcement officers. Credit card details were also used to supply digital rights organisations with funds to support their activities in alerting the public to the activities of law organisations.

Arrests and Punishments

In the history of Anonymous, some members have been arrested and charged across the world, although jailing of them is not as common. In this section two examples of arrests and punishments illustrate that people in hacker groups can be found out. In the first example, the arrest across the world of LulzSec members which enraged Anonymous is discussed and an example of one Anonymous member who participated in the Church of Scientology fun hacking is examined.

The catching of Anonymous and LulzSec hackers was illustrated when Aaron Barr, who was the Chief Executive Officer of HBGary a company that offered computer technology security products and services to protect systems from hackers, decided to target Anonymous. The stories of the technical and political details of how he did are written about on websites.
(Anderson, 2012; Anderson, 2011; Greenburg, 2011; Sweatman, 2016), but the result was damage to his reputation and having to leave the company.

The verbal public arguments between Barr and Anonymous resulted in information being published about the underestimation of what Anonymous could do. In these extracts, Barr’s activities are described and the response of Anonymous is given to show that the hackers were persistent in countering everything Barr did:

Sweatman (2016):

He was trying to correlate Facebook and IRC activity to reveal the identities of the group’s key figures. In the shadowy world of black-hat hacking, getting your true identity revealed is known as getting doxed, and is something every hacker fears. Going after such a well-known group would be sure to get his struggling company some needed publicity. It would also have the most unfortunate side effect of getting the hacking groups attention as well.

Anderson (2012):

When Anonymous defaced the HBGary Federal website, the hackers made the same point. “You think you've gathered full names and addresses of the 'higher-ups' of Anonymous?” said their note. “You haven't. You think Anonymous has a founder and various co-founders? False…. We laughed. Most of the information you've 'extracted' is publicly available via our IRC networks. The personal details of Anonymous 'members' you think you've acquired are, quite simply, nonsense.”

Hackers from Anonymous and LulzSec were identified. The arrests over time from Barr and others trying to identify members did occur. Some examples were (Sweatman, 2016):

- Jake Davis - Scotland, online name Topiary
- Mustafa Al-Bassam - London, online name Tflow
- Ryan Ackroyd - South Yorkshire, England, online name Kayla
- Hector Monsegur – New York City, online name Sabu, a founder of LulzSec

These are among the most famous members of Anonymous and LulzSec that were arrested and charged with various computer crimes. As Arthur (2013) states, Monsegur was told to cooperate or be arrested and held in jail, but decided to assist the FBI as Monsegur feared being separated from his nieces he was caring for. This illustrated, although justifiable in this case, the lack of loyalty hackers could have towards each other when confronted with law enforcement and possible incarceration.

Olson (2012, 88-92) in the book, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, tells the story of how Anonymous members were not immune to being caught. In this book extract, young hacker, Brian Mettenbrink, is confronted at his home by FBI agents and eventually is charged with hacking offences for his part in the Church of Scientology hacking activities:
The Federal Bureau of Investigation, meanwhile, was just getting started. Also by the summer of 2008, the FBI, or “feds” as Anons referred to them, had managed to track down and apprehend two out of the hundreds of people who participated in the DDoS attacks on Scientology. They would be the unlucky sacrificial lambs and the first of scores more arrests over the next few years. Anons had always thought till now that they were immune to arrest, or well hidden from the authorities. One of the first to learn the hard truth was Brian Mettenbrink, the bored college student who in January 2008 had left LOIC running in the background of his computer for a little too long.

“Were you involved in the DDoS attacks?” one of the men asked. Mettenbrink shifted in his seat. “I was involved for a little bit,” he said. The computer he had used to run LOIC was now sitting downstairs in the basement.

“Did you…enjoy taking part in the attacks?” “Yeah,” said Mettenbrink, thinking back to how dull he had found college. “It was fun. It was something new and interesting to do.”

“Did you know that your actions were a criminal violation?” one of the men asked.

“Sure,” Mettenbrink said, “I just didn’t think the FBI would be showing up at my door.”

Mettenbrink didn’t hear from the FBI again for months, and it was a year before he truly realized, during a conversation with his lawyer, the seriousness of his offense. “Do you have any idea how much monetary damage the Church of Scientology is saying you caused?” the lawyer had asked during one of his meetings with Mettenbrink.

The young man thought for a moment. “I can’t imagine there was any monetary damage,” he said. All he’d done was help send a bunch of spoof traffic to a website and slow it down for a couple days.

“They’re claiming one hundred thousand dollars,” the lawyer replied. Mettenbrink was stunned. He had attacked Scientology.org on a whim, his weapon a tiny, freely available program he’d run in the background for three days while he browsed an image board. How could that have cost someone a hundred thousand dollars?

Like Monsegur, Mettenbrink was left to defend himself, although any arrest was viewed with disdain by Anonymous members and spurred them to continuously hack law enforcement agencies.
Part 2: Targets and Causes: Documenting Anonymous Attacks

Anonymous has been implicated in many documented high-profile attacks against individuals, corporations, political parties, terrorist organisations and governments. Exploring this is difficult because of the large number of attacks Anonymous and their splinter groups have done. The four main Anonymous hacking events that will be discussed are:

1. Operation MegaUpload
2. The Church of Scientology
3. The Westboro Baptist Church
4. Wikileaks

These four are considered representational of the types of attacks and conflicts that mirror Anonymous activity. The target of the attack is discussed, background of why the conflict and hacking occurred and what events happened.

Operation MegaUpload

Anonymous supports the idea that the Internet should remain free. They state that people have the right to upload copyrighted material, such as movies, television and music, to sites for others to have, such as the Pirate Bay hosting site. Their involvement in protesting the raid on the file sharing company Megaupload that occurred in 2012 was significant not only as retaliation, but raised awareness of how closing down Internet file sharing sites were to many a form of censorship. The debate about paying for music or films, as well as the morals and ethics of copyright law, are out of the scope of this book. However, it is important to be aware of both sides of the file sharing argument and the pay or should not pay for files shared online.

File host service MegaUpload was founded by German computer programmer, entrepreneur, political activist and hacker Kim Schmitz, also known as Kim Dotcom\(^{14}\) and was based in Hong Kong. Its notoriety was those using it would upload copyrighted movies, music and television program files. On the 19\(^{th}\) of January 2012, MegaUpload, along with some of its related websites, were closed down by United States Justice Department and the FBI, with Schmitz and four others arrested near Auckland by the New Zealand police.

The allegations against MegaUpload were that the site violated piracy laws and caused over $480 million Australian dollars in damages to copyright holders. There was an objection by many affected by the piracy that up to $168 million dollars of profiteering from the site was made (Crozier, 2012). Another organisation representing artists, the Motion Picture Association of America (MPAA) took figures from Megaupload and using that and other evidence as data keep it for use in criminal trials.

All this infuriated members of Anonymous who believed that such file hosting sites should be left as they were with no censorship of them or closure. Ten sites, including those involved in the raids such as the FBI and various entertainment industry websites, were temporary hacked and shut down by Anonymous. In a CNN news report, Anonymous posted a message claiming credit for the attack (CNN Wire Staff, 2012):
“We Anonymous are launching our largest attack ever on government and music industry sites. Lulz," the group said in a statement posted late Thursday on an associated Twitter account. "The FBI didn't think they would get away with this did they? They should have expected us.”

To mark Operation MegaUpload, Anonymous changed one of their logos using the MegaUpload symbol. Figure 27 shows how the symbol for the operation appeared:

![Anonymous logo for Operation MegaUpload](https://www.knowyourmeme.com/memes/anonymous-logo-for-operation-megaupload)

Not every hacker, information technology expert, cultural commentators or members of the media supported Anonymous and their takedown of the sites. Chen (2012) of Gawker.com condemned the widespread posting on the web and social media of a link that when clicked made the person who clicked it into an accomplice in doing an illegal Denial of Service attack one on of the targeted website; Chen called this ‘evil’.

CNN gathered as much information as it could over the other news networks about the story. Amber Lyon, a reporter on the *Quest Means Business* television show, conducted an interview with an Anonymous member about the operation. This interview transcript is, claimed by CNN, authentic, but also shows that despite remaining at that time in 2012 an underground force, Anonymous were prepared to make a point by launching bigger, more organised cyberattacks.

The interview, aired during the attacks in January 2012, is reproduced from the CNN (CNN Transcripts, 2012) transcript site that encapsulates and illuminates this important even in Anonymous’ history:
<table>
<thead>
<tr>
<th>Lyon: So, Anonymous sees the shutdown of Megaupload as a type of internet censorship?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANONYMOUS MEMBER: Exactly. It's a violation of freedom of speech, and Anonymous and a lot of other movements regard the internet as sort of independent from any government, and they regard the government interfering in the free flow of the internet as stopping outside of their jurisdiction.</td>
</tr>
<tr>
<td>Lyon: How long did it take for the Department of Justice's website to go down?</td>
</tr>
<tr>
<td>ANONYMOUS MEMBER: I would give it seven or eight minutes, not even.</td>
</tr>
<tr>
<td>Lyon: Seven or eight minutes?</td>
</tr>
<tr>
<td>ANONYMOUS MEMBER: I say seven minutes.</td>
</tr>
<tr>
<td>Lyon: Is - what was the thoughts within Anonymous that it was that easy to take down the Department of Justice's website.</td>
</tr>
<tr>
<td>ANONYMOUS MEMBER: With enough power and with enough manpower you can take down pretty much anything.</td>
</tr>
<tr>
<td>ANONYMOUS MEMBER: It's basically the power of an absolutely massive group of people coming together. They're not happy. And this wouldn't be possible with one or two people. It's one of those things which is very genuinely an expression of how many people are angry.</td>
</tr>
</tbody>
</table>

Anonymous took the position that although copyrighted material was on MegaUpload’s servers, it constituted an invasion of privacy to raid the company. It was also concerning that the FBI and others had access to the personal data of its users. Those using MegaUpload may have uploaded copyright material, and not necessarily had been punished after the raid, but it suggests Anonymous may have had a valid point in that governments can obtain private citizen data. This is an ongoing debate in the field of ethics and technology. Operation MegaUpload did prove that Anonymous could shut down sites in retaliation quickly and in an organised manner.

**Operation Chanology: The Church of Scientology Protest**

Anonymous hackers also practice hacktivism for protesting against many organisations and corporations for the ideologies, beliefs and practices of them that Anonymous dislike. A significant protest in February 2008 by the group was against the Church of Scientology. Anonymous believed that the church’s practices and secrecy were causing harm to people. Although it did not stop the Church from continuing to exist, the events of that time have become folklore in the hacker community.
Background to Attack on the Church

A large discussion of the Church of Scientology is beyond the scope of this book, but some details need to be discussed to illustrate the controversies that spurred on Anonymous. The Church of Scientology was founded in 1953 in New Jersey by Lafayette Ronald Hubbard. It has three core beliefs in a creed that Urban (2011) reports as:

1. Being free to enjoy religious expression
2. The idea that mental healing is inherently religious
3. Healing of the physical body is in the spiritual domain

Hubbard wrote a book called *Dianetics: The Modern Science of Mental Health; A Handbook of Dianetic Therapy*, published in 1950, as a guide to Scientology practice. It is still in print. A major claim Hubbard (1950) makes is that most illnesses are psychosomatic. These are illnesses caused when the mind influences the body to create or complicate an illness (MedicineNet, 2018). However, on the Church of Scientology website (2018) the word ‘Dianetics’ has a more esoteric meaning as being “what the soul is doing to the body”.

What is significant about the Church are the controversies and its guarded practices, as well as its worldwide spread in many countries that has made sure it tries to remain a mysterious organisation. There has also been criticisms when famous people from politics and entertainment have become known as scientologists. Five reported examples, as at 2018, are: musician Beck, actresses and actors Kirstie Alley, John Travolta, Nancy Cartwright and, notable, Tom Cruise.

Also of note are issues about the church’s aggressive publicity and public behaviours. The notable ones are as follows, but a common pattern is how they seek to control their public image with intimidation of people and strictly controlled social media content. A English BBC documentary released in 2007 called *Scientology and Me* famous for host John Sweeney yelling at a Scientology leader, was greeted with distain by the Church and unsuccessful attempts to stop its showing by John Travolta and other Church members occurred.

Attempting to stop church information being presented was a key part of Anonymous targeting the Church. The Church had a policy created by Hubbard called The Dead Agent Doctrine. This was enacted when threats from outsiders occurred and the Church would try to destroy the person’s reputation and discredit them to make them ostracised by the Church and followers and disbelieved by the public (Scientology Critical Information Directory, n.d.). The Church is hostile towards psychiatry and psychology in the treatment of mental health issues. Disconnecting friends and family from those who join the Church has also been practiced.

Although caution must be exercised, and information read critically, much information from Wikipedia is reasonably useful in providing an overview of the Church and its practices. Five Wiki pages are given at note 16 that can assist with understanding the Church’s background and why Anonymous targeted them in Operation Chanology.
The Tom Cruise Video Inflames Anonymous

Operation Chanology began when a highly promoted video of actor and scientologist Tom Cruise was released in 2008. The church wanted to remove some of the information in the video to create a version they wanted the public to see. Cruise is seen in the 9 minute video discussing his involvement with, and his beliefs in, the Church’s creeds. He used much of the Church’s jargon and also criticised psychiatry. A Church representative claimed that “The video is of Mr. Cruise making an acceptance speech to fellow parishioners at a private church event in 2004” (WikiNews, 2008). The Church felt it was leaked to YouTube and other platforms, with YouTube removing the video under a threat of litigation and copyright volitation claims from the Church.

Anonymous considered the Church’s actions Internet censorship. On the 4chan and other messages boards, Anonymous members decided to take action and, using IRC chat channels, formulated a loose but powerful plan to damage the Church. On a YouTube video created by Anonymous (ChurchOfScientology, 2008) the following message to the Church was read out as a notice of action to the Church:

Over the years, we have been watching you. Your campaigns of misinformation; suppression of dissent; your litigious nature, all of these things have caught our eye. With the leakage of your latest propaganda video into mainstream circulation, the extent of your malign influence over those who trust you, who call you leader, has been made clear to us. Anonymous has therefore decided that your organization should be destroyed. For the good of your followers, for the good of mankind - for the laughs - we shall expel you from the Internet and systematically dismantle the Church of Scientology in its present form. We acknowledge you as a serious opponent, and we are prepared for a long, long campaign. You will not prevail forever against the angry masses of the body politic. Your methods, hypocrisy, and the artlessness of your organization have sounded its death knell.

The main activities Project Chanology Anonymous did were sending blank and black faxes to many Scientology Centres across the world. This was followed by Denial of Service attacks on the Church’s website. It was reported that the Project Chanology website, set up to be the public face of the attack, was hacked by Scientologist hackers, either from the Church or those opposed to Anonymous (Shah, 2008). The Church did report the attacks to law enforcement, so if they retaliated on their own accord with hacking the question to ask is were they breaking the law as well? Anonymous also launched a second attack in March on the Church on L. Ron Hubbard’s birthday, the 15th of March.

Views on Project Chanology

The Anonymous attack on the Church, while not stopping its existence, did damage the reputation of Scientology. Even Anonymous, however, published views clarifying the reasons for the protests and attacks. In a second video, Anonymous posted their rationale for attacking the Church (Vamosi, 2008):
Your religious beliefs are not wrong, like any other religion, and they are yours to keep. However beliefs should not come at a price. Not from your wallet or compromising your thoughts.

Those who have left feel a new life, a rebirth into true freedom. You can join them if you wish. You may not believe us. We ask of you one thing: Make up your own mind. That is a sentence of more profound meaning for you now than at any other time in your life.

Many incidents occurred between the Church and Anonymous. Media and scholarly analysis of Project Chanology is overall positive. For example, Elliott (2009, p. 106) viewed Anonymous and the Church conflict in this way:

Project Chanology has been such a rousing success because of public interest in it, and because of the user-base's desire to be involved in it. Public reception of Project Chanology can also be attributable to the effect of memetic transmission, with the criticisms laid against the Church of Scientology being seen as real, credible complaints, worthy of investigation.

To some scholars, mocking Tom Cruise and the Church was a form of LULZ, doing it for the laughs, but some members had grudges against the Church’s practices. The incident brought Anonymous to the fore as a formidable force. Stoehrel and Lindgren (2014, p. 243)

In this performance then, threats were expressed with a sense of humour – at least from an Anonymous perspective – and through intertextual aesthetics, making popular identification (and in extension, support) possible. In particular, the video formed and symbolically unified the previously fragmented layers of Anonymous. It gave rise to Anonymous as part of a field of struggle and/or as a larger movement of political activism, beyond, but not excluding humour and enjoyment. From this perspective, the Anonymous community media mobilised the lulz – here also understood as a political passion; engaging in resistance against the anti-democratic structure of the Church of Scientology to communicate and create a new political environment, working on the fringes of the political and legal.

What these authors reflect on is that the protest against the Church lead to Anonymous moving from hacking as fun to being a force for serious hacktivism and online protest. This did also occur offline as members, most of who did wear the Guy Fawkes mask but some did not, made their protests physical as they appeared on the streets marching against the Church. This was a significant event that would influence later hacking activities and protests, which despite Anonymous being a loose collective, made people aware of their potential power.
The Westboro Baptist Church and the Newtown Sandy Hook Protest

Before proceeding with this third example of significant Anonymous hacker activity, this section may contain material that may be distressing to read due to its descriptions of the crime and the behaviours of the Westboro Church.

In the case of the Westboro Baptist Church, some felt hacking was justified because of Westboro’s history of offensive protesting and radical beliefs. However, the clash with Westboro came from a tragic incident and Anonymous did receive support for their actions. It was not a case of just for the laughs; Westboro angered many people over the insensitivity of the followers and leaders of Westboro attacking the school shooting.

Westboro frequently target homosexuals using the term ‘fag’ including using it as their domain website name http://www.godhatesfags.com/ (2018). These terms used in this context are considered homophobic. Yet Anonymous, especially when it operated on the 4Chan message board, would use terms like ‘fag’, ‘faggot’ or ‘gay-fag’ as well. As Potter (2015) says, although Anonymous does not have a racist, sexist or homophobic agenda, it can be seen as hypocritical for Anonymous to target a church that espouses homophobia yet use homophobic terms as well. This may be seen as Anonymous having a double standard.

Westboro Baptist Church Background

To appreciate the Anonymous campaign against Westboro over the Sandy Hook shooting, some background information is needed. As is the case of Scientology, Anonymous were not against religion as something to follow, but rather the acts that organised religions do. Many view Westboro as spreading hate speech and fail to understand that among their many targets are returned soldiers (of all genders) either living or not who have served to protect the United States or other countries.

Westboro Baptist Church has its headquarters in Topeka, Kansas, in the United States. According to their website (God Hates Fags, 2018b) it was established in 1955 by the late Pastor Fred Phelps. He had been put in charge of a branch of the East Side Baptist Church, but after a promotion to Westboro, broke from the established Baptist church. In 1991 they began the long-standard method of gaining attention; picketing beginning with a park in Topeka that they believed harboured sexual encounters between men.

This church has strict beliefs based on the teachings of John Calvin called Calvinism, a domination of Protestantism. Although not a Calvinist idea, it is based on the concept of predestination, where only certain types of people will go to heaven (Christianity.com, 2018). The idea of a chosen few destined for heaven exists across religions and faiths. Westboro believe in Calvin’s ideas and adhere to them. However, their beliefs that everyone other than themselves are sinners covers many people in society.

Homosexuals are especially targeted with Westboro claiming there is a homosexual agenda across the world. Other targets include other churches, such as the Catholic Church, music concerts, actresses and actors, writers, musicians and politicians. An example of a high profile picket was Apple Founder Steve Jobs memorial service. Another group they picket is that of returned soldiers and the memorial services for them. They are also vocal opponents of Islam, the Jewish Faith and Hindus, but condemn racism and groups such as the Ku Klux Klan.
A highly vocal person and spokesperson for Westboro was Fred Phelps’ daughter, Shirley Phelps-Roper. She has clashed with many people on radio and television, including members of Anonymous. The final point about Westboro’s background that pertains to Anonymous is a decision for church members to picket in 2012 the Sandy Hook Elementary School in Newtown, Connecticut. This school was the scene of a mass shooting on the 14th of December 2012.

The Protest against Westboro by Anonymous

The outrage about the planned picket was swift with Anonymous organising cyber and other attacks as soon as knowledge of the school’s picket became known. Westboro wanted to picket the victims’ memorial vigil. It was especially abhorrent to many because most of the victims were children. *The Huffington Post* reported that the reason given for Westboro’s protest was the acceptance of Connecticut’s Same-Sex Marriage legislation (Sieczkowski, 2012).

The hacking attacks began quickly, followed by Anonymous arguing in the media with church members. Many Newtown citizens, outsiders from all over the United States and elsewhere, various motorcycle and other types of gangs and the media shielded the vigil, resulting in Westboro not getting close to it and the picket not occurring. Anonymous was also helped by various people living in the town. Two hacking strategies were to take down the Church’s website and publish the names and other data of many members of the Church. A hotel employee secretly gave Anonymous the address in Connecticut of a hotel where members were staying.

Anonymous posted their agenda against Westboro online, as reported by Thomson (2012):

“We have unanimously deemed your organization to be harmful to the population of the USA, and have therefore decided to execute an agenda of action which will progressively dismantle your institution of deceitful pretext and extreme bias, and cease when your zealotry runs dry,” the hacking group said in the now-traditional video.

“We recognize you as serious opponents, and do not expect our campaign to terminate in a short period of time. Attrition is our weapon, and we will waste no time, money, effort, and enjoyment, in tearing your resolve into pieces, as with exposing the incongruity of your distorted faith.”

What also occurred were other hacker groups joining and copying Anonymous, including the group cosmothegod, as well as Shirley Phelps-Roper’s Twitter account being hacked (Bender, 2012). Anonymous claimed victory by posting on social media Westboro’s failures. For example, Figure 28 shows a highly-circulated tweet where Anonymous claim they forced the Church members to vacate a hotel (Johnston, 2012):
There were also many across traditional and social media that while not always supporting Anonymous or hacking, but were in favour of the actions against Westboro. Pavlo (2012), a writer and lecturer of white collar crime, stated that Westboro’s use of free speech arguments had gone too far. This view was openly and secretly held by many people across society. Anonymous had been able to influence people to consider the positive side of hacking.

The legacy of the conflict between Anonymous and Westboro is the presence of a video on YouTube of an episode of *The David Pakman Show*. Shirley Phelps-Roper and a spokesperson for Anonymous were brought onto Pakman’s show. The person from Anonymous was represented by an image and spoke in a British accent. During the interview, Phelps-Roper is amused by Anonymous’ claims and she tries numerous times to interrupt the conversation. Her claims are that the Church knew of attacks through supporters sending emails.

The interesting event during the interview is that Anonymous claimed another hacker had taken down the Church’s collection of websites. Phelps-Roper attacked Anonymous calling them ‘criminals’ and ‘kicking their ass’ (InfamousN3WS, 2012). However, Anonymous hacked a Westboro site during the interview, saying they have ‘a surprise for you’. Phelps-Roper continues to argue with the spokesperson greeting the hacking act with amusement. The interview concludes with no resolution and Phelps-Roper claiming victory over Anonymous as being portrayed better than the hackers.

**The WikiLeaks and Anonymous Conflict**

As part of hacker culture one hacker group may decide to support another group doing similar work. This is not just computer hacking, but social justice protests or exposing governments’ and organisations’ secrets. One prominent international non-profit organisation who have been at the centre of many controversies for the information they provide is WikiLeaks (https://wikileaks.org/). The founder of it is Australian Internet activist Julian Assange. A clear definition from Sifry (2011, p. 171) is that it is an online media organisation publishing leaked and secret information. Documents that are released to WikiLeaks become stories that alert the public to concerning government and corporation activities, but also protect those who gave information (Sorell, 2015).

Although it is not possible to list all activity WikiLeaks as the focus of this section is to discuss the clash with some members of Anonymous, consulting the World Wide Web and the Wikipedia entry. Overall, the assessment and usefulness of WikiLeaks as a site for assisting society is debated among scholars, ethicists and journalists. Much praise is placed...
on it for many reasons. As a vigilante site it allows potential massive volumes of private
information on documents to become available (Fenster, 2012). Older media institutions,
especially newspapers, are suspicious of the new online model of WikiLeaks in news
reporting and question its validity as an ethical news source, although this may be tied to their
self-preservation (Benkler, 2011). By contrast, Roberts (2012) is highly critical of it arguing
its attempt to be always transparent creates an illusion because even WikiLeaks may censor
information it gives to the public.

Anonymous gave support to WikiLeaks in 2012 when WikiLeaks set up a public fund on its
Global Intelligence File page, show in Figure 29. The issue that Anonymous had was an
overlay on the site that was viewed as a paywall, something they did not agree WikiLeaks
should have done. Anonymous members claimed WikiLeaks had become just about Julian
Assange, but the main issue was a dispute between both groups over a money donation site.
Previously, Anonymous had hacked Visa and Mastercard when those companies refused to
deposit the money from donors into the WikiLeaks page, also preventing PayPal from
processing donations.

![Figure 29. Feature that caused WikiLeaks Anonymous conflict (Kerr, 2012)](image)

Although the paywall was removed to appease Anonymous, it was later reinstated further
infuriating Anonymous members. Parnell (2012) reported that the hacker group felt that
WikiLeaks donations were funding Julian Assange’s lawyers and that it had become ‘all
about him’. Assange defended the paywall saying it was needed for WikiLeaks infrastructure
costs. Osborne (2012) claims that the group released statements which she reported as:
“Regardless of any workarounds, the fact remains that a meretricious page is placed for the majority of visitors that cannot be closed. The obvious intention is to force donations in exchange for access. This is a filthy and rotten, wholly unethical action - and Anonymous is enraged.”

“No longer will Anonymous risk prison to defend WikiLeaks or Julian Assange from their enemies. No longer will Anonymous risk prison to supply material for WikiLeaks disclosures. Anonymous turns its back on WikiLeaks. WikiLeaks has with its actions this past 48 hours betrayed Anonymous, and thus has lost its biggest and most powerful supporter.”

Anonymous however still do not support Julian Assange’s alleged sexual assault charges in Sweden and oppose any extradition of him to the United States. It is rumoured that should Assange leave the Ecuadorian Embassy in London he will be arrested and forced to first go to Sweden and then possibly be extradited to the United States. At the time of publication of this book he is still living in the Embassy.

The significance of this part of Anonymous history is that it shows it has no allegiances or loyalties to anyone. Even those that they have previously supported Anonymous or been supported by them have displeased the hacker group and been subject to online attacks. WikiLeaks and Anonymous have mixed reactions from the public, information technology security specialists, governments and the law. Groups fighting for the same types of causes that fall out can present a problem for supporters of both sides. To date, Anonymous still indirectly support WikiLeaks, but the incident did leave a division.

**Other Anonymous Attacks and Causes**

This section gives an inconclusive and incomplete list of attacks that are placed in chronological order as Table 4 shows. They can be consulted for further research and reading. 22.
Table 4
Anonymous attacks and causes

<table>
<thead>
<tr>
<th>Year</th>
<th>Description of Attack or Cause Taken Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td><strong>Epilepsy Foundation forum invasion</strong></td>
</tr>
<tr>
<td></td>
<td>Hackers placed JavaScript animations in forum to trigger migraines or seizure attacks in users reading the posts in the forum</td>
</tr>
<tr>
<td></td>
<td>Note: claim was made that the Church of Scientology hacked the forum to discredit Anonymous after the hacking group’s attacks during the Sandy Hook vigilante picket, but was not totally proven</td>
</tr>
<tr>
<td>2008</td>
<td><strong>Politician Sarah Palin’s personal email attack</strong></td>
</tr>
<tr>
<td></td>
<td>Done by one member who obtained her personal Yahoo account</td>
</tr>
<tr>
<td>2008</td>
<td><strong>Defacing of Hip Hop websites – Support Hip Hop Online and AllHipHop</strong></td>
</tr>
<tr>
<td>2009</td>
<td><strong>No Cussing Club Website and attacks</strong></td>
</tr>
<tr>
<td></td>
<td>McKay Hatch runs from California a website called <a href="http://www.nocussing.com/">http://www.nocussing.com/</a> (2018) which he created when he was 14, with Anonymous defacing the website and sending threats to his home and family</td>
</tr>
<tr>
<td>2009</td>
<td><strong>The 2009 Iranian election protest – Operation Iran</strong></td>
</tr>
<tr>
<td></td>
<td>The Iranian government during the election period wanted to suppress information and stifle debate, not only in Iran but also in other countries, with Anonymous collecting suppressed information and broadcasting it online</td>
</tr>
<tr>
<td>2009 and 2010</td>
<td><strong>Internet Censorship Plan in Australia – Operation Didgeridie and Operation Small Tits</strong></td>
</tr>
<tr>
<td></td>
<td>Anonymous made denial of service attacks on the Prime Minister of Australia and other government websites over attempts to legislate censorship measures against the Internet</td>
</tr>
<tr>
<td>2010</td>
<td><strong>Zimbabwe’s attempting to block WikiLeaks</strong></td>
</tr>
<tr>
<td></td>
<td>Involvement in attacks on the Zimbabwe Government and its then leader Robert Mugabe</td>
</tr>
<tr>
<td>2011</td>
<td><strong>Attacks on the Sony Corporation and PlayStation</strong></td>
</tr>
<tr>
<td>2011</td>
<td><strong>Various attacks across the world on anti-piracy23 organisations</strong></td>
</tr>
<tr>
<td>Year</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 2011 | **Attack on Irish Centre Right Party Fine Gael**  
Noted attack for the warning about the party that Anonymous put on Fine Gael’s website |
| 2011 | **Arab Springs and Operation Tunisia** |
| 2011 | **HB Gary Federal Attack** |
| 2011 | **Koch Industries Attack**  
Anonymous responds with online attacks in response to Republicans the Koch family and their donations towards groups in the United States that were seen to represent only the Republican interest |
| 2011 | **Spanish Police**  
Anonymous makes a DDoS attack on the website of the Spanish Police as a response to the arrests of hackers who may have been associated with Anonymous |
| 2011 | **Attacks on Malaysia, Orlando in the United States and India**  
Various hacking attacking in response to political corruption and censorship |
| 2011 | **Operation Intifada**  
Anonymous hacked the Knesset, which is the legislature of Israel because of hacking attacks from Israel, possibly the military |
| 2011 | **Operation BART**  
The Bay Area Rapid Transit in San Francisco website was hacked due to them shutting down the mobile (cell) phone network so that protestors to a crime could not communicate with each other to get others to come to the protest |
| 2011 | **Operation Syria**  
Anonymous hacked the Syrian Defense Ministry placing a flag image of the democratic pre-Ba'athist flag and messages of support to the Syrian uprising members |
| 2011 | **Operation DarkNet**  
A campaign against child pornography hosting services, obtaining the user names of those using them, but also, in a more co-operative event, Anonymous handing over the data to the FBI and Interpol |
| 2011 | **Operation Brotherhood Takedown**  
Anonymous take down websites of the Muslim Brotherhood |
<table>
<thead>
<tr>
<th>Year</th>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td><strong>Operation Pharisee</strong></td>
<td>An unsuccessful but high profile attack by Anonymous on the Vatican website for World Youth Day 2011</td>
</tr>
<tr>
<td>2011</td>
<td><strong>Operation Deepthroat</strong></td>
<td>An attack by Anonymous in partnership with others on the 9gag online message board</td>
</tr>
<tr>
<td>2011</td>
<td><strong>Operation Empire State Rebellion</strong></td>
<td>Anonymous obtains emails from the Bank of America suggesting corrupt practices occurring</td>
</tr>
<tr>
<td>2012</td>
<td><strong>CSLEA Hacking</strong></td>
<td>The California Statewide Law Enforcement Association is hacked in response to claims of police brutality</td>
</tr>
<tr>
<td>2012</td>
<td><strong>Occupation Nigeria</strong></td>
<td>Anonymous joins the People’s Liberation Front and Nigerian hackers resulting in the hacking of websites</td>
</tr>
<tr>
<td>2012</td>
<td><strong>Polish Government Denial of Service Attacks</strong></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td><strong>Operation Russia</strong></td>
<td>Anonymous identified hackers obtain emails from pro-Kremlin officials</td>
</tr>
<tr>
<td>2012</td>
<td><strong>Boston Police Department</strong></td>
<td>Hacked website due to the police arresting Occupy Wall Street protestors</td>
</tr>
<tr>
<td>2012</td>
<td><strong>More Syrian Government Attacks</strong></td>
<td>Anonymous access leader Bashar al-Assad’s staffs’ emails</td>
</tr>
<tr>
<td>2012</td>
<td><strong>AntiSec Leak, CIA Attack and Interpol</strong></td>
<td>Various attacks on law enforcement agencies</td>
</tr>
<tr>
<td>2012</td>
<td><strong>AIPAC Attack</strong></td>
<td>American Israel Public Affairs Committee website is taken down with Anonymous posting a YouTube message about the attack</td>
</tr>
<tr>
<td>Year</td>
<td>Event Description</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>The Vatican Website Denial of Service Attacks</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>United States Bureau of Justice Statistics Data Stolen by Anonymous</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>The Judge Rotenberg Center Protests</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anonymous hacked websites in response to the torture of students</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Monsanto Hungarian Website Hack</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Large attack on Chinese Websites</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Bahrain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attacks on the website of Formula One organisation in response to anti-government protests</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Occupy Philippines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anonymous attacks against the China University Media Union website due to Chinese hackers who defaced the University of the Philippines website</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Quebec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Major long attacks due to the Quebec Government trying to restrict freedom of association</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Japan Responses to Copyright Laws</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Anaheim in Response to a Shooting</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>AAPT Hack Australia in Response to Data Retention</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Mexican PRI Party Website Attack</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Myanmar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Still ongoing as at October 2018, Anonymous and other hackers continued attacks on Myanmar government websites</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Attacks on Uganda Government Websites over LGBTI Rights</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Steubenville Rape Case</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anonymous release personal details of suspects and also others who were alleged to have covered up the rape</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Operation Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2013</td>
<td>Operation North Korea</td>
<td>Attacks on North Korea including altering the leader’s image and the stealing of confidential data</td>
</tr>
<tr>
<td>2013</td>
<td>The Government Communications Security Bureau</td>
<td>Hacking of their site due to new laws allowing intelligence surveillance on New Zealand citizens</td>
</tr>
<tr>
<td>2013</td>
<td>Operation Singapore</td>
<td>Various attacks on Singapore institutions</td>
</tr>
<tr>
<td>2014</td>
<td>Operation Ferguson</td>
<td>Details of law enforcement personal details leaked by Anonymous due to a shooting incident</td>
</tr>
<tr>
<td>2014</td>
<td>Operation Hong Kong</td>
<td>Attacks on various government and other websites in Hong Kong due to the government’s use of force in protests in the city</td>
</tr>
<tr>
<td>2014</td>
<td>Operation Infosurge</td>
<td>Anonymous release information suggesting Philippine government officials did not act quickly or in the interests of the victim of Super Typhoon Yolanda</td>
</tr>
<tr>
<td>2015</td>
<td>Operation Charlie Hebdo</td>
<td>Posting of condolences and a declaration of war against terrorism in response to the shootings in Paris of the office of newspaper Charlie Hebdo</td>
</tr>
<tr>
<td>2015</td>
<td>Operation Ice Islamic State of Iraq and Syria (ISIS)</td>
<td>The start of an, ongoing campaign of cyber attacks against ISIS</td>
</tr>
<tr>
<td>2015</td>
<td>Operation Death Eaters</td>
<td>Attacks on various international pedophile rings</td>
</tr>
<tr>
<td>2015</td>
<td>Operation Stop Reclamation</td>
<td>Philipses Anonymous members hack Chinese websites in response to China’s reclaiming land in the South China Seas, that remains a controversial act even in 2018</td>
</tr>
<tr>
<td>2015</td>
<td>Operation KKK</td>
<td>Attacks against Ku Klux Klan members including publishing private details about members</td>
</tr>
<tr>
<td>Year</td>
<td>Operation Title</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2016</td>
<td>Operation Comelec</td>
<td>Anonymous hack the Commission on Elections which included voters’ details leaked</td>
</tr>
<tr>
<td>2016</td>
<td>Operation Single Gateway</td>
<td>Anonymous attacked Thailand Government sites in response to existing computer crime legislation</td>
</tr>
<tr>
<td>2017</td>
<td>Operation DarkNet Relaunch</td>
<td>Anonymous hack many sites where those using the Tor browser, that is claimed to protect the user’s Internet Service Provider address when browsing the Dark Web, received a message saying they had been hacked and that Anonymous had their details</td>
</tr>
</tbody>
</table>

These Anonymous attacks show the dilemma that not all of the group’s activities are necessarily black hat hacking. They do cause disruption to peoples’ use of the Internet and not every attack has been fair to all whose private details are disclosed. These also demonstrate the success of Anonymous as a loose collective. They are able to organise and mobilise quickly. Governments and organisations, as seen with ISIS, can strike back against Anonymous, but generally the assessment is not many members are caught, arrested and punished.

Anonymous has ongoing targets and give ongoing support to individuals and organisations. Julian Assange, for example, is overall not supported by Anonymous. Another target is Edward Snowden, who leaked United States government classified information to Wikileaks, where Anonymous members both support and abhor his activities. Donald Trump, as at 2018, is still targeted and watched by Anonymous with them ready to take action against him at any time. By contrast, Chelsea Manning who also leaked confidential government information was supported by Anonymous when she was attacked by the media and many others not just about the leaks but also her gender reassignment surgery. Her leaks about the Iraq and Afghanistan war were damaging, but although have not brought down the United States Government, are valued by Anonymous and are deemed to be worthy of protecting Manning from future attacks on her.

**Conclusions and Summary**

This case study examined the social, cultural and technological existence of hacktivists Anonymous. The history of the group showed how it was born on a messageboard to become a global, powerful hacking organisation. Conflicts with various organisations, Scientology, Westboro for ideological reasons, with companies over copyright issues and with governments and law officials, are all driven by a social justice paradigm Anonymous has. However, doing hacking for the thrills, the LULZ, is still present but perhaps less so. The long lists of hacks are samples of their reported attacks, for we do not precisely know how many unreported attacks have been done.
This case study chapter presented Anonymous and its activities. They are still operating as at the time of this book’s publication, but have left a legacy that has alerted the public to the fact that governments, organisations and individuals do not always have our best interests in mind.
Notes

1. The Anonymous group’s logo.

2. Anonymous use this slogan to describe the group.

3. Comment from Gabriella Coleman from Goodreads

4. Alfred Julian (1999) stated that it is difficult to verify hactivists’ claims. In this case study, the material is gathered from many sources, so it is taken at face value as accurate, but the authenticity of all the information in this chapter was difficult to fully verify.

5. Anonymous official website is at https://anonofficial.com/

6. The three main social media platform locations on the World Wide Web are:
   - Facebook: https://www.facebook.com/anonews.co/
   - Twitter: https://twitter.com/youranonnews?lang=en
   - YouTube: https://www.youtube.com/user/AnonymousWorldvoice

7. Available on YouTube as at November 2018 at https://www.youtube.com/watch?v=bC1ex2zRCYA

8. A Vocoder is device, mostly used in music, to alter the human voice to sound different to the voice that is entered into it.

9. A concise history, with video of animation of Guy Fawkes can be found at BBC Bitesize https://www.bbc.com/bitesize/articles/zdrrcj6

10. There are many resources to find out about the Church of Scientology and the many controversies surrounding them, with YouTube being a reasonably good place to find such information.

11. Encyclopedia Dramatica (2018a) can be found at this web address: https://encyclopedia dramatica.rs/Main_Page, but I caution that much of the material on it may be offensive to views for many reasons. An ironic part of this site is that it has also been critical of Anonymous with its own parody of the group (Encyclopedia Dramatica, 2018b).


13. The quote telling the story of Mettenbrink in Olson’s book is not in exact running order, with some sections left out to avoid too much detail.
14 Reading two accounts of Kim Schmitz is interesting to show the types of people Anonymous will support. As creator of MegaUpload, Kim Dotcom, as he is legally known as now, is a colourful character who has tried to become a politician in New Zealand. Although not interviewed on either site, to read on his life the Wikipedia (2018) entry on his life is substantial while a more critical profile is written by Breeze (2012).

15 As at October 2018, a full documentary can be found on video hosting platform Dailymotion, https://www.dailymotion.com/video/x12cdw1 (The Root AKA Rootbrain) although it is an extension of the Scientology and Me documentary. It is still interesting viewing for Sweeney’s view of his interactions with the Church.

16 As cautioned in the text, Wikipedia entries can be changed and may contain inaccurate information and facts. However, although readers can use search engines to find out much about the Church of Scientology, the background to Operation Chanology may make readers curious about the Church and its issues. These are:


17 As at October 2018 a copy of the uncut video that the Church did not want published is at this YouTube address: https://www.youtube.com/watch?v=UFBZ_uAbxS0 (Aleteuk, 2008).

18 Although this video, located in October 2018 at https://www.youtube.com/channel/UCNcuAYRX9J_lTj9TGNQnjrA is the message Anonymous sent the uploader of this video is Church0fScientology. It is unclear if the Church posted this, Anonymous or another account.

19 As previously stated, Wikipedia entries must always be read critically and with caution. However, the Wikipedia entry for Project Chanology is extensive and acts as a good starting point, with reasonably good factual content, to read about this protest. The entry as at October 2018 is at this web address: https://en.wikipedia.org/wiki/Project_Chanology

20 As at October 2018 the web address of this YouTube video is at https://www.youtube.com/watch?v=1o3bHkoSDck

Although Wikipedia was consulted for an overview of Anonymous activity, the listings in the table are from a wide range of sources. They are factual, reported attacks. Wikipedia provides a long list of attacks that may be of interest. It is located at https://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous

Anti-piracy in this context means preventing unauthorised use of copyrighted material.
CHAPTER FOUR
AN EXAMPLE STUDY OF HACKER BEHAVIOURS

Well, well, well... My friend, I know it might be a painful experience, but if you've just arrived here, we all must surrender to the burden of proof: you are a newbie, or even more affectionately, a newb! But right from the start, let's throw away any anxiety about that fact: not only have we all gone through that stage, but moreover, we have good reason to envy your position. As a matter of fact, all of us would have loved to find such a place as this site, at the time when we were in your current shoes. – Quote from website The Neuro Hacking Association

Plonk excl.: The sound a newbie makes as he falls to the bottom of a kill file. – Eric Raymond

Arguing with a script kiddie, I hate them more than the black hats, I think I'll just hack him after he gets his "point"across". #DillWithIt – DillonTheHacker #i62

Researchers have tried to understand hackers’ behaviours, why they commit crimes and why increasing numbers of people are interested in hacking. Doing studies on hackers are difficult to conduct as they often do not want to participate for fear of being reported to law enforcement. Yet studies on hackers can assist in understanding their culture and how they operate in society.

Hacking studies are conducted in academia, private enterprise, government, defence and law enforcement. They are divided into two groups: philosophical and technical. Many journals of computer security are devoted to developing code and systems to secure computer networks. Studies of hackers that are philosophical are broad in approach and can appear in any discipline, such as sociological, legal, business, psychology, political studies, cultural studies and social technology studies. Researchers take theories developed well before hackers became the problem they are now and apply them to understand hacker behaviours.

This chapter presents an example of a study I conducted in 2015 that was published in 2016 (Nycyk, 2016). It is about interactions on a public hacker advice virtual community where newcomers to hacking, called Newbies in hacker culture, try to obtain information on hacking from experienced hackers. This forum is on the World Wide Web, but although it is a hacker’s forum the ethos of it is towards practical ethical white hat type hacking discouraging illegal hacking activity. The posts in the forum were viewable by the public. What is interesting about the interactions are the way the newbies try to obtain information on how to illegal hack systems, and are put in their place by more experienced hacker forum members.

Newbies are unique to the hacking world because they are eager to hack, but often seem to be portrayed as hackers wanting to do damage to systems. This is not always the case, but from reading their questions online, it is more likely they are young, mostly male but not always, people who may be fascinated by the hacking world. They are also treated with contempt by experience hackers. Hacker groups are disjointed and are a rarely homogenous groups (Van Beveren, 2001; Denning, 1998). Newbies entering this field can feel overwhelmed on how to start hacking, but may also have a grudge and want to destroy or damage computer systems.
I wanted to explore how newbies were treated and once finding a forum and checking what ethical considerations where needed to use the posts as data, commenced analysis. Wible (2003) suggested that being kinder to new hackers and allowing them to hack systems legitimately would contribute to lower rates of them becoming black hat hackers. While a good idea, I found in my study that the experienced hackers did this but were also rude and admonishing to those newbies who wanted to do black hat hacking. In the hacking world the despised group are script kiddies, who are considered low in the hacker hierarchy because they lack an understanding of why they are exploiting systems.

This chapter presents a copy of my study called ‘The New Computer Hacker’s Quest for Skills and Knowledge: Contesting Experienced Hackers in Online Hacker Forums’, published in the International Journal of Cyber Criminology. It is included in this book because it gives an example of a sociological, criminal field study to show what occurs online between hackers. It is the full text with references set out as a journal article.

The Study’s Theoretical Framework: Power and Capital Concepts

Research studies employ some form of a theoretical framework to assist in searching for data to support the claims a researcher makes. In my study I used the work of French sociologist and philosopher Pierre Bourdieu. His work takes time and study to understand and apply his concepts and ideas. However, his work is very useful in understanding human behaviour and explaining the roles and positions of people in any social setting. Two concepts he worked with are important in understanding roles and positions in any field: power, how much a person has and how they can obtain it, and capital, which can be money, roles, position in society or material acquisition that supports power and privilege, often determining one’s place in a hierarchy in any part of society.

Although his philosophical explanations of power and capital take much reading to understand how they operate, power is a fundamental dynamic of society. We all compete at some area of life so we can enjoy power, which gives us a privilege and opportunity over others. Bourdieu claimed that life was like a football game where people entered an arena and competed for something to advance their knowledge, their social position and, importantly, maintain their position they had fought for.

Hackers do this because they know newbies, law enforcement and other experienced hackers want this knowledge for their own gain. That knowledge is power but collecting and acquiring it is called capital, because the acquisition of any form of capital gives further advantages over others. His concepts suited the study to explain the field (setting) of the hacker forum and why through the language used in the posts hackers kept trying to make sure newbie hackers remained ethical who understood if they wanted the capital, that is the knowledge of technical ways of hacking, they had to respect the experienced hackers’ position as forum experts as they were the holders of the capital that was wanted by newbies.

Chovanec (2018) states Bourdieu’s concerns over his academic life to describe how power operated in French and Algerian society, but was applied to many disciplines and areas of life. This quote tries to simplify why Bourdieu’s work is used by scholars to understand how power and acquisition of capital to gain power and privilege over others is useful despite its complexity to master:
Bourdieu’s work was primarily concerned with the dynamics of power in society, and especially the diverse and subtle ways in which power is transferred and social order maintained within and across generations. In conscious opposition to the idealist tradition of much of Western philosophy, his work often emphasized the corporeal nature of social life and stressed the role of practice and embodiment in social dynamics.

Practice, in the hacker context, does not only mean the act of hacking, but the social and cultural ideas that inform behaviours around it. So the power dynamic in the hacker forum is that the newbies want what the experienced hackers have in terms of how to hack, but if the newbies do not follow the forum’s rules, and refrain from challenging experienced hackers on the forum, they are denied such knowledge. This may not always offend or hurt a newbie, but it does slow them down in gaining the needed knowledge to hack and they can become resentful towards the experienced hackers.

Although Bourdieu did not invent the term capital, the ideas he had of cultural, symbolic and social capital, and how he applied them to his studies, demonstrated how objects, knowledge, social or economic position in society, education, prestige or location all contribute to how one advances their life. Yet this is not straightforward or guaranteed. For example, if someone who was poor wins a major lottery that does not grant them entry into a particular rich society, demonstrated richly in the F. Scott Fitzgerald’s (1925) novel, *The Great Gatsby*, where Gatsby’s wealth did not grant him membership to the more powerful established wealthy people he lived near. Rules determine one’s position in a part of society. In this study’s case, newbies faced a situation where although there are many resources to learn hacking, they needed to turn to other hackers for advice. But often they had to learn to follow certain rules for interacting in those hackers’ circles to obtain the capital they needed, which was the knowledge and advice to hack.

The paper is now presented with a conclusion and summary section at the end of it.
The New Computer Hacker’s Quest for Skills and Knowledge: Contesting Experienced Hackers in Online Hacker Forums

Abstract

As computer system hacking crimes grow in sophistication and reach, there is a need for supportive research on the activities and motivations of new hackers, also called newbies. The hacker community forum is one place that offers such insights. This study examines a sample of 500 threads from a public online hacker forum. It is guided by Pierre Bourdieu’s Field Theory’s elements of identifying field, habitus, social capital and cultural capital, to demonstrate how newbies attempt to gain a place in the hacking field amongst experienced hackers. Using thematic analysis methods, the results explained how the forum field works, the dispositions of those in the field and four themes, one for cultural capital and three for social capital. The significant finding was the theme of contesting social capital which showed the types of strategies employed by experienced hackers to prevent or hinder newbies obtaining the skills and knowledge, the social capital, to advance in the forum and gain skills to hack systems. It suggests that hackers do follow an ethical code to protect their community and insist that newbies must do likewise. The study concludes with suggestions for practice for although security agencies do monitor hacker forums, a sociological and behavioural perspective contributes to understanding motivations of newbies, what they seek, and how they will attempt to become hackers.

Keywords: Bourdieu; Contestation; Field; Habitus; Hacker Forums; New Hackers (Newbies); Social and Cultural Capital;

Introduction

The considerable body of literature seeking to understand computer hackers’ motivations and behaviours still needs further inquiry as hacking cybercrime grows in sophistication and geographic reach (Décary-Hétu & Dupont, 2013; Nikitina, 2012; Turgeman-Goldschmidt, 2008; Yar, 2005; Taylor, 1999; Jordan & Taylor, 1998). Needing further investigation is the area of new computer hackers or newbies. This study specifically examines newbie hackers’ acquisitions of skills and knowledge in their interactions with experienced hackers in a public hacker forum. The framework this study uses is Field Theory by Pierre Bourdieu (Bourdieu, 1990; Bourdieu, 1985; Bourdieu, 1977) with an emphasis on hackers’ skills and knowledge trading, the cultural and social capital of the field (Bourdieu, 1986; Bourdieu, 1984) between newbies and experienced hackers.

Although social media sites such as Facebook and Twitter are used by hackers, online community forums are still utilised as spaces hackers gather online (Kubitschko, 2015). Newbies join to gain access to highly specialised skills, information-sharing, networking and support from experienced hackers (Turgeman-Goldschmidt, 2008; Meyer & Thomas, 1990) but may experience admonishment, mocking and insults for their lack of skills and types of questions they ask (Décary-Hétu & Dupont, 2013; Meyer & Thomas, 1990). Hence the field of the forum operates on power relations; that is, in Bourdieu’s terms (1990), the capital of skills and knowledge is contested by newbies because they want what the experienced hacker possesses. This exploratory study focuses specifically on this aspect. Research on newbies
has not adequately focused on describing and analysing the relationships between newbies and experienced hackers in online community hacker forums.

The investigation of hacker forums to discover their characteristics and activities for cyber security has occurred. For example, Imperva, a global computer network security company, conducted a qualitative content analysis of threads within a large hacker forum. Their report identified descriptive trends, such as increased Structured Query Language (SQL) injections discussions to cause Denial of Service (DoS) attacks to a noted increase in newbies joining the forums from previous years’ analyses (Imperva, 2012). Although using a considerably larger sample size than this study, 250,000 members’ threads were examined (Imperva, 2012), it is clear that hacker forums require further analysis to give computer network security professionals insights into hacker behaviours and identify trends in hacker culture.

Newbie hackers desire to be a part of a hacking community even if their individual goals differ. Hackers’ desire, as Nissenbaum (2004) describes, total and free access to computers and information, and mistrust centralised authority, have a disdain for obstacles erected against free access to computing and desire to be evaluated by their technical virtuosity and accomplishment. Hackers hack for reasons such as: conflicts with authorities and revenge motives (Chiesa, Ducci & Ciappi, 2009), beliefs that breaking into computer systems benefit society by showing how to increase computer security (Kao, Huang & Wang, 2009), achieving feelings of power due to low self-esteem (Föttinger & Ziegler, 2004), gaining entrance to a social group (Kilger, Stutzman & Arkin, 2004), and to satisfy an addition (Taylor, 1999). These also play a part in a desire newbies have to join a hacker community and work with experienced hackers to learn skills and knowledge to hack computer systems.

Yet newbie hackers face a constant battle to be accepted by hackers from the beginning of their quests to obtain the capital they need to hack. For example, experienced hackers resent script kiddies and unskilled hackers who use hacking tools such as code and scripts developed by experienced hackers. In a display of power by experienced hackers, script kiddies are identified, shamed and called pestilence and other terms, and banned from hacker communities (Taylor, Fritsch, Liederback & Holt, 2011). Hacker ethics, rules hackers in the particular community abide by, vary, and experienced hackers will often want proof from the new hacker, such as completing a fake or real hacking mission, before joining. Newbies may resent such activities to enter the field, but will contest the knowledge and skills of the experienced hacker by posting threats, abuse, and pleas or try to outsmart hackers with superior displays of knowledge.

The research problem explores the relationships between the newbie hacker and experienced hackers in one public hacker community forum. There is, in Bourdieu’s (1986) terms, a contestation over capital because newbies struggle to gain acceptance and obtain the hacking knowledge and skills to be a part of a hacker community. They also experience ridicule, shame and abuse if they violate not only the formal rules of a hacker forum but also the beliefs and ethics of the group. This study uses hacker forum threads as data like Décary-Hétu & Dupont’s (2013) study. Other studies, such as Bachmann’s (2010) survey of hackers at a conference, and Shachaf and Hara’s (2010) and Turgeman-Goldschmidt’s (2008) interviews of hackers’ motivations and behaviours were effective in gaining insights into hackers’ worlds. Using textual data only can be just as valuable despite some concerns that will be addressed in the methods section.
This study is guided by three research questions which aim to describe and analyse newbies and experienced hackers interactions as the newbie tries to obtain knowledge and skills, the capital of the hacker forum. These questions are:

1. What are the types of capital, skills and knowledge, newbies seek and how do they seek them?

2. How do newbies challenge the established order of the hacker community forum and what strategies do experienced hackers employ to maintain power and control over newbies?

3. What insights can be drawn from these forum interactions on the relationships between new and experienced hackers?

The study’s framework is based on Bourdieu’s Field Theory, the elements of which are now discussed.

**Framework: Bourdieu’s Four Elements of Field Theory**

Four of Bourdieu’s concepts create a framework to investigate this research problem. These are: field and habitus, which allow a rich description to be made of what the group is doing in the field, and social and cultural capital which are types of resource gained on attaining group membership (social) and forms of knowledge and skill that allows a person a greater financial or social status in a group (cultural) (Bourdieu, 1990, 1986, 1984; Bourdieu, 1977). Central to this research is how power operates; that is, the power experienced hackers have to control what newbies need to do to obtain capital, but also how newbies will challenge the established order to attempt to obtain capital.

**Field**

Bourdieu explains a field as a system where social positions exist structured internally by hierarchical power relationships (Bourdieu, 1990, 1984) much like a football game field. It is a space where struggles over the appropriation and acquisition of capital occur. In the context of the hacker forum, the posts on the forum threads are the space where the hackers communicate, but these also exert power relationships over newbies by the words posted in the thread. First, newbies want knowledge and skills to hack, obtaining social capital, but struggle because they may not receive the answer they want. Second, they also want to be accepted and be taken seriously, which also a struggle because they may be dismissed by experienced hackers and not allowed to advance in the hacker field.

The comparison between newbies and hackers is described as a power relation because one group has control over the actions of another, much like Bourdieu says exists in the legal system where judges have control over the actions of lawyers (Bourdieu, 1984). Newbies can advance in the hacker community field, which is symbolised by the removal of the word newbie off their post and replaced with hacker, by the completion of hacker missions and contributing more than two posts to a thread. This advances their position in the field as it means they can access more features in the forum such as the ability to become administrators and remove or warn newbies if the newbie acts inappropriately.
Habitus

While field describes the space activities are occurring, habitus describes the individual’s values and expectations aligned with the social group they are a part of (Bourdieu, 1990, 1984). Bourdieu’s critics clarify habitus as the habits and dispositions, ways of acting in certain ways that always occur (Hanks, 2005). Describing habitus accounts for the reproduction of social and cultural domination because people must act in a certain way to be a part of a group and demonstrate this to others (Mander, 1987). Habitus is a product of the environment people operate in often determined by pre-existing values those in the field have. It is contested when people want change or when a group changes their habits or values as society or their circumstances around them changes.

Habitus describes particularly well how the values, habits and dispositions of one group, the hackers, impact on another, newbies. Habitus insists people in a group think and act in certain ways or they cannot gain the capital they desire (Bourdieu, 1986, 1984). Giving capital to others is influenced by the group’s habitus. For example, experienced hackers want newbies to act in ways that do not waste their time, which is an established habit to deride newbies if they do, and newbies have difficulties working out what these are. If the newbie does not align themselves with the group’s habitus the result is they will not obtain the capital they need to hack.

Social and Cultural Capital

Capital is the skills and knowledge embedded in the group members’ field possessed by everyone but at different levels, which determines their position in a field. Using Bourdieu’s (1986) formal definitions for this study, the two types of capital defined are:

1. Cultural Capital: The forms of knowledge, skills, education, and advantages that an individual has, which give them a higher status in a society or field

2. Social Capital: The resources available to an individual on the basis of honour, prestige or recognition, and serves as value that one holds within a culture

In this study the cultural and social capital are the skills and knowledge of hacking systems, combined with information about the formal learning needed to hack and the attitudes and values of the larger hacking community. To obtain capital, as Bourdieu (1986) argues, depends on skill and performance in the field. However, newbies may not be satisfied with these demands and contest the field.

It is this contestation over capital which is important to describe and analyse. The struggles newbies have will depend on their willingness to conform, but if they do not receive the capital they need they can argue with other hackers in the threads. Sometimes a contestation over capital means the field will change when those in it see the unfairness of their decisions. Nevertheless, withholding capital can also have some positive effects, such as newbies can give up their aspirations to hack and potential cyber crimes can be avoided as they are discouraged by hackers.
Method

The section describes and discusses the methods used to investigate the hacker forum and Bourdieu’s concepts, using the rigorous and most appropriate method, Thematic Analysis (Braun & Clarke, 2006). This method aims to understand current practices of individuals, allowing the detection and identification of factors that influence issues generated by those in the field or group (Alhojailan, 2012). It identifies, analyses and reports patterns or themes within a data set in detail but also helps interpret various dimensions of the research problem (Braun & Clarke, 2006).

First, a public hacker forum was identified which was representative of a field where newbies seek capital. For anonymity, the site is not named in this paper to protect informants. However, the posts can be viewed by the public but as an added consideration in the data examples the user names are left out. The data are reliable because members have to join the forum to post. Five hundred posts were chosen at random from the forum with the main criteria that a newbie posted in the threads. Once collected the data were organised and analysed with qualitative software.

Second, the method chosen, thematic analysis, is appropriate because it involves searching across a set of data to find repeated patterns of meaning (Braun & Clarke, 2006). Two advantages are: it suits finding evidence of the operation of Bourdieu’s framework, field, habitus, social and cultural capital, but also opens the possibility of finding other unexpected themes that answer the research questions.

Undertaking thematic analysis involves a number of steps. Thinking about concepts being sought, guided by the questions and framework, categories of each concept are created using a deductive approach in finding them. The data are then coded to the concept, with the creation of categories and subcategories that clarify and explain the concept. Importantly, and what contributes to the rigor of the study, is pattern finding and constantly going over categories to compare and contrast data to demonstrate with evidence what is occurring (Braun & Clarke, 2006). The iterative process is time-consuming, but by not rushing it allows assumptions about category and data examples to be clearly explained and justified. The categories and then summarised and titled with a named category and a number of elements identified that describe the theme.

Ethical considerations of using data from a public online community site for this study need clarification. Kollock (1999) warned that digital artefacts researchers use can subject the informants to surveillance. With more sophisticated tracking and data mining software available, Skågeby (2015) cautions that forum search engines are now sophisticated to the point they can pick up exact text of informants.

The study is still considered low-risk, but precautions were used to preserve as much anonymity as possible. Using advice from Markham and Buchanan (2012) of the Association of Internet Researchers, Madge (2007) and Bruckman, (2002), these strategies where used to minimise informant risk:

1. The site is officially and publically achieved
2. No password is required for accessing it nor joining the site as a member should occur
3. No site policy prohibits using data for research purposes
4. The topic is not highly sensitive
In the results section although the text is reproduced leaving out usernames assisted with protection of posters. It is also argued that the data are public but the risk of those seeking those who posted for criminal prosecution is likely non-existent.

Results

The findings suggest that Bourdieu’s contestation over capital is explicitly shown in the interactions between experienced and newbie hackers in the field of the hacker community forum. An overall description of the major theme is that experienced hackers will use their cultural and social capital they possess to either advance or suppress the advancement of the newbie. As Bourdieu (1990, 1986, 1985) argues, having a form of power over what others want means those entering the field have to negotiate it by adhering to established rules. This power held by the experienced hackers was identified as the requirements newbies must achieve before improving their position in the hacker forum field.

This observation was evidenced in four themes, one from cultural capital, the experienced hacker’s forms of knowledge and skills giving them a higher status in the community (Bourdieu, 1990, 1985), and three themes from the social capital concept which are the resources that newbies can obtain based on group membership participation and co-operation. The types of capital, skills and knowledge newbies seek and how they are sought is answered by both the interchange of hacker advice, technical advice and experiential advice, through interactions within threads.

The second research question was answered by the fourth theme showing the level of contestation over capital. Newbies challenged the established order of the hacker community by asking questions which caused the experienced hackers to use their positions to stop these behaviours. For example, even with the explicit rules in place for using the community, newbies do make requests for hacking techniques and procedures which should advance their position to go and hack but are disallowed. What was unexpected was the level of protectionism of the forum with consistent admonishment if illegal activities were mentioned by newbies. Hacking, despite years of claims from hackers to the contrary, is still seen as a ‘criminal act’ to be feared, a form of social deviance and a threat to world information systems security (Dremliuga, 2014; Kirwan & Power, 2013; Taylor et al., 2011; Kshetri, 2010; Warren & Leitch, 2009; Flowers, 2008; Mitnick, 2002).

The results showed that the experienced hackers will advise newbies how to hack, including posting programming code and Structured Query Language (SQL) database hacking codes, yet in turn will use the power they have gained to censor and admonish newbies who ask for such knowledge. This group protect their interests in the field and will prevent illegal activities being discussed. Yet newbies do get confused about how to act is evident despite the rules of behaviour and participation clearly posted on the forum’s site. The site displays the warning “The Site Does Not Support Legal Activities” but is clearly ignored in the sample of threads. In the field the identified struggle, as Bourdieu uses that word, is the contradiction that newbies must learn the habitus of the community yet often choose not to do so hence limiting their acquisition of capital.

The four themes identified from the analysis and their components are presented in Table 1. Cultural Capital only occupies one significant them, while themes two to four are findings about Social Capital:
Table 1 Capital Type, Theme Names and Theme Elements

<table>
<thead>
<tr>
<th>Capital Type</th>
<th>Theme Name</th>
<th>Theme Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cultural</td>
<td>Impart Skills and Knowledge</td>
<td>▪ Give advice and knowledge to maintain skills</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Possess specific skills sought after</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Use skills to advance position in field</td>
</tr>
<tr>
<td>Social</td>
<td>Advice Seeking</td>
<td>▪ Newbie freely given needed information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Newbie seeking specific information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Newbie wants learning advice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Newbie wants starting point for hacking</td>
</tr>
<tr>
<td>Social</td>
<td>Advice Giving</td>
<td>▪ Give needed information freely</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Impart experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Solve a problem for another</td>
</tr>
<tr>
<td>Social</td>
<td>Contesting Social Capital</td>
<td>▪ Admonish, insult and humiliate newbies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Experienced hackers criticisms of newbies’ behaviours</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Newbies’ criticisms of community rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Warning newbies of illegalities and punish them</td>
</tr>
</tbody>
</table>

These results are now discussed in-depth. The third research question about the insights drawn from the study is discussed in the results section.

**Theme 1: Impart Skills and Knowledge**
The theme describes the types of cultural capital held by the experienced hackers that demonstrates how they maintain the position in the field they occupy. Their acquisition of hacking skills and knowledge is sort after by newbies and is exercised in the willingness of the hacker to impart this capital by posting it in the threads. In giving advice it is bestowing information and knowledge, therefore capital, onto others to advance their position while maintaining their own skills in the field. This example demonstrates an advice interchange:

**HACKER:** As mentioned above python is a great language to start learning. If you choose to learn it I would recommend lawofcode.com and for books 1. Learn Python the Hard Way by Zed Shaw 2. Violent Python (and/or) Gray Hat Python. In that order btw.

Maybe something in the following order  
1. Codecademy  
2. Learn Python the Hard Way  
3. Read - Violent Python (Hacking with Python ebook)

**NEWBIE:** You really helped me out :) Thank you!

By recommending resources to the newbie, the hacker shows those in the community they know the exact resources that can advance another hacker. This is interpreted in Bourdieu’s (1985) theoretical terms as the distribution of capital as an instrument for the appropriation of the product of labour which is defining the state of the power relations occurring in the field and the position of the person in the field. This simple information interchange does potentially change the position of the newbie who may take the advice and use it. This type of attempt at advancement in the field was seen throughout the data and demonstrates how it was consistently operating.

When cross-checking the data that makes up the themes, a subtle overlap was seen between cultural and social capital when an element of this theme was identified. The majority of newbies wanted specific skills and advice. Hackers would provide complex and detailed posts on how to hack. In this example an experienced hacker gives information on the correct code to hack a file:

**HACKER:** A local file inclusion means that it is possible to load some local file (a file on the machine) in some given path or input, allowing the hacker to read the contents of the file.  
An example of expected input using a $_GET parameter  

Code: Select all  
https://www.yoursite.com/members.php?member=pythonhacker

Malicious code:  

Code: Select all  
https://www.yoursite.com/members.php?member=../../../../../../etc/passwd%00

The experienced hackers also used such information to advance in the field by completing more complex hacking missions set by the community and interacting with experienced
hackers to give their experiences of the hacking mission. A posting which shows this is a hacker developing code for others to use:

```
import httplib2
#h = httplib2.Http('.tmp')
response, content = h.request('http://checkip.dyndns.org')
print((str(content).split(':
')[-1]).split('<')[0])
```

Any C++ compiler should be able to compile C code just fine

The conclusion of this theme is that the cultural capital that the hackers post in the community can earn them a higher and more credible status amongst others. They are genuine postings to help others hack, but do function as capital growing that earns respect from other hackers in the community.

**Theme 2: Advice Seeking**

The giving and receiving of advice on how to hack, and on hacker philosophies and rules, underpins the growth or loss of social capital in this community. The habitus of experienced hackers is to help others, but only under certain defined assumptions brought to the community. Hackers, regardless of their status of being called white (good), black (bad) or grey (elements of both) do foster an informal but powerful collective worldwide community by frequent swapping of capital online and through hacker conferences or publications of experiences in books and other written means (Holt, Strumsky, Smirnova & Kilger, 2012, Chiesa et al, 2009; Schell & Dodge, 2002; Jordan & Taylor, 1998). The type of social capital sort are hacking skills and knowledge, but in order to obtain it the advice must be worded correctly within the boundaries of the hacker community or it is withheld.

Four elements of advice seeking were identified. First, the newbie is given the information freely without the expectation of even a thank you to the hackers, although many did thank those who gave the advice. Here a hacker freely gives information on how to fix an operating system issue:

```
HACKER: This isn't something that should happen on a normally functioning system. In your first post, you said you had recently installed windows7. If it was me, considering how frequently i use the browser and how suspicious this is, and since i have the installation cd, I'd do a fresh install again. That's all I've got. Good luck bro
```

Further examining this theme, the continuous advice seeking was seeking specific information, for example how to remain anonymous online, SQL code for hacking databases or what hacking tools could be obtained to hack systems. Newbies consistently sought specifically how to remain untracked by authorities and others by using a proxy server, which can connect their computer to other indirect network connections to other networks services.
to hack. This example of specific information seeking generated much advice and was a
frequent request newbies made in the community seeking hacking knowledge:

NEWBIE: I thought this might be the best place to ask this. What’s the best way
to hide yourself online so that people who might be looking for you can't track
you when you’re doing "stuff"? ok I guess I don't care if they know I'm online... I
just don't want them to be able to track me.

Some questions suggested the newbie knew certain information already, as shown in this
example where a more specific question about anonymity was asked:

NEWBIE: If i spoof my MAC address and use an unencrypted and public
network access point, is there any way to connect me to my actions?

Nevertheless, all advice seeking posted was responded to and no newbie was criticised for
asking about topics, although the way they asked questions caused friction as will be seen in
theme four.

Aside from skills, newbies sought general advice about learning to hack, as in what
programming languages and hacking techniques were needed, and what was a starting point
to hack. This was seen as important social capital for those how joined the community to
begin hacking. In this representative example, the newbie asks what is valuable to learn to
continue hacking:

NEWBIE: I don't know if I'm in the right path on becoming a hacker. I'm a 3rd
year college student and the language I only know is Java. I know a little about
HTML, CSS and JavaScript because we have a web development class in our
college. Will I continue learning Java? Because almost all the posts I've seen here
suggests learning C or C++.

By contrast, many newbies may have known of hacking tools and programming languages,
but still needed a starting point. In this example, which experienced hackers would often
respond kindly to, the newbies would ask similar type questions on how to start hacking:

NEWBIE: Hi guys, I'm new here and recently I've been wanting to learn network
security and pen testing. In the past I’ve worked a bit with some basics of SQL
Injections and some metasploit but that’s about as far as my experience goes. As
for programming, my knowledge is close to non-existent. So my question is,
where do I go from here?

Overall, this theme captures the type of capital that is sought by newbies to advance their
positions as hackers in the community and outside of it. The next theme that arose
demonstrates how the hackers advance a newbie’s acquisition of capital by giving advice.

Theme 3: Advice Giving

This theme demonstrated that experienced hackers in the community would give detailed
advice freely on how to solve problems and warn of the pitfalls and challenges a newbie can
experience hacking. They also imparted their experiences of hacking, not just practical skills
to hack, but also the experiences and philosophies they had hacking. The information to hack
was given freely, yet the hacker would warn the newbie if the activity was illegal. In terms of social capital, advice given is valuable to newbies and is crucial to their advancement in the field. Two examples of freely given information were:

1. HACKER: This is a very neat tool a friend introduced me to. Depending on what 'nix OS you're rocking, it may have a different name. You may just have to Google it to find which one goes with your OS. But anyway, this tool sets a terminal to drop down at the press of a button, then wrap itself up and get out of your way when you press it again.

2. HACKER: What specifications are you looking for? Just for a run of the mill website with nothing fancy, check out http://www.freewebs.com

Hackers would also give advice to newbies based on their experiences of being a hacker and the field they occupy. The data also suggest this is the way hackers impart their habitus to the newbie expecting it to be respected, reinforcing the boundaries of the field (Bourdieu, 1986, 1985, 1977). These examples illustrate this:

1. HACKER: Hacking is like a tool it can be used all kinds of ways. In some cases yes it can destroy privacy, for instance the NSA using a JavaScript exploit to find people on tor. As far as learning to do this though what better way to protect your own privacy than to learn how to break it. Similarly the purpose of a learning a martial art is probably not to go around beating the crap outta peoples. It can be about exercise, self-defense, competition etc. In general this site also teaches the hacker mindset, thinking out site the box and finding clever solutions to problems, and provides a community of people with similar interests.

2. HACKER: Python is a great language to start with, it's not terribly difficult, resulting code is pretty easy to read, and it's powerful to boot! Where are you in the Codecademy course, and what exactly are you having issues with? My python is a tad rusty, but I don't mind giving you advice!

The first example imparts general knowledge about hacking activities whilst the second imparts experience with a programming language which the hacker is willing to share with the newbie. Both are social capital because they are imparting advice and knowledge the newbie can use practically to advance their position in the field.

A main element of this theme was the gaining of social capital through the solving of hacking problems. The first example shows a hacker advising a newbie about how online website forms can be hacked because the newbie had their website hacked through this method and wanted to know why it happened. The second example came from a newbie who was hacked and wanted to minimise the attacks that their system was experiencing:

1. HACKER: It may be that the search field, or any field in the forms that allow user input have not been properly sanitized to protect against JavaScript injection, i am speculating because the website is not in my native language and i can’t check it out. If this is the case then a visitor could even post a comment with html meta tags and redirect every one or any number of things with JavaScript...
2. HACKER: You can use a virtual machine and load the same protected image each time you use it, effectively starting with a clean slate. This offers some modicum of protection from tracking cookies, malware, etc.

The information needed is given freely with the choice for the newbie to act on it. This did not always mean the newbie returned to the forum to continue interacting, but the presence of hackers who gave advice freely, imparted their skill and philosophical advice and solved newbie problems, was highly valued. However, as seen in theme 4, this capital was contested. Whereas themes 1 to 2 suggested a highly co-operative field where capital was easy to obtain, which answered the first research question of what types of capital could be obtained and how newbies obtained it, newbies did challenge the field for resources which lead to hackers protecting it.

**Theme 4: Contesting Social Capital**

This theme demonstrates the operation of power over newbies when social capital is contested. In this sense, contestation means challenging the established order of a field to obtain capital. The practice the first three themes showed was the operation of habitus; the history of the community was to produce and reproduce collective practices which insist on what Bourdieu (1990) states is a correctness of practice. Up to this theme the newbies mostly co-operated by doing the practices the field demanded to advance from the newbie to hacker title. Clearly, some newbies either did not know how to ask in specific ways questions about hacking or were impatient, posting questions without reading the forum rules. When the hackers would not give them the advice or information they wanted, newbies would challenge the hackers, in turn the hackers used the collective habitus of producing strategic responses such as admonishment and other tactics to maintain power and control over the newbies.

Contestation is a struggle in the field for capital (Bourdieu, 1990) and operates in this hacker community by four elements. The first element is by using admonishment, insults and humiliation against newbies. One noticeable strategy employed as a warning to newbies was the yearly ‘Idiot of the Year’ prize voted by the hackers as the worst of the year:

HACKER: It's about time to continue tradition with our Idiot of the Year contest. Voting ends on December 31st or January 1st, depending on your timezone. With the seemingly decreasing activity in the forums, there have been a less amount of good idiot. So from the idiots that we do have, pick wisely!

The next two were frequent examples of admonishing newbies, using insults and humiliation, as tactics to reinforce the community’s habitus of newbies conforming to certain rules and losing capital if they did not comply:

1. HACKER: First of all.. Don't post in colors. It looks retarded.

2. HACKER: Ok you are new. You need guidance. Firstly we don't talk like that, and using colours and lots of emoticons. This is what you should have said:

   SAME HACKER: wrote:
I don't know what the hell I'm doing. I'm really good with computers but I've never seen this type of thing before. Could someone please help me? Please!

Ok that is much easier to understand, so please type like that in future.

Using abusive language and name-calling to admonish was frequent:

**HACKER:** My first impression was that you're an idiot, but it quickly came to light that you are in fact a moron.

The struggle for the newbies here was to make the choice to endure the abuse and apologise or not reply and go to other hacker forums. It still meant that they did not receive the capital they needed to advance their hacker knowledge.

As part of their habitus, hackers also would criticise newbies for the wording of the questions the newbies would post. If the post asked for advice deemed illegal the hackers would warn, admonish and sometimes ban newbies. This was strongly tied to the constant need to enforce the image of the hacker community as being ‘legitimate’ and not encouraging criminal behaviours. If the newbie criticised the rules they would be admonished. These four examples show the operation of power in the field as newbies are criticised for their posts:

1. **NEWBIE:** well tbh thought this was a hacker community, but you can’t ask for specific downloads or help, even the admins refuse to give some good information, you call yourself hackers but I’m sure only 0.5% of these people is worthy to be called one, I’ll be leaving this site to join a real community where people help each other instead of being scared to something wrong. hail black hackers and hail my old community where you had special room to insert sites / people that needed to be dealt with

2. **HACKER:** The fact that I haven't seen it, doesn't mean it doesn't happen (though I doubt that). Either way, no-one will help you do something illegal here. At best a mod will come along to lock this thread and move it to the graveyard, at worst you will be banned from the site too. We'll see what happens...

3. **HACKER:** I am a professional hacker. Let’s not talk about "illegal activities" on a "hacking form" pm me

   I don't understand why this even has to be explained. It should be common sense.

   These are the type of people who deserve to be caught or scammed.

4. **HACKER:** On a hacker's forum, you really shouldn't really say that. Should the party van catch someone who's part of this community, we won't look like saints either, you know?

Notice the disclaimer at the bottom of this page: (community name) does NOT condone or support illegal activities. Seeing as you have so much time on your hands, you should be able to figure it out yourself if it's really that pressing of an issue. While you sound benign, you could be attempting to bring down the
network/wreak general havoc, etc. Sorry, but seeing as this is likely to be illegal, we can't really help you.

This contestation raises some questions as to why newbies choose to challenge the field. As it is working from text, the reasons may not be clear but in reading the posts the suggestion is that newbies just did not read the taken-for-granted community rules. It also calls into account newbies’ motives. Some of the newbies’ requests fall into the category of acts of force or fraud undertaken in pursuit of self-interest, or criminality, as defined by Gottfredson and Hirsch (1990). Even with explicit rules for behaviours, some may view even this public community as a source of black hat activity. However, although there is conflicting information; that is, the hackers do tell people specific hacker methods, this contestation of the hackers protecting the community show they create a community of practice that is creating ethical frameworks to guide field activities (Pike, 2013).

New and established hackers believe they may gain respect and recognition from hacker peers (Young, Zhang & Prybutok, 2007). Yet obtaining this capital is often a struggle for the newbie if they do not follow or know the established rules of the field. It can be a counter-argument that many do not take the time to study the rules of a field and eagerly rush in. This can be assumed in reading the posts. However, what is evident from the results of this theme is that contestation is a powerful struggle. The community welcomed newbies but did not hesitant to give out punishments, including banning newbies. Bourdieu (1977, p. 40) illustrates the operation of a contestation over capital in a field that supports these findings:

To possess the capital of authority necessary to impose a definition of the situation, especially in the moments of crisis when the collective judgment falters, is to be able to mobilize the group by so lemmizing, officializing, and thus universalizing a private incident (e.g. by presenting an insult to a particular woman as an affront to the huma of the whole group). It is also to be able to demobilize it, by disowning the person directly concerned, who, failing to identify his particular interest with the "general interest", is reduced to the status of a mere individual, condemned to appear unreasonable in seeking to impose his private reason - idioites in Greek and amahbul in Kabyle.

Therefore, applying this to the forth theme, the moment of crisis is when the newbie requests illegal information or challenges the community; therefore, disowning the newbie is the response. Not obtaining social capital may not concern the newbie, but it is seen that the newbie is unreasonable and imposing their reason onto the community. As example 1 in this part of the analysis showed, newbies, and sometimes established hackers although only one instance was noticed, hit back at the community. It is important to get capital and to some newbies it is a devastating experience not to gain it and advance their own hacking cause in, or out of, the community.

Discussion, Conclusions and Future Research

The sophistication and frequency of cyber attacks must start from the mind of the newbie as they seek skills and knowledge, the capital of the hacker field to hack (Décar-Hétu & Dupont, 2013; Yar, 2005; Taylor, 1999; Meyer & Thomas, 1990). Using the sample set of threads, this study gave insights into newbie hacker behaviours in an online public hacker community. This section discusses findings and conclusions, as well as giving direction on
future research of newbie hackers, and answers the third question, what insights can be drawn from these forum interactions on the relationships between new and experienced hackers?

Using Bourdieu’s Field Theory concepts, an overall thematic picture of what occurs in one public online hacker community emerged. The field is the hacker forum itself where it is compulsory to contribute to advance. Hackers reproduce habitus which newbies must adhere to in order to gain capital. Habitus was seen as dispositions to reproduce practices which kept the community being seen as a white hacker, ethical place despite giving specific advice on how to hack. Newbies had to navigate this process and act accordingly.

The thematic analysis discovered themes of the gaining and contestation of capital hackers and newbies wanted. Bruan and Clarke (2006) argue, this method allowed a rich description of the data set, which this method achieved in the four themes. However, there was more evidence of the operation of social capital rather than cultural capital. The process operating was that hackers had power to give capital as their cultural capital, their knowledge to give was high. In the other themes it was the social process of asking, correctly, for social capital in an ‘ask and give’ advice process. If this failed, which it frequently did, Bourdieu’s contestation in the field concept was activated and often the newbie could not advance in the community or gain capital to hack. These results answered the research question.

What was not expected was the depth of conflict between the rules and ethos of the community site, seen in the habitus where hackers would admonish newbies and sometimes each other for perceived illegalities. Contempt for newbies who wanted things done for them without making effort occurred frequently. The skills and information given contained code, methods and techniques to hack a network, software or a device. Newbies did ask how to perform illegal hacking activities, consequently getting admonished and warned, yet the experienced hackers would tell each other specifically how to hack something. As Taylor et al. (2011) stated, experienced hackers will ban newbies and script kiddies who waste their time yet hackers still claim there is a form of community amongst hackers. A newbie may find such a community confusing and in the data they often begged for information but the hacker’s choice to answer depended on the specific way the newbie requested something. This can be difficult and perhaps even a deterrence for newbies to learn hacking.

The insights drawn from the forum interactions, the third research question, were that newbies must learn, as Bourdieu (1977) states, the ‘rules of the game’ in the field to advance their hacking activities and not challenge the others in the field. For example, although not frequent, some newbies expressed frustration that they were not being answered. Their complaints were often met with contempt though some hackers would be sympathetic and correct newbies’ behaviours. It is difficult to ascertain confidently if this hacker community was encouraging criminal activity because of the continued stating some activities were illegal. However, newbies if they worked out the rules of the community and learned to ask questions correctly could advance quickly which was evidenced by newbies being given a new title such as Experienced Hacker on the forum. This was the best symbol of the acquisition of capital.

A limitation of the study is the questioning of results as being speculative because the data are only textual. This is a legitimate concern because unlike interviews researchers cannot always check details with participants. Not knowing the full outcome of some interactions could have led to speculation of what was going on, influencing rigor. However, it is argued that the posts gave accurate representations of the interchange, or not, of capital acquisition,
sharing and contestation over both capitals. Researchers undertaking most textual discourse analysis work can subject themselves to the criticism that they put their own meanings on the text not capturing what is occurring from the participant’s point-of-view. Although valid, this study was aided in rigor by using a sociological framework and a strong qualitative research method, combined with good data reliability, to produce a thematic insight into the ways newbies operate when trying to gain entrance to a competitive field such as hacking. It is also fact that the greater the sample size, which would require more work to analyse, the more insights and frequency of occurring issues could be uncovered.

Future research would depend on the information security industry’s resolve to stop hackers. From a research view, perhaps a larger sample would give even more insights and show patterns a smaller study like this cannot. The study could be replicated with multiple coders who could bring more insights as this project could not do this. However, although concerning as researchers could be risking informant’s safety due to the illegality of hacking, the interview and observations of newbies and hackers would yield a rich data set of understandings. For example, in their study of Wikipedia trolls, Shachaf & Hara (2010) conducted the study strictly by email to protect informants while Kubitschko (2015) sought data with permission from a major European hacking community becoming involved with them by attending their meetings. The ethics of doing any hacker research may be of interest to authorities; therefore, careful study design must be strictly adhered to in order to protect the researcher, informants and the institution or company they are researchers for.

To conclude, this study has given insights of newbies who face a formidable process to be accepted into the hacker community and earn titles more in keeping with what they want to achieve. The contribution to cybercrime prevention is in understanding the specific ways newbies operate in such environments. As the reach and frequency of cyber-attacks grows, perhaps with catastrophic results, such research which seeks to understand behaviours and motivations can support the practical security measures that governments and security firms are trying desperately to implement and deter newbies from entering the world of hacking.
References


Conclusions and Summary

This chapter presented a study of new computer hackers who are part of an online virtual hacker community and the way they are treated by experienced hackers. It also clarified the use of sociologist Bourdieu’s work and explained why it is important to understanding forms of power that exist in the examined hacker forum. The study illustrated an insight into how hackers think and behave especially in virtual communities. Although some researchers may view such a study as not contributing to the key research priority of stopping hacking and cyberwarfare, I argue that understanding motives and culture through reading the language hackers use give insights into why they hack.

The next chapter discusses two other dimensions of hacking: gender and cinema.
Notes


3. Quote take from DillonTheHacker #i62 Twitter account.

4. The references that appear at the end of the study in this chapter are included in the Works Cited section of this book.
CHAPTER FIVE
Hacking and Gender, Hacking and Cinema Portrayals

A few years into my career, I still see myself as an oddball: I rock platinum blonde hair, write bad malware pick-up lines, secretly place unicorns throughout my error code to add some flair, and love graphic design just as much as coding. In the cybersecurity industry though, I fit right in. By becoming an expert in my field and exceeding expectations, I’ve pushed my peers to overlook my gender and solely respect my ability to do the work and get the job done. You see, behind the computer screen, your gender and superficial characteristics don’t matter. Hackers have no identity; they’re anonymous. It’s the work you produce that earns you respect among peers. – Amanda Rousseau, Malware Researcher

“The moment you connect, you lose control. This isn't about money. This isn't about politics. I can target anyone, anything, anywhere. No fingerprints, no trace, no mercy. – Character Gary Baker, Hacker, in Blackhat Movie

I am totally unappreciated in my time. You could run this whole park from this room with minimal staff for up to three days. You think that kind of automation is easy? Or cheap? You know anybody who can network eight Connection Machines and debug two million lines of code for what I bid for this job? Because if he can, I'd like to see him try. – Dennis Nedry, Hacker Film Character Jurassic Park 1993

Two areas needing a discussion in this book are women hackers and presentation of hackers in cinema. Both of these have taken time to become considered important social and cultural representations of the hacker world. In the case of gender, the long-held belief was that hacking was a considered male dominated only area. In the case of cinema, though television and books did discuss hackers, it became interesting to note that hacking was not just done by humans but also machines.

This chapter will discuss a selection of women hackers, their achievements and their place in hacking culture and history. The second part selects movies from 1968 to 2014 that portray hackers, either exaggerated in science fiction and other thrillers, to more serious attempts to show what hackers do.

I found it interesting when researching this section that there still exists beliefs that women, especially young women, do not hack. The male hacker culture has obviously dominated the publicity of hackers, but women have continued to learn hacking and moved towards the good and negative aspects of hacking attacks. Another experience I encountered was when I wrote a short story about a young female hacker (Nycyk, 2017) I received negative feedback that I could write about a female and younger person doing hacking. They would not do that it was said to me. Yet now female hackers start from a very early age, although again it needs to be emphasised not all are hacking for malicious purposes.
**Woman Hackers**

There were many reasons that women were not considered hackers for decades. Much research in the 1990’s found commonality of reasons. Computer-mediated communication (CMC) was dominated by males outnumbering women (Luckman, 1999), there has been a long and continued history of online harassment towards women (Hardaker, 2013; Jane, 2017) and denigration of woman’s achievements (Spender, 1995). Women and girls as hackers, either malicious or not, have increased. It is important to recognise that increasingly females do hack computer systems, they attend hacker conferences and have also become white hat security experts who have developed software to stop hacking.

Taylor (1999) argued that more males than females hacked because of a strong link between ICT’s and technology being a predominantly male preserve, which at the time Taylor argued was borne out by major hacking studies. Yet as discussed in Chapter Two, women played a large part in hacking type activities during the Second World War. Liz Mundy (2017) researched and wrote a book called *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. It tells of the lives of women recruited by the United States defence forces who lived and worked in Washington learning how to code-break enemy messages. Its significance is in telling these womens’ stories that, due to secrecy, were almost forgotten in hacking history.

The women who broke the codes leaned technical skills in hacking type techniques. Although the women were all from different places and backgrounds, their skills acquisition got them jobs previously not open to women in the 1940’s. In an excerpt from Chapter 8, Mundy writes an observation of the lives of the women code breakers (Book Browse, 2018):

> Annie Caracristi surprised everybody, most of all herself, with her cryptanalytic feats. Though she had been an English major in college, she possessed the mind of an engineer. It was fascinating for Wilma Berryman - the West Virginia schoolteacher who had been one of William Friedman’s early Munitions Building hires, now supervising a major unit at Arlington Hall - to see what Annie could do. Nothing the Japanese did could shake her off. Conversion squares, encipherment tables, cleverly cannibalized additive books - Annie was onto all their ruses. So gifted was she that Wilma made Ann the head of her research group. At Arlington Hall, to have a recently graduated female in charge of a key unit was not unusual. It was normal.

This except showed that despite opposition and dismissal from males the contribution of female code breakers who hacked enemy codes was proven to have existed. Their contributions are now recognised in hacker history. Exclusively female hacker groups now exist for white hat and hacktivism activities. An example is the group Women Who Hack.

Although not in the scope of this book, it is important to recognise that women still face issues when hacking or attending conferences where harassment and bullying still takes place. In 2017 Facebook Chief Security Office, Alex Stamos, reported that harassment of women still takes place even at Def Con and other hacker events (Brewster, 2017).
Ten Women Hackers

These examples of women hackers are diverse in their hacking activities, their location and their nationality. Some women hackers have taken up causes such as being crusaders for child pornography prevention or have forged ahead with computer security careers in male dominated areas. However, some have caused damage to computer networks or committed cybercrimes.

1. Carmin Karasic

In Chapter Two Carmin Karasic was mentioned as one of the founding members of the hacktivism group Electronic Disturbance Theatre. Leonie Tanczer (2015) interviewing Karasic asked about the motivations for her hacktivist activities:

Leonie: This is related to the actual Call for Papers which is called ‘Hacking the Black-White Binary’. I would therefore like to ask how you interpret this phrase, especially in regard to your own involvement in hacktivism and being part of the people of colour community?

Carmin: To me it describes a way of putting the spotlight onto a particular issue. But it goes back to what I was saying earlier, which is that I do not try to label what I am doing. So in some ways the title bothers me a little bit. I do not want to focus on a particular group, because then I have to ignore significant things that are happening elsewhere. I would rather see no labels, and we are recognised for the work that we do, rather than clustering people into different groups.

Karasic is an example of a hacker who is driven by the need to express a point-of-view for the good of a nation. She feels that her being a woman of colour is irrelevant. She has continued at the time of writing to be doing some of the same hacktivism, but also other activities.

2. Alisa Esage Shevchenko (Russian Spelling Алиса Шевченко)

Shevchenko is a hacker from Russia who had her own company called Zorsecurity and worked with companies as a cybersecurity researcher to find system issues and vulnerabilities to stop hackers. She also became known for becoming involved in a controversy with the United States Obama Administration. This was significant because she claimed she did not assist Russian intelligence services with technical research and development (Glance, 2017). She is prolific on Twitter, sharing ideas and views as this Tweet giving hacking advice and opinions as this illustrates (Alisa Esage Шевченко, 2018):

Personally, writing an exploit for VirtualBox was never a priority, as it’s rather trivial. More crucial is to discover new attack vectors, especially for a VM escape from *unprivileged guest with default settings and no Guest Additions installed*. Still zero public info on this.

As Barth (2017) states about this incident, regardless of why she is hacking, a female hacker obtaining such a level of attention and notoriety is still considered a fairly rare thing to occur.
3. Raven Adler

Adler was the first female to be a presenter at a Def Con conference. Her past included leaving school at an early age to attend college due to her academic giftedness. Generally, her work is in the security industry finding weaknesses in systems including security vendor software. In an interview she spoke of her frustration at security software problems (InfoSec News, 2004):

But it's not all smiles and sunshine in the security business for Adler - she once found a serious vulnerability in a “very popular security product”.

“I wrote up some proof of concept exploit code, and took it to my boss,” she explained. The makers of the product didn't really seem to care about the issue nor want to fix it.

“I carefully explained the importance of the problem, and the possible ramifications of exploiting it. People are trusting this product with their security data, and if the product itself is [insecure], it's un-trustable and you can't have faith in the veracity of that data,” she said. Still, the vendor was unmoved, claiming no one would ever find the glitch.

Alder was by this point annoyed. She had found the problem, so others could too. But the vendor simply refused to fix the problem.

This view from a hacker is unusual and concerning to read because she discloses that a security firm is not taking hacking seriously.

4. Kimberly Vanvaeck

Vanvaeck is a Belgian hacker nicknamed Gigabyte. It is difficult to accurately label her work as white, black or grey hacking. However, she created the first ever C# Virus (or worm) at 17 years of age called Sharpei. This worm was unusual, demonstrating the creativity hackers have to create new code to keep pace with new technologies. In this case it was the .NET Microsoft technology that was being hacked and the code replication (worm) was being written in that at that time new programming language. Yet it was considered a low risk virus (Leyden, 2002). The incident was described on the Soldierx (n.d.) website as:

She was 17 at that time when she released Sharpei, which is designed to infect computers loaded with the .Net framework. The worm appears in an e-mail with the subject line ‘Important: Windows update’ and the following message attached: “Hey, at work we are applying this update because it makes Windows over 50% faster and more secure. I thought I should forward it as you may like it.” If the attachment is opened, then the worm uses the Outlook address book to send messages--with a copy of the virus attached--to every address in the book. It then deletes the e-mails from the sent folder and removes the copy of itself.

She was arrested for making this worm but as she was underage in 2004 under Belgium law she was given bail and not jailed. Vanvaeck has also kept a reasonably high media profile online.
5. Xiao Tian

Tian is a Chinese hacker who founded the China Girl Security team while still a teenager. It expanded quickly. However, what has been reported is her team has been linked to many infamous hacker groups. Danchev (2008) profiled the group in 2008:

“In the male dominated world of Chinese hackers, females find it difficult to be accepted as equals. Their technical skills are often viewed as inferior to their male counterparts. As far as I am aware, the first group of female Chinese hackers to break this mold were the Six Golden Flowers. The Golden Flowers have since broken up and gone their separate ways, but a new and larger group has taken their place, the Cn (China) Girl Security Team. The website for the China Girl Security Team was registered on 12 Mar 2007 and currently has 2,217 members. The leader of the group Xiao Tian, is only 19 years old”.

Although there is much criticism of Tian’s hacking, it is unclear if she fits the grey or black hat hacker label.

6. Jude Milhon

Milhon was an American hacker and an author who was called St. Jude and became known as a cypherpunk, a person who valued online privacy as a way of enacting social change. They are well-known for advocating the use of cryptography and that privacy is not about keeping secrets but having boundaries with those who could control information, like governments (Hughes, 1993). Her encouragement of women to take up hacking was well-known. Before moving to San Francisco she participated in the American Civil Rights Movement including organising marches and civil disobedience events including one in Mississippi where she was arrested.

Of her quotes, her best known was when she gave a definition of hacking (Delio, 2003):

“…the clever circumvention of imposed limits, whether imposed by your government, your own skills or the laws of physics.”

She wrote many books to support women to become hackers. Her involvement in pioneering computer network creation, being an editor of technological magazines and worked for technology companies.

7. Natasha Grigori

Grigori used her skills to track down owners of sites that hosted online child pornography. The information would then be given over to law enforcement, mostly in the United States where she lived. She encouraged other hackers, especially women, to work with her to track down these sites and prosecute those that posted such material.

Her name is not real but is taken from an American cartoon show called The Adventures of Rocky and Bullwinkle and Friends where one villain was named Natasha Grigori. In a media report (Segan, n.d.) she stated about hacking:
“Because of our tech capabilities, we have been able to develop some tools to help ferret out child porn. Law enforcement was just overwhelmed with it. In four hours, this (software) can glean 2100 different URLs” worth investigating, Natasha said.

8. Ying Cracker

Cracker’s reputation is high among hackers because of the help she gives online and as an educator to hackers. There has been debate about her motives and her presentations; they are thought to be educational to prevent hacking, but some teach how to hack illegally. However, as Bui (2015) states, Cracker has created a mystique and sense of mystery about her:

Amassing a huge fan base on online message boards initially for her stunning looks, Ying Cracker has set out to convince the world that an Asian female hacker can dominate her field without sacrificing the pleasure of being a physically attractive female. Ying Cracker has multiple Facebook accounts with the same user name and ingénue-like modeling photos, all of which reveal nothing about her life other than her preference for promoting humanitarian causes and cute pictures.

9. Joanna Rutkowska

Rutkowska, from Poland, is considered an ethical hacker and is noted for the work that she did with the Windows Vista operating system. She founded the Invisible Things Lab and Qubes OS projects. Her skills in being able to find vulnerabilities have been documented and praised, with her also presenting at many conferences including Black Hat hacker ones.

10. Susan Atrach

Atrach, at the time a 21 year old woman from New Jersey in the United States, gained notoriety for her hacking of singer Selena Gomez’s email account. The extraction of personal data from Gomez’s emails attracted criticism from fans and the media. She was charged with 11 hacker felonies, including identity theft and fraud. At the time of writing the case had not been dealt with and it is unknown if she was jailed for the full nine years as the law states as punishment. Gomez had had naked photos of her stolen off email and cloud servers and posted online by other hackers.

Conclusion of Women Hackers’ Profiles Samples

These examples of women hackers represent the broad range of female expertise in hacking, but also illustrate the chosen good or bad paths, or both, they have taken. It is clear that women in the future will continue to perform many types of hacking as they grow in number and ignore the male-dominated ethos of hacking.
Computer Hackers’ Representations in Cinema

Hackers have been filmmakers’ subjects in drama, comedy, science fiction and other genres, with many movie, television and documentaries made about them. Many are filmed as negative or stereotypical geek portrayals. Some present nightmare or apocalyptic scenarios or are exaggerated in characters and plot. The hacker is also not always a human being but a computer system. These films effectively tap into audiences’ paranoia and anxiety (Adil, 2006) although the action-based Hollywood hacker films are usually made for entertainment purposes.

These films have also alerted the public to the possible scenarios and consequences of hacking. Some of these films have shown technologies and hacking that has become possible. Film critic Haridy (2016) is critical however of such portrayals as the majority of well-known films are made in Hollywood:

- For the past 30 years, Hollywood has consistently struggled to depict computer hacking in accurate and exciting ways. The history of Hollywood and hacking is littered with lazy writing, absurdly unrealistic computer interfaces and stereotypical “nerd” characters. But in amongst the idiocy we’ve also seen certain films influencing governmental policy, inspiring entire sub-cultural identities and guiding mainstream attitudes around computer security.

Haridy’s comments are accurate. What is on the screen can be exaggerated, and unrealistic in the portrayals of hacker for dramatic effect. Yet they are still entertaining and some can be thought-provoking in understanding the potential danger of hackers. Most films do characterise the hacker as a villain.

The follow list and description of 15 hacker films is not substantive or complete, but do illustrate the types of films about hacking that have been considered significant in terms of plot, character and differing portrayals of hackers and hacking. They are presented in chronological order with their relevance to hacking described but may contain film spoilers.

1. 2001: A Space Odyssey (1968)

This science fiction film was directed by Stanley Kubrick and was written by him and science fiction writer Arthur C. Clark. The plot is about a group of astronauts on a mission to Jupiter. The hacker in this movie is not a human, but the spaceship’s computer called HAL 9000, which stands for Heuristically Programmed ALgorithmic sentient computer. HAL controls the operations of the ship, displays humanlike qualities, is a form of Artificial Intelligence and interacts with the crew, especially the film’s main human character Dr David Bowman.

HAL is portrayed in the film as a hacker, in a scary, menacing and violent way, but has a mental breakdown as Bowman begins to dismantle him (Boylan, 1995) in a scene that evokes sympathy for HAL. The popular image of HAL from the film is seen in Figure 30:
Upon Bowman dismantling HAL’s circuits, HAL begins to express fear and tells Bowman not to continue as HAL is afraid, and with his last words of him singing *Daisy Bell*. HAL is considered a hacker because he can alter the functioning of computer systems the ship has, and has an agenda that hijacks the mission and causes the deliberate malfunction of some of the crews’ life support systems. In terms of cinema, people praised the film for showing primitive artificial intelligence technology and that such technologies may develop independent thought and action.

2. The Italian Job (1969 Original Movie)

A British comedy film about a robbery heist set in Turin Italy starring actor Michael Caine. The main hacker is played by comedian Benny Hill as Professor Peach who creates the magnetic tapes that cause the Turin car traffic system to malfunction, while a character named Birkinshaw jams the traffic closed circuit television system. Figure 31 shows the hackers manually breaking into the traffic control centre to swap the magnetic tapes for the hacked ones:
Figure 31. Hackers manually hack Turin Traffic Control system (Stack Exchange, 2015)

This hack causes mass traffic jams all over Turin, allowing the gang to use Mini Coopers to obtain gold without harming the guards and drive fast through Turin pursued by police. It is also a rare showing of hacking done by a manual way, not by entering data onto a keyboard.

3. World on a Wire (1973)

Director Rainer Werner Fassbinder made this film about a supercomputer that when a person put on a helmet it could show artificial worlds. This is now known as virtual reality. There is limited hacking in this film, but is mentioned because like HAL in 2001 the computer is able to start thinking for itself and hacking to alter the types of reality the people who participate in those world see. Like 2001 is considered ahead of its time and the hacking that both this film and 2001 show is now considered unlikely, but possible.

4. Demon Seed (1977)

A scientist creates an artificial intelligence called Proteus IV that almost immediately begins thinking for itself. The scientist’s wife, played by Julie Christie, had lost a child to a disease so Proteus starts working out how to eradicate what caused the child’s illness. Christie’s character, Susan, is separated from her husband, but he had designed the house so that the computerised and artificial intelligence systems could do chores such as closing the lights. When Proteus rebels against the husband and other scientists, it finds its way into Susan’s house and begins building a robot in the basement.

The hacking Proteus performs is disturbing, including sexual assaults on Susan, as well as accessing her brain to program it to love a child that Proteus has created inside her. It also murders a scientist friend of Susan’s and continues to shape a robot child figure in the basement. Susan tries to kill the robot but is prevented from doing so by her husband, while Proteus self-destructs. In the end of the film Susan’s late daughter is alive again but has Proteus as her voice suggesting Proteus is reborn as Susan’s daughter cured of the disease that the daughter had showing how all the hacking Proteus did led to the creation of a living human being.

Tron, produced by the Walt Disney Company, was ahead of its time in 1982 in terms of its visual animated effects and in creating a film based on a video game. The hacker in the film is Sam Flynn, played by Jeff Bridges, whose conflict with those in his father’s company causes him to enter an electronic only fantasy world. Although it is unclear if the word Internet was used in the movie, the leaking of information he does in a hack is placed onto what is a primitive Internet system. Flynn’s son is the main hacker character is the sequel Tron Legacy.

Miller (2011) describes the opening scene of Tron that immediately gives the audience a sense of a hacker ethic as Flynn performs hacking techniques to bypass access to the building and the computer servers:

This overwhelming feeling of nostalgia in a high-tech, computer movie would be noteworthy in and of itself, but it is particularly interesting when considered in conjunction with another main theme of the movie - the valorization of the hacker. In an opening scene, Sam rides his motorcycle to the headquarters of ENCOM, his father’s company, hacks into the security system to get into the building, and then sneaks up to a server room near the top of the building. At the same time, the ENCOM board of directors is meeting, preparing for the release of their latest computer operating system - which they themselves admit is just a repackaged version of the older system. Sam hacks into ENCOM’s network, disrupts the presentation in the board meeting, and releases the code for the operating system to the Internet at large. Pursued by a security guard, Sam then runs to the top of the building, climbs outside, and jumps off the building, using a parachute to glide to safety. The excitement, openness, and sense of play in Sam’s actions, and the corresponding uptight, greedy, and mean-spirited attitude of the ENCOM board, clearly position Sam’s actions as the right, moral choice.

Tron, and to an extent its sequel, are regarded as unique in showing the hacker versus a corporation (or in other films government) in a good and evil scenario. Although both films have been criticised for plot and acting, in terms of showing hacking and virtual worlds the films have been influences on later films, especially the film The Matrix and its sequels.


This film is considered by critics and audiences as influential in the hacking cinema genre. The reason for this, as Adil (2006) argues, is that in 1983 the Cold War between Russia and the United States was still occurring with the fear of a nuclear confrontation. D’Angelo (2016) comments on why the film is considered important in hacker history:

One of the abiding characteristics of the Cold War era was a general fear that it would eventually trigger World War III. A nuclear confrontation between the U.S. and the Soviet Union, which might potentially kill millions of civilians with little or no advance warning, seemed all too plausible, especially in the wake of the Cuban Missile Crisis; kids were routinely shown educational films instructing them on the proper steps to take (1. duck; 2. cover) should the bomb go off in their vicinity. By the early '80s, however, the nature of the paranoia had shifted. Decades had passed without incident, and it was fairly clear that cooler heads had
prevailed, on both sides - nobody was likely to intentionally launch a pre-emptive first strike. Home computers were just starting to become popular, though, which raised another frightening possibility: What if someone were to remotely access the country’s missile defense system? The word “hacker” wasn’t yet widely known back then, but the concept itself didn’t require much knowledge or imagination. Maybe it wouldn’t even be a malicious enemy agent who pushed the button via modem. Maybe it would just be a couple of bored teenagers with an expensive toy and a deficit of common sense.

The character of David Lightman, the Seattle-based teenager hacker played by Matthew Broderick, is portrayed as a ‘geek’ but also has a black hat hacker streak. In one scene he changes his girlfriend’s school grades after she tells him not to. Jackson (2018) points out that originally it was not about hackers, but that real-life hackers inspired the film and it was mostly easy to obtain how to hack systems material across online networks and Bulletin Boards without being arrested.

The film’s plot sees Lightman connected by a phone line through his home computer with the United States War Operation Plan Response (WOPR) which is controlled by a North American Aerospace Defense Command (NORAD) supercomputer. Thinking it is another player, Lightman engages with NORAD taking on the role of the Soviet Union in a game of Global Thermonuclear War. The computer also uses a voice to communicate with humans. In the movie, the coldness of the computer was claimed to be unnerving as illustrated in Figure 32 where even in the absence of the robotic voice, suggests a sinister side to the computer. The computer had been programmed with many nuclear scenarios to attack and defend the United States from nuclear missiles, but is still in some way thinking like a chess opponent and sees Longman as the enemy to defeat:

![Figure 32. NORAD challenge text on computer from War Games (Ion Music, 2014)](image)

Lightman is arrested after playing this game and along with his girlfriend and taken to NORAD where he finds out about WOPR refusing to stop the simulation of the war game against the Soviet Union. This is all a game but to the computer it is real, with Lightman returning to NORAD after initially escaping from it. The movie ends with a successful hack
into the computer convincing it that nuclear war is a futile act. War Games was important back in 1983, but even as a retro curiosity it has a lot to say about what hackers can do. Early films like War Games alerted the public to what is possible, but was back then unlikely to occur.

7. Sneakers (1992)

Sneakers is considered another influential hacking film as it gives an insight into how hackers think in terms of their motivations for hacking. The film, considered a comedy, has a large mostly Hollywood star cast, such as Robert Redford, Sidney Poitier and Dan Aykroyd. In Chapter Two Ian Murphy, named Captain Zap, was discussed, and his hacking was reported as an influence in the film’s plot.

The plot involves Redford’s character, a computer security specialist and original black hat hacker named Martin, being offered by the National Security Agency to have his past criminal record cleared in return for his hacking skills to obtain a black box. He assembles a team of hackers to help him promising rewards to them. As happens in many films things do not go to plan but Martin and his team are successful in obtaining the box and their rewards.

Various commentators have discussed the film’s merits as a film about hacking. Brew (2017) comments that the 1992 hacking techniques are still possible now adding to the view that the film has not dated even in this new sophisticated hacking environment. Another view is that the film predated how governments would use information technology on people, such as online surveillance, against people (Breeden II, 2012).


This film was directed by Steve Spielberg based on a novel by Michael Crichton about a theme park on an island which is populated by dinosaurs created by DNA. During a fierce tropical storm the power is cut and the dinosaurs being to take over the park including the vicious Raptors and Tyrannosaurus Rex.

The hacking in the film came from the lead computer programmer of the park’s operations, Dennis Nedry, played by Wayne Knight. After a bribe from a rival corporation to obtain dinosaur embryos, he deactivates the park’s security system, steals the embryos and drives escapes, only to become a victim of a dinosaur attack. Nedry not only hacks systems, but also made the system so protected emergency passwords did not initially work. In one scene, a child actor tries to decipher Nedry’s code to reactivate the security system, which eventually she does, and this message appears on the screen:

This film is the 17th James bond film about a villain using satellites called GoldenEye to steal money from the Bank of England. One character in the film is Boris Grishenko, a master hacker who is central to helping the main villain, Trevelyan, carry out the plan from a base in Siberia. In one scene he demonstrates to a colleague how he can hack into the U.S. Department of Defense using a spike, preventing his being tracked. His character is also notable for his bragging about this exploits with the catchphrase “I am invincible” which he yells out before being covered in liquid nitrogen and freezing at the film’s climax.


Starring Sandra Bullock, the film was criticised for acting and plot, but her portrayal as Angela Bennett a systems analyst has been labelled as realistic. The plot involves her becoming involved in a conspiracy where she unexpectedly finds a program that can manipulate databases. This allows any government or power to alter a person’s identity. After an incident in the Caribbean, Bennett finds herself with a new name and identity. The name she is given is a criminal who has an arrest warrant. The film has some good examples of hacking, but is overshadowed by a thriller plot. It does still show an example of the types of hacking, such as identity theft that is now possible.

11. 23 Nichts ist so wie es scheint (Nothing is What it Seems) (1998)

This is a German film based on the true story of hacker Karl Koch, who suicided. He was associated with the Chaos Computer Club, but was thought to have sold United States confidential information to the Komitet Gosudarstvennoy Bezopasnosti (KGB). The film’s accuracy has been disputed, as has his suicide. The documentary concentrates more on his life, but it also suggests he played some part in the Chemobyl nuclear disaster, which is not proven.

Despite heavy criticisms from film critics and hackers, Swordfish is still put on the list because it is about criminal hackers. The main character is Stanley Jobson, played by Hugh Jackman, who infected the FBI’s systems with a virus. A villain named Shear, played by John Travolta, asks him to invent a worm that will take money out of government accounts. The rest of the film is about Jobson’s involvement with Shear’s gang, but has some scenes where hacking is shown.


This film combines hacking with science fiction and like other mentioned movies suggests that hacking can come from machines that develop intelligences of their own. The film does show catastrophic consequences of hacking, such as poisoning of water systems and causing planes to crash. The hacking scenes are mostly fantasy, yet drew on the growing paranoia of larger hacks on infrastructure and transport.


This twenty-third James Bond film highlights computer hacking as a weapon with a cyber terror attack at M16 headquarters. The sequences of computer hacking are adequate to show the effects of such attacks, although they play a small part in the overall expected action sequences Bond films are known for.

The film received praise and criticisms for the depiction of hacking with some security experts and hackers claiming while some of the things in the film were possible, the scenes were exaggerated for the movie. Hsu (2012) states the gas explosion attack on M16 is this possible as occurred by hackers using the Stuxnet worm on Iran’s nuclear plants. Newitz (2012) agrees with Hsu, but the gas lines would have to be attached to Internet cables to allow the explosion to occur. Curran (2012) though criticises the film because unrealistic hacking scenarios that are unlikely, at the time of writing, to occur are depicted in the film.

15. Algorithm (2014)

This film is about a hacker who while breaking into government databases discovers a mysterious program capable of destruction. The portrayal of hacking, such as accessing user screens to type in passwords, is realistic. A key part of the plot is the tapping into paranoia of what governments may be doing to the population’s private data. Hackers can and do steal data, but the film suggests the government is an enemy of the people. The film has received mixed reactions from hackers and film critics, but some have praised the film saying it is a realistic portrayal of the conflict between hackers, governments and corporations in the battle for peoples’ data and private information.

Conclusions and Summary

This chapter discussed gender and cinematic side of computer hacking and hackers. Only sampling the vast array of woman hackers and films made about hackers, the chapter showed the richness and diversity of the field. First, women have advanced in the hacker field. They have been hacking for decades in the face of gender inequality, trolling and abuse of all
kinds. Yet they have continued to become visible, contributing to stopping hacking but also have participated in serious hacking crimes.

The second is the sample of films given that involved portrayals of hackers and hacking. These films have mixed results in success, some well-known and respected more than others. In choosing a sample of movies over several decades, they represented a diversity of hacking situations and stories. The exaggeration in these films for some form of cinematic effect cannot be discounted. Perhaps though machines being able to hack after developing some form of artificial intelligence might be possible. Cinema can tap into the fears and emotions of audiences; hackers and hacker stories may be unrealistic, but to show what is possible to hack will continue to interest filmmakers and audiences.
Notes

1 Amanda Rousseau female hacker commenting on being a hacker.

2 Quote from Blackhat movie, actor Spencer Garrett plays a hacker.

3 Played by Wayne Knight in 1993’s original Jurassic Park movie.

4 In this book I report only women as females, but it must be acknowledged due to the cultural morays of 2018 that one’s sex or gender as a hacker is irrelevant. How the person identifies themselves as male, female, intersex or whatever they wish is important. It is just for this book all identified hackers investigated were females.

5 For space considerations, and that this book is intended for a generalist and academic audience, it is only films that have had cinematic releases that are discussed. However, it is acknowledged there is television, documentary and online content that shows fictional and non-fictional accounts of hacking. Also, although some of the films are based on real-life events, but are still considered fiction.

6 The excerpt quoted from Mundy’s was taken not from the book but from a review web site called Book Browse.

7 Women Who Hack is a group in the Portland, Oregon area in the United States, whose group members are women, cis and trans women, and genderqueer person, with a website at http://womenwhohack.org/ (n.d).

8 C# is a computer programming language created in the year 2000 for Microsoft. It has an interesting history that, although out of the scope of this chapter, can be found in this article written by Bolton (2017) at https://www.thoughtco.com/all-about-the-c-programming-language-958330
CHAPTER SIX
Can You Protect Yourself from Hackers? Views and Advice

The scariest part of all is that some hackers, like the infamous “Anonymous” group, don’t necessarily want your personal data for any type of financial gain. As we saw in the 2015 Ashley Madison scandal, some hackers may see it as their personal duty to tell the world your secret(s), especially if you are a political figure, celebrity, or a C-level executive of a major corporation. – Davis (2016)¹

When you make all of your passwords for e-commerce, banking and government websites the same, you’re really making a hacker's day. – Quote from Kaspersky Lab website²

In other words, security and privacy is not a set-it-and-forget-it process. Above all, it’s not a set-it-and-forget-it process. Above all, it’s important to learn not only from security experts, who know the tools, but also from hackers, who know how to socially engineer their way into your phone or laptop. – Elgan (2016)³

Since the public were alerted to hackers, a quest to protect personal computers and corporations, government and law enforcement computer systems has been ongoing. These methods of protection are not without controversy and have not always worked. Computer security has become a large, world-wide industry and a profession. Skilled hackers have joined government and organisations to assist with finding security vulnerabilities. Yet there is also a sense of fatigue and complacency people and organisations have towards security.

This chapter explores the topic of computer security asking if you can effectively protect your computers from hacking. All information technology is at risk, including tablets, smart phones or computerised home appliances. As mentioned in Chapter Two, our reliance on computer technology is such that the risk of large-scale attacks on infrastructure, or the obtaining of personal data, has occurred. To ignore the possibility of hacking attacks is inadvisable.

This is not a technical advice chapter on how to protect your computer. It discusses software that is used to protect data and systems, and methods computer users can employ to minimise their computer being hacked. These methods are in some way also used by business, governments and other organisations. Three issues are discussed. First, a section on attitudes towards using computer security shows how attitudes towards this issue are mostly complacent and concerning. Second, a brief presentation of the views of a computer security expert towards cybersecurity issues enlightens us as to how concerning hacking issues are. Third, the last section lists and discusses issues and examples of software and techniques to use to minimise hacking.
Attitudes towards Computer Security – Home and Business

One unique discovery I made when reading the academic and non-academic about hackers I made was that there exists fear not just around hackers, but around protecting systems from hacker attacks. It is not just fear or an unwillingness to spend money on security measures, but compliancy. As the scale of cyberattacks and hacking increases, people rely on technology further and the use of mobile computing devices continues, it is obvious that computer crimes will increase.

It is easy to dismiss cybersecurity experts’ views and not take steps to secure data and information systems at home or in business. People may feel pressure to purchase anti-virus and other protection software, with no absolute promise of totally safeguarding their systems. Yet convincing evidence suggests that personal and business computer users are lax towards securing their devices systems and data.

The following views from a variety of cyber researchers, company researchers and experts highlight the current and future issues of cybersecurity. They demonstrate the depth of the problem of effective computer security from hackers. While not always guaranteeing total immunity from hackers, this chapter’s suggestions are worth considering. Constant updating of virus definitions or updating passwords do take effort. Concurrently though, the cybersecurity home and business industry is a large industry, with some feeling it profits off unreasonable fears. These comments give an appreciation of the importance of computer security.

It's no secret that computers are insecure. Stories like the recent Facebook hack, the Equifax hack and the hacking of government agencies are remarkable for how unremarkable they really are. They might make headlines for a few days, but they're just the newsworthy tip of a very large iceberg.

The risks are about to get worse, because computers are being embedded into physical devices and will affect lives, not just our data. Security is not a problem the market will solve. The government needs to step in and regulate this increasingly dangerous space.

The primary reason computers are insecure is that most buyers aren't willing to pay - in money, features, or time to market - for security to be built into the products and services they want. As a result, we are stuck with hackable internet protocols, computers that are riddled with vulnerabilities and networks that are easily penetrated.

Schneier (2018a)
Increasingly, everything is a computer: not just your laptop and phone, but your car, your appliances, your medical devices, and global infrastructure. These computers are and always will be vulnerable, but Spectre and Meltdown represent a new class of vulnerability. Unpatchable vulnerabilities in the deepest recesses of the world’s computer hardware is the new normal. It’s going to leave us all much more vulnerable in the future.

Schneier (2018b)

The home computer user is often said to be the weakest link in computer security. Security and privacy threats such as Web cookies and phishing require some form of user complicity or acquiescence. Adequate security does not come with the purchase of the computer but requires additional software, careful settings within applications, appropriate choices of passwords, regular updating of patches, etc. Moreover, as applications are becoming more interesting/ useful and businesses are moving away from paper, home computer users are performing more sensitive tasks online and storing more private data on their computers. Anecdotal evidence, surveys, and studies suggest that home computer users often do not adequately understand the threats, or have the time, desire and knowledge to be able to handle them. As large outbreaks of worms and viruses have shown, even systems administrators are not diligent enough in applying patches to improve security.

Howe, Ray, Roberts, Urbanska & Byrne (2012, p. 209)

‘It won’t happen to me’ is a prevalent mindset among senior executives in the private and public sectors when considering targeted cyber intrusions. This is exacerbated by the long-term adoption of a ‘fortress mentality’ towards cyber security, and by the attitude of many of our cyber-security professionals, who speak a different language when it comes to communicating cyber-security events to senior executives. The prevailing approaches to cyber security have clearly failed. Almost every week another serious, targeted cyber intrusion is reported, but reported intrusions are only the tip of the iceberg. Why have we got it so wrong? It must be acknowledged that cyber security is no longer the domain of cyber-security experts alone. Many more of us at various levels of leadership must understand, and be more deeply engaged in, the cyber-security challenge if we are to deal with the threat holistically and effectively. Governments cannot combat the cyber threat alone, particularly the so-called advanced persistent threat; they must work closely with industry as trusted partners. Industry will be the ‘boots on the ground’ in cyber security, but there are challenges to building this relationship, which must be based on sound principles.

Scully (2011, p. 195)

Approximately 16% of Australian enterprises do not have an action plan in place in the event of a data breach, which is the highest compared to the other countries in this study. More awareness about the need to develop a proper incident response plan is critical as currently, most enterprises surveyed react to a data breach based on previous experience.

Frost & Sullivan (2017, p. 19)
Ashford (2016) claims that Lloyds of London in 2016 stated 54% of European Chief Executive Officers (CEO) take responsibility for their organisation’s cybersecurity. This needs to be changed because CEO’s are becoming responsible for making sure hacking prevention and data security measures are in place. In the case of Equifax CEO Richard Smith was forced to resign after the company’s major data breach (NeSmith, 2018). Data protection is now closely tied to customer loyalty, with breaches, as Facebook in 2018 discovered, damaging brand reputation and trust (KPMG, 2018).

Discovering reasons why business and government have such compliances yields many reasons, but overcoming complacency is becoming a necessity when it is tied to customer loyalty and business profit. Kemp (2018) claims that a study resulted in a finding that 60% of CEOs surveyed preferred to invest in strategies to prevent malware infections but less against access abuses and password stealing by employees. Ismail (2017) states that between 2016 and 2017 business staff did not attend training on cybersecurity and that 40% of firms in one survey did not have a formal cybersecurity policy. Although such reports take place within certain countries or industries, generally such results and findings are concerning as hacking and cybercrimes grow in scale.

The same argument of complacency and apathy is true of home computer users, although it is also the cost and willingness to trust antivirus and other security software that plays a part in deciding to protect data. This can be alarming in that ransomware on home computers, for example, requires home users to pay by Bitcoin crypto currency, which they may be unwilling to do. One unusual way of viewing the relationship between the home computer user and the computer is one of being similar to lovers or close friends and feeling emotionally vulnerable to risks to its running (Lupton, 1995). This may be an odd view, but the home computer, laptop, tablet and increasingly the smartphone are used for multiple and different purposes, often at once. They entertain and connect with others; they are not just machines for productivity.

Commentators are often harsh on home computer users for failing to take basic security measures. Computer users can take risks such as downloading files that may contain malware or viruses and not have an anti-virus software program on their computer. This has been seen as laziness and ignorance on the part of the computer user (Tuesday, 2001). Some researchers, however, argue training and knowledge are a crucial part of avoiding such mistakes as users with higher knowledge of computer skills will employ more security on their computers and think before committing risky action (Howe et al. 2012; LaRose, Rifon, Liu & Lee, 2005). Therefore, the user has the responsibility to be aware of issues, but training, in whatever form that takes, and awareness through advertising or stories acting as warnings about computer security all assist in influencing a user lower the risk of being hacked or experiencing security issues.

To conclude, the subject of why people will not, or do little to, protect their business or home computers is an interesting area that is developing. It is a priority, however, as hackers learn to hack new types of technologies and increase the scale of their attacks. One compelling reason is that buying antivirus software, or downloading a free antivirus package, are the constant updates of new virus definitions which constantly protect the system. There are conspiracies antivirus companies purposely create computer viruses to ensure people continue to buy their products. A website called Computer Hope (2012) refutes this.
claiming, among several points of proof they do not create viruses, that an antivirus company couldn't protect itself from the virus before it was released without raising suspicion.

This book advocates that the reader uses their own judgement in deciding to secure their computer. It is acknowledged that not every security measure may work. Hackers can create worms or other malware quickly. In including this section, it is still advisable to be aware of hacking and what steps and measures are available to minimise its harm.

**One Professional’s Views on Cybersecurity Issues**

Four general questions were asked of a cybersecurity expert, covering topics such as user complacency, seriousness of cyberattacks, protection and views on media reporting of attacks. The four questions asked were:

1. Studies suggest that home computer users are often complacent about securing their computers and smart phones? Do you agree or disagree with this statement, and why?

2. Is the seriousness of cyberattacks on any country underestimated by law enforcement, government and the public?

3. What in your view is an appropriate or best way to maximise protection of all data and systems, naming what you think is the most effective such as firewalls on any business or personal computer system?

4. The media and entertainment industry has made many films that present nightmare cyber warfare on infrastructure and massive data breaches, some of which has happened, such as Ashley Madison and other attacks on Iranian Nuclear Plants with malware. In your view, are these movies accurate or exaggerated, and/or do you think the hacks that are presented in movies possible?

These answers were given:

**Question 1:**

I agree with you and as per my experience this behaviour lies within the immature and non aware thought process about cybersecurity. In some cases it is overconfidence and belief that nothing bad will happen to me or whenever it happens I will take care of it. Some home users also heavily rely on free security software which also exposes them to greater risk.
Question 2:

This is not the case now as countries and organisations have lost considerable to cyber attacks. But some countries where internet penetration is less, they are least bothered about cyber-attacks. Law enforcement are the civilian defenders against the cyber attack and unfortunately they are ill trained and ill equipped.

Question 3:

I feel every company needs a different security cyber security strategy, not what all organisations need in common is developing cybersecurity culture in the organisation. Once organisations establish an effective culture and each one of them are self aware about security incidents and effective resilience is achieved. More than a device readiness, human readiness has to be given importance.

Question 4:

Movies are often reflection of our society and incidents, the attacks which they show are possible, but the ease attacks happen they show is not possible. Cyberwarfare is played daily by countries in the cyber space and that’s why they have cyber command or equivalent defence structures. Cyberwarfare is immediate and present danger, but the lacuna is world doesn’t have an international law in the event of a full scale cyberwar.

Four points emerge from the expert’s view:

1. People may have an over reliance on obtaining free protection software over paid software that may have risks associated with it. The risk here is likely to be the free software will not cover every risk or pick up all hacking.

2. Countries are taking cybersecurity seriously; however, as the last section showed, business and home computer users tend to be more complacent overall about security.

3. Developing a cybersecurity awareness culture, especially in organisations, is vital.

4. Films about hacker attacks show what is possible but the ease at which they are carried out is usually exaggerated and there is a lack of coherent and cooperative international laws to deal with cyberattacks.

The conclusion reached that although films, the media and the cybersecurity companies have persistently portrayed a catastrophic scenario of hacking, clearly it is a major concern for society even if it seems alarmist. A home computer user can become caught up in a hack with identity theft or loss of data. The attacks are happening daily. Ransomware remains the most
feared for of attack, with having to pay hackers by Bitcoin a major challenge for the computer user who may not know how to use cryptocurrency.

With the annual cost of identity crime estimated at $2.2 billion dollars and rising (ThinkUKnow, 2017) there is a compelling case to take the security of computers and other technologies seriously. The cost of some software is high and a yearly subscription may be unaffordable. In the next section, the software types used and the methods to prevent hacking are discussed that bring awareness to the issue of hacker protection and harm minimisation.

**Computer Hacker Protection and Threat Minimisation**

This section looks at a wide, but incomplete, list of software and methods that can be done to minimise hacking and security breaches. Most are well-known, but the format of this section in informing security options, as at 2018, is to name the measure or software with an explanation of it. The emphasis is on home computers, but can be applied to any size computer system such as a business or government computer.

In researching and compiling these measures, several sources were consulted. One book that was consulted was Jacobson and Idziorek’s (2012) *Computer Security Literacy: Staying Safe in a Digital World*. Although published in 2012, it still acts as a general and easy to read guide on taking measures to protect a computer system. Any text quoted from that book is referenced. Caution needs to be exercised, and advice from experts if needed sought, to make the right decisions on what software to use before buying.

There are two points about this section that need clarification. First, the advice is for computers and laptops, but as hackable technologies change some may still be relevant to emerging technologies. It is advisable to seek advice for protection for new technologies that come onto the market, although this section includes a brief discussion on protecting the smart phone. Second, the advice is for general computers that run Microsoft Operating Systems, not Linux or alternatives that have their own protection software. Second, the Apple Mac and Apple computer systems are considered safer, but are not immune from viruses and although rarely experience getting Malware compared to Microsoft, it does occur (Thomas, 2018).

**Software Protection**

*Antivirus Software*

Landesman’s (2018) describes such software as code designed and written to detect, prevent, remove and quarantine (place viruses in a sector of the computer that cannot be broken out of) malicious software. Henry (2013) acknowledges that there is confusion over the terms antivirus and antimalware as viruses are specific codes but malware can encompass any type of code. In 2018 many computer security combine virus and malware protection in their software. For this section the term antivirus will encompass antimalware software.

Ten examples of antivirus software are listed here, although it should be noted that some are free, some need to be paid for or some are initially free but advanced security features need to be paid for often as a yearly subscription:
Avast
• AVG
• Bitdefender
• Comodo Antivirus
• Kaspersky Anti-Virus
• McAfee
• Microsoft Security Essentials
• Norton AntiVirus
• Panda Cloud
• Trend Micro

It is advisable to look at the technical features of the chosen software rather than price. If you have confidential data or photo/music/video files, then it may be worth investing in paid antivirus software. Running antivirus scans on USB and external hard drives is also a good strategy even if they are infrequently used.

Many antivirus programs continuously run in the background and are not noticed, although they can slow down the computer’s processor, hence noticing when you are using the computer it seems slower to open applications or save documents. An important part of using antivirus software are updates or updating virus definitions to prevent new viruses infecting the computer. A technical description of this is out of this book’s scope. However, a concise explanation of what software companies do to stop virus infections is the use of heuristic modeling behaviours to stay ahead of hackers. Heuristics use the basic characteristics of current viruses and seek out new ones (Musson & Hukill, 2004). Computer users can set their software to automatically update new antivirus definitions, but this can slow the computer’s processing power.

Figure 34 is an example of an interface of an antivirus software suite of protection from Auslogics displaying the tabs and options available to perform antivirus tests and protect the computer:
Figure 34. An antivirus interface with choices for actions (Auslogics, 2017)

Figure 35 is an example of a warning window message that Avast will bring up on the screen when a virus is detected:

Figure 35. Example of virus warning (tothepc.com, 2010)

There is a need to be aware when going onto websites of scareware. It is malware that attempts to trick computer users into buying an antivirus program. These frequently appear on popup windows; that is, extra windows that open when you click on a website. The
message states there are infected files and the purchased software will fix them; there are actually no files there and the software may put malicious software into the computer (Fraud Watch International, 2017a). Figure 36 shows an example of a scareware message:

![Figure 36. Scareware message on computer screen (Fraud Watch International, 2017b)](image)

Antivirus software protection is not perfect, but is a minimum requirement for those using personal computers and is vital for business, government and all large organisations. It is accurate to state they may not find every virus or malware file and eliminate it. Jacobson and Idziorek (2012) strongly advocate that once installed to get updates from the Internet regularly as safeguards, such as patches (also called updates), so that virus signatures are updated that can find new malware. It is reasonable to expect that unless patch downloads are running in the computer’s background that this will not be done every day, but it is necessary to be mindful that it must be regularly updated. Finally, be aware when visiting a site or downloading other software you may be asked to disable the antivirus software. This is not advised, and also many antivirus software programs are incompatible; that is, you cannot run two or more on one computer.

**Anti-ransomware software**

There are two common types of ransomware (Savage, Coogan & Lau, 2015 p. 5):

1. **Locker ransomware (computer locker):**
   Denies access to the computer or device

2. **Crypto ransomware (data locker):**
   Prevents access to files or data. Crypto ransomware doesn’t necessarily have to use encryption to stop users from accessing their data.

Suberg (2017) shows the cold, threatening nature of a ransomware screen message which is a manifestation of, to date, the worst type of hacking, that is called Bad Rabbit:
An example of a free anti-ransomware tool is Bitdefender that can prevent ransomware from entering the computer’s system. Backing up data onto multiple devices, a strategy that should be done regardless of threats, is advisable. The concerns about ransomware for personal, business and government computer systems are serious. Networks Plus (n.d.) advise these steps:

- See if the security suite (the antivirus software) has anti-ransomware and run automatic scans at least weekly
- Check all email addresses and do not open attachments if unsure of source
- Avoid clicking on unknown links in emails and on websites
- Install firewall software
- Consider storing files in cloud services; however, this needs to be thought out as cloud services have been hacked

Overall, ransomware hacks are increasing, so to apply caution to protecting files and systems from them, consideration needs to be given to implementing measures to do so.

**Firewalls**

A firewall is a piece of software, and a network security device, monitoring incoming and outgoing network Internet traffic to the computer make decisions to block or allow specific network traffic based on a set of security rules (Cisco, n.d.). An example of an adequate firewall is Zone Alarm. A disadvantage can be having to reset rules if the settings are placed at maximum protection. Some antivirus software suites may include a firewall.
**Anti-Keylogging Software**

Keylogging software, which can be malicious or a productivity tool, is a software program or hardware device that records the actions of the person typing. If used without knowledge, especially if a hacker has installed the software onto a person's computer system, it is possible to record and view private data, such as passwords or financial account data. An example of anti-keylogging software is Spy Shelter.

**Cookies Removal**

Cookies have attracted controversy for decades since their inclusion in web browsing software. A good description is from the website allaboutcookies.org (n.d.):

> Also known as browser cookies or tracking cookies, cookies are small, often encrypted text files, located in browser directories. They are used by web developers to help users navigate their websites efficiently and perform certain functions. Due to their core role of enhancing/enabling usability or site processes, disabling cookies may prevent users from using certain websites.

Cookies are created when a user's browser loads a particular website. The website sends information to the browser which then creates a text file. Every time the user goes back to the same website, the browser retrieves and sends this file to the website's server. Computer Cookies are created not just by the website the user is browsing but also by other websites that run ads, widgets, or other elements on the page being loaded. These cookies regulate how the ads appear or how the widgets and other elements function on the page.

Cookies are especially contentious as they have been implicated in privacy issues. One example where cookies called forged cookies were used by hackers to access private data on Yahoo accounts in 2015 and 2016. The best way to clear cookies is to use the browser settings, depending on the name of the browser (Chrome or Firefox for example), manually or placing an automatic clear setting. Websites do allow advertisers to use third party cookies to track user browsing habits Jacobson and Idziorek (2012). Figure 38 is an example of what box to click when clearing cookies:
Figure 38. Clear cookies (The Windows Club, 2018)

**File Encryption**

This is the process of encoding files into code that can only be unlocked with a key, usually a password. The process can be easily done, but certain software can be difficult to use for home computer users. Examples include: Folder Lock, AxCrypt and Cypherix SecureIT. Again, it is possible for hackers to open the encrypted files, but it would depend on the nature of the files and their importance to hackers. Encryption is vital for business, government, defence and law records. It is debatable if home computer users would use it, but if sending files over the Internet encryption can make files private and less likely to be hacked.
Common Methods and Procedures for Minimising Hacking

While software assists in finding viruses, malware, key logging software and other issues, user habits can determine how much their data and systems are protected from. In this section some of these habits are discussed, beginning with the crucial issue of password changing and protection.

Passwords – The Most Important Issue in System Protection

Passwords are important for the right person to gain the right access to a system and its data. They are considered an annoyance because people are expected to know many passwords for different websites, phone apps and if they are in an organisation may have multiple ones for several systems. Jacobson and Idziorek (2012, p. 5) explain the security versus convenience problem which makes systems vulnerable to hackers:

In the physical world, security often involves extra steps or procedures to protect a valued object. For example, houses are often protected with a locked door, and a key is then needed to gain access to the house. Information security is similar; passwords are used to gain access to information, requiring the user to remember and use the password every time the desired information is accessed. The more security mechanisms added to a computer system, the more intrusive security measures might be, often causing user frustration. This frustration may cause individuals to take shortcuts, like leaving a door unlocked or using a simple and easy-to-remember password that weakens the security safeguard.

Passwords are crucial first lines of defense against intrusions into computer systems and, as Gehringer (2002) argues users do not appreciate the potency of the tools a hacker may use against them. The issue of remote hacker access through a hacker guessing passwords and entering systems was recognised well before Windows and other operating systems became standard (Morris & Thompson, 1979).

To highlight the problem further, Podd, Bunnell and Henderson (1996, p. 304) state:

Self-generated passwords are often the only line of defence against intrusion into computer systems. Yet research has shown repeatedly that the majority of passwords are simple words linked to a user’s biographical data, or immediate environment. It is a relatively simple matter to discover such passwords and gain access to the system. However, these simple passwords endure because system operators and users alike find them attractively simple.

It is understandable that creating complex passwords, which for some users can be over 100, is a major problem. Writing them down is risky, as the paper copy can be lost or given out by mistake. In organisations the need for secure passwords is a major imperative with the burden on the user and system administrator to create good passwords. In their study (Zviran & Haga, p. 180) found the following in the sample of users they surveyed:

- 50% of users reported having passwords of five or fewer characters
- 80% only used alphabetical passwords with no numeric or symbols in them
- 80% never change their password
- 78% based password on meaningful details, suggesting not using more abstract passwords such as li*44%33mi for example which is less meaningful

Home users can only be educated and reminded. In organisations there are many checks that it is the right person keying in the correct password, especially the inconvenient but necessary three tries and then you are logged out. Many e-commerce and virtual communities have this as a protection feature as well. Facebook will allow you back into your account using the same password after it gives you a test, such as recognising your friends’ photos or sends to your mobile phone a numeric code. The steps to gain access back in can be frustrating when the account needs to be reset, but are deemed necessary to maximise account protection.

Sasse, Brostoff and Weirich (2001, p. 122) give an example of the seriousness of someone ambushing another’s access to a system because of poor password strength:

A user is told that his password has expired, and he must change it immediately or be locked out of the system - he feels stumped, and ends up choosing his wife’s name. This is exploited by a colleague who wants to look at files he has no permission to access. He tries out the user’s family member’s names to get into the system, and succeeds. Many password systems “ambush” users without warning. People have difficulty designing and memorising strong passwords, and they have even more difficulty under pressure.

In this case the hacker is another person in the office. They are deemed one because they are accessing a system to cause disruption and commit illegal activities. That the user has used their wife’s name allows this to happen. Hackers will often attempt to use names like this, but it depends on if the hacker knows the person or not. They can guess personal details or find out a person’s family, friend or pet name depending on how much of it is placed online.

The Internet is often unsecured so care needs to be taken when using passwords. Packet sniffing, user disclosing passwords to anyone by mistake or not and clicking on links all contribute to passwords no longer being the first line of defense when accessing systems and websites. Figure 39 is a diagram that shows how hackers through the Internet gain access to user passwords and some common mistakes users make to allow this:
The question becomes how to minimise these threats. Generating a secure password is challenging but must be done as is considering changing that password often. When researching the current advice on how to do this, several sources were consulted that gave a list of optimal password practices to stay safe as possible. A search of the web combined with consulting security books suggest several common practices. The effectiveness of them can be debated, but specific password procedures can minimise hacking and identity theft.

Jacobson and Idziorek (2012) were again consulted, and some of their advice is paraphrased, because they provide good strategies for strong passwords. The other two sources consulted were: The Australian Communications Consumer Action Network (ACCAN) (n.d.)9, Tech Thought (2017)10 and Connect Safely (2018)11. The following list is a combination of advice based on these information sources:

1. **Do not give out your password to anyone**

   There may be some exceptions such as a system administrator in the workplace who will ask for it, but in general do not give it out and if you do change it as soon as possible.

2. **Composing a password that is a mix of the following**

   - Lowercase letters
   - Uppercase letters
   - Numbers
   - Special Characters

   Two examples may be (note these are made up): a7%$h4exo or o#xUtIe5*9.
3. Try to use passwords that are long with eight or more characters

Although difficult to remember, an example might be Ch4&w@0T. Connect Safely (2018) suggest 12 characters at a minimum, though it is debated if this is feasible for many to remember without recording it manually on paper or electronically.

4. Consider an acronym as a password

Jacobson and Idziorek (2012) suggest combining a set of song lyrics, poems or quotation using only the first letter from each of the words. This creates a string of random characters. For example:

```
Come as you are, as you were, as I want you to be¹² – select first eight to make acronym Cayaaywa
```

They further suggest substitution of letters to make it more difficult but that the mind can still relate to and remember, for example C@3a9a@a.

The acronym can be also a phonetic replacement such as “I love to laugh” “EyeLuv2L @ff” or an encapsulation which is the use of symbols to separate words or phrases, such as “sunGlasses4” becomes “(sunGlasses4” (Jacobson & Idziorek, 2012, p. 78).

5. The challenge of the pass phrase

A passphrase is a combined string of words that, taken together, forms a password (Jacobson & Idziorek, 2012, p. 79). This is considered a fairly high ranking way of creating challenge or near impossible to crack passwords. They can be challenging to remember due to their length. Connect Safely (2018) recommends this strategy:

```
Such a phrase should be relatively long - perhaps 20 characters or so and consist of seemingly random words strung together along with numbers, symbols and upper and lower case letters. Think of something that you can remember but others couldn’t guess such as YellowChocolate#56CadillacFi$h. that’s relatively long - perhaps 20 characters or so - using seemingly random words strung together along with numbers, symbols and upper and lower case letters. Think of something that you can remember but others couldn’t guess such as YellowChocolate#56CadillacFi$h. Avoid using famous quotations that might be easy to guess.
```

6. Log out of accounts

The temptation to stay in accounts is common. Logging out just means having to type the password in again later. Disable web browsers to memorise account passwords. If asked to remain log in a website consider not doing as a way of minimising hacking.

7. Do not create a password based on easily guessable personal information

Pets, friends, family, spouse or partner, sports teams, airlines, name of car or object, all are examples of easily guessable password names hackers may be able to obtain (Jacobson & Idziorek, 2012)
8. Do not use words spelled backwards as passwords

An example may be elpmaxe which is example backwards which is a weak password.

9. Regular password changing

This is likely to be compulsory in a work or academic setting, where the system will tell the user they must key in a new password. Home users should do this regularly especially with financial accounts such as online banking.

10. Avoid sequences and repeating passwords

Example is rccD1234 – the numbers make it slightly easier to crack a password.

11. Avoiding the dictionary type password

As (Jacobson & Idziorek, 2012) argue, a base and suffix technique is easier to crack, for example, lemein66 is easier to work out than 5@leT99.

12. Rank accounts according to their importance

In ranking them this may avoid password fatigue (Jacobson & Idziorek, 2012). For example, the most secure accounts should be money and email, while Facebook less so. With the most secure accounts change passwords every six months while with less secure one a year. These are just a guide, however, and you can change them more often.

13. The Password Manager debate

One way of generating unique passwords and storing them is downloading a password manager. This is a software program that stores them in one place and autofills, which means when you log into a site you have a password for it will automatically fill in the password so you can just click on the login button on the page. Figure 40 is an example of an interface of a password manager called Safe in Cloud:
There are controversies over using password managers. Stokes (2018) argues that they can be targeted by hackers as the passwords are valuable data. The problem lies in the password manager having a browser extension, which is a small software plugin application used to add functionality such as Video Download helper which captures videos from the web browser and downloads them. Therefore, caution must be exercised if deciding to use on.

**Multi-factor authentication (MFA) and Two-factor authentication (2FA)**

Authentication from a computer perspective is simply when the computer will recognise that the correct person is logging into a system. It is evidence of who you are as only you know this information. Passwords are the main authentication types, but new layers have been added to prove one’s identity and right to access a computer system. Not all systems use this, but with some social media or websites if you get locked out you may need to use several methods, not just passwords, to access them.

Multi-factor authentication means the user will go through a series of sequenced checks to prove their authenticity. This may be a combination of something known, something one possesses or owns, and something unique to one’s physical being, normally the fingerprint or facial recognition. What needs to be noted is that this will be three or even more things that will be asked.

By contrast, the Two-factor authentication will only involve two steps. The basis of authentication lies in the idea that a person may not know two or more things about you to
obtain access to a system. While not a guarantee it has become an industry standard and is recommended by cybersecurity experts to assist in stopping hackers from obtaining access.

**Web Certificates, Secure Sockets Layer and the https Protocol**

Millions of financial transactions are made online daily. Sites like PayPal, eBay and many others are under a large obligation to protect their customer’s financial data such as credit cards. Unfortunately, as stated in this book, financial data hacks are common. The choice to use credit or debit cards, cryptocurrency or electronic funds transfer is the individual’s. There are three types of techniques companies will use to try to protect their customer data and privacy over often unsecured networks. The first is the web certificate that attempts to prove the website is authentic while the second is the Secure Sockets Layer (SSL) represented by the

**Web Certificates:**

A definition of a web certificate or certification is given by Techopedia (2018) as:

> A website security certificate is a validation and encryption tool, part of the HTTPS protocol, which secures and encrypts data going back and forth between the server and the client browser. It is issued by a trusted certification authority (CA) who verifies the identity of the owner of a website. The certificate then ensures the user that the website it is connected to is legitimate and that the connection is safe and secure. They ensure individual websites are proven valid and give owners of them accountability for the privacy and security of all their users and visitors.

As it is an industry standard, it is reasonable to trust such sites but still treat them with caution. Precautions should be done with networks that are free; that is, it is better to buy online at home then at an Internet Café for example, and protecting passwords still must apply. If the network or browser suspects something is wrong a warning message will come up to alert the user to be cautious:
SSL and HTTPS

Another industry standard for e-commerce and financial sites is the use of Secure Socket Layers and the https protocol that distinguishes a site from a less secure website. A technical explanation of SSL is given by GlobalSign (2018):

SSL Certificates are small data files that digitally bind a cryptographic key to an organization’s details. When installed on a web server, it activates the padlock and the https protocol (over port 443) and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

Figure 42 shows how an SSL appears in a web browser bar:

![SSL https shown in browser bar](image)

Figure 42. SSL https shown in browser bar

Jacobson and Idziorek (2012) argue that it is a misconception that a site that uses https is totally secure. They do state that the communication between the buyer’s web browser and the company’s server, so eavesdropping is less likely. Overall, the SSL and https will assist in a safer experience with buying. Hackers can still get around this.

Email

Although newer messaging systems have made email systems use lessen in 2018, it is still widely used. It is a method of exchanging messages and files which in some form has been in use for over 50 years. Most emails make use of the @ symbol, for example,
error90@yahoo.co. An email system is usually client-based, the most popular being Microsoft Outlook, or web-based that operates within a web browser such as Firefox. Examples of web-based are: Gmail, Yahoo and GMX Mail.

The crucial strategy to avoid when using email is not to click on unknown links. Phishing still remains a constant threat. As a reminder to what to look out for, Figure 43 posted on the SiteMinder (2018) shows an example of a phishing email from eBay that contains a link that must not be clicked on as the receiver did not request a password change:

![Figure 43. Scam email using eBay (SiteMinder, 2018)](image)

The key logger threat is also still present, but much anti-virus software can find these. Spam is annoying but many email programs can detect spam and place it automatically in a spam folder. Email addresses can be blocked. The technical explanations of how to do this can be found on the web, though it may take some tries before mastering it as every email program is different.
One area that does need attention is the Internet scamming of older people. Generations will become technology literate, but scamming on a global scale frequently targets the elderly. This can take many forms but is done through the Internet and also phone calls. People may pretend to be from a bank. If have elderly people in your family or friendship networks, check to see that they are aware of such issues.

**Protection for Smart Phones**

Hacking is not just confined to computers and laptops. Smart phones, or cell/mobile phones, have become a device where private data is stored, financial transactions and location services. Although many smart phone models exist, it is the Android and Apple iPhone where security risks are high. It is common knowledge how to hack a smart phone. Johnson (2018) wrote an extensive blog entry on the website *The Truth Spy* explicitly how to hack a smart phone demonstrated by this extract about a hacking technique called The Midnight Raid:

This attack is known as the “Midnight Raid” and generally performed at night on the target phones when the person owning is asleep with the phone charging but is turned on. All you need to do is send a simple graphic text with the words ‘You are being hacked’ which is surely going to invoke a response form the phones internet explorer. You need send another push message to run the application on the target device to transfer the data.

It serves as an example of the types of hacking that could possibly be done to a smart phone.

When researching the ways to protect smart phones it became clear at the time of writing this book that there are not many full proof methods to do so. Considering the smart phone is so open to hacking, an unrealistic but wise method is not to do personal banking on the device. Apple Pay and Bitcoin payments are also possibly hackable. Suggestions to protect smart phones are:

1. Do not use public free Wi Fi as hackers could constantly be monitoring phone calls and app usage
2. Do not leave apps open when not in use as hackers are able to break into the phone app while it is on a network
3. Update all apps as they may have new security patches, being mindful that it can cost money to download new updates
4. Use two-way authentication to gain access to the phone, such as fingerprint and password
5. Erase all data when disposing of phone
6. Using a Virtual Private Network app on the phone to protect privacy

These are six steps that minimise hacking to a smart phone. The use of the smart phone and its attractiveness to hackers will become more frequent as their spread across the world continues. Their affordability and the lack of attention to security precautions makes them easy targets. As these phones evolve from communication devices to personal assistants and
entertainment carriers, the need to consider measures to minimise hacking for smart phones and future electronic devices is vital.

**Conclusions and Summary**

This chapter focused on the question can you protect yourself from hackers? The conclusion is that it is possible, but it is about minimising risk through use of anti-hacker software and doing strategies to support being safe. Attitudes towards security are complacent. The scale of hacks for business suggest that compliancy needs addressing across the world. Although this chapter discussed technical and strategic ways of protecting a computer system, it is advisable to investigate more up to date knowledge on software and anti-hacking techniques. As technology changes and more of life is automated or mediated by phone apps, hackers will find ways to hack new and existing technologies. The key is to be aware and make the decision to take needed steps based on what one wants and needs to protect their computers and other technologies.
Notes

1 Quote from Davis from blog post https://www.infosystems.biz/blog/what-do-hackers-want-and-why-do-they-want-that/

2 https://usa.kaspersky.com/resource-center/threats/top-10-computer-security-mistakes


4 A virus definition is binary pattern (a string of ones and zeros) that identifies a specific virus. By checking a program or file against a list of virus definitions, antivirus software can determine if the program or file contains a virus (TechTerms, 2018).

5 Computer Hope’s view on computer security companies deliberately creating computer viruses can be found at https://www.computerhope.com/issues/ch001013.htm

6 A USB is a Universal Serial Bus and is usually a device to connect into a computer port to save and transfer data to. However, they can also contain many types of computer viruses and malware especially if public Internet terminals, such as libraries and Internet Cafes are used. Always run an anti-virus scan on them before using them on your home computer.

7 This is not an endorsement of Bit-defender anti-ransomware software but an example of a free software tool to minimise hacking.

8 The diagram is based on Jacobson and Idziorek’s diagram of password threats which appears on page 62 of their book Computer Security Literacy: Staying Safe in a Digital World. The diagram in this book also contains images from the free photo sharing site Unsplash (https://unsplash.com), that allow images to be used royalty and copyright free. The server image is Microsoft clipart so is not referenced. The two photos are: the man with the sunglasses, who is not a hacker just a representation of a man at a laptop taken by an Unsplash user named NeONBRAND, while the women at the computer was taken by another Unsplash user named Tran Mau Tri Tam.


10 https://www.teachthought.com/technology/10-tips-for-better-password-security/

11 https://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/

12 Password example taken from Nirvana’s song Come as You Are (Nirvana, 2009).
CHAPTER SEVEN
Conclusions and Closing Thoughts about this Exploration of Hackers Lurking Behind the Screen

It’s time for people to stop thinking of cybercrime as something that only happens on a computer. With the rise of ‘smart’ devices and the Internet of Things (IoT), the maturation of the online black market as a multi-billion dollar industry and the widespread commercial and recreational markets for do-it-yourself hacking tools, cyberattacks will become far more invasive, dangerous and even physical. – Comment on Fox Business Website 2016

American society (sic) has evolved to the point where it believes in storing everything about itself on computer; birth records, death records, credit reports, telephone bills, hospital data, and so on. While all these computers are not yet trading information, it is remarkably easy to obtain a detailed profile of someone in a very short time by glancing at key files. – Emmanuel Goldstein in 1991

If one of today’s cybersecurity systems fails, the damage can be unpleasant, but is tolerable in most cases: Someone loses money or privacy. But for human-level AI (or above), the consequences could be catastrophic. A single failure of a superintelligent AI (SAI) system could cause an existential risk event - an event that has the potential to damage human well-being on a global scale. – Roman V. Yampolskiy

In exploring hackers lurking behind the screen, I have discussed a sample of the the types of issues surrounding the topic of computer hacking. Clearly, hacking is a crime, yet if we did not employ hackers to prevent attacks, we may be at a loss to protect ourselves and our computers. It is accurate that there has been exaggeration and moral panic over hacking. Yet people still continue to, and at a greater rate, use phone apps, websites, electronic commerce and dating sites exposing themselves to hacking. Fluctuating feelings exist as well; for example, we may abhor the activities of Anonymous yet applaud when they bring down hated targets. We also get annoyed at installing and updating software or constantly changing passwords. Risks of hacking are higher and nightmare scenarios are possible. As our reliance on technology continues so does our need to protect our data, identity and our computer systems.

In selecting the themes and subjects to cover for this book that functions as a general reference guide, I decided to cover a wide range of topics. The historical, cultural and technical aspects are not exhaustive, but gave an overview of hacking and the debates that arise from it. There is a vast supply of information and literature of many types on hackers. It is wise to read them with some background knowledge of it. It is important to consider protection for your data and computer systems as best as possible for harm minimisation. It is said that a hacker attack is a case of when, not if, although what type of attack that could be on one’s personal computer is debatable if some precautions are met.
Reviewing the six chapters, two overall assessments of hackers and hacker are:

1. Hacking is growing exponentially as technology and Internet use grows but criminal law and anti-hacking technologies are not keeping pace.

2. Hacking is still a criminal act, but it is no longer committed by male only hackers, and is now an industry with its own conferences and publications.

When compiling the research there was a concern that most of this material was influenced by that coming out of the United States of America. Other countries have been waging hacking and cyberwarfare, China, Russia and North Korea for example. A Westernised view of good/evil comes across in much book, academic and non-academic literature, especially news stories.

To reiterate this book’s topics:

Chapter One gave an introduction to hacking and hackers with definitions, types of hacking and introduced the concept of hacker groups, white, black and grey. The chapter gave a broad spectrum overview of the hacking field, acknowledging that it is not a simple problem to solve. Not all hackers do harm, yet the overall picture of hacking is one of fear and disdain.

Chapter Two was an extensive, but selective, discussion of the history of hacking. The interesting dimension was how it began as a prank activity and also helped in times of war and conflict to save people. Many key figures such as Kevin Mitnick and Robert Morris, and their activities, were reported as their exploits became enshrined in hacker history. It was also clear laws to punish hackers were reactionary and did not keep pace with growing hacker attack sophistication. The chapter concluded with showing how cyberterrorism and identity theft have become serious issues of our time that will likely escalate.

Chapter Three was a comprehensive case study of hacktivist group Anonymous. It used many sources to construct a description of the group, their identity and practices such as the wearing of the Guy Fawkes mask, their history and their structure. Four of their targets and conflicts were discussed showing the lengths they employ to keep people, governments and organisations accountable for actions. We may judge them harshly or support them but many have agreed or supported their hacking actions and protests.

Chapter Four reported a study I conducted in 2016 of the workings of a computer hacker’s public virtual community forum. The main finding was how the beginning hacker, the popular cultural label newbie, tried to obtain information from experienced hackers. More experienced hackers within the community tended to be admonishing of new hackers, especially those who wanted information on how to do black hat activities. The idea here is that hackers do take their activities seriously. If they follow an ethical hacking path they expect others to. They also value and protect their positions within the community as owners of specific hacking knowledge, and have the power to shape new hackers’ attitudes by giving that knowledge or withholding it.

Chapter Five was considered important for two reasons. First, the male-dominated hacker world has been challenged by women (and those who identify as other specific genders). Although only a selection of women hackers were profiled, it showed that over a long time period women have played a part in ethical and unethical hacking. This will increase as
women and girls take up hacking, although this does not suggest all will become black hat hackers. Second, a sample of cinematic films were discussed that involved some form of computer hacking. Although these scenarios are exaggerated in some films (James Bond especially) it is not beyond possibility that artificial intelligence may program itself, or large global hacking is possible.

Chapter Six asked if computers could be safe from hacking, concluding that perhaps it can only be minimised. The when, not if, of being hacked is a strong message to heed, yet it is about being mindful, but not paranoid, about hackers. In writing this section, a selection of strategies to minimise hacking were given, though there are many websites and books that can assist, as can professional computer help service organisations. The computer security industry is a business and relies on fear to continue making profit, but also offer free programs. What was unexpected were the studies down on the compliancy of home computer users in securing their computers. It was well-known that many business and governments were also lax in their computer security. Passwords are especially contentious because users have to remember so many with complex combinations of text, symbols and numbers.

**Should Hackers be Feared?**

Elliot: I never want to be right about my hacks, but people always find a way to disappoint (IMDB, 2018)

In the television series *Mr. Robot*. Cybersecurity Engineer and hacker Elliott Alderson is hired by a man named Mr. Robot to wipe out debts. Joining a group of hacktivists, the series depicts his life as a hacker ruled by clinical depression and social anxiety as he tries to make sense of his life and the world of hacking he inhabits. In this quote he might be referring to his need to be ethical, but people who use computer systems disappoint because they do not take security precautions. Although this is not a call to find every piece of security software and install it, there is little doubt that hackers can inspire fear. Your data and identity are crucial. Ransomware especially causes anxiety as people are forced to pay in cryptocurrency. It is subjective that hackers are always out to get people. Their ability to hack infrastructure and private records does, however, cause anxiety.

Fearing them will not make the problem disappear. Films may exaggerate the threat, but will a non-human hacker exist one day? Remote hacking has been proven. Some cybersecurity experts paint a bleak future where the risks of identity theft and data breaches are commonplace. The hacker represents a figure behind a screen, but hackers will employ new and remote ways and techniques to continue to hack your data.

What the legal system and lawmakers will do across the world is also a vexed issue. Are Anonymous correct that governments have too much power over individual’s data? How far should governments legislate with deterrent laws and punishments? The Internet has always been viewed as a place of free speech and activity. Crackdowns have resulted in the Dark Web where hackers can learn the hacking techniques they need. This again is tied to the fast evolution and development of technology. As more technology is considered hackable, what can be done to deter hacking? That question is still being grappled with.

Then there are the hacker’s motives to consider. Some hackers see hacking as a challenge, but some are doing it for fun. How do we distinguish the difference? Having your computer hacker system hacked is intrusive, though people may be playing a prank on you. Spam
emails and phishing emails do need care, as does clicking on unknown links or opening email attachments. Exercising caution is the most valuable skill in minimising hacker attacks, as well as being aware of hackers, to minimise fear.

**Conclusion**

Be aware of hackers lurking behind the screen, but do not cease using technology out of fearing them. Hackers are indeed a fascinating group to study. This book has sought by examining a collection of themes about hackers and hacking to inform the reader about this world. Hackers are unique in the way they act and the targets they select, but they do have power over the way we choose to use technology. Finally, it sought to understand those that are lurking behind the screen and in doing so assist in making the right decisions for themselves about how to protect valuable data and computer systems.
Notes

1 Comment found on Fox Business website which is part of the American Fox TV Network.

2 Quote from Goldstein from Index on Censorship.

3 Quote from Yampolskiy from Harvard Business Review website.
WORKS CITED

Academic Journals, Conference Papers and Theses


### Books and Book Chapters


**Internet Sources**


Electronic Frontier Foundation (EFF). (n.d.). About EFF. Retrieved from https://www.eff.org/about


me.me. (n.d.). We do not forgive we do not forget. Retrieved from https://pics.me.me/we-are-anonymous-we-are-legion-we-do-not-forgive-20476304.png


Revolvy. (n.d.). Level Seven (hacking group). Retrieved from https://www.revolvy.com/page/Level-Seven-%28hacking-group%29


Works Cited under Internet Sources include material obtained from Internet sources such as the World Wide Web, emails, mobile (cell) phones, photographs, videos, social media such as Twitter, YouTube and Facebook, blogs, virtual communities or elsewhere, but not academic journals, conference papers, honours, masters and PhD Thesis’s, or any research papers obtained online. Please note that some web material will change or be removed after publication of this book.
Computer hackers and hacking has a long history of disruption to computer users’ lives. They are feared as hacking becomes harder to manage and attacks on computer systems become global. This book examines issues around those lurking behind the screen.