Hackers gonna hack: Investigating the effect of group processes and social identities within online hacking communities

Helen Thackray

Thesis submitted for the degree of Doctor of Philosophy

Bournemouth University

October 2018

Hackers gonna hack: Investigating the effect of group processes and social identities within online hacking communities

Helen Thackray

Abstract

Hacking is an ethically and legally ambiguous area, often associated with cybercrime and cyberattacks. This investigation examines the human side of hacking and the merits of understanding this community. This includes group processes regarding: the identification and adoption of a social identity within hacking, and the variations this may cause in behaviour; trust within in the social identity group; the impact of breaches of trust within the community. It is believed that this research could lead to constructive developments for cybersecurity practices and individuals involved with hacking communities by identifying significant or influencing elements of the social identity and group process within these communities. For cybersecurity, the positive influence on individual security approaches after the hacker social identity adoption, and the subsequent in-group or out-group behaviours, could be adapted to improve security in the work place context. For individuals involved in the communities, an increase in the awareness of the potential influences from their adopted social identities and from other members could help those otherwise vulnerable to manipulation, such as new or younger members. Further discussion on such information, as well as historical examples, will lead to informed behaviour by these communities. Whilst this may not cause the group behaviour to change, it would ensure there would be understanding and acceptance of consequences to unethical or illegal actions, which is hoped to discourage cybercriminal behaviour.

The research employed a mixed methods approach, with online questionnaires and individual participant interviews. This approach primarily utilised the netnographic approach (Kozinets, 2015), with the results providing more qualitative information than originally anticipated. Informal data collection for this research included observation of relevant websites and forum discussions as well as observation at hacking related conferences; the subsequent surveys and interviews were conducted with volunteers from these communities. Formal data collection was initiated through a pilot study, carried out in early 2016, with 44 participants. This was followed by the first study survey in early 2017, completed by 155 participants. The second study was individual interviews, conducted with 14 participants throughout 2017. These interviews were analysed in the context of Social Identity Theory (Tajfel, 1974). The third and

final study was another survey, conducted early 2018 with 197 participants. Thematic analysis was conducted on all data.

There was limited evidence of manipulation of group process or trust observed in forums or reported by participants. The adoption of a specific social identity does have strong and influential behavioural norms; however, the adoption of a specific social identity category does not prevent individuals from identifying and confirming to multiple categories which may use or accept different behaviours. The majority of particiapnts in these studies appeared to position themselves as positive deviants, acknowledging past or minor “black-hat” behaviour.

This work contributes to the development and improvement of methodologies in online environments: this research was exploratory in accessing a hard to reach demographic that is often untrusting of outsiders. Adaptions to ethical procedures ensured complete anonymity for the participants, improving the participant recruitment rate. Key findings from this research demonstrate that hacking communities can be very positive and supportive for their members, functioning primarily as meritocracies. This is regarded by the communities as an important positive trait, in conjunction with online anonymity. The conclusions of this research consistently support the findings of previous studies.

Author's declaration

I confirm that this thesis is the result of my own work with the following exception of the reports detailed below. Additional material used in this thesis have been fully referenced and acknowledged throughout.

Chapter 2 is in part published as a book chapter in collaboration with one co-author. It was conceived by HT and JM, researched and written by HT; JM provided commentary, review and support.
Thackray, H., and McAlaney, J., 2017. Groups Online: Hacktivism and Social Protest. In *Psychological and Behavioral Examinations in Cyber Security*. 194-209. IGI Global.

Chapter 6 is in part published as a conference paper in collaboration with four co-authors. It was conceived by HT and JM and researched and written by HT; JM, JT, CR and HD provided commentary, review and support.
Thackray, H., Richardson, C., Dogan, H., Taylor, J. and McAlaney, J., 2017. Surveying the Hackers: The Challenges of Data Collection from a Secluded Community. In: 16th European Conference on Cyber Warfare and Security (ECCWS), 29 - 30 June 2017, Dublin, Ireland, 745-748.

Presentations by lead author:

- Thackray, H, McAlaney, J., Taylor, J. (2018). “Talking to hackers: A social psychological approach to improving Cybersecurity”, Presentation at Behavioural and Social Sciences in Security (BASS18), July, Lancaster, UK.
- Thackray, H., McAlaney, J., Dogan, H., Taylor, J., Richardson, C. (2017). “Challenge accepted: Data Collection from hacking communities”, Presentation at 22nd Annual CyberPsychology, CyberTherapy and Social Networking Conference (CYPSY22), 26th June, Wolverhampton, UK.
- Thackray, H., McAlaney, J., Dogan, H., Taylor, J., Richardson, C. (2016). “Social Psychology: An under-used tool in Cybersecurity”, Position Paper at 30th British Human Computer Interaction Conference, July, Bournemouth, UK.
- Thackray, H, McAlaney, J., Taylor, J. (2016). Anonymous Online Hacking Groups. Presentation at 3rd Interdisciplinary Network for Social Protest Research (INSPR) Conference, June, Cambridge, UK.

Published Papers and Articles:

- McAlaney, J., Thackray, H., Taylor, J. (2018). “Behaviour Change: Cybersecurity”, British Psychological Society.
- Sample, C., McAlaney, J., Bakdash, J. Z., Thackray, H. (2018). “A Cultural Exploration of the Social Media Manipulators”, in 17th European Conference on Cyber Warfare and Security (ECCWS), Oslo, Norway.
- Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., and Dale, J. (2017). “Teaching psychological principles to cybersecurity students,” in Proceedings of the IEEE Global Engineering Education Conference, Athens, Greece.
- Thackray, H., McAlaney, J., Dogan, H., Taylor, J., Richardson, C. (2017). "Hackers gonna hack: Data Collection from hacking communities", WIP Paper in 16th European Conference on Cyber Warfare and Security (ECCWS), Dublin, Ireland.
- McAlaney, J., Thackray, H., Taylor, J. (2016). “The social psychology of cybersecurity”, The Psychologist, Issue 29, 686-689.

Poster Presentations:

- Thackray, H. (2016). Anonymous Online Hacking: From a Social Psychology perspective. Poster at The Faculty of Science and Technology's Second Annual PGR Conference 2016, May, Bournemouth, UK.

- Thackray, H. (2016). Anonymous: Online group processes, social identity and cybersecurity. Poster at Bournemouth University 8th Annual Post Graduate Conference, March, Bournemouth, UK.

Hacking Conventions:

- Thackray, H (2018). “Can’t hack, love to lurk: Sharing academic research”, Presentation at SteelCon, July 2018, Sheffield, UK.
- Thackray, H (2017). “Hackers gonna hack: But do they know why?” Presentation in the Social Engineering Village, DefCon25 Hacker Convention, July 2017, Las Vegas, USA.
- Attended BruCon, October 2016, Ghent, Belgium.
- Attended Hacktivity, October 2016, Budapest, Hungary.
- Attended DefCon24 Hacker Convention, August 2016, Las Vegas, USA.

Contents

List of Figures

List of Tables

Acknowledgements

I would like to thank all the individuals involved in the hacking communities for their participation in the surveys and interviews, especially those who have continued to support my work, and helped me get results of the best possible quality.

My sincerest gratitude to Bournemouth University for giving me this opportunity. I would like to thank the Bournemouth University Psychology and Computing departments, especially my supervisors, Associate Professor Jacqui Taylor, Dr Christopher Richardson, and Dr Huseyin Dogan, for their expertise and insights which improved my work, as well as their continued support and encouragement. Thank you to the P104 PhD Students, past and present, for the tea breaks, moral support, and general hijinks. Above all I need to express my eternal gratitude to my main supervisor Dr John McAlaney, for guiding me with patience and humour through my PhD journey. Your input and advice were invaluable, thank you.

I would like to thank my excellent friends Leah Thomas, Dr Jennifer Mark, and Rachel Parisot for their long-distance encouragement - thank you for being my personal cheerleaders, always there to reassure and re-motivate me, and for your eternal patience listening to me talk about my “ugly baby”. Thank you to my partner Oliver Worley for his unwavering support and ability to make me laugh, and for the numerous occasions he has restored my confidence and belief in myself. You joined me part way through this journey, and I know you will be with me on all others to come.

Last but not least, I would like to thank my family. Those no longer with me: my grandparents, Leslie and Maisie Thackray, who always encouraged my reading and thinking, I hope you know somehow that your love of learning has helped me get to where I am. Ron Hayler, I simply wouldn’t be who I am without you. Thank you for constantly challenging me, always encouraging me to think critically, introducing me to the weird and wonderful world of online communities, and especially for all the glorious happy memories. I miss you every day and I hope you are pleased my stubbornness has finally come in useful.

To Jean Hayler, thank you for helping to raise me, and for being a tiger who would always fight my corner, it meant the world. To my siblings, Katie and Alex Thackray: I cannot imagine life without you. Thank you for loving and supporting me through this, with tough love and a dose of reality when needed. I hope I make you proud.

And finally, my mother, Margaret Thackray. I could not ask for a better parent or role model; your wit and wisdom have always inspired and entertained me, and your kindness and humour meant that I could grow into myself with the knowledge that I will always be loved and accepted as I am. You are one of the best, most intelligent people I know; everything I achieve in life is due to your hard work and love. Thank you for your unconditional love and support for everything I do.

Chapter 1: Introduction

Online groups can be a significant part of everyday life for those with internet access; there are many forums, networks, and communities all offering companionship, support, and information, ranging from general forums or social networks, to those dedicated to specific activities or problems. This research was concerned exclusively with those forums and networks created around hacking. Social psychology examines human behaviour, which can be seen to change depending on the social setting or group; and there is evidence to suggest the social psychological influence of others on the behaviour of individuals transfers to the online domain (Beenen et al, 2004; Hsu and Lin, 2008). The purpose of this research is to investigate the effect of the group processes upon the members within these hacking communities; this includes the process and categorisation of social identity formed by the individual. This chapter will provide context on the area under investigation and explain the need for, and the purpose of, the research.

1.1 Problem Overview

The ease with which one can find like-minded people and interest groups through the internet has often been stated as positive motivation in its use (Shah et al, 2001; Teo et al, 1999). Despite its long existence however, the norms and rules of the online world are still evolving; these are shaped not only by nation state legislation, or global corporation policies, but also by individuals coming together within online groups. One of the invaluable contributions from both cyber psychology and social psychology is that both fields highlight the importance of not only what is said but also how it is said (McMahon, 2016). Whilst there are those that argue online communication suffers (Suler, 2004) due to the loss of visual face-to-face clues and prompts regarding “how” things are communicated, this is where the group identity, language, and norms all assert themselves (Dobusch and Schoeneborn, 2015). It is argued that a better understanding of the factors behind individual and group behaviour online would allow these expected norms to be clearly defined for all users (Attrill, 2015).

Spread across many different forums and websites, old and new, there exists a veteran community of those interested in computer hacking. The literature review in Chapter 2 will discuss the various arguments and definitions surrounding the word and its connotations; however, concerning the community involved in this research, hacking is a topic for computing and technology enthusiasts who want to learn more about how things work. Regardless of legal or moral status of the methods involved, to hack is to find a new or improved way to use technology. Indeed, the hacking

community have been involved in the computer and the internet since their inceptions, and many would argue without hackers we would not have the technological capabilities that we have today (Levy, 2010).

Despite the existence of online hobby forums and online groups for several decades, outside of marketing and health related fields (Shiao and Luo, 2012), there is currently little psychological research into the social and group influences on behaviour and motivation when individuals act online as part of a group. As more individuals become involved in online communities, the potential for influence within these groups grows; as does the potential for manipulation. Identifying the social psychological processes that influence members of online groups and communities allows insight to the ways in which these collectives interact and perceive themselves, and how this in turn affects the actions of the groups and individuals. Within the context of hacking communities, this information would be invaluable for both security and social improvement. It would also help to combat the conflation of "hacker", with "cybercriminal" or "cracker", and the negative stereotypes that are often reported via media outlets (Blue, 2016; Chandler, 2006; Tynan, 2016; Vegh, 2002).

That there are hackers who pose cybersecurity threats is not in doubt; it is, however, difficult to ascertain the true level of threat from an individual hacker as an attack vector. It has been reported that the accurate attribution of the attacks to individual hackers is challenging but it is slowly evolving past the binary concept of solvable or unsolvable (Rid and Buchanan, 2015). It has also been argued that security and antivirus companies have a vested interest in overstating the size of the problem (Dupont et al, 2016; Tynan, 2016); and it is thought that many cyberattacks go unreported, to protect a company or organisations reputation (The Economist, 2016). The reporting of these attacks is an important element of impression management for both the attackers and victims; attackers gain status from their successful strike; victims can be affected in terms of reputation and loss of profits or customers, as seen with the TalkTalk hacks in 2015 (Farrell, 2016). When the attacks are reported, there then follow the problems for attribution (Rid and Buchanan, 2015).

Whilst there is existing research into the online anonymous communities (Bernstein et al, 2011; Fogel and Nehmad, 2009), online communal identities (Sun et al, 2014), and their mobilization to collective action (Postmes and Brunsting, 2002), these researchers have been focussed on the use of the internet as a medium. Recent articles on hacking and hacktivism (Goode, 2015; Tanczer, 2015; Turgeman-Goldschmidt, 2008) focus on the role of the individual or ideological perspectives, rather than the group and the effect on their actions. There is plenty of relevant and informative sociological research into the identities and communities which have developed alongside and within hacking (Anderson, 1991; Castells, 1996; Jordan and Taylor, 1998; Turkle, 1984), and

cyberpsychological research on hacking as a phenomenon (Attrill, 2015; Papadimitriou, 2009; Power and Kirwan, 2014) but there does not appear to be psychological research into the social influence and processes within these groups or arising from these shared identities.

The overuse of “hackers” as the pejorative by the media in these situations has meant that there is a warped perception (Blue, 2016; Chandler, 2006; Tynan, 2016; Vegh, 2002). The hacking community has seen the rise and decline of “hacktivism” as a subcategory of hacking, where people use online resources to express their dissatisfaction with elements of political and social reality. Whilst there are many who see this as a threat, social protest and change have always been a part of society (Scheuerman, 2016; Schrock, 2016), and it has been argued that hacktivism is the progression of social protest (Kubitschko, 2015; Postill, 2014).

This research also highlights that not only can hacking communities be a positive space, but that the boundaries between cybersecurity professionals and hackers are not always distinct, nor are their methods greatly different (Bojarski, 2015; Jordan and Taylor, 1998). There are various instances of “reformed” hackers being employed in information security (InfoSec) roles or taking part in activities such as state sponsored hacking or penetration testing (pen-testing) for defensive improvement to computing for businesses.

It has been suggested that some individuals, often adolescents and young adults, become involved in the activities of hacking or hacktivism groups associated with cybersecurity incidents without a clear understanding of the risks involved (Olsen, 2012; Wolfradt and Doll, 2001). This involvement and arrest of adolescents and young adults has continued with events such as the TalkTalk hack (Farrell, 2016) and the hacking collective “Crackas with Attitude” (Whitehead, 2016). It is now recognised that cybercrime is a societal issue, with the UK’s National Crime Agency’s launching a campaign to educate young people about the dangers of getting involved in cybercrime (NCA, 2016). There is currently a strong emphasis on teaching coding, programming and further computer skills in the UK. When teaching individuals’ skills that are essential in cyber hacking (regardless of intention), it is also necessary to inform the individuals about the risks and consequences of their actions online. Social psychology is arguably best for research where it can help to highlight mistakes in interpretation, which could otherwise lead to underestimating risk or creating unnecessary tensions between groups.

The highly publicised hacking exploits of collectives such as Anonymous and LulzSec, as well as the political focus on cybercrime and whistle-blowers, has led to a change in the way that online anonymous groups operate. Research into hacking has always been a challenge due to its private and secretive nature, but increased awareness of observation and the overt presence of law

enforcement online have made potential participants even more wary of talking to strangers on the internet. Through participant observation a certain amount of activity can be recorded, such as tracking users through their online name. Group members do use tactics such as sharing user names to avoid being tracked in this manner. It would be difficult to be certain of what is genuine and what is exaggeration or boasting. Misleading information is now a recognised method of protecting personal information, especially in teens and young adults (Davis and James, 2013).

This research concurs that there needs to be an acceptance within cybersecurity of the importance and significance of human behaviour when using and developing cybersecurity technology (Pfleeger and Caputo, 2012). Whilst cybercrime is a growing concern, with hacking a common exploit, it could be argued that the positive role of these online communities has been overlooked. Some individuals use their hacking skills and knowledge to become cybercriminals, but there are also those who enjoy hacking as a pastime, a career, or a way of making positive changes in the world. The misperception of hackers as solely consisting of cybercriminals is a damaging and false categorisation; with the lack of insight into online communities, this is a classification error which risks alienating a capable and engaged community. By identifying significant elements of the group process within hacking communities, this research can lead to positive developments for both global cybersecurity and those who identify as hackers; for example, a reduction in the criminalisation of new members who are curious and exploring, encouraging their interest and skills via legitimate routes. The findings of this research could aid and inform future state policy decisions, specifically regarding the ways in which online collectives are treated and cyberattacks are handled and resolved.

1.2 Research Context and Scope

The central aim of this research is to investigate the group processes and social identities within online hacking communities. Through examining these communities, the groups' processes will be identified. These will then be investigated for potential influence on individual actions, as well as when acting or communicating as a group. Processes include: trust and the impact of breaches of trust within the community, decision making with personal and group norms, and risk taking on individuals and groups. The results should provide insight into the influence and function of group processes in an online setting, the impact of anonymity and the potential disinhibition in the online setting, as well as member awareness of the group influence. The findings will be used to suggest amendments and improvements to legal policy with regards to the use of the internet. These results may also be relevant to educational purposes; to ensure members of online communities are aware and make informed decisions online, to educate the general public to the risks of cybersecurity and to combat harmful stereotypes of hackers. The exploratory methodology developed within this

research will be able to provide a useful foundation for further investigation into online and difficult to access communities.

1.2.1 Aims and Objectives

This aims of this research are to:

1) Ascertain how accurate and reliable the hacker social identity is currently. This includes analysis of the hacker subcategories according to Social Identity Theory (SIT) (Tajfel, 1974) and Social Categorisation Theory (SCT) (Turner, 1985).

Data on what constitutes the hacker identity will be gathered from the literature review and the participant observation; this will include shared beliefs based on the hacker ethic, and the social norms of the group. The data from both sets will be integrated, and the evaluation of the hacker social identity will be presented in the conclusion of Chapter 4 and then compared to the results from the studies carried out in this research in order to establish if there are strong links between the previous observed identity and the self-reported identity. Hacker subcategories will be clearly defined and variations in the social identities will be noted. SIT and SCT will be applied to the data to examine the process of self-identification within this community. It is anticipated that the stages of SIT and SCT will still be applicable within the online community. See section 1.3 below for social identity definition.

2) Determine to what extent is there an observable effect of group process within hacking communities. Processes considered include group norms, influence, groupthink, conflict, and trust.

The above group processes will be identified through the participant observations; this data will be combined with self-reported data from the online surveys and interviews (Studies 1, 2, and3). Evidence of the processes and behaviours will be analysed and summarised in each data chapter discussion. The presence of these processes will be reviewed in terms of potential and observable effect on individuals.

3) Assess the level of awareness within hacking communities of the potential influences in online groups, especially in vulnerable members, and examples of informed behaviour online.

This will primarily be assessed through participant observations, online and offline. Age is an initial consideration in classifying vulnerable members; the data from studies 1, 2, and 3 will be examined for evidence of awareness and influence by members. Informed behaviour, regarded as acting with

knowledge and acceptance of consequences (e.g. in relation to law breaking and enforcement), will be further defined from secondary sources and then combined with the datasets; there will be recommendations in Chapter 8.

4) Clarify the relevance of hacking related activity for cybersecurity development; Is there potential to develop mitigation and prevention techniques from cyberattacks? Is there evidence of a strong link between hacking communities and cyberattacks?

There is no dispute that hacking leads to cyberattacks; the role of the community however will be examined. Discussions online will be observed to investigate if there is common instigation to commit cybercrimes in standard forum conversations.

1.2.2 Research Ethics

Bournemouth University's Research Ethics e-module and an Ethics Checklist were completed and approved for every element of research. The ethics for the pilot study, participant observation, and studies 1, 2, and 3, were all separately approved by Bournemouth University (see Appendix 9.1). All studies had an information sheet detailing the purpose of this research.

There was some initial concern in the ethical approval submission, due to the community under investigation. Standard participant information sheets, necessary for ethical approval, require the name and signature of the participant. This was obviously not an option in a community that is very secretive and private and may have on occasion broken the law in their respective country. Preserving their anonymity was of the upmost importance; for this reason, the information sheets on the online surveys stated that submission of the surveys would constitute informed consent. With the interviews, participants were sent the information sheets in advance of the interview, and at the beginning of the interview they were asked verbally to confirm that they had read and understood them, and that they gave consent for their data to be used; this was asked again at the end of the interview.

Further ethical considerations are discussed in Chapters 4-8.

1.3 Key Terminology

This section introduces and defines some of the key terms used.

Website and forum communities

These were the bases for observing online interactions between individuals involved in hacking related activities. This research emphasises that the activities may or may not include illegal hacking.

Online behaviour

Building on previous research, this research looked for examples of online behaviour that is comparable to or divergent from offline behaviour in similar situations. This comparison was aided by observations made in person at conventions and conferences related to hacking and information security. Previous research includes online disinhibition and cognitive dissonance. Online behaviour is linked to the group processes investigated.

Social Identity

Social identity refers to the individual self-concept which is formed from involvement, or perceived involvement, in a relevant social group (Turner and Oakes, 1986). There is a strong social identity within hacking, with various subcategories. This supports Social Categorisation Theory and Social Identity Theory. Categories people submit themselves to appear to have to meet certain criteria: ethical or moral justification; rebellious and anarchistic tendencies; or alternatively a cynical, almost "laissez faire" attitude.

Group processes

Evidence of cohesion and conflict in group activities is clear. While decision making appeared to be on an individual basis there is the suspected influence of group in some cases. Others appeared to be rebelling against perceived group norm, whilst remaining within bounds of group rules, or else they were banned.

Trust online

There is an examination of what does or does not prompt trust or distrust within these communities. Well written and informed posts gain a far more favourable response in InfoSec and general hacking forums, however in the more immoral/illegal areas this appears less important for members; this is possibly due to the nature of the website, where trusting others would be regarded as naïve or stupid.

Cybersecurity impact

This research reinforces that even security experts can be vulnerable. The steps they take can easily be taken by members of the public and average users, but awareness needs to be raised. Even experienced security practitioners reach security fatigue, it is accepted that one can never be entirely secure. There was a significant portion of participants who felt that privacy online was gone, exchanged for a concept of security that was not going to be achieved.

1.4 Thesis structure

This thesis consists of an introduction (Chapter 1), followed by a literature review (Chapter 2), and the methodology (Chapter 3); there are then four data chapters each addressing a stage of data collection (Chapters 4-7). Each data chapter will contain its own discrete introduction, methods, results and discussion sections. Chapter conclusions will be linked in a final discussion (Chapter 8). An outline of structure and chapter content is given below.

Chapter 1: Introduction. This chapter will provide an overview on the research topic and demonstrate why this research is needed. It will introduce the areas of online groups and the hacking communities.

Chapter 2: Literature Review. This chapter will explore in more detail the existing research on hackers, and the community relationship to cybersecurity. It will then describe the key aspects of social psychological investigation within this work including; social identity concepts and theories; group processes applicable to this research; and trust models and theories.

Chapter 3: Methodology. This chapter outlines the research approach taken, the research design applied, and methods used. It explains the reasons for these choices, as well as the analysis employed.

Chapter 4-7: Data Chapters. These chapters examine the separate data collection methods. They explain the reasons for choices during the data collection in further detail, as well as the impact of these choices on the data analysis and interpretation. These chapters also discuss problems that were anticipated, prevented or experienced, and how they were dealt with. The results for each study are described and examined.

Chapter 8: Discussion and Conclusion. This chapter brings together the findings from the preceding data chapters. This chapter also uses the results to draw informed conclusions and relevant recommendations, both for further research and cooperative developments between the groups involved.

Chapter 2: Literature Review

This chapter will provide detailed background and context on the area under investigation. The literature review will begin by discussing the various meanings surrounding the term “hacker” and the extent of the existing literature, before introducing the subcategories that hackers divide themselves into. Although not the focal point of this research there is an introduction to hacktivism, discussing the different approaches used by hacktivist collectives. Then social identity is introduced, including the theories that will be applied to this research, followed by previous research on group processes, and finally trust.

The interdisciplinary nature of this project means there is a wealth of primary and secondary sources on relevant aspects across a wide range of related disciplines. For some concepts this means there are similar definitions from different fields, with different terms. Where appropriate these concepts have been identified, and the intended meaning clarified.

2.1 Hackers

The verb “to hack” has three main meanings given by the Oxford English Dictionary (2012):

1) In senses related to chopping, cutting, or striking

2) To engage in writing computer programmes or software, especially purely for personal satisfaction.

3) To manage, accomplish; to cope with; to tolerate.

This research is interested in the second type of hacking, relating to computers. Despite this definition the term ‘hacking’ is still debated between academics and the hacking collectives. Attempts at definitive categorisations of ‘hacker’ have been contentious, and the use has been observed to have evolved over the last couple of decades (Chandler, 1996). Turkle (1984) stated that a good hacker had to use three elements. The hack had to be: simple but impressive; use technical expertise; in opposition to the “rules” (be it legal, social or institutional). In the nineties “hack” developed less strict requirements, with a general consensus that it meant solving an issue within a piece of technology in an innovative manner, for enjoyment, to improve the technology, or to learn more (Raymond, 1996); hacking also grew to be simplistically represented as unauthorized access to computer systems or networks (Jordan and Taylor, 1998).

In recent years, “hacking” has spread, being used in everyday parlance in terms such as “life hacks” which simply means finding a quicker, cheaper, or simper way to do a task, unrelated to technology (O’Brien, 2004). With relation to computing and technology however, the term “hacking” has become pejorative both inside and outside of technology related communities and fields, unless explicitly stated (Chandler, 1996), with the common perception being that all hackers pose a national security threat (Halbert, 1997). The term is widely used to signify any criminal act using technology, especially by media sources; this research however emphasises the different types of cyberassailant, in addition to the hacking community (see Table 1).

(Computer) Hacker	One with the ability to access a computer or system without admission (Raymond, 1996).
Cybercriminal	A criminal who uses a computer or network to commit the crime (Anderson et al, 2013, Halder and Jaishankar, 2011, Moore, 2005, NCA, 2016)
Cyberterrorist	One who uses computer/network technology to terrorise opponents to further political or social objectives (Rogers, 2003).
Cyber delinquent	One who engages in illegal behaviours, such as verbal violence, hacking, and illegal copying of software in online environments (Hong and Kim, 2011).

Table 1: Cyber Definitions

Skibell (2002) however states that computer hackers are more a myth than reality, as few computer hackers possess sufficient skills or desire to commit more than crimes of inconvenience, such as those carried out for the “lulz”. “Lulz” is a corruption of the term “lol” which was used to communicate that the author was “laughing out loud” in response to something; “lulz” signifies something that is purely for the purposes of entertainment and amusement, e.g. “I did it for the lulz”.

There are various studies on the motivations of hackers, ranging from financial gain, prestige, curiosity (Seebruck, 2015) as well as the motivations that drive individuals to find online groups and activities in the first instance, such as traditional bullying or isolation (Hay, Meldrum and Mann, 2010). This is not a new concept for hackers however, who have regarded antiauthoritarian tendencies to have merit, and have positioned themselves, in their thoughts at least, as "positive deviants" regardless of their specific practices as hackers (Turgeman-Goldschmidt, 2008). Previous research has demonstrated that hackers have a distinct image, the imagined identity that unites them, even if they never meet in the physical world (Jordan and Taylor, 1998). Within this however, there are differences between the subcategories; these are classified depending on their areas of interest and behaviour patterns (Voiskounsky and Smyslova, 2003). The problem with the term "hacker" can be attributed to the fuzzy definition of the term, and the ambiguous borders that

separate computer experts and hackers (Jordan and Taylor, 1998), as well as those characteristics of the subgroups (Turgeman-Goldschmidt, 2008).

Within this research “hacking” is understood to signify an umbrella term, covering many different types of hacking (Rogers, 2010), in the same way that “sport” signifies a variety of games and physical activities. The various types of hacking all appear to have their own values and interpretations of the purpose of hacking. Hacking has long been associated with “intellectual curiosity and fascination with the technology” (Bissett and Shipton, 1999:904) which is evident on every forum. There also remains the 'anti-authority impulse' (Kirwan and Power, 2013), which was noted even in the early days of hacking (Levy, 2010), although it is argued that this has moved from hacking to hacktivism (discussed in section 2.1.1.1). Hacking, as this umbrella term then, is used to denote the ability to access and alter the networks and computers of others, without being given admission, although not always without permission (Raymond, 1996). Raymond goes on to state that hacking is undertaken for the purpose of finding flaws or weaknesses, but not exploiting them; this is supported by the survey data from this research, discussed in Chapter 5. Despite the wealth of research on hackers, the social psychology of these communities has not been addressed, with focus being on cybercrime prevention and motivation in hacking; this research aims to provide more context on the group influence, as well as a psychological perspective.

2.1.1 Typologies

Typologies for hackers have been created and updated throughout the history of the term (Chantler, 1996; Landreth, 1985; Seebruck, 2015; Taylor, 1999). Table 2 gives the names and simple definitions of the subcategories commonly used and which are used in this research. It is acknowledged that there are other smaller more specific subcategories, but that level of detail was impractical for the scope of this research.

Sub-Category	Definition
White-Hat Hacker	A hacker who uses legal and ethical methods; can also be referred to as ethical hackers
Grey-Hat Hacker	A hacker who uses both Black and White -hat methods
Black-Hat Hacker	A hacker who uses illegal and unethical methods; can also be referred to as crackers
Cracker	One who access the systems to damage or exploit weaknesses, often for financial gain (Raymond, 1996, Smith and Rupp, 2002)
Script Kiddie (Skid)	A novice hacker, who primarily downloads and uses tools designed by others (Nissenbaum, 2004)
Elite Hacker	A hacker whose skill and expertise is recognised by other skilled expert hackers
Hacktivist	Those with social and ideological motivations in the hacking they conduct (Seebruck, 2015)
Cyberpunk	A hacker who identifies with the cyberpunk ideology and aesthetic, based on sci-fiction writing

Table 2: Hacker Subcategory Definitions

Madarie (2017) stated that focusing only on hackers with destructive intents is unhelpful and lacks insight to these communities, supporting the fact that it is often neglected that hackers form heterogeneous communities (Barber, 2001). There is positive change evident, with the propensity to categorise hackers as either 'good' or 'bad' lessening, highlighted by the the growth of less binary and simplistic categories, such as hacktivists and script kiddies. Madarie (2017) argues that the current classifications are based more on the individual's motivation or intent but warns that there remains the inclination to classify hackers as malicious or non-malicious, since such classifications are often meant to assist in criminal profiling (Meyers, 2009; Rogers, 2006; Smith and Rupp, 2002). Similarly, it is being recognised that even in the cybercriminal community, not all members are equal in category (Benjamin et al, 2016); their study recognised that there are varying levels of cybercriminal capability, knowledge, and interest among those that frequent the relevant forums. Some individuals have little to no skill and may only be there from curiosity, whilst other more established members ingrain themselves (Benjamin et al, 2016); generalised negative perceptions from "outsiders" could have the impact of pushing those who are merely curious into action in order to feel they belong to a social group (Marques and Paez, 1994).

Zhang et al (2015) examined the behaviours in knowledge exchange when classifying hackers. The fuction of knowledge acquisition and knowledge provision allowed them to classify observed hackers into four types: guru hackers, who are knowledgeable and respected and share ideas; casual hackers, who act as observers; learning hackers, who seek knowledge and share more over time; and novice hackers, who are new learners (Zhang et al 2015). The overall conclusion rached by

Zhang et al was that hacker communities very much represent learning communities where meritocracy is in place (2015).

2.1.1.1 Hacktivism Groups

Originally a key point of interest within this research was the effect of group processes within hacktivism; however, the decline of open participation and relectuance of those previously involved to discuss their roles meant that this subcategory became impossible to reach. It is however still an important distinction and subcategory within hacking, raising the profile of both hacking and cybersecurity, and so the background and examples of two groups will be discussed in this section.

Recent hacker typologies have included the increase in social and ideological motivations in hacking, incorporating those who are seen as 'hacktivists', a combination of 'hacker' and 'activist' (Hampson, 2012, Krapp, 2005). This growth of social and ideological motivations has been attributed in part to the fact that a generation has been raised in a time of digital evolution and innovation (Seebruck, 2015), with increased user-generated content and unrestrained communication increasing the confidence and perception of the power that individuals possess. Mass social movements were historically regarded as being negatively influenced by personal elements of self-esteem or satisfaction with life. It was believed that personality attributes such as "impotence, selfishness and boredom characterised the…individuals prone to join mass movements" (Travaligno, 2014:5). In the 20th century however, with the closer study of such movements, and the growth in popularity and public support, these activities became regarded as more of a symptom that something was wrong in society (Travaligno, 2014), for example the movements for civil rights and anti-war protests in the USA. These periods emphasised the differences between the academic explanations for mass social movements, and the reality that was being witnessed. These significant contributions marked the departure from classic views of masses and crowds as irrational and disorganised (Gamson, 1975; Jenkins, 1985; cited in Travaligno, 2014). In fact, there developed socio-psychological models which showed that social movements were "more likely to emerge under conditions of structural stability, social connectedness and favourable mobilisation of resources" (Travaligno, 2014:5). Protesters came to be understood as rational actors, who weighed the cost and benefit of participating in such protests (Travaligno, 2014). As such, it has been assumed that those involved in social movements, including hacktivism, will be equally rational actors.

Within hacktivist groups, the entry requirements do not entail elite computing knowledge, and those wanting to participate in hacking and hacktivism now can find multiple resources in seconds through search engines; it is similarly quick and easy to download computing tools written by others. Groups like Anonymous have been proponents of such techniques, making it simpler for people to be

involved, and using strength in numbers rather than a smaller group of experts. The forms of hacktivist groups are dictated by the medium used; the internet allows them to exist in a decentralised "community without structure" (Leach, 2009:1059). As such, the most common feature across different groups is a consensus-based based approach to their activities. For the most part this means that through necessity hacktivist groupings are still relatively small and regulated by trust and loyalty (Milan and Atton, 2015).

One example of a hacking group that partakes in hacktivism is The Chaos Computer Club (CCC), Europe's oldest and one of the world's largest hacker organizations. Whilst not directly addressed in the research, the CCC is mentioned as an example of a hacking group, one with a very different approach to the one made popular by the hacktivist group Anonymous, described below. The CCC has long aimed to legitimise its presence and use this in a positive way. Created via a newspaper advert in 1981, the CCC started as a loose group of individuals, but formally became a not-for profit association in 1984, with continued interactions with institutions and political organisations (Kubitschko, 2015). This active decision to remain legal in the face of "anti-hacking" government legislation is one of the most interesting elements about this group. The group describes itself as a non-governmental, non-partisan, not-for-profit, and voluntary-based club that is sustained by membership fees and donations (Kubitschko, 2015). The CCC supports the principles hacker ethic (Levy, 2010) which stresses openness, sharing, decentralization, free access to computers and world improvement, as well as advocating more transparency in government, communication as a human right (Coleman, 2011, Kubitschko, 2015, Nissenbaum, 2004). What makes the CCC significantly different to other hacker collectives is not their political dimension but their insistence on working as a legitimately recognised collective, even if they use illegitimate methods. One of the Club's aims is to teach the public to use technological skills and bring about political change. The group has been involved in hacks which have either been a Grey are or clearly illegal; this led to a period of decline in popularity in the 1990s. Within this group there appears to be the need to continue their legitimacy within the state of Germany, which struggled when members were conflicted about the group methods. It is emphasised that the CCC has a reputation for expertise, which they believe needs to be brought to the established centres of power by engaging with politicians, legislators and judges, (Kubitschko, 2015), because for the CCC, hacktivism is only one part of their purpose (Coleman, 2014, Kubischko, 2015). Despite the fascinating presence of this group, it was not actively included in this research as the organisation of these formal groups was not the focus of the research; however, its aims and procedures make it a potential model for other hacking communities to be formally recognised by their home nation state.

Another example, and possibly the most infamous hacktivist group, is the one known as Anonymous. With its origins on 4chan, the group started by pranking and "trolling" other online (and offline) communities, for entertainment. Over time this evolved into people trying to use this group activity for "good" causes. This eventually led to a division in the group; those who wanted to prank and enjoy the "lulz", and those who wanted to be "White knights" (see Coleman (2014) for more details). As participation within Anonymous became more about political and social causes, rather than just mischief making, many of those who became involved in hacktivism cited their motivation as a desire to counteract the increase in surveillance and repression of such activities (Coleman, 2014, Douglas et al, 2017). Anonymous has frequently used these motivations as a recruitment tactic, manipulating publicity, both negative and positive, to draw attention and support. This policy however has attracted criticism, due to the imprisonment of a number of hacktivists who took part in large operations, as well as a general lack of transparency and poor accountability from the group (Douglas et al, 2017). This is an example of the problems in hacktivism where groups, Anonymous especially, have always maintained that they do not have leaders and hierarchy (Coleman, 2014). The hacks or "operations" carried out by Anonymous have ranged from simple pranks to serious on-going campaigns. For the past few years, the name or brand has almost exclusively been used for hacktivism; those who claim Anonymous involvement in causes that do not meet the criteria have been denounced publicly, often through official Twitter accounts. This has in turn led to a lot of in fighting, as some argue that there are no leaders, therefore no one can decide who is or is not a member of Anonymous. One of the methods the group uses to monitor, and control group membership is assertive speech; it is the mode of communication not the speaker that matters; therefore, by using and maintaining control via social media accounts, this is how they get the message across to others. The group has also been noted for their controversial control of group identity and have doxed individuals (revealing their real-life identity and personal information), revoking their Anonymous membership (Dobusch and Schoeneborn, 2015). Anonymous are a contentious topic; some members feel they made serious contributions to bringing hacktivism to the fore of current activism and protest, other commentator and critics feel it was a group of children and "wannabes" causing trouble. Regardless of which argument is supported, it cannot be denied that Anonymous did draw attention and awareness to the importance of Cybersecurity.

"Anonymous" is now regarded as a general hacktivism collective for whoever wishes to use the name/identity, rather than denoting a specific group. There has been little objective evidence about hacking groups such as Anonymous but in recent years their notoriety and influence have decreased dramatically. The cohesiveness of newer hacking collectives was affected in 2012 by the exposure of a high profile member of Lulzsec, Sabu, as having been an informant for the FBI. His information led

to the arrests of prominent group members in the USA, the UK and Ireland. There have been significant changes to the group behaviours since (Coleman, 2015), with greater antipathy of 'leader-fags', or those wanting to take charge, suspicion of new or unknown members, and of any one who seems to be desiring attention. This is again despite repeated claims from groups such as Anonymous that they do not have an official leader or hierarchy (Coleman, 2014); this may or may not be the case, but regardless it is relevant that many members of such collectives believe this to be true, which potentially leaves them open to manipulation. After all, the creation of the internet was heavily influenced by those who wished to see technology move towards a "decentralised, and non-hierarchical version of society," (Rosenzweig, 1998:1552), and so those that follow these ideals may prefer to believe that a non-hierarchy has been achieved, a form of confirmation bias. It cannot be assumed that there is a complete lack of hierarchy in these communities, as there are obvious examples, especially in forums or Internet-Relay Chat (IRC) channels where it is necessary for administrators to moderate the content submitted by users (Dupont et al, 2016, Uitermark, 2016).

This does not mean that hacktivism has diminished entirely however, more that people are working in smaller groups and projects to achieve their aims and attempting to gain legal recognition and protection for forms of "digital protest" or for awareness raising: one example is the use of the multiplayer online role-playing game World of Warcraft (WoW) to transform an off-line event—the Race for the Cure, to benefit breast cancer charities—into an online event called the Running of the Gnomes (Collister, 2017); this is an example of disruptive civil disobedience including elements of hacktivism. Though the event follows the game's rules, the mass collective action of the Running of the Gnomes disrupts the player experience, inundating the game's chat with messages about breast cancer, and disrupts the game by crashing the server through the sheer volume of player participation. This disruption has been embraced as an integral part of the event (Collister, 2017). This is an example of the successful non-destructive hacktivism being integrated into the online world. Despite the high profile arrests of those involved in hacktivism in previous years (Coleman, 2014) Solomon states that the pervasive use of technology has led hacktivists to regard it as an effective mode of available protest in the modern world, despite the fact that there is no legal distinction between hacking and hacktivism (Solomon, 2017).

2.1.2 The Black – White Spectrum

This research posits that the traditional "hacker" identity has usually been assigned to the middle of a spectrum from Black to White -hat. The extremes of the spectrums can include hackers, but these can equally be assigned other applicable labels, such as cybercriminal (Black), and cybersecurity (White) leaving hacker to its ambiguous nature (see Figure 1).

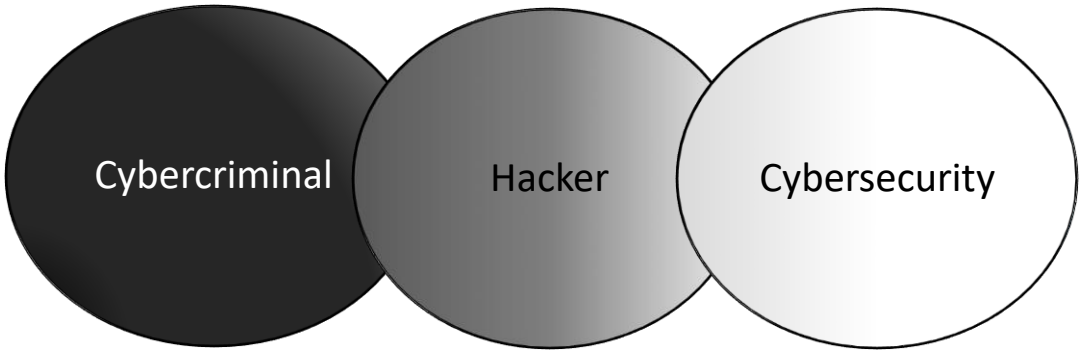

Figure 1: Hacking Spectrum

This researcher, for the purposes of clarity, designed this basic Venn diagram (Figure 2) as a way of illustrating the Black to White -hat leanings of the different subcategories. Whilst this would doubtless be contested, with individuals stating that they categorize themselves as one sub-group but belong to a different section in terms of morality or ethics, this is a broad depiction of the assumed spaces in this study.

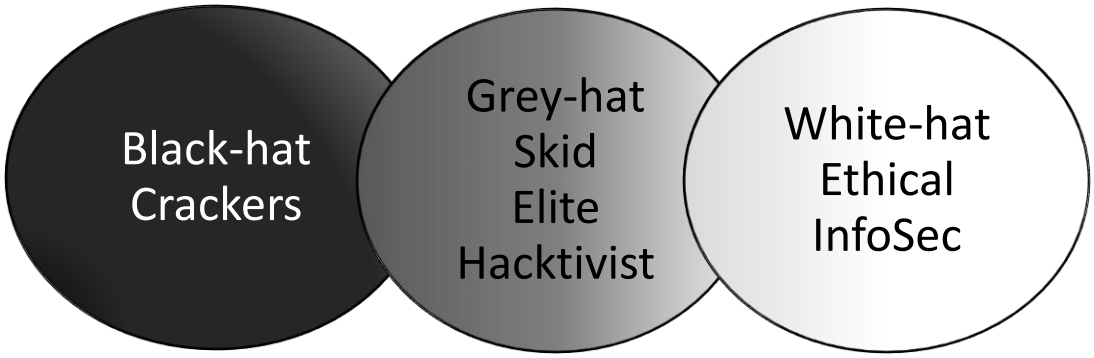

Figure 2: Assumed hacker subcategories on Black-White spectrum approach

Within this research, Crackers have been classified not as hackers but as a separate category, those who are destructive rather than constructive (Raymond, 2011). Although forums relating to cracking were included in the research, there was limited response and this subgroup was not actively pursued. The traditional view of the relationship between hackers and cybersecurity has been one of perpetrators versus defenders. This assessment however neglects the obvious overlap between InfoSec professionals and hackers; the self-categorisation by individuals into one or the other aside, there are many traits that are shared between these two groups.

2.2 Social Identity

Identity is a concept that appears across many disciplines in social science; it is considering the “self” as a reflexive object which can be categorised, leading to how people define and consider themselves and others. There are many different applications of identity (e.g. political, national, cultural), but these can all be encapsulated within the concept of social identity. Stryker and Burke (2000) stated that there are three distinct uses of identity: firstly, to refer to the culture of people, e.g. ethnicity; secondly, to refer to common identification within a collective or social category, e.g. Social Identity Theory (Tajfel, 1974); and thirdly, to refer to the combined meanings that people attach to the multiple roles they play. Tajfel defined social identity as “the individual’s knowledge that he belongs to certain social groups together with some emotional and value significance to him of this group membership” (1972:292), and categorization as a method of giving order within the social environment.

Social identity denotes the connection between the self and the collective, allowing investigation of the “psychological processes that interact with and make possible the distinctive "group facts" of social life” (Turner et al, 1994:2). The social identity is also an individual’s definition of their position within the social system (Tajfel, 1974; Turner, 1975), distinct from personal identity, where interpersonal situations are governed by individual variables. Social identity can also be more inclusive to the individual’s perception of self; for example, categorising oneself as a "hacker" is more inclusive than "White-hat", allowing a larger group membership, but the “hacker” identity is less defined, leading to schisms and and subcategorisation.

Groups have a profound impact on the individual and their identity, with people’s concepts of who they are being influenced and shaped by the groups which they feel they belong to (Hogg et al, 2004). Tajfel et al (1971) stated that mere classification into a group is sufficient to create ingroup and outgroup behaviours, including favouritism and discrimination between the different groups, even if the groups are randomly assigned; this supports the previous research conducted by Sherif (1956). When individuals perceive themselves to be a part of certain categories or groups (self-categorization) it becomes a motivational element of their self-esteem; there is a need for that group to have positive identity (Stets and Burke, 2000). This can be achieved through social comparison with other groups (Turner, 1975). A key point made by Stryker and Burke (2000) is the importance of the comprehension that social identity can provide regarding the relationship between the self and society; the salient identity within the context or situation defines and dictates the individual’s behaviour, even if the presence of others is not actual, only implied or imagined (Allport et al, 1954).

2.2.1 The Social Identity Approach

The Social Identity approach utilised in this research incorporates Social Identity Theory (SIT) and Self-Categorization Theory (SCT), focussing on group processes and intergroup relations (Hornsey, 2008). Whilst there are similarities to the theories, they are separate and distinct; one of the key differences is their scope. SIT was fostered in order to explain the problems connected to intergroup relations, whereas SCT was more relevant to the group processes present, including stereotyping and group influence (Brown, 2000).

SIT can be summarised into three broad stages:

1) Categorisation: Individuals observe and define the appropriate behaviour for the group,
2) Social Identification: Individual adopts the group identity, creating their "in-group",
3) Social Comparison: Compare in-group with others ("out-groups"), often to emphasise positive characteristics of the in-group (Turner, 1975).

A key element of SIT is the hypothesis that the in-group will discriminate against an out-group, with real or perceived negative aspects of the out-group, in order to increase their self-esteem and self-image. This can only occur if the individual has progressed through all three stages in adopting the social identity of the in-group.

By contrast, SCT is concerned with how individuals categorize themselves, and how the change occurs where they categorize themselves more as their social groups and less as an individual. Whilst SCT evolved from the SIT research, it suggests that the basic ability of engaging in collective behaviour (group formation, social influence, stereotyping, etc.) is related to the important type of self-process, allowing individuals to modify or alter aspects of themselves in order to gain social acceptance (Turner et al, 1994). The group does not influence or modify the individual as a set of external social forces but is "an authentic expression of the self" (Turner et al, 1994:2); the individual internalises the group norms and acts accordingly. The key element for SCT is the hypothesis that as a shared social identity becomes more salient individuals tend to define and see themselves less as singular persons and more as the representatives of their social group. It can be described as the "subjective stereotyping of the self in terms of the relevant social categorization" (Turner et al, 1994:4). As such, observations will note any evidence of SIT and SCT within online and offline hacking communities and the behaviours of individuals.

2.2.2 Online Identity

When dealing with individuals and groups online, cybersecurity is often portrayed as both benefitting from and struggling with the lack of identity and prevailing use of anonymity (Crews,

2007). Since the inception of the internet, anonymity has always been a significant element of the networks. Zajacz (2013) suggests this was partially due to neglect in considering the importance of user identity; as it was used on a small scale, users were known to each other; therefore, nothing was put in place to ensure identification of users. Anonymity is now a highly disputed element of the internet, with some like the Electronic Frontier Foundation (https://www.eff.org/, 2018) seeing it as a fundamental right to be anonymous online, with others, such as law enforcement agencies, seeing it as a potential threat. Within cyber forensics there is the common assumption that only a complete redesign of the internet would allow reliable attribution following an attack (Rid and Buchanan, 2015). Online resources and communities have meant that people from all over the world can search for and join online groups based on their self-categorisation or self-identification that might not be available offline in their local community. It has been suggested by Bernstein et al (2011) that anonymity being available online may in fact foster stronger communal identity, supporting previous work by Tanis and Postmes (2005).

Whilst it is agreed that the internet has brought about change in social interaction, opinion is divided on whether this is positive or negative (Postmes and Brunsting, 2002; Shah et al, 2001; Turkle, 1984; Wellman et al, 2001). Using data from mail surveys conducted in 1999 Shal et al (2001) found that each generation and their social capital production is tied to the leading media source of that era (for example, internet use for Generation X, television use among Baby Boomers and newspaper use among the Civic Generation). Whilst this study is 15 years old now, the inclusion of a wide range of age groups highlighted the relevance of the dominant media, which is now the internet. A more recent study by Joiner et al (2013) supported the generational differences found, referring to new generation of technologically literate young people as "digital natives" (Joiner et al, 2013:549) who have developed with the technology. Postmes and Brunsting (2002) argue against the assumption that computers damage social ties (Turkle, 1999), stating to the contrary that the Internet "strengthens existing social movements, stimulates the formation of new ones, and mobilizes sizable numbers of people for collective action," (Postmes and Brunsting, 2002:294). It is therefore no surprise that groups and communities formed online can have substantial impact and meaning within a person's social identity and even their offline life.

It is known that hackers exist within social groups that provide expertise, support, and training within their communities (Jordan and Taylor, 1998:757). It is argued by the researcher that hackers as a community are no different from other social identity group, and that in this sense, are an "imagined community" (Anderson, 1983; Jordan and Taylor, 1998), where there is no physical or geographical connection within the shared identity, but it is a socially constructed community,

where the presence of others could be actual, perceived, or imagined (Allport et al, 1954). It should be noted that studies investigating unifying identity traits have emphasised that the "hacker" stereotypes may not be as reliable as once believed (Rogers, 2010; Tanczer, 2015); as this research will conclude in Chapter 8, the hacker identity has evolved.

Turkle believed that the online world was changing the way individuals think, "the form of our communities, our very identities," (1999:643). Whilst she was intending this as a criticism, this idea aligns with the concept of fluid identity, which could be viewed as a positive. Papadimitriou (2009) offers only simplistic motivations for hacking (dissatisfaction at work, or belief in free internet), however he highlights that whatever the motivations, it is clear that hacking raises "serious questions to our ethical, legal, political and social beliefs," (Papadimitriou, 2009:1331). He concludes by stating that there is fluid identity, an identity that changes and evolves, rather than a fixed or static identity that may be assigned (Howard, 2000). Although used both positively and negatively, fluid identity is becoming a more commonly accepted concept; these fluid identities are used throughout internet communities, and it is possible that this is how all social communities will develop (Papadimitriou, 2009). In this way, it could be argued that hackers are leading the way in slowly changing social norms, as well as assisting technological advances.

It should be noted, there is a wealth of studies relating to gender and the internet in this context (Joiner et al, 2013; Postmes and Spears, 2002); although these are significant and informative, gender is not the focus of this research, nor a variable being considered. If it is seen as significant by community members, this is included in the data. There will be observations on the impact of gender in Chapter 8 and discussed as appropriate in the data Chapters 4-7.

2.2.3 Online Disinhibition Effect

Alongside the debate surrounding anonymity is the concern that being online, as opposed to in physical real-world situations, effects the behaviour of individuals. Online disinhibition effect (ODE) is a term used to describe the reduction of psychological restraints, which often control behaviors in the online social environment (Joinson, 2007; Suler, 2004). It has been argued to have both positive and negative impacts. The scope of this research does not permit an indepth examination of the potential online disinhibition within hacking communities, however the observations will look for evidence of it; for these reasons a brief description is necessary.

Suler describes the positive aspects as "benign disinhibition" (2004). This disinhibition can allow individuals to share very personal things, revealing secrets and emotions that feel that they must otherwise conceal, with some individuals expressing relief after being able to share them (Lapidot-

Lefler and Barak, 2015). There are also acts of unusual kindness and generosity, with people sometimes going out of their way to help others with no personal connection (Suler, 2004; Lapidot-Lefler and Barak, 2015). The opposite to this is "toxic disinhibition" which leads to what is commonly known as online "trolling" behaviour, including rude language, harsh criticisms, anger, hatred, and threats against individuals (Suler, 2004). Toxic disinhibition also includes use of the internet for illegal or nefarious purposes that an individual might never consider in the offline world, such as using the "dark web" for various types of pornography, crime, and violence (Suler, 2004) which are often associated with the "dark" (mis)perception of the hacker identity.

The use of online communication reduces the potential negative consequences of social interactions, enabling people express themselves more easily (Lapidot-Lefler and Barak, 2015). Because of this Suler argues that some benign disinhibition is an indication that the individual is attempting to understand and develop themselves, using the internet and available communities to resolve their personal problems or explore new dimensions to one's identity (2004). In contrast, he suggests that toxic disinhibition may "simply be a blind catharsis, a fruitless repetition compulsion, and an acting out of unsavory needs without any personal growth at all" (Suler, 2004:321).

2.3 Group Processes

Group processes refer to the behaviours of group members as they collaborate and make decisions, deal with any problems, and achieve tasks, in groups of at least three members (Brown, 2000; Castellan, 2013). A group will develop their own norms, defined as "regularities in attitudes and behaviour that characterize a social group and differentiate it from other social groups" (Hogg and Reid, 2006:7). When involved in online communities, there are various processes that can influence the participation of the individual, including "social interaction ties, trust, norm of reciprocity, identification, shared vision and shared language" (Chiu et al, 2006:1872). There is also evidence that a lack of "individuating cues in group communication may lead individuals to shift their personal identity to group identity" (Xu and Lombard, 2017:153). This means that group members have the potential to exert social influence on individuals through the salient group identity or norms (Reicher, Spears, and Postmes, 1995; Spears and Postmes, 2015).

The identity and norms of a group can be highly affected by the cultural influences; a study examining deliquency (Harris-McKoy and Cui, 2013) highlighted the importance of considering cultural approaches when examining group behaviour. There has been a trend to place more importance on cognitive factors, looking at the cognitive influence on individual perception of risk, which has meant that cultural and social influences are sometimes neglected. For example, Eastern

cultures stress group solidarity and relationships with other people; Western cultures emphasize the self and autonomy (Wright et al, 2015). Whilst it is not within the scope of this research to examine the global cultural affect, it is acknowledged that this research is highly western, and as such the emphasis is likely to be on the self, within the group identity.

Groupthink is another significant offline group phenomenon must be considered in the online group context (Packer, 2009). Janis (1972) defines groupthink as the psychological drive for consensus at any cost that suppresses is agreement and prevents the appraisal of alternatives in cohesive decision-making groups. He also identified the symptoms of Groupthink, which transpire when a group tries to make decisions. These include the illusion of invulnerability; collective rationalisation; stereotyped views of different groups; group pressure to conform; and self-censorship (Janis, 1972). Although groupthink does not always occur, it is more common when the groups are highly cohesive, especially in high-pressure situations. When there is pressure for agreement it has been found that group members can be more vulnerable to inaccurate and irrational thinking; as such decisions formed by groupthink have reduced probability of attaining successful outcomes (Janis, 1972).

The influence of such group processes has been seen in some hacktivist attempts, such as the manipulation of individuals in the case of the Paypal 14. In 2010 the hacktivist group Anonymous launched "Operation Payback[1]", part of which involved online anonymous group members being encouraged to download software called the Low Orbit Ion Cannon (LOIC) in order to carry out DDoS attacks, with little information given, as well as reassurance from other group members that this was a good and constructive action to take for the benefit of their cause. Of the many people that downloaded and used the software, 14 individuals were later tracked down by the FBI, arrested and prosecuted by the US government (Coleman, 2014).

There has also been documented evidence of the presence of attributes and biases in hacktivist groups. Confirmation bias is where people tend to seek information that is consistent with their current hypothesis and are unlikely to seek information expected to be inconsistent with it (Chapman and Johnson, 2002; Tsohou et al, 2015). This is sometimes seen in social movement behaviours where members will not look for external sources of information, trusting the other group members (as demonstrated in the Paypal 14 case). Confirmation bias is considered to be one of the most prominent biases affecting decision making (Kahneman et al., 2011). There are also

[1]Operation Payback was a hacktivist "op" in the military sense of the term, protesting the embargo, by Paypal and other finance companies, on donations to Wikileaks following the Snowden revelations (Coleman, 2014). Wikileaks is an international non-profit organisation that publishes secret information, news leaks, and classified media provided by anonymous sources.

many accounts from Anonymous members or former members having examples of optimism bias (Olsen, 2012, Coleman, 2014). Optimism bias leads individuals have a consistent belief that they are less at risk of experiencing a negative event themselves compared to others (Tsohou et al, 2015), therefore even if they did take part in an illegal activity they would be at less risk of being tracked by law enforcement agencies. This has been disproved through the arrests of those involved in Lulzsec, the PayPal 14, the TalkTalk hack, and Crackas with Attitude (Coleman, 2014, Farrell, 2016, Olsen, 2012, Whitehead, 2016). When recounting their individual experiences within the groups, the individuals stated that they were aware of the risk, aware that they were carrying out illegal actions but felt that they would not be caught, in part because they were aware of the risk and "it wouldn't happen to them" (Olsen, 2012, Coleman, 2014), as found in the study by Young et al (2007).

Festinger's (1962) cognitive dissonance theory suggests that there is a need for consistency between attitudes and behavior, the principle of cognitive consistency. If the dissonance is caused by behavior, the expectation is that the individual can change or eliminate the behavior; however, changing the behaviour can be problematic for people and so it is believed that an individual may instead alter or change their attitudes or beliefs, in order to justify the behaviour to themselves. Given the controversial nature of hacking activities, there is anticipated to be some evidence of alteration. Other social influences that may be of relevance in this research include informational social influence: when individuals voluntarily conform to group standards because they are uncertain about the correct answer or behaviour (Smith and Hogg, 2008). This comes from the desire to be correct and therefore more socially acceptable to others (Festinger, 1950), so people observe others for how they should behave and receive their information and news through the group. There is a tendency for people to rate the judgements of others as being more reliable than their own; this ensures that the individuals conform to the group view for the 'correct' answer. This in turn is linked to the normative influence, the pressure to conform to the norms of the group; whilst an individual might disagree with the group consensus, they will not say anything in order to remain in the group (Nail, 1986). If an opinion is expressed and others agree, this can often lead to stronger opinions being expressed. It has been found that whether people believe they are being watched by a larger group is an important factor, especially if there is perceived conflict between the groups, such as different aims. It has also been found that the salient social identity is the common strategy for self-enhancement , allowing individuals to achieve or maintain a sense of ingroup superiority relative to the outgroup. This may include feelings of ingroup pride and loyalty as well as derogatory attitudes toward outgroups (Hornsey and Hogg, 2000).

2.3.1 Intergroup behaviour

Intergroup attribution research (Branscombe and Wann, 1994; Cialdini et al, 1976; Hewstone and Jaspars, 1982; Tarrant and North, 2004) has shown that the achievements of group actions could strengthen individual members' beliefs that their group and members are highly skilled, while the success of opposing groups is attributable to external circumstances and luck. This may encourage online groups to carry out additional actions in hacktivism and against other cyber adversarial groups, especially if the group identity is reinforced by media reporting. It has been observed that early news reports about Anonymous generally exaggerated the cohesiveness between members and the organisational structure of the group (Olson, 2012), which then contributed to the group becoming more cohesive and organised. With regards to hacking, there is an expectation of intergroup behaviours that could lead to cooperation or conflict, depending on the subcategories involved.

As discussed in the online identity section, 2.1.2., identity can be fluid; for this reason, the groups formed around the identities might be better understood as fluid collectives (Dobusch and Schoeneborn, 2015, Papadimitriou, 2009) rather than traditional groups, without defining characteristics or rules that must be abided by. The groups are flexible and always able to adapt or change. For example, Anonymous has used assertive speech to form identity, through established lines of communication that can be used by many individuals; it is the mode of communication that is significant not the speaker. They also use controversial control of group identity through methods such as doxing (revealing a person's real-life identity and private details, including home addresses) showing that even anonymous groups expel members. Some Twitter accounts, especially ones belonging to anonymous users, have their motives called into question on occasion. Then it appears that the individual is validated or rejected by other members of the collective in question, reinforcing the fluid boundaries of group membership (Dobusch and Scheneborn, 2015). These fluid boundaries could then encourage the membership of multiple social identity subcategories.

2.3.2 Conflict

Conflict between and within groups usually follows certain patterns, defined by the collective needs, the collective mood, and the collective fears (Kelman, 2008). It has also been shown that the moral values of a group have strong relationships to the group identification and impression, and how they view those with differing morals (Brambilla et al, 2013). This is highly significant in hacking communities as the "moral nature of 'computer deviance' is slightly more ambiguous and far more complex than we often recognize" (Thomas, 2005:599). For example, in the context of hacking communities, the in/outgroups are frequently defined through rivalry between different "hats" or

motivations behind the group membership. It has been stated that these groups need the motivation of having an "enemy" and use the outgroup to negotiate their community boundaries (Jordan and Taylor, 1998, Kelman, 2008). This is a potential source of greater motivation than the in-group fighting witnessed in the growth of Anonymous. There is sometimes an assumed inevitability of in-group fights, due to the growth in numbers and diversity behaviour moves from cooperation to competition, and there is less consensus on the methods acceptable to achieving the group goals (Brambilla et al, 2013). It has been observed that whilst "forums foster a sense of group identity and community…rhetoric on the forums stirs up emotions, inspires action, and promotes a sense of "us vs. them."" (Denning, 2015:172); this could be used to mobilise a group into acting against a perceived outgroup.

2.4 Trust

Trust is complex and abstract concept, with the elements being difficult to define; this leads to many researchers adapting definitions to work in their particular context (Wang and Emurian, 2005). An appropriate definition within this research must emphasise the adaption required when going from offline to online. When people engage in trusting behaviour they are increasing their vulnerability to others, whose behaviour they cannot control (Zand, 1972). Trust is commonly regarded as an expectation regarding the behaviour of another, with the acceptance of and exposure to vulnerability (Beldad et al, 2010); a definition of online trust is as an "attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited" (Corritore, Kracher, and Wiedenbeck, 2003, cited in Beldad et al, 2010:860).

Generalised trust is believed to make a person more willing to engage in collective efforts and cooperate with other people (Sturgis et al, 2012, Van Lange, 2015). In the context of hacking, there is usually a paranoid and suspicious mind-set, so how do these groups establish trust? (Dupont et al 2016). Online disinhibition effect is the removal or reduction of the social and psychological restraints that individuals experience in everyday face to face interaction (Suler, 2004, Hu et al, 2015, Joinson, 2007, Lapidot-Lefler and Barak, 2015). It could be argued that anonymity and online disinhibition can be positive, allowing the internet to be an open place where individuals can be honest on subjects that they may otherwise not wish to be identified with. This privacy combined with openness is what many involved in hacking and hacktivism claim to want to protect.

Wang and Emurian (2005) discuss the concept of online trust as a barrier to e-commerce, and whilst they focussed on issues such as design to improve the culture of trust, their discussion of the concept is still highly relevant to other areas. Trust is complex and abstract, with the elements being

difficult to define; especially in online contexts, it is used “interchangeably with credibility, reliability, and confidence” (Wang and Emurian, 2005;108). It is worth noting that there is relevance of trust and e-commerce to some hacking communities as there are forums that do specialise in e-commerce, usually selling items of an illicit and illegal nature, offering hacking tools, stolen bank or card details, or access to paid or subscription accounts. Sometimes, the technology (mainly the Internet) itself is an object of trust (Marcella, 1999).

Trusting behaviour requires the individual to relinquish control over valuable outcomes with the expectation that the other will reciprocate: it has been shown that group membership is a strong predictor of trusting behaviour (Tanis and Postmes, 2005). The behavioural consequences of trust are especially interesting with a group setting; the perception of social presence online is believed to increases online trust (Beldad et al, 2010). Social presence refers to the degree of feeling of being connected to another through a text-based encounter (Tu and McIsaac, 2002). This perception can be influence by the social relationships and the context of the online environment (Tu, 2002). It has been found to have a positive impact on an individual’s identification with online groups and communities (Schimke, Stoeger, and Ziegler, 2007) and on their participation (Tu and McIsaac, 2002). Therefore, the more prominent a member is in a community, with a visible history, the more likely it is that other users will trust them without having had significant interpersonal interaction.

2.4.1 Signals

When the Internet was in its infancy, privacy and security were critical elements that online businesses addressed to earn consumer online trust and they were often cited as antecedents to trust. However, with the maturation of the Internet, consumers have come to expect more from online businesses and their requisites for trust have also increased (Shankar, Urban, and Sultan 2002). As such, online groups have evolved on the internet, developing alternative ways to signal identity and status that may not be obvious to outsiders. An example of the communities subtly creating the in-group, through methods based on knowledge, is as triforcing on the /b/ “random” board of 4chan (Bernstein et al, 2011). Triforcing originated on 4chan as a challenge to post a correctly formatted Triforce, originating from video game The Legend of Zelda (Zelda Capital, 2009). It has since evolved into an in-group indicator, as the individual must know how to create it in order to display it correctly. If they try to copy and paste someone elses, the Triforce will be displayed in the incorrect format, and it will be obvious to all that they do not know how to Triforce; this will not be apparent however until after the message has been posted on the board (Figure 3).

Figure 3: Triforce examples

Other examples of signs and signals used in online forums include use of in-group jargon to signal ones understanding and membership, although this can backfire if the group believes that a person is merely mimicking the group behaviour to give the appearance of assimilation without actually identifying with the group (see Chapter 5 forum comments). The availability of signs and signals online are "a fundamental part of deciding whether to trust'' (Bacharach and Gambetta, 2001:155); the different online communities have different requirements. It is believed that online hacking communities, due to the value of meritocracy (Zhang et al, 2015), regard evidence of curiosity and commitment to learning as signs that an individual could be trusted however this would be contingent on other facts. For example, expression of hacker ethics or concepts would be a possible way of signalling the hacker identity, which can provide a foundation for trust (Tanis and Postmes, 2005). This will be examined in Chapter 7.

Chapter 3: Methodology

The aim of this research was to investigate the social identities and group processes present within online hacking communities. The researcher's stance was informed by the literature review and prior to data collection it was felt that there is a misleading stereotype about hackers. There was the strong belief that, overall, this is a community that is engaged and interested in developing technology and security, as well as furthering one's knowledge; it was believed that the decisions of how this information is used are made on a personal and individual level, but with influence from their chosen groups. To explore this area, a netnographic mixed methods approach was used. The reasons underlying this choice of methodology are covered within this chapter and also a discussion of other avenues or methods that were initiated within the pilot stage but discontinued.

3.1 Research outline

As discussed in Chapter 2 there exists a diverse background surrounding the concepts and schemas involving hackers. Involvement in a community or group can and does affect individuals via the group processes according to social psychological theory. The aim was to collect data to examine group impacts and individual awareness, as well as the potential for this information to improve cybersecurity. The Social Identity approach, incorporating Social Identity Theory (SIT) and Social Categorisation Theory (SCT), was used to help understand the data and add to existing research and methodological advances.

The method used for this research was netnography (ethnography via the internet, Kozinets, 2015); the reasons for this choice are discussed in section 3.1.2. Data was collected via quantitative online surveys and qualitative interviews. The purpose of combining these two methods was to gather data that gave a broad picture of how the hacking communities perceived themselves and use that as a starting point for the more in-depth interviews. Using that initial research, a more informed and focussed survey was constructed, providing more generalisable results on aspects of the hacker identity and trust in online communities. There were various challenges with online data collection, from participant recruitment to ensuring the integrity and representativeness of the results. Previous studies, including Coleman (2014) and Olsen (2012), have found that research of this type is not universally welcomed in such private communities, with reactions ranging from wary to hostile. To avoid problems with the communities, the research used an overt approach – the researcher, although not giving out personal details, did not hide their identity. This has been successful in the past (Coleman, 2015) and was found to be the best approach. Whilst there still was the risk of

"verbal" abuse or even a form of attack on the researcher, it was hoped that the lack of challenge or entertainment value in finding the identity of the researcher meant that individuals would be disinterested in doing so; this proved to be the case. Previous approaches to these communities have also led to the potential participants demanding details of the research, including ethical approval; this was provided and proved to be a necessary step in recruitment; the participants were informed and interested but wanted to verify the researcher's authenticity.

Within hacking communities there is usually a paranoid and suspicious mind-set (Levy, 2010); the interviews began to investigate signs and behaviours that made the participants more inclined to trust other group members. The online disinhibition effect (Suler, 2004) refers to the removal or reduction of the social and psychological restraints that individuals experience in everyday face to face interaction (Barack et al, 2008; Hu et al, 2015; Joinson, 2007; Lapidot-Lefler and Barack, 2015; Suler, 2004); the effect of this was also examined through participant responses. It has been argued that anonymity and benign online disinhibition can be positive (Suler, 2004), allowing the internet to be an open place where individuals can be honest on subjects that they may otherwise not wish to be identified with. This privacy combined with openness is what many involved in hacking and hacktivism claim to want to protect.

3.1.1 Methodological Framework

This topic demanded a flexible approach to the research; due to the sensitive nature of this subject and the demographic. After consideration of alternate methodologies, such as a purely qualitative one, it was decided that a mixed method approach would enable insight to be gained but also to retain the context for the data in each study. For this reason, netnography was chosen; although previously used more for health-related, market, and consumer driven research (Kozinets, 2015), it was felt that its emphasis on the importance of communication and interaction would be the most appropriate for the study of a complex community and the behaviours found there. Whilst often confused or used interchangeably with digital ethnography, netnography has distinct differences. For this research it is significant that these offline individuals form the online groups, but the online groups come together to interact offline. Kozinets described netnography as "a specialized form of ethnography adapted to the unique computer-mediated contingencies of today's social worlds" (2010:1). Kozinets investigated four distinct areas of ethnographic research in computer-mediated contexts: the alteration of interactions through technology; the anonymity of actors; the ease of access, both for participants and researchers; and the automatic archiving of data and conversations. Although the last point was not applicable to this research, the focus of the other areas was highly pertinent, confirming the suitability of this methodology.

Of particular importance for the researcher were the ethical considerations and the debate surrounding consent with regards to online forums as a source of data; these considerations are a central part of the netnographic approach. Kozinets emphasised the importance of gaining permission, as well as how to protect participants through the researchers' choices on citing, anonymising, or crediting their contributions (2010). This research followed the guidance and credited participants when they agreed and had provided their real world names, for example in their blog posts; where online community nicknames or usernames were used, these contributions were anonymised. The British Psychological Society internet research guidelines state that the following must be considered when looking at internet-mediated research; valid consent, withdrawal, confidentiality, anonymity, fair treatment, and rights for privacy (British Psychological Society, 2013); adherence to these principles is demonstrated and discussed in section 3.3.1. It is acknowledged that there is continued discussion around whether or not online forums are public domain or private; however, Langer and Beckman (2005) argue that if there is no restricted access then it can be regarded as public communication but emphasise the importance of researcher awareness to the potential to harm participants. If it was straightforward and possible for the researcher to create an account on the websites and forums, this was considered unrestricted; some sites required answers to questions or riddles that were not common knowledge, and this type of barrier to joining meant it was regarded as restricted, and so no research accounts were made.

Netnography has different process levels, which can overlap and interact with each other (Kozinets, 2015), which were loosely followed throughout this research. The initial investigation phase included developing the research aims, before considering the ethical practices that would be appropriate and acceptable for the study. The sites were chosen to include different sorts of site, topics, and people (see Chapter 4). The Iteration phase involved examining the available data for general rules and patterns of behaviour. The Integration phase presented findings and discussions with the researcher's conclusions and recommended potential action, detailed in Chapter 8. It must be acknowledged that Koznets criticised the approach utilised by this researcher, that of lurking, downloading data, and analysing "while sitting on the sidelines" which he regarded as not appropriate for netnography, as it was intended to offer "deep understanding and thick description" (2010:75) of online communities. This researcher would argue however that within the context of hacking communities, the 'sideline' approach is the most common and appropriate for understanding and becoming involved with the hacking communities, both for researchers and community members alike. It is suggested that Kozinets stance is due to his focus on marketing and commercial communities, where participation is far more common in day to day life and the social norms are more widely understood.

3.1.2 Analytical Framework

The original intention of this research was to use mixed methods as equally as possible, as it was felt that the trigulation of data was an important part of validating this research. An inductive approach was utilised to progress from the broad perspective at the beginning to the detailed elements addressing the research questions. The use of quantitative data and analysis provided an initial dataset that allowed the researcher to analyse self-reported behaviour and present the findings in an accurate way. The survey research was conducted around a specific community group, but the participants who completed the surveys were self-selected, and therefore random; the researcher had no control over who completed the survey, aside from the selection of websites it was posted on. The exploratory nature of this research meant that a correlational or comparative approach between pre-designated groups was not possible; however, the approach used meant that there was an interesting mix of respondents, which added variety and range to the dataset. In the final study (Study 3, Chapter 7), the data was expected to be quantitative; however, the number of participant comments led to the results becoming more qualitative.

The quantitative data was used alongside the participant observations and the qualitative data. For the qualitative data, thematic analysis was employed (Braun and Clarke, 2006). Whilst conversation analysis (CA) and discourse analysis (DA) were considered, these place the emphasis on 'talking' (Fox, 2004): this was impractical in this research, due to the divergences on the types of data collected. For example, although no dataset was collected, the participant observation (Chapter 4) was a vital part of this research; however, analysis of online threads as conversation would have yielded little, as these discussions were often short and involving multiple respondents. By looking at the themes, a more comparable view was developed across the online forums and the conferences attended. In Study 2, the participant interviews (see Chapter 6), some participants were verbally interviewed, via Skype, or in person, others in writing; the written responses were much briefer than the spoken, but the information contained was just as informative and relevant. In Study 3, (Chapter 7), the data results were surprisingly mixed between qualitative and quantitative. To have used another mode of analysis would have meant disregarding data provided (Braun and Clarke, 2006); therefore, working with the themes, rather than focusing on the conversation meant the resulting data could be completely integrated in this research, allowing the researcher to explore the depth and variation in these communities.

3.2 Research Strategy and Design

Data was collected through various methods; initially the researcher spent several months conducting observation of participants online and offline. Each separate online data collection questionnaire and offline interview was conducted as a cross-sectional study, although interview participants were asked about the changes they have witnessed during their involvement with the community. Most of the data for this study was collected in several stages:

- Preliminary data was collected through informal participant observation, both online and offline, gathered throughout the duration of this research. There was no strict data set for this, but the observations are used throughout this thesis;
- Pilot Study: online survey;
- Study 1: online survey;
- Study 2: individual interviews;
- Study 3: online survey.

Questionnaires were used to collect both quantitative and qualitative data, on the basis that it could be distributed to a much larger number of people than it would be possible to interview. All questionnaires were self-reported. Some of the data collected was not easily quantifiable; for example, detailed information on the demographic was not gathered, and after the pilot survey only gender and age were requested. This was due to the nature of the target population; those involved in hacking, especially the more interesting (and potentially less legal or moral) areas are protective of their personal information and are highly suspicious of giving any potentially identifying information. In practical terms, it seems highly unlikely anyone could be identified based on their age, gender, country of residence, or ethnicity, but asking for this information would severely discourage participants, as they regarded it as unnecessary for the study and infringing on their privacy; therefore, this demographic data was sacrificed.

As this research was seeking to measure potential parameters within the target community, questionnaires were an ideal way to collect opinions and category data, allowing for comparisons between groups to be made. Each question only expressed or targeted one idea in the interests of clarity. The use of some jargon and abbreviations was unavoidable, as excluding it would suggest to participants that the researcher was not truly familiar with their community, and therefore that the research (and their contribution) would be less valuable. The language used was common on the forums and related discourse. Some participants commented or criticised the lack of inclusion of further and more specific subcategories, although they themselves were given opportunity to include these.

Throughout the questionnaires, leading questions were avoided; the exception was the inclusion of obviously biased statements which were used to gain participant opinions. These answers enabled initial analysis and potential clarification on trust signals in an online text only framework.

3.2.1 Discontinued Avenues

Initially, Internet Relay Chat (IRC) channels were included as a source of data; IRC is a computer-mediated communication system, for text-only chat, originally intended for real-time group use, commercial or social, across the globe (Benjamin and Chen, 2012; Reid, 1996). Whilst it has lost 60% of its users since 2003, with content moving to piracy and social media sites (Pingdom, 2012), the users remaining have become more niche and specialised. Part of its appeal for hackers and hacktivists may be that it is open standard, and therefore does not belong to anyone (Delony, 2017). Despite its long history, IRC is best known to many for the significant part it played in the activities and coordination of Anonymous (Coleman, 2012; Olsen, 2012). It is still used by many in hacking-related communities (Benjamin et al, 2016) and technology development and is regarded as a convenient mode of communication with experts; many hacking-related forums advertise their own channel or chatroom. For these reasons, it was attempted to include IRC in this research. However, upon investigation it became evident that more insider knowledge is needed to find the channels with conversations relevant to this research. In the relevant channels which were advertised, even minimal data collection in the context of this research was time-intensive. For example, significant conversation might only take place for 40 minutes within 24 hours in that specific channel, as well as across many different time zones. It is also known that new channels can be created for specific discussions. For example, Coleman (2012) reported that people involved in Anonymous moved to the new channels when they started talking about specific details for cyberattacks. These channels were accessible through invite only, and then discarded once the purpose was served, with no evidence available to anyone not immediately involved. Therefore, use of IRC was not deemed a practical or efficient use of the researcher's time, and was therefore not continued in this research.

The first example of data collection for this research was carried out on Twitter, completed through Collaborative Online Social Media Observatory (COSMOS): Social Media and Data Mining platform. This software collects information in the form of tweets from Twitter for the duration of a set period. Initial data collection with this platform was carried out over 40 hours, covering the 4-6th of November 2015. This data set contained over 50,000 tweets which contained "#Anonymous", referring to the hacktivist group. The dates were specifically used as Anonymous adopted Guy Fawkes (masks from the film "V for Vendetta" (2005)) and the 5th of November as symbols of their

hacktivist movement. In 2015 this date also marked the apparent conclusion of their campaign against the Ku Klux Klan. Whilst this method gained a significant amount of data, it quickly became obvious that much of it was not particularly interesting in terms of this research. Because the "#Anonymous" search term was commonly used, it collected tweets and retweets that were promoting activities for the collectives or media organisations, rather than anything informative in terms of the group processes. This was valuable to realise early in the research. It was hoped that the tool could be used more accurately in future, however, the collaboration ended in 2015 with no updates since 2014 according to the website (http://www.cs.cf.ac.uk/cosmos/). Whilst the software is still functional, it is limited and so the decision was made to focus on data collection from participants recruited via websites and forums, as these do not have the low character restriction or duplication of retweets found on Twitter.

The Linguistic Inquiry and Word Count (LIWC) Text Analysis Software was originally considered as an analytical tool for this research. To acclimatise the researcher to the software and understand its functions, three texts relating to hacking communities were analysed. The three texts were written for different purposes. They all relate to aspects and purport beliefs of the hacking community that were and are very important. The first was the Hacker's Manifesto, written following the arrest of the author for hacking and is considered an important element of hacking culture (see appendix 9.2). The second was a paper written by a founder of the Electronic Frontier Federation (EFF), an international non-profit digital rights group. The paper addresses the governing of the internet, or rather, state government's lack of right to govern the internet; it has gained praise and criticism. The third was an article on the changing perceptions of hackers, within the communities and in the public eye, by Stephen Levy, an author who has long been involved with the subject of hackers. As this was the first full analysis being completed with LIWC, the texts were not edited, leaving all spelling and netspeak as they were in the original. Whilst LIWC provided insight into the use of language and its meaning, the focus was on the language, which overlooked the importance of the themes and context within the texts analysed. LIWC was also impractical in terms of analysing forum text, as these texts commonly had multiple authors and short sentences. For these reasons, the insights to be gained by LIWC analysis were deemed to not be appropriate to analyse the data collected for this research.

3.2.2 Data Collection

The pilot survey completed in early 2016 had a better response than expected, with minimal obviously false answers. It was believed that those who would be inclined to give false data were less likely to take the time to respond. All responses were checked by the researcher before

inclusion, and suspicious and dubious responses were removed (see Chapter 5). The quantitative online surveys for Study 1 and 3 were hosted by Qualtrics, whose privacy and security statements were checked. Qualtrics states in its terms and conditions no data is collected about participants, including location and IP address. However, if participants were concerned about their privacy when completing the survey, the use of Tor browser or a VPN was recommended. As stated, there was interest in participation both for interview and survey from the beginning of this project. Whilst it was anticipated that "ethical hackers" would be more inclined to participate, the participants' self-categorisation showed a wider range of individuals.

Study 1 used an online survey hosted by Qualtrics to gather anonymous responses regarding involvement in the communities, hacking identities, and used Likert scales to gain opinion on privacy, anonymity and security online. Questions were selected to cover a broad range of concepts within the research area, with the aim of identifying any trends or contentious areas, mostly based on the interactions and discussions seen on forums (see appendix 9.1).

Study 2 was comprised of individual interviews, which questioned how the individual became involved in the communities, and their opinions on the social identity, the groups that form, and the concept of trust within these groups and communities. These questions were influenced by the survey responses from Study 1, in particular the responses to the social identity categories commonly used, as well as the importance of self-identification within hacking. For the Study 2 interviews, participants were offered the choice of verbal interview, through Skype (where it is easy to set up an anonymous account), or written, through instant messaging or email, which can both be safely anonymised; they were also at liberty to choose another method or arrange to meet in person. The first interview participants were known members of different hacking communities who publicly speak on hacking related events and activities. These participants were approached via email and were willing to participate and support the research. The participation of well-known actors within the community did to an extent encourage the snow-ball effect for participant recruitment, although not as far as anticipated; further recruitment was made by approaching those who identified themselves publicly as involved in hacking and asking if they would participate. The interviews were semi-structured, based along the group processes and themes evident from the pilot survey, the first study, and the participant observation, online and offline. In Chapter 8 comparisons are drawn regarding awareness and presentation/self-presentation to an audience in these different methods of data collection.

Following on from these interviews, Study 3 used a second online survey, focussing again on hacker categories, specifically asking Black, Grey, or White-hat hackers to place themselves on a scale of

Black to White, and then asking for their responses regarding trust online. Based upon previous research for trust related "symbols" or signals (Bacharach and Gambetta, 2001), statements were used from different forums and social media and participants were asked to respond on different criteria.

This combination of data collection was used in order to gain different insights from the different collection stages, with each study building on the previous one. For example, in Study 1, the first survey, participants were asked if they would classify themselves as hackers, only half said yes, the others saying no or preferring not to answer. However, in the interviews it became apparent that although not every participant would claim to be a hacker they each identified with a specific subcategory. This was then incorporated into the second survey, where participants were asked to categorise themselves, rather than directly asking if they were a "hacker". Another development in a similar vein was that in the first survey it became evident that there was no sense of definition of the boundaries between Black/Grey/White-hat hackers, and it was fairly subjective; in Study 3, the second survey, those that identified themselves as any of these categories were asked to place themselves on a scale of hacking behaviour, from Black (illegal/immoral) to White (legal/moral).

For each data collection stage, participants were informed of the purpose of the study and were asked to confirm that they understood and were happy to have their answers used (see section 3.3.1 below and Appendix 9.1 for further detail). For the online questionnaires the sampling method was based on convenience sampling and self-selection; the researcher was aware that online self-selection is at risk from selection bias; however, this was the best way to safely access the required demographic for this research. It is also put forward by the researcher that the nature of hackers, requiring evidence to support ideas and valuing knowledge, meant that aside from those involved in illegal or illicit behaviour, many individuals from this community were supportive of the research and encouraged participation. The all studies were advertised on various forums and subreddits[2] asking for participants to volunteer. With Study 2, the interviews, this led to Snowball Sampling – the process of referrals to gain participants; it is possible this also happened with the online surveys for Studies 1 and 3, but this cannot be verified. There are some restricting factors in this research, for example the language and geography relating to the researcher; the interviews and surveys are conducted exclusively in English. In the interview's participants were asked if English is their native language, but this was not asked on the surveys. The links to the surveys were posted on English speaking forums (although some have language specific subsections).

[2] Subreddits are the smaller forum groups on specific topics within the Reddit website.

It is important to remember that this community is a hard to reach population, valuing their privacy and often being suspicious of outsiders, and unwanted surveillance. Bearing that in mind, questions had to avoid making participants feel that they were risking personal or identifying information. Because of this minimal personal information was gathered. This means that there was no verification process on participants abilities as a hacker, it was purely self-categorised. This is discussed further in Chapters 4-7.

At the request of participants in the first study, the results of each study were shared and reported back to the hacking communities where participants had originated. There was interest and discussion in the results but very little dispute about the data; this was interpreted as a form of data validation.

3.3 Ethics

For the methodology of this research the ethical considerations were highly important to the research. The University's research ethics committee gave their approval for the research project. In addition, the researcher consulted the British Psychological Society's (2017) internet mediated research ethics for each study. The initial data from the Study 1 and 3 (the online surveys) was made publicly available at the request of multiple participants. This data was not of a kind that could be used maliciously, for example by deanonymizing participants, and the sharing of the results encouraged further participation and discussion.

For the participant observations both online and offline, it was not possible for to obtain signed informed consent. Any interaction with the researcher meant that the purpose of her presence and the research was explained fully, but no personal data or individual observations were made. This was in part to avoid identifying any participants; this approach was the best course, as the observations were carried out on the public Internet, and used for research on collective behaviour, without no aim of identifying specific members. Further precautions taken include not identifying individuals (including not publishing usernames) and presenting results objectively.

The following was explained before participants answered any questions, both on surveys and in interviews:

- The purpose of the study
- The type(s) of data that will be collected
- The procedures used to collect data
- How data will be reported
- Confidentiality and anonymity are provided to participants.

The informed consent agreement explicitly explained that participation in these studies was voluntary.

3.3.1 Further considerations

The researcher's lack of technological knowledge was viewed as a potential limitation; although it did not impede the progression of the research it was believed that there would be more opportunity for in-depth conversation with participants, and possibly easier acceptance, with the knowledge. It was hoped this knowledge base would be improved through the learning and understanding of jargon and technical terms during the research.

Throughout these studies, the researcher was mindful of the different cultures that would be encountered; whilst the dominant culture was highly western, due to the researcher's location and native language, there were many non-western individuals present in the forums visited. There is also the impact of the overarching "hacker" culture that was considered. The influence of group norms is a central element of this research; however, it is acknowledged that there will be minor norm divergence within the sub-categories. Unless it is determined to be highly influential or significant to participants, the smaller differences will not be noted in detail.

Chapter 4: Participant Observation

This chapter details the participant observation carried out via forum investigation and conference attendance throughout the duration of this research. It includes explanations for inclusion or exclusion of different sites and sources, as well as brief sentiment analysis of discussions pertinent to hacking communities. Although no specific data sets were collected from the participant observation, it formed the backbone of this research, giving context and insight to behaviour and participant responses; discussions from forums are used as examples throughout this thesis.

4.1 Ethical Considerations

Before detailing the participant observations, mention must be made of the ethical considerations for this part of the research. Privacy and anonymity are core values within hacking related communities, with individuals using online user names and pseudonyms in both online and offline contexts. As stated in Chapter 3, the methodology for this research places much importance on the ethical considerations and privacy of participants; but this was more problematic in the context of offline participant observation. Each subsequent study data set informed the participants on the need for their valid consent, their ability to withdraw at any point, and ensuring confidentiality, anonymity, fair treatment, and rights for privacy (British Psychological Society, 2017). A slightly different approach was needed however for the participant observation.

The target group for this research made the use of signed consent forms impractical and wholly unsuitable; these communities would not give their real names or personal information to a researcher. To overcome this, the offline participant observation was initially covert, but as and when community members invited the researcher to join groups or conversations, they were informed of the purpose of researchers' attendance and given information on the aims and methods of the research. This was made clear to any participants interacting with researcher. All of the participants were adults; many of the meetings and conventions attended were for over 16s or the child had to be accompanied by a parent. Children and teenagers who were in attendance were never included in the observations.

As there was no signed consent, body language and non-verbal signifiers were monitored during any conversation or observation; any sign of discomfort from the participants and the observation or interaction ceased immediately. Continued interaction with the researcher after being informed of the researcher's purpose however was taken as explicit consent; participants were informed of this verbally. There were no audio or visual recordings, it was more casual conversation and relevant

observations arising from that were noted; no direct quotes were attributed to individual participants. Participants were informed on the collection and storage of data if they wished to know, and informed that all data was anonymous from the point of collection.

Whilst the observation was initially covert there was no active deception. If asked, the research was fully explained, and the researcher offered to provide the written participant information by directing participants to the survey recruitment posts on various forums. This also allowed participants to opt-in to the survey section of the research (which had also been ethically approved). These individuals are members of groups who may have connections or members that have broken the law or are highly concerned about surveillance and privacy. It was confirmed by the researcher in discussion with members of the various groups that minimising the amount of written information and consent forms physically present, reassured the participants, both active and potential.

4.2 Online Participant Observation: Forums

The initial stages of this research involved finding and observing hacking-related forums, websites and places (hereafter referred to as forums) where online hacking-related discussions arose. This was simply done by using various search engines both on the internet and the dark web. Different search engines were used to reduce the potential risk of any algorithm bias. Search engines included Google and Bing, as two of the most well known and popular; and Duckduckgo, which does not allow users to be tracked, and therefore is often recommended on hacking forums as a more trusted search engine. On the dark web, websites are purposefully hidden and inaccessible through standard web browsers (Greenburg, 2014). In this situation Tor directories such as Hidden Wiki were used; these are internet directories that list the different sites available through the dark web, categorised by purpose. These searches were conducted throughout the research period, to enable the list to be updated with new forums and remove the defunct ones. It has been observed that there is an ephemeral quality to hacking related forums compared to other areas or interests (Coleman, 2014); this supports the concept of the fluidity of the hacker identity, as discussed in Chapter 2. If a forum could no longer be found through the search engines or directories it was recorded as no longer active, although it would still be included in future searches, in case of reactivation.

If the forum could only be found on Twitter or Facebook, again through search engines and directories, with no external links, it was excluded from the list of active forums; aside from not having a forum to observe, it was felt that any group exclusively on social media was not going to be relevant to this research. Although many forums do have Twitter or Facebook accounts, this is in addition to the forum, as a means of advertising and promoting themselves, rather than the

foundation of the community. If the group only had one-way communication (the account holder posted their opinion) but no formal space for discussion between multiple users, it was not regarded as a genuine source of information or community behaviour. For example, Twitter allows for conversation in the form of replying to other people's tweets, but this is not a distinct or easy method of discussion by a larger group. It was usually found that if a tweet or comment was relevant to a hacking-related community they would post a link to it on their respective forum and then discuss the post there. Although Facebook groups do allow discussions in the form of comments on a user's post, it is not it does not facilitate a real exchange of ideas or opinions for a large group; after a certain number of replies, older or unpopular replies are hidden unless the post is expanded to see all replies. Facebook accounts are usually personal and even when using fake names, a lot of information is routinely collected about the user and their Facebook use, which is contrary to even basic privacy which hackers' value[3]. Facebook groups about hacking and privacy are therefore not regarded as particularly secure, private, or anonymous and as such are not included in this research. This decision was supported by the attitudes of hacking communities who regard social-media-only groups as unreliable sources[4], in addition to the traditional hacker ethic which has long held a cynical attitude towards even traditional news sources[5] and a distrust of authority (Levy, 1984). This distrustful attitude towards social media as a source of information is also becoming more widely prevalent in the general population (Media Insight Project, 2016), especially following events such as the Facebook/Cambridge Analytica scandal (Adams, 2018).

The types of websites listed below were selected as sources and bases for anonymous discussions on hacking. The purposes of the individual websites vary: some are hobby forums, where members discuss different aspects of hacking-related activity; several are purpose-made websites, such as WhyWeProtest, with an obvious agenda; others are websites on the dark web which require membership to view discussion threads. The dark web sites requiring membership invariably have sections dedicated to the buying and selling of personal or credit card details or hacking tools or botnet services. Regardless of the site, all those included in this research offer news, advice and updates on hacking, hacktivism and hacking techniques. It was observed that Twitter has "trusted" or verified accounts from hacking collective members and forums (including HackForums, DefCon,

[3] "You are giving them all of your information, your photos, your private life, at this point they control every piece of info you post on your wall." Forum member response to the news that Facebook had been altering news feeds as part of a psychology experiment (2014).

[4] "Fake news does exist. But it's not just coming from the news outlets…It's coming from idiots on the internet mostly, Facebook, and other news sites that have a clear agenda. It's 21st-century prop[aganda]." Forum member response to thread on Fake News (2018).

[5] "There is no such thing as unbiased news. You need to compare articles from multiple sources across the political spectrum in order to get a complete idea of what actually happened." Forum member response to a thread asking for unbiased news sources (2017).

Rustle League, Chaos Computer Club); many of these accounts have an accepted legitimacy within these communities. It can be problematic however when multiple accounts are present, each purporting to be the main account for a group, as is often the case with Anonymous, which led to in-fighting in the past (see section 2.1.1 in Chapter 2) and accusations of "false flag" attacks, where misleading or inaccurate information was given about an operation or "op" in order to dilute the strength of Anonymous, which arose primarily from its large membership base rather than skill.

Having identified the relevant forums (see Table 3), discussions were observed to categorise and examine the group behaviours. Some forums were excluded at this point, due to a lack of activity on the forum (for example if the last posts with discussion were from before 2013). Ones that focussed on illegal activities or which were more profit-driven were initially investigated, but the contents and attitudes of members led to concerns about the researcher's privacy and safety if they explored the site too far. Sites of this nature that were approached for data collection via online survey in later stages usually banned the researchers account.

All forums had terms and conditions of use that must be accepted when registering as a member. Disobeying these terms could result in the member being banned. A sample of the different forums' terms showed that there was a certain template, with forums warning users against any illegal behaviour; this sample of terms was taken from the forums that had high member registration and moderately frequent activity (in the past six months). In many cases it appears that the forum rules, found on the discussion boards, rather than the registration terms set the social norm for the forum. The terms of the website were sometimes in direct conflict with the aims and numerous discussions found on the sites; for example, it is common on cracking-related forums for the terms of use to state that credit cards, bank, and Paypal account details are not allowed to be posted or discussed but there are still posts in the market sections offering these. This suggested that the terms appear more to be for show, that the forum owner was complying to legal requirements with the registration terms and conditions; the forum rules did not seem to reflect the same stance or be enforced. This was far more common on the Black/Grey-hat forums, the White-hat/InfoSec forums were far stricter.

Forum Name	Registered Members (Feb 2016)	Registered Members (Feb 2018)	Comments	Study 1 Posted	Study 3 Posted
4chan*	n/a	n/a	(/b/) Registration not required	No	No
AIOCrack	911	Not found	Could not authenticate account	No	No
Antionline	91,327	92,562	InfoSec/White-hat	Yes	Yes
BiTS Hacking	170,484	234,457	Predominantly Black/Grey-hat	Yes	Yes
bl4ckhatsecurity	1,505	No data	Not found Feb 2018	Yes	No
Black Storm	7,936	8,046	Could not pass security	No	No
Broad Product	361	No data	Banned – Black/Grey-hat	Yes	No
CorruptZone	181	No data	Forum seemed to come and go	No	No
Crack Hack Forum	128,827	No data	Banned - Not found Feb 2018	No	No
Cracking Forum	527,467	539,682	Banned - Cracking	Yes	No
cryptoworld	726	No data	Not found Feb 2018	Yes	No
Darknet	No data	No data	Not popular/active forum	No	No
DEF CON	No data	No data	Forum for the Defcon convention and related topics	Yes	Yes
Evil Zone*	13,042	No data	Hacking education forum – has changed purpose from original	No	No
Greysec	1,290	2,586	White/Grey-hat	Yes	Yes
Hack Forums	No data	640,678	Minimum no. posts required, limited activity (text only)	No	Yes
Hackaday	6,366	6,707	General hacking forum	Yes	Yes
Hackerthreads	16,441	16,928	Posts not approved by admin	No	No
hackrally / Luxor*	138	1,865	Forums merged	No	No
Hacksden†	5,833	No data	Banned	No	No
HackThisSite	69,995	76,457	Hacking training/challenges	Yes	Yes
Hellbound Hackers	95,682	104,165	Hacking training/challenges	Yes	Yes
Infinity Forums	2,299	No data	Not found Feb 2018	Yes	No
ISA Hackers*	21,822	No data	Hacktivism – frequently offline	No	No
Offensive Community	26,732	33,820	General hacking forum	Yes	Yes
Pen testing Linux*	201	617	White-hat/InfoSec	No	No
SEForums*	No data	9,993	Social Engineering	No	No
Sinisterly	24,564	40,365	General hacking forum	Yes	Yes
SocialEngineered*	No data	43,896	Banned	No	No
WhyWeProtest	95,637	100,189	Hacktivism/Activism	Yes	No

Table 3: Hacking Forums

* These forums were judged by the researcher to be unsuitable for participant recruitment due to the communities' negative attitude or responses towards outsiders.

There are also many users that were interested or involved in hacking that use Reddit. Reddit is a hybrid of social media and forum, combining social news aggregation, web content rating, and discussion (Reddit, 2018). Users can create their own groups (or "subreddits") on any topic they desire. To avoid confusion, the subreddits that were monitored have been listed in a separate table (Table 4) to the forums. These subreddits are often as active as the forums, if not more, with users discussing the different forums available, as well as discussing the specific topic of the subreddit. It

must be noted that whilst the subreddits were observed and used for data collection, the discussions were often less open than those on forums. Because they are part of a larger website, Reddit, the rules and legality of content is strictly enforced. Where there is no data for subscribers in 2016 it was not being monitored by the researcher at that time.

Subreddits	Subscribers (Feb 2016)	Subscribers (Feb 2018)	Description (from the sub)	Study 1 Posted	Study 3 Posted
/r/actualhacking	-	441	"This is a subreddit where people that actually know how to hack can post. This includes SQLi, rooting, any sort of hacking you can think of, post it here."	No	Yes
/r/anonynet	56	84	"Online community for the human-rights group, Anonymous."	No	No
/r/CyberSec101	-	1,092	"CyberSec101 is the home of cybersecurity videos including: Hacking, Privacy, Anonymity, Whistleblowing and Interviews with industry experts like Jacob Appelbaum and Edward Snowden."	No	Yes
/r/cyberpunk	123,128	207,995	"A genre of science fiction and a lawless subculture in an oppressive society dominated by computer technology and big corporations."	Yes	Yes
/r/Defcon	5,338	8,508	"Official subreddit of world's largest hacker convention!"	Yes	Yes
/r/ethicalhacking	873	1,588	"A forum for discussion on computer hacking done for ethical purposes."	Yes	Yes
/r/hackbloc	14,232	17,294	"Hacktivism, Crypto-anarchy, Darknets, Free Culture - Proudly Feminist, Anarchist, Anti-Capitalist, Anarchist hackers"	Yes	Yes
/r/hacking	104,706	266,561	"A subreddit dedicated to hacking and hackers. What we are about: constructive collaboration and learning about exploits, industry standards, Grey and White-hat hacking, new hardware and software hacking technology, sharing ideas and suggestions for small business and personal security."	Yes	Yes
/r/hacking101	117	208	"Learn basic hacking or die trying."	Yes	Yes

/r/hacktivism	349	592	"Ethical hacktivism discussion, ideology, and philosophy. Along with notable hacktivism projects. No illegal activity is condoned; no unethical activity by any entity is condoned either."	Yes	Yes
/r/howtohack	44,501	84,074	"The guide to resources to expand your knowledge and from there you can access our stronger resources for hands on training and wargames...."	Yes	Yes
/r/netsec	167,481	238,046	"Technical news and discussion of information security"	Yes	Yes
/r/privacy	67,114	165,857	"The intersection of technology, privacy, and freedom in a digital world."	Yes	Yes
/r/pwned	21,691	26,515	"A subreddit for data breaches, site defacements, rm's, hack logs."	Yes	Yes
/r/Real_hacking	148	496	"All other hacking subs have ether died down or the mods abandoned it. So we hackers need a new sub that can have relevant news."	Yes	Yes
/r/socialengineering	81,211	103,927	"A subreddit dedicated to the art and science of human manipulation and social hacking, as well as public relations at an individual level."	Yes	Yes
/r/youranonnews	386	423	News and discussion about Anonymous, hacktivism, internet culture, and related matters.	Yes	Yes

Table 4: Subreddits

All the forums and subreddits have been listed in alphabetical order. As noted in previous studies on online communities (Dupont et al, 2016), the methods of examining these forums have limits. Often the number of registered users does not portray an accurate number of active members; some accounts may have been long abandoned, some may have been one of multiple accounts created by one user in order to manipulate forum rankings or retain anonymity. Awareness of the infiltration of researchers, journalists and law enforcement investigators has meant that some forums are by invitation only or deliberately made difficult to find; it has been found that the higher in status the members are, the harder it is to access the websites and forums that they use (Dupont et al, 2016). Some sites also have an elite members section or membership status, only granted by invitation or once the member has been vetted and approved by administrators. However, as this research

focussed on the psychological processes in groups involved in hacking, rather than "elite hackers" this restricted access was not an issue.

4.3 Forum Discussions

This section attempts to determine to what extent there is an observable effect of group process within hacking communities online. Selected forums and subreddits detailed above, jointly referred to throughout as forums, were joined to enable the researcher to act as a "lurker" and observing message boards without posting or interacting. The observation (or lurking) on the websites was not explicitly for the purpose of data collection, but there are examples of discussions in Appendix 9.3. As noted in Chapter 3, there is some debate surrounding what is public and private online; therefore, if simple registration was required in order to view the forum threads they were included, but the forums with additional measures or requirements for membership were not observed. Some forums had sections which required additional membership registration, so these areas were also not included, but the rest of the forum was observed. If the researcher account was banned, this was taken as refusal of consent, and again, the forum was not observed further.

Across the various forums and subreddits listed, there were distinct similarities in the topics and discussions depending on the salient subcategory identity, as well as the behaviours of the members interacting.

Forum Name	General Hacking	Technology discussion	Coding	Market /Money	VIP	Community /Off-topic	Subcategory
Antionline	x	x	x			x	White-hat/InfoSec
BiTS Hacking	x	x	x	x	x	x	Mixed
DEF CON	x	x	x			x	Mixed
Greysec	x	x	x			x	White-hat/InfoSec
Hack Forums	x	x	x	x	x	x	Mixed
Hackaday	x	x	x			x	Grey/White-hat
HackThisSite	x	x	x			x	Education/White-hat
Hellbound Hackers	x	x	x			x	Education/White-hat
Offensive Community	x	x	x	x	x	x	Mixed
Sinisterly	x	x	x	x	x	x	Mixed

Table 5: Common Forum Sections

Table 5 focusses on the 10 forums that engaged most with this research and the researcher, with participants requesting updates and results from the data collections, either on the forums or through survey feedback. The content of forums in general was similar, with the main difference being that the White-hat/InfoSec forums did not have sections for VIP or marketing scams.

General hacking sections included the forum introductions, the rules, and usually the community section for off topic discussions. This was the place where examining the group norms initially occurred, as the threads containing forum rules were usually more relevant to the behaviour than the terms and conditions that one had to agree to in order to become a registered member. Technology and Coding sections focussed on reviews for hardware, software, techniques and training, with recommendations and advice being given. The forums that had a Market section acknowledged the cracking/spamming behaviour of the members, with these sections specifically catering to monetising hacks, trading data or hacked accounts, and techniques on scams. One of the "mixed" forums even advertised directly that the forum moderators could sell you spamming techniques or hacked data.

The educational sites were slightly difference again, focussing on the challenges and tasks that they set members to improve their hacking abilities. One of these required that members complete the first 10 basic challenges before the member could post on the forum; this was not however interpreted as a tactic to prevent spammers, rather a gatekeeping method for those interested in the community. The researcher completed the challenges, and the community was very positive towards her presence, which signified the interpretation had been correct.

Whilst there were disagreements and members banned in the course of these observations, these were not hugely common in the established communities. Usually these negative interactions involved n00bs (new or inexperienced group members) or trolls, who were either reposting or purposefully trying to start arguments. Even on the mixed subcategory forums, where people identified themselves anywhere along the Black-White -hat spectrum, arguments were expected to be evidence based rather than just opinion, but when consensus could not be reached, a common closing statement was "agree to disagree" (see Appendix 9.3.5).

The online observation was also the best method of observing the Black-hat behaviours, as they had far less inclination to participate in the formal data collections carried out in this research. Whilst there did not appear to be groupthink or conformity for the sake of it, the Black-hat and illegal behaviours were highly normalised, with the mixed forums never objecting to the topics. For example, if a member went for advice on what to do with data that they had hacked from another source, the comments invariably advised selling the data or spamming the companies or individuals involved. Even if in the original post the author had stated innocent or neutral intentions, the advice given was always illegal or immoral. Because of the awareness of observation in these communities it was difficult to find examples of decision making in these discussions. If the topic was illicit in any

way it was always referred to private messaging, or an outside method of communication, with members frequently stated that such conversations should not be shared on the open forum.

Conversly on these sites, the general/community sections often had interesting discussions, including reflections on the hacker identity and requirements to be considered as a hacker (see Appendix 9.3.6). In such discussions there were often references to the Hacker Manifesto (see Appendix 9.2) or other works such as Raymond (2001). These sources were used as evidence of the hacker traits one should have or aspire to have if they want to become a hacker. The often-cited hacker "stance" is stated to be:

1. The world is full of fascinating problems waiting to be solved.
2. No problem should ever have to be solved twice.
3. Boredom and drudgery are evil.
4. Freedom is good.
5. Attitude is no substitute for competence. (Raymond, 2001).

4.4 Offline Participant Observation: Hacking Conventions

Early in the planning of this research, one of the obvious avenues of offline participant observation and potential participant recruitment was hacking-related conferences. As discussed above and in later chapters, these forums and communities were not always welcoming to outsiders and were very sceptical of people asking for help, be it academic or otherwise. Posts made anonymously on forums that introduced the researcher were met with suspicion, derision, and occasionally hostility. It was strongly felt that a good alternative to making connections, and building a reputation, would be by meeting the communities in person. To this end, various hacking-related conferences were attended throughout the duration of this research.

As anticipated, these were excellent networking opportunities, allowing the researcher to speak with a wide variety of individuals with diverse interests and links to hacking, discuss the research and its purpose, as well as make contact with experts in the field. Although various individuals were happy to talk in an informal manner about their interests, there was initially a general disinclination to become more involved with the research. Such attitudes noticeably improved as the researcher gave talks at local and international conferences, as well as shared results as the research progressed. These conferences were invaluable for being able to observe the various possible identity groups and the ways in which attendees categorised and presented themselves at these events.

Conferences	Groups	Hacker Identity	Cybersecurity Stance
DefCon London	N00bs welcome but groups formed, sometimes hard to join existing group	Hacker/InfoSec personal/professional identity	Education, hacking techniques, find flaws, improve security
DefCon Las Vegas	N00bs welcome but groups pre-formed, easy to join existing large groups, personal/intimate groups harder	Strong hacker identity – large number of professionals but still conducted as hacker conference	Find flaws, showing off, improve security, disclosure to companies sometimes made after presentation on weakness
Hacktivity	Professional. Many lone attendees	InfoSec Professional Identity	Find attackers, improve security
BruCon	Groups formed, overlap between professional and enthusiast	Hacker/InfoSec personal/professional identity	Find flaws, improve security
SteelCon	Central group but many lone attendees, mixed	Hacker/InfoSec personal/professional identity	Education and information sharing, hacking techniques

Table 6: Key findings and differences at offline events

4.4.1 Local DefCon Meetups, London, UK, and DefCon24, Las Vegas, USA (2016)

DefCon (https://www.defcon.org/) was founded as a social gathering in Las Vegas in 1993. This group was mainly composed of people interested in computing and hacking, and so was held with the aim of sharing interesting discoveries and ideas relating to these topics. The popularity of the meeting within the group led to its being held again the following year, after which it continued to grow. The annual conference, regarded for many years as one of the most significant events in hacking calendars, is still held in Las Vegas. Its popularity has led to the formation of smaller DefCon groups around the world with their own regular meetups, which include talks and discussions on technology and hacking.

After the initial few months of forum observation, the researcher attended a local London DefCon meeting in May 2016 in order to conduct offline participant observation. The meeting was held in the function room of a central pub with seating at tables for up to 140 people. That evening there were an estimated 60-80 people in attendance. The researcher was one of four female attendees and the only one who was not accompanying a male. There was an evident hierarchy of known and regular members, but newcomers were common and welcomed. It was obviously a valuable networking opportunity for all in attendance, with introductions being one of the initial parts of the meeting. It was observed that there was some reaction from other attendees to the presence of the researcher as an unknown lone female, as if this were a slightly unusual occurrence. While the meeting had a relaxed atmosphere, with jokes and audience interaction encouraged, it was also

emphasised that all are welcome to give talks and that speakers, especially newcomers, are treated with patience and respect. The second talk at the meeting was quite casual, regarding a light-hearted look at the security of the Internet of Things (IOT), taking examples from the bizarre selection of devices that can now be connected to the internet, including sex toys. Although not explicitly stated, this talk seemed at points to be aimed more towards a male audience. During this talk a male attendee repeatedly turned to observe any reaction from the researcher following jokes that referenced sexual stimulation and female genitalia; this was uncomfortable, however subsequent attendance at these meetings made it clear that this attendee, who was not a regular, was behaving abnormally compared to the rest of the group. After the talks had finished the floor was opened up for questions, the majority of which were obviously attempting (and succeeding) to get a laugh from the audience or made to demonstrate the member's technical knowledge. Again, jargon and group in-jokes were used as a subtle way of reinforcing group boundaries; if you did not understand, you were not in the in-group (Terrion and Ashforth, 2002). Subsequent visits to this group saw fewer female references and reactions to a lone female, although this may be in part because the later topics were more serious or technical, and the researcher presented her work and therefore became more familiar to members of the group.

Attendance at DefCon24 in Las Vegas, August 2016, was a great help to this research. The attendance numbers that year were over 20,000. The conference has always been held in a casino, and due to its growth was held in the Bally and Paris Casino. The conference was divided into groups by specific areas of interest or topics, such as car hacking, social engineering, or lockpicking. These specific interest groups are referred to within DefCon as "villages". Each village had their own room and schedule of talks or activities, such as Capture the Flag (CTF) challenges, hands-on demonstrations, or workshops, all related to village topic. Space seemed to be allocated to villages according to popularity and what was available within the casino. Due to the size of the convention it was not possible to make contact with the overall organisers or attend every talk or village. However, leaders of the villages and some speakers were approached and were found to be incredibly helpful and willing to talk about the research. There were more obvious sub-groups, some identifiable by attendance of different talks or workshops. There appeared to be a lot of respect for all those involved in the conference, whether their contribution was technical or in talks. Goons (the name for conference volunteers) were often mocked for taking their roles too seriously or appearing to enjoy their "power" over normal attendees, but they were obeyed, and the organisers emphasised that the Goons were there for information and safety. There were some obvious in/out group references and sentiments, where preference or perceived superiority of one group or village

over another was expressed, or “in jokes” referencing events from previous years, that “n00bs” or new attendees would not understand.

Awareness of gender was less defined; although men outnumbered women greatly, no one expressed surprise or interest in the presence of lone women and the researcher was by no means the only one. It was, however, remarked to the researcher several times that as a female – and therefore a sought-after minority – it would be easier to meet more people. Conversations were easily struck up when queueing for entrance to talks, both with people who were attending for the first time, or regular con-goers. A common joke on forums and discussions leading up to DefCon was that people were looking forward to “LineCon” as a large amount of time is spent queueing for entrance to the talks and villages. Years of attendance were used as an icebreaking question, and possibly as a method of establishing informal hierarchy; those who were attending for the first time would, at least initially, defer in conversation to those who had been going for longer, even with no personal connection or proof of knowledge. Having conversations in queues was the easiest way to access attendees, including more established members of the community, although it was very much down to luck. More famous or infamous attendees tended to have a crowd around them and, depending on their status and involvement with the conference, different access. The researcher quickly found that examples of technical knowledge, even basic, led to conversations being taken more seriously, but most conversations were casual, with participants being more interested in the background of the researcher and reasons for attendance. As stated in the ethics outline for this convention, participants were informed at the beginning of conversation of the purpose of the researcher’s attendance, and it was made clear that the conversation may be recorded in the form of notes by the researcher, but no personal or identifying information was recorded in the notes. Although contact was not made with as many attendees as hoped, the experience in terms of furthering the researcher’s understanding of the hacking communities was invaluable. When asked how they became involved in the hacking communities, most people said that they had found these groups through their friends or at school, college, or university. There were a lot of attendees who were in the information security industry, but all emphasised they were there to learn and that attending was often the highlight of their year.

4.4.2 Hacktivity, Budapest, Hungary (October 2016)

Hacktivity is an IT Security Conference, the largest in Central and Eastern Europe, which started in 2004 (https://www.hacktivity.com/). Although there is no available data on the number of attendees for 2016, between 900 and 1,100 individuals attended the 2015 and 2017 conferences in Budapest (Hacktivity, 2018). In comparison to the DefCon convention, this was a more formal

conference, which orientated itself towards the defensive company viewpoint. This was not a surprise, considering it was focussed on IT Security, although it tried to emulate a “hackerspace” feel, with a room with bean bags and screens, to allow people to relax and talk more casually. There was however a strong professional presence, with companies taking a larger role in participation and sponsorship booths. There was another space with locks and tools for lockpicking, often regarded as an entry way to hacking, as well as some soldering equipment. However there did not appear to be any people to ask for help, or guidance as to what could be done, so whilst some sat and worked away, many attendees appeared to lack the confidence to join in when there was space available.

Despite the name of the conference, it was observed throughout talks and conversations that the term hacker was usually used to signify the “bad guy”, rather than a neutral term describing ability. The talks were quite defence orientated, but there was the occasional emphasis on the need for interdisciplinary approaches to security. There was a key talk which centred on behavioural economics, possibly because this field, whilst being similar, does not have the negative connotations that social psychology does within more technical fields. There were multiple discussions throughout all the talks on ways to modify and influence how people behave, and the ways that they “should” approach IT security. There were brief discussions on the differences between group and individual biases, as well as an overall bias within information security (InfoSec); speakers argued that there is too much emphasis and attention given to stop the sophisticated attacks rather than improving the basics of security and awareness. They suggested that this led to preventable attacks being overlooked and urged that individuals consider their aims and goals as InfoSec professionals. Within this discussion it was suggested that there is a possibility of a bigger threat from script kiddies (skids), who are unskilled, using programmes designed by others, rather than hackers.

Again, although there were one or two lone women in attendance including the researcher, the vast majority were men; in contrast however to previous conferences or meetings, there were no comments or interest given because of this. There was also a slight language barrier at this conference; as it is an eastern European conference, there were a lot more attendees from various European countries, with English being the international language. This was not just an issue for the researcher, other attendees were also heard talking about the language barrier. Wi-Fi access was given but required user registration to access it; it seemed to be trusted by a lot of attendees, with no problems reported. There was also a less obvious array of in/out-groups, for example, new vs old attendees, although it could be that veteran attendees were European and in their own groups, therefore this difference was potentially disguised by the language differences. At this conference there were significantly fewer people huddled round laptops together, most people appeared to be

alone or in pairs, with others in work related groups. There appeared to be a wide variety of ages present, although all within the standard working age ranges (18-65).

This conference, whilst not such a typical hacker conference was also valuable; it gave good insight into the attitudes of those in InfoSec who felt that hackers were a significant problem, whilst not acknowledging the overlap between their InfoSec work and hacking.

4.4.3 BruCon, Ghent, Belgium (October 2016)

BruCon is a 2-3-day Security and Hacking Conference hosted in Ghent, Belgium (https://www.brucon.org/2018/). This conference was smaller, with around 600 attendees, but in terms of attitude and atmosphere it marked a middle ground between DefCon24 and Hacktivity 2016; this is unsurprising as the conference states an aim as being to "create bridges between the various actors" within InfoSec (BruCon, 2018). There were more notable speakers from the InfoSec world that also regularly appeared in the "hacker" circuit, as well as a slightly more casual and familiar feeling to the conference than at Hacktivity; there were noticeably more Americans, and English was spoken more. This led to a greater mixing between different groups.

Again, many talks touched on behavioural economics; however, these talks did not always make their point well to the audience, as speakers tried to get volunteers for physical demonstrations and performative skits, with many of the audience unwilling to join in, which led to the talk losing momentum and becoming disjointed despite having an interesting premise. The researcher observed the audience during such talks, and the reactions suggested that many people were interested in a more human based approach to InfoSec but were perhaps not completely convinced by the suggestions they heard. Speakers were trying to encourage designers and developers of software and solutions to take more responsibility for adapting to human factors and changing their mindset when managing their work; there was no obvious enthusiasm for this. To the researcher it seemed that, despite the interest, the individuals felt that their technology-first approach was the best way to conduct their work. This is understandable, as many of them take pride in their work and want it to be the best technical demonstration of their skills; however, this inflexibility can result vulnerabilities and flaws being left undetected until spotted by someone else.

4.4.4 Local DefCon meetings, London, UK, and DefCon 25, Las Vegas, USA (2017)

Following on from attendance in 2016, a talk was submitted and accepted for the Social Engineering Village at Def Con 25 (https://www.social-engineer.org/sevillage-def-con/). The Social Engineering Village is recognised as the "human track" at Def Con, with the content and talks being on how to socially engineer others, how humans can be manipulated and hacked, and how it can be defended

against, rather than a technology focus. They hold various competitions and challenges for adults and children, including learning physical penetration, via assault courses featuring lock picking and detection technology, as well as their Capture the Flag (CTF) challenge, which involves participants conducting live telephone calls to a target company to try and capture information that could be used to penetrate their security.

Before presenting at DefCon25, a draft version of the talk was given at a local London DefCon meeting in February 2017. It was well received, with the audience engaging positively; there were however many questions regarding how the data was collected. Specifically, the group wanted to know how it was verified that the participants were "really" hackers; it was explained that there was no test or criteria to be met in order to take part in any of the studies. The majority of the audience seemed sceptical about this and therefore the veracity of the data. This was interpreted as a form of gatekeeping within the community, as it was the more known and established members questioning the reliability of such participants. It was explained that even by being on the related forums and subreddits, the participant was at least interested, even if they were not experts in hacking, and the research was looking at the communities as a whole, not just the "elite" members; considering the challenges in recruitment it was neither practical nor necessary to present barriers. This seemed to make sense to them, which in part is believed to be because these meetings tend to have a fair amount of novice or "n00b" members, who are interested and want to learn, and this is encouraged. It was also questioned how the results are verified. It was explained that that is impractical in any voluntary data collection. There is no way to know that a person has answered truthfully throughout, but even if some participants are purposefully misleading, there are still patterns to be seen in the majority of the data. This line of questioning however is yet another demonstration of the interest and critical thinking that is so often present in hacking communities; they want further understanding and to learn, and despite the at times critical phrasing of comments and questions, this group has continued to be very supportive of the research. The link to the first study survey was also shared by the group on their website. There were various individuals interested in participating in the research, and a couple more emails registering support; one of these also attempted flirtation, and because of this did not receive a reply.

The DefCon25 presentation was given in August 2017, at the halfway point through the research; the talk introduced and discussed the influence of group processes in hacking communities, as well as the initial results from the online surveys. It was well received, with positive and insightful comments and questions. It also increased the exposure of the research, potentially leading to more survey participants, although this cannot be confirmed due to the anonymity of the survey. The

status of speaking, even in a village rather than the main talk sessions, had a noticeable effect in casual conversations; when it was mentioned that the researcher was giving a talk, regardless of the fact that it was untechnical, the other person either deferred to the researcher, or provided evidence of their own expertise that had not previously been mentioned.

4.4.5 SteelCon, Sheffield, UK (July2018)

SteelCon (https://www.steelcon.info/the-event/) started in 2014, as the first northern hacking conference in the UK. Growing from 120 attendees to 450 since, attendance is capped by the capacity of the building. It is a far smaller conference than others attended for this research but very popular in the UK hacking community, with tickets selling out within minutes.

This was the last hacking related conference attended for the purpose of this research. The researcher presented her work and also volunteered to help at the conference, as a way of observing from a different perspective. There was a light-hearted approach to this conference, with sweets and toys being included in the "swag" bags – whilst people pay to attend the conference this is more to ensure that those who purchase the tickets attended; the fee is spent on the contents of the swag bag and the rest donated to charity.

As with previous conferences, there were well known members of the hacking community presenting, with an interesting mix of topics. There seemed to be a high number of students in attendance compared to other conferences, although this is believed to be due to the university hosting the event, and as well key organisers being staff at the university. There was also a free kid's track running alongside the main convention, which was aimed specifically at children interested in hacking related activities.

The researcher's talk was well received, with the room almost full. After the talk there were several questions, as there was with the London DefCon group, on how the data was collected and which communities had been approached. After the presentation had ended two younger audience members came to the researcher and thanked her for the presentation; they were interested and able in coding, they identified with the hacker identity (subcategories were not discussed) and expressed relief that they were not the only ones who didn't know if they "counted" as hackers. They also said that knowing that others felt like that made them feel more secure in their identity, as well as their hacking activities. This suggests a potential out-group within the in-group that had not been considered by the researcher, or a hesitation or deviance from the described stages of adoption within social identity theory. Another audience member later wrote about his SteelCon experiences in his blog and discussed the talks he had been to. The researchers' talk was described

as “an interesting insight into how hackers and their community perceive themselves, how being part of a group (or feeling that you are part of a group) can influence actions and decisions. I found this subject matter an interesting departure from traditional conference subject material, so good job SteelCon for promoting a different take on our community and industry,” (Nisbett, 2018). This did support other comments and feedback, that although the researcher’s topic was not what people attended for, it was interesting and stimulated conversations around the hacking community and the identity.

Another talk at the convention must be mentioned, due to its departure from the usual subject content at such events. The speaker detailed his journey into his InfoSec career, having overcome depression to the point of suicide. It was a moving talk, emphasising how he had turned to computing to alleviate his real-world loneliness; he referenced the researchers’ talk, acknowledging the community support and help he received from individuals he never met in real life. This was the first talk the researcher had attended that openly discussed mental health problems and was impressive given the social stigma attached to talking about such things, especially in work related or masculine environments. The talk was very well received, with a positive and supportive atmosphere, and the speaker invited others to contact him if they needed to talk to someone about their own problems with mental health.

4. 5 Discussion

As stated at the beginning of this chapter, there was no formal collection of data sets through participant observations. Observations from forums and conferences however are extremely valuable for contextualising the data presented in subsequent chapters; it also allowed the researcher to gather a collection of observations for expected norms and behaviour within these groups.

From the initial observations, there are similarities across the sites, which would seem to be familiar in any online forum, such as the information for new members. There are also the “in” jokes between more established members, as well as group jargon and language. The languages associated with hackers, for example “1337/leet[6]” speak (Mitchell, 2005) can be used as inclusive and exclusive: it can signal that a person is a genuine member of the community, those that do not know the terms are new or outsiders; alternatively, some groups regard those who use a lot of

[6] An alternate representation of text that replaces letters with numbers or character combinations.

"1337/leet" speak as posers or n00bs (new and inexperienced individuals), arguing that those with real ability and knowledge do not need to prove it through exclusionary language.

Table 7 lays out the key comparisons between the online and offline behaviour in these communities. All had elements of the group processes displayed except for offline events, where conflict was not observed; this could be that those who are more likely to engage in conflict avoid these events, or because the groups that might come into conflict avoid each other in these settings; alternatively, it could be that potential conflict is negated by the social norms in the offline world.

Behaviour/Process	Online (Forums)	Offline (Events)
Impression management	Present: Moderators in charge of the site, individuals in their posts.	Present: Hacker or professional identity, often combined. Previous conference t-shirts or badges worn.
Conformity / Groupthink	Varied: General consensus but debate always present. No evidence of groupthink.	Varied: General consensus on topics, but with debate.
Social norms	Present: Expectation of following forum rules.	Present: Expectation of following both social norms of the physical location and social norms of hacker identity.
Social roles	Present: Status displayed through length of membership, number of posts made, approval ratings from other members.	Present: Status not overtly displayed; often brought into conversation if person felt they had significantly different status (both positively and negatively) to others.
Conflict	Varied: Mostly forum members in the same in-group, some conflict with newer members or trolls.	Absent: No evidence of conflict between different groups.
Trust	Varied: Trust related to social roles and context specific.	Present: Trust shown in relation to the salient social norm.

Table 7: Comparative Online and Offline Behaviours

A consistent element across online and offline behaviour is the use, or rather lack of use of age to categorise and stereotype members: it is not often asked unless the individuals behaviour suggests an immaturity, and it is then used as a potential explanation, but it is not used to judge any potential hacking ability. Age of membership and established reputation is more often used to determine an informal hierarchy, with ability being its own merit. It was observed offline that older community members happily deferred to younger members when there was evidence of greater knowledge on a topic.

The focus of this research initially intended to be as balanced as possible across the Black-White hacker spectrum, but these observations were the first concrete confirmation of the researcher's

belief that there would be an imbalance. Online Black-hat behaviour was consciously withdrawn to private communication by the members; the observable group processes on these forums was limited by this. At the offline events individuals were likely to identify themselves as White-hat or InfoSec, but it cannot be assumed that those who did not do this were Black-hat. Therefore, it is impossible to estimate the presence of those who would self-categorise themselves as Black-hat.

The offline observations also reinforced to the researcher the importance of the hacker conferences, as described by Coleman (2010). She stated that these conventions are important to the community and often overlooked in their significance. The offer face to face interactions for an online identity and were obviously deeply meaningful for the attendees. It was evident that attendance at these events embodied the online spirit faithfully, makes social bonds and creating festive atmospheres (Coleman, 2010) for the community that otherwise tends to avoid close scrutiny. An element of this is evident in the impression management, where attendees are encouraged by organisers to enjoy the conference but to remember and respect the social norms (including personal hygiene) and the legal restrictions on activities.

Chapter 5: Study 1 – Online Survey

This chapter details the methods, analysis, and results of the pilot study and the first data collection study carried out.

5.1 Background

This chapter will discuss the resources used in designing and implementing internet-based data collection, especially with hard-to-engage participants. The target demographic is known to not share personal or identifying information, as well as having subcategories of collectives that enjoy "trolling" outsiders. Data discussed has been collected via mixed method online surveys. There are various challenges with online data collection, from participant recruitment to ensuring the integrity and representativeness of the results; and when the data is being collected from hacking communities who value privacy the challenges become more thought-provoking.

5.2 Pilot Study (2016)

To investigate the potential problems with recruitment and participation, a pilot study was carried out in January 2016; the aim was to ascertain the best methods of approaching the communities, as well as clarifying the most efficient collection method. The responses to this survey, although interesting as preliminary results and interaction with participants, are not included as part of the formal research data; it was felt that the data had more value related to informing the research design and it was not known how reliable or valid the results would be. This online survey was hosted on Google Forms for 3 weeks and shared across subreddits related to hacking. Following the participant observation of forums and subreddits (see Chapter 4), newcomers and questions were responded to in a more neutral fashion than on the forums; as such, it was hoped the users might be more accepting of the pilot study on Reddit as it is a well-known popular website, offering a less intrusive entry into the private hacking community.

The study had 49 submitted responses, which was better than anticipated, and encouraging considering the limited circulation of the survey, and the secluded community. Questions included: age, gender, continent, ethnicity, level of education attained, hacking activities, motivations, self-identified hacker subcategories, opinion on privacy and anonymity (see Appendix 9.1.1.1 for the full survey). The survey combined multiple choice questions with free typing answers. For example, when asking about gender it listed male, female, transgender or other with the option to add text.

This of course attracted some disingenuous responses, with one participant identifying themselves as a dolphin (who valued privacy online so others "could not see his flippers"), and another as a jar of mayonnaise. After removing these fake responses, the study had 47 participants complete it.

The threads were still met with suspicion and hostility (see appendix 9.3.2 for an example), voicing suspicion about the use of Google Docs and their tracking of user IP addresses. However, the overall consensus of participants was that, although wary, the majority would welcome further academic research on the social processes, stereotypes and cultures that are associated with hackers.

5.2.1 Results

The results shown in Figures 4-8 are the responses that were pertinent to the main studies, as they informed the design of subsequent surveys; for the full results, see Appendix 9.1.1.1. It was expected that the majority of participants would be male; the option of transgender was included, and this proved to be a positive inclusion for participants, who commented on often feeling overlooked or forgotten in such research. This was also the case in the subsequent studies (see Chapter 7).

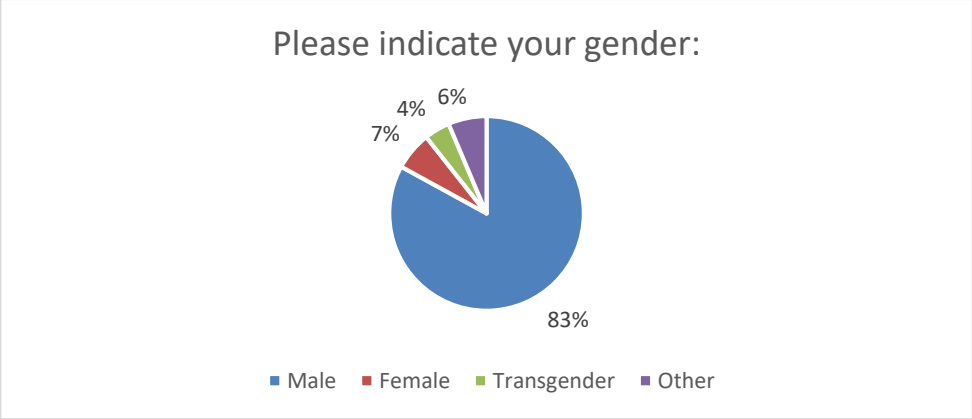

Figure 4: Pilot Study: Participant Gender

Of the questions in the pilot survey, the geographical region (Figure 5) was one of the more contentious; no matter how vague the region was made, participants did not want to reveal a geographic location. Various participants commented in the discussion threads that they would not take part in the study, purely because of this question. For this reason alone, in subsequent surveys conducted, no mention was made of location. In terms of the responses given, the regions were as anticipated, due to the language and physical location of the researcher. It is not considered representative of common hacker regions, as there are known hacking communities within South America, but this suggests that the survey was not accessed by individuals in these regions.

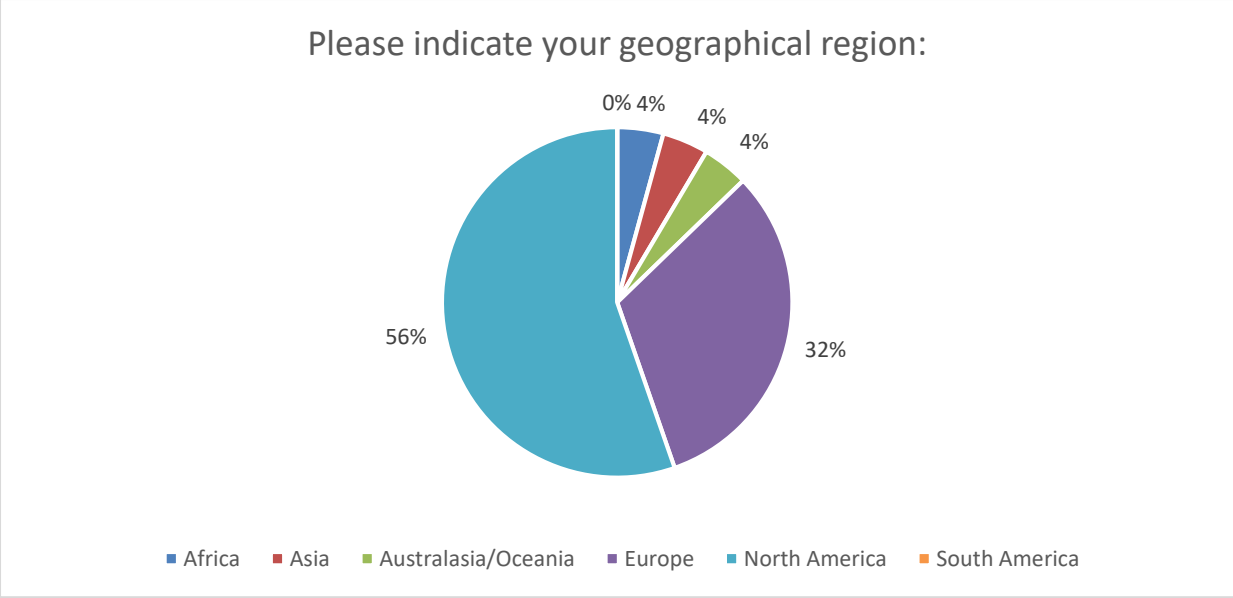

Figure 5: Pilot Study: Participant Region

Although an interesting addition to demographic data, the level of education (Figure 6) did not seem to offer any new insights into hackers, compared to the general population (Eurostat, 2018). As, again, some participants complained about its inclusion, it was not regarded as necessary in the studies, due to the risk of putting off potential participants.

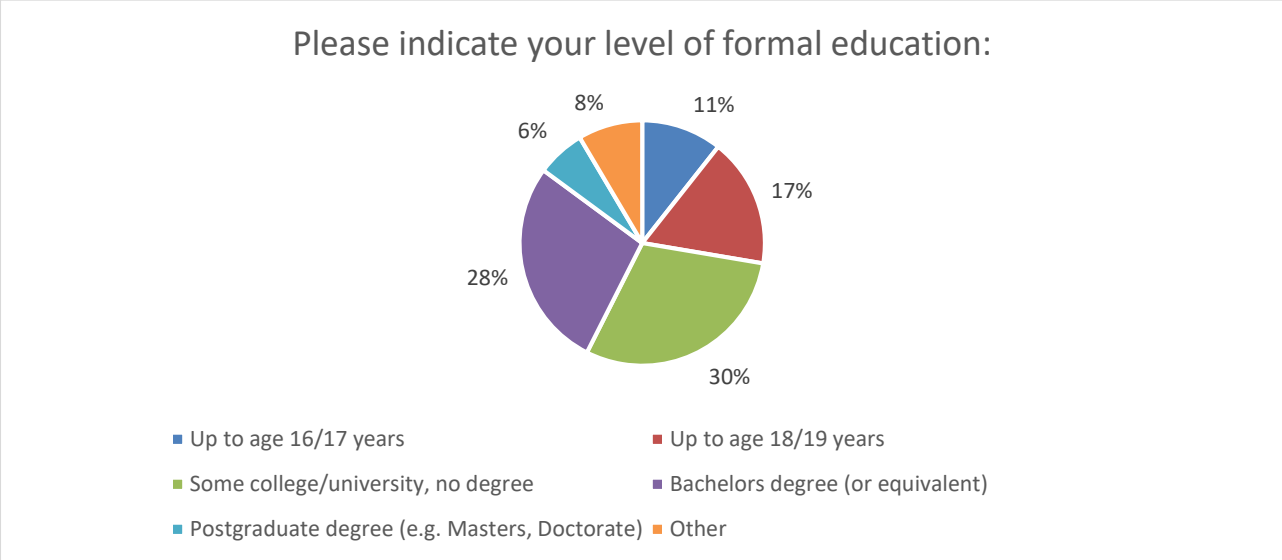

Figure 6: Pilot Study: Participant Level of Attained Education

Previous studies have investigated the motivations for hacking (Barber, 2001, Seebruck, 2015). These results support the previous findings, that curiosity and entertainment were common motivators. Therefore, it was decided that this question would not be used in subsequent surveys, partly as it was not contributing new knowledge, and partly to avoid repetition for prospective participants.

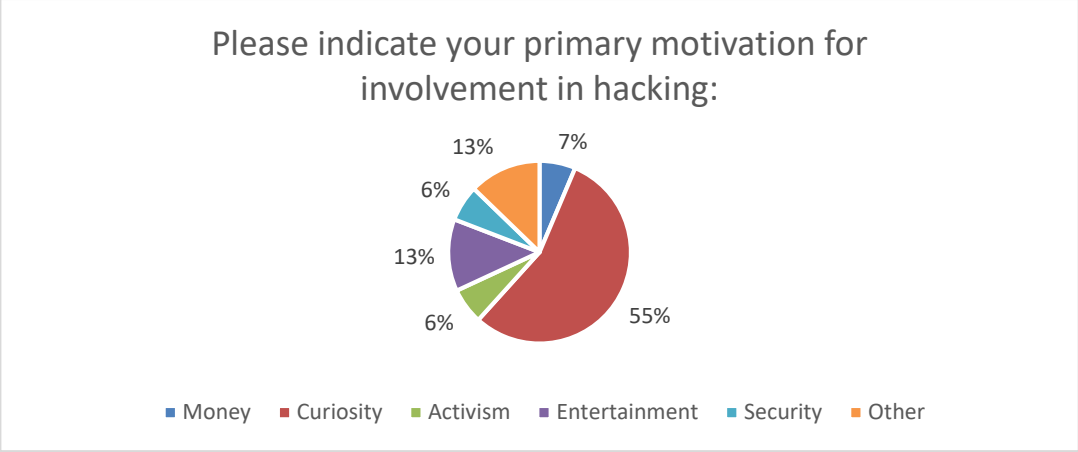

Figure 7: Pilot Study: Participant Motivation

The range of self-defined category (Figure 8) was diverse enough for it to be of interest, with a good level of response from participants; this question was expanded on in the following studies, as these categories were considered too narrow. It was also commented in the threads and comments below that one might not see themselves as only belonging to one subgroup and trying to decide on one category alone reduced the importance or significance of what they felt to be other elements of their social identity. Consequently, a wider range of subcategories was included.

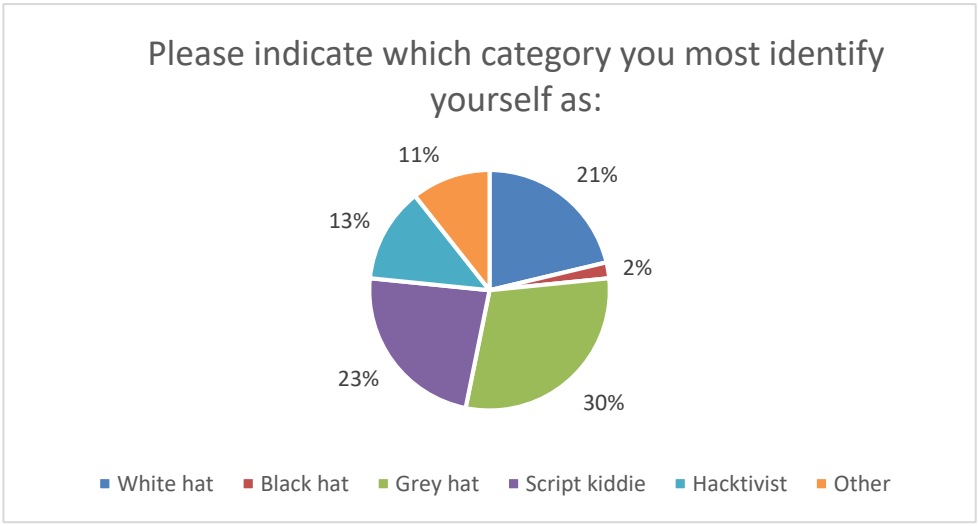

Figure 8: Pilot Study: Hacker Self-Categorisation

At the end of the survey, there was the option for participants to leave comments on the survey (Table 8). Whilst not every participant chose to leave a comment, the number made was surprising; the majority showed that the participants were engaged and interested in this research. As this data was to be used only in planning and constructing the survey for the first formal data collection, the comments were not formally analysed, partially as the comments were brief and to the point, and also as this was an explorative pilot survey.

Participant Comments (Pilot Survey)
Very well done.
Some of the questions [were] restrictive
This is a narrow range of definitions you're cramming us into.
Kind of gay
This survey takes for granted that "hacking" is in some way related to, or specific to, computers. This is not true.
You are mixing definitions (hacker vs cracker). The goal of these questions is not very clear.
This is probably the last place you want to look for genuinely skilled hacker groups. 4chan is probably better, but certainly isn't as active as it used to be in this regard. There are subreddits that have decent attendance of skilled code monkeys that would probably give you good results. But most hacker groups communicate with each other via IRC. As far as your study goes, I think that it's a fantastic idea and that the public NEEDS a better understanding of these people. I wish you the best of luck!
I have aids
I didn't like how the default for the questions was that you were hacking without permission. Hacking is NOT breaking into systems without permission. There are Black-hats but their activities shouldn't define the default of us all.
Could have more options at times. Also few people that are a member of a hacking collective will say that. You might get a number of false positives of script kiddies pretending to be Anon, Lolsec and lizzardsquad.
I support some [hacktivist] actions and will devote time to assist. I.e. Running scripts to identify Isis twitter accounts for further action. I also report shitposts and spam to improve the community.

Table 8: Pilot Study: Sample of comments

5.2.2 Discussion

This pilot survey highlighted several flaws in the design, with some participants objecting to the lack of scope for different definitions or understandings of terms used in relation to hacker categories. It was a short survey, gathering non-identifiable information, attempting to understand the range of people that become involved in hacking and what their basic reasons or motivations are. This was to find evidence that would support or refute generalised assumptions that are made about these collectives.

In terms of the demographic, this appeared to follow the general stereotype, being male, predominantly from North America and Europe, although this was highly likely to be influenced by

the fact that the survey was only shared on English speaking websites. The motivations and level of education were interesting, but it was felt that these questions did not meaningfully contribute to the aims of this study. There was an awareness that potential participants would be put off by long surveys, so the decision was made to not include these questions.

Part of the purpose of this pilot study was to attempt to identify key words and concepts and use them correctly according to the hacker community group norms; although participants complained about the small range of subcategories, no one argued that they were irrelevant or incorrect. This, in combination with the participant observations, informed the language and direction of the first full survey and qualitative interviews. The subsequent survey, for example, made greater use of the Likert Scale, giving more value to personal opinions, and allowed participants to select more than one hacking typology/subcategory.

5.3. Study One

Following on from the pilot survey, further websites and forums with relevant users and discussions were identified, using the same approach as previously detailed. This was done through simple web searches using keywords, and later recommendations from other forums. A user account was registered with these websites (through an anonymous email), so that conversations and threads could be observed. These accounts were used for observation not interaction. Participant observation has demonstrated processes and structure do appear to be enduring within the groups for this study (see Chapter 4), where there are multiple benefits to building a reputation on the forums. It was observed that across these sites there is an almost universal process for new members. There is always the expectation that they read the specific rules for the website or forum. The most common advice given is to “lurk moar”, or spend more time observing (lurking) the group behaviours on the forum and learn the social norms of the group. Those that do not follow this advice and break posting rules risk being penalised or permanently banned.

It was particularly useful to search these forums for previous discussions on academic research. Some discussed reported research; others were instigated by researchers conducting studies. Both were very informative in terms of what the groups were interested in and/or approved of; threads where researchers tried to engage the members were subjected to thorough questioning about methodology and ethics, as well as the purpose, of the research. In several threads posted by undergraduate students, when it was found the research was part of an undergraduate degree, it was generally dismissed as not being serious work, or not worthy of engaging with, and the student was advised to go back to lurking. The researcher also experienced this type of reaction. An example

of a more hostile community was WhyWeProtest, an Anonymous Activism forum[7]. This reaction was in part due to the fact that if someone searched for “Anonymous Forum” this forum was displayed, and subsequently attracted a lot of attention from researchers and journalists looking for Black-hat hackers and hacktivists.

This was invaluable knowledge when it came to compose the call for participants for the online survey as the researcher was prepared for a negative reaction when requesting participants. The pilot survey highlighted several flaws in the design, with some participants objecting to the lack of scope for different definitions or understandings of terms, and above all, the use of Google Forms which tracks and retains user information. These were altered and corrected, making sure of details such as tracking IP Addresses.

With regards to the risk of a cyber-attack or cyber-bullying it was unclear how real the threat would be for different enquiries. However, to avoid the possibility this research employed an overt approach – the identity of the researcher was not concealed. This has been successful in the past (Coleman, 2015), and whilst this still holds the risk of “verbal” abuse or cyber-attack, the aim was to minimise any challenge or entertainment value in finding the identity of the researcher.

5.3.1 Method

The survey was carried out using Qualtrics, which states in its terms and conditions that all data is owned by the researcher. Included in the recruitment posts was information about the study, the site hosting the survey and the researcher. It was recommended that readers used Tor browser or a VPN connection to help keep IP addresses private. Again, previous approaches to these communities have led to the potential participants demanding details of the research, including ethical considerations, which were provided. To minimise the uncertainty of genuine or false information, as well as exaggeration or boasting, the questions were designed to be simple opinion on widely used terms and shared beliefs, rather than asking questions about individual experience or skill. For the full survey questions please see Appendix 9.1.3.1.

5.3.2 Results

The online survey recorded 157 submitted responses over the course of two months, shared across thirty websites and subreddits. Two responses were removed, as they did not appear to be genuine,

[7] “Grad student, or eager-beaver undergrad. Meaning: they don't understand anything about the subject of their research whatsoever. Nothing wrong with that. However, when their research subject is a social group at very high risk of personal threat, ticking off university ethical guidelines is... less than adequate. I'm sympathetic to their goals…but the world doesn't need another poorly-conceived research study on the "hacker community".” Comment in reply to call for participants.

one participant, for example, citing 100 years' experience and answering every question with the same answer. Throughout the survey and recruitment there were no repercussions from posting this survey, despite the inclusion of the researchers' university and topic, which made the researcher easy to find online. Feedback and responses on the forums covered the entire range of possibilities; confirmations of completion, polite and impolite refusals, and users who made clear their disapproval of the research and the presence of the researcher. Four forums banned the researcher's account entirely and deleted the recruitment post. Due to the anonymisation there is no way of knowing if anyone from these websites completed the survey. The demographic questions elicited similar results to the pilot study.

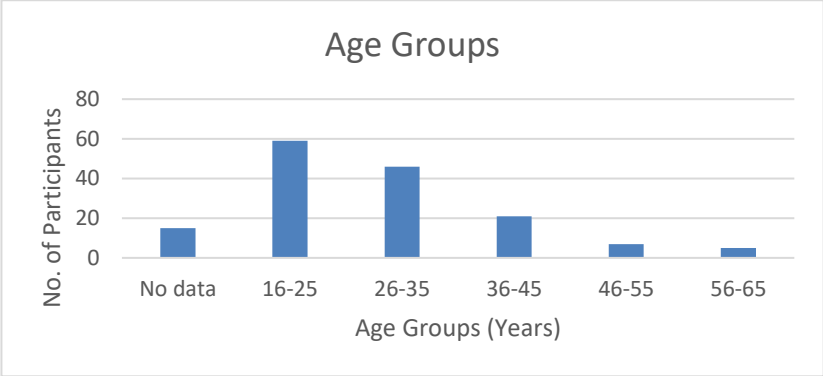

Figure 9: Study 1: Participant Ages

The range of ages recorded were 16-63 years, with the average (mean) age being 30 years. The median age of participants was 27.5 years.

As there was a gender imbalance (Figure 10), not only in the participants but also in the field of hacking and coding, there was a limited use for this specific demographic data; however, the general values were consistent with the results from the pilot study (see Figure 4).

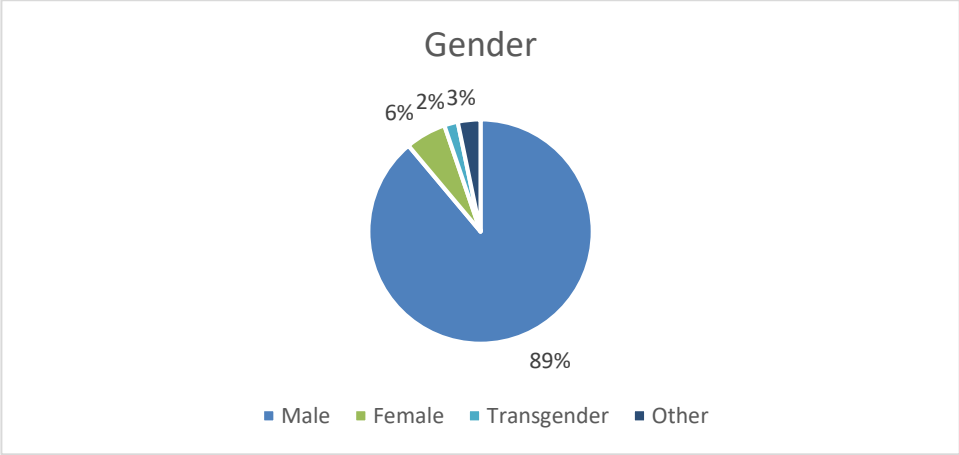

Figure 10: Study 1: Participant Gender

Participants were asked whether they were members in different types of forums (Figure 11), all related to hacking activities. As there were no clear definitions or sites mentioned in the survey, it is possible that different participants classified the same forums differently within the suggested categories. It appears however that overall the differences between the forums were self-explanatory, and these types of forum are distinct enough. Relatively few participants acknowledged being involved in cracking forums; this however, was anticipated, as the researcher was banned from four of these forums.

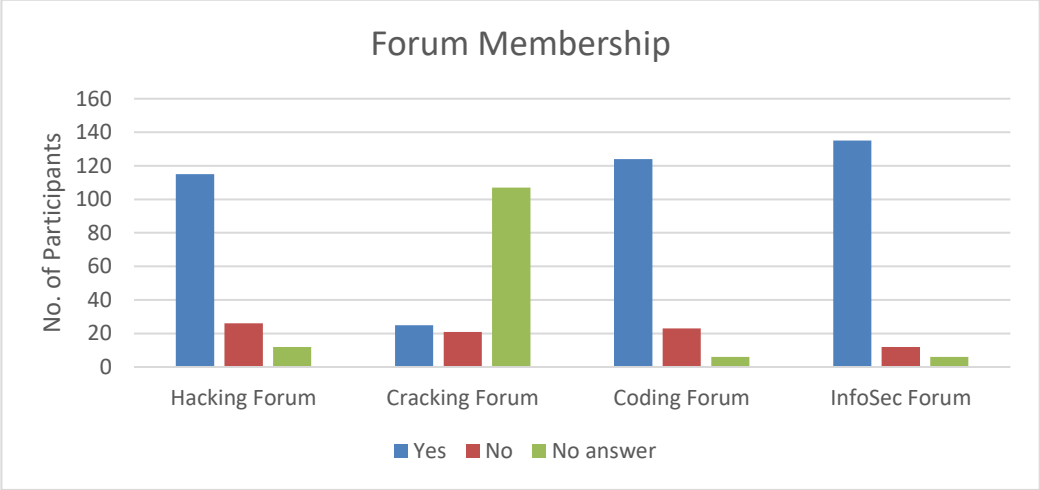

Figure 11: Study 1: Forum Membership

The initial results show that those involved in the hacking communities, including forums specifically dedicated to hacking, do not necessary identify themselves as hackers. When asked "Do you consider yourself a hacker?" only 52% of participants said "yes" (see Figure 12).

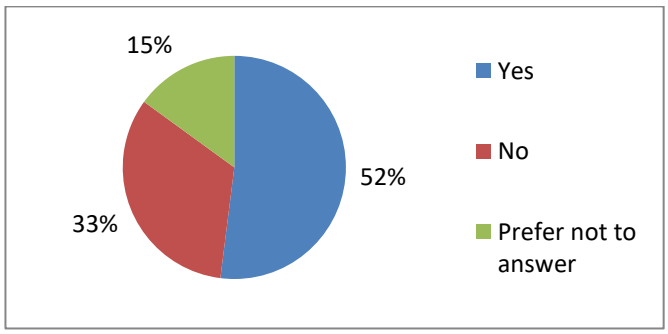

Figure 12: Study 1: Hacker Self-Categorisation

If participants answered "yes", they were then asked an additional question that was not available to other participants; they were offered different hacking sub-categories and were asked to select all that were applicable to themselves. No definitions were given for these sub-categroies, participants self-selected on their own knowledge of the meaning. As they could select multiple options, the

results are the percentage of all participants who identified with a specific category for this question (52% of the overall participants).

Category	%	No. of Participants
I consider myself a White-hat hacker	23%	30
I consider myself a Black-hat hacker	5%	7
I consider myself a Grey-hat hacker	30%	39
I consider myself a cracker	2%	3
I consider myself a script kiddie	4%	5
I consider myself an elite hacker	4%	5
I consider myself a cyberpunk	11%	14
I consider myself a hacktivist	8%	10
I disagree with these categories	7%	9
Other	8%	10

Table 9: Study 1: Selection of hacking sub-category

Aside from the breadth of different self-categorisations (Table 9), there is a mixture of assumed ethical stances within these categories, as discussed in Chapter 2 (see Figures 1 and 2). The assumption is that those defining themselves as White-hat hackers tend to be "moral and ethical", whilst hacktivists argue good intentions but potentially utilise illegal methods. Black-hat hackers and crackers are regarded as having unethical and illegal methods. Script kiddies, elite hackers, and cyberpunks are assumed to be in the Grey-hat hacker category, selecting a mixture of moral and legal stances and methods, as applicable to their aims. Whilst these stances are subjective, the ambiguity could explain in part why Grey-hat is the most chosen category.

There was also the option for participants to give an "other" subcategory. Whilst there were not many additional categories, some gave an explanation for their selection:

Participant Comments:
"Cryptoanarchist"
"Depends on the situation who i am"
"Former recreational hacker, now professional Pen tester."
"I assumed you meant cypherpunk and not 80s literary genre cyberpunk[8]"
"I consider myself uber."
"I would use the word "Tinkerer" as the most appropriate word to describe myself"
"I'm Black-hat for hack but I like money"
"I dislike the idea of White/Grey/Black in general. I also dislike the term hacker. Everybody uses their knowledge in profitable ways, it's just a matter of whether or not you pay taxes on it."
"Wouldn't generally use these terms but know what you mean"
"Whitehat, though I'm not that skilled yet. Learning everyday though."

Table 10: Study 1: Participant comments on subcategories

To try to verify "hacker" traits or values, participants were asked to respond to statements using a 5-point Likert Scale. These statements covered key hacker tenets, from the "hacker ethic", as discussed in Chapter 2, including attitudes towards online privacy and anonymity. It was anticipated that there would be strong agreement towards the positive aspect of privacy and anonymity, results are presented in the frequency tables below (Figures 13 and 14). Opinion was relatively divided when it came to whether online security should take priority over personal privacy. A possible explanation for this is the number of participants involved in InfoSec; although they value privacy, their work dictates the need for security to be prioritised at this stage of the research. However, InfoSec was not a subcategory option, so this is difficult to confirm.

[8] A cypherpunk is an advocate of strong cryptography and privacy-enhancing technologies (Narayanan, 2013). Cyberpunk is the literary genre, but also still a subcategory and counterculture with which some hackers identify, and this is what was being referred to in the survey.

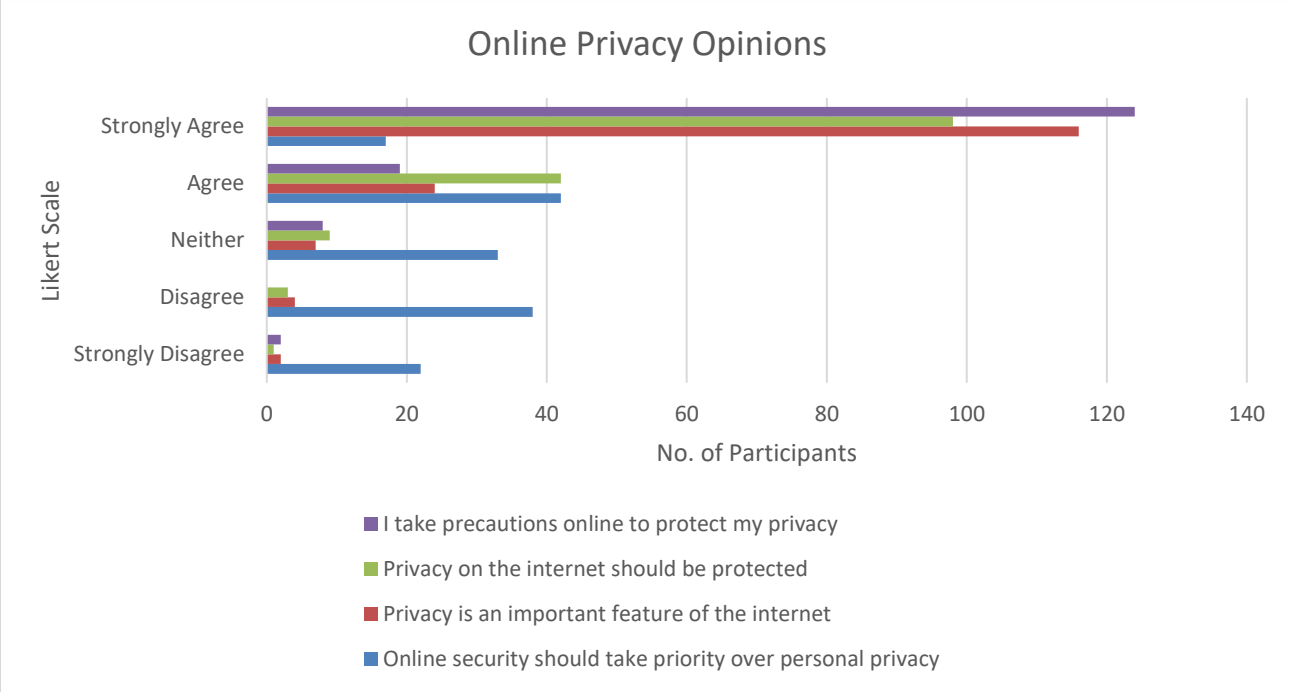

Figure 13: Study 1: Online Privacy

It is also possible that regardless of their hacker subcategory, participants were split relatively equally with regards to the security vs privacy debate. There was an option to make comments on the statements and some made it obvious that they felt it necessary for the safety of the online world, others argued that you can never be fully secure and therefore personal privacy is being relinquished needlessly. These arguments were found again in the subsequent study (see Chapter 6).

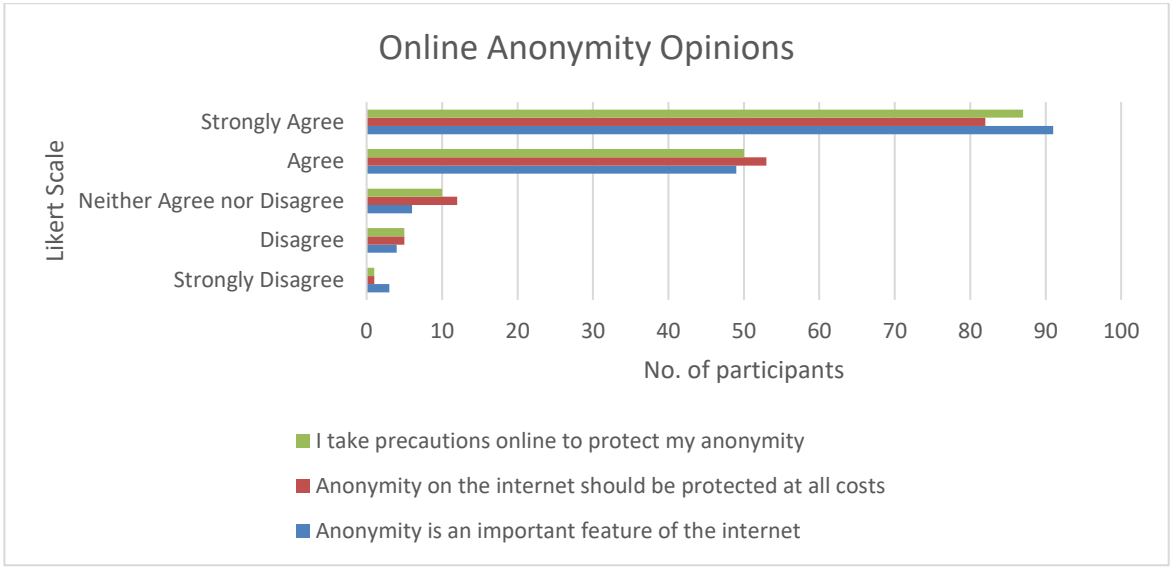

Figure 14: Study 1: Online Anonymity

It was expected that the "finding flaws and weaknesses" statement (Figure 15) would be strongly agreed with by many of the participants, as it is often an active element within hacking practices –

find and fix or use the problem. What is more interesting is the sharp agreement in *exposing* problems, as opposed to *exploiting* them, where the majority were in disagreement or neutral. It is felt that this is contrary to general opinions about hackers, along with their negative stereotype, suggesting that rather than wanting an advantage over others, many hackers want technology to improve and be more secure.

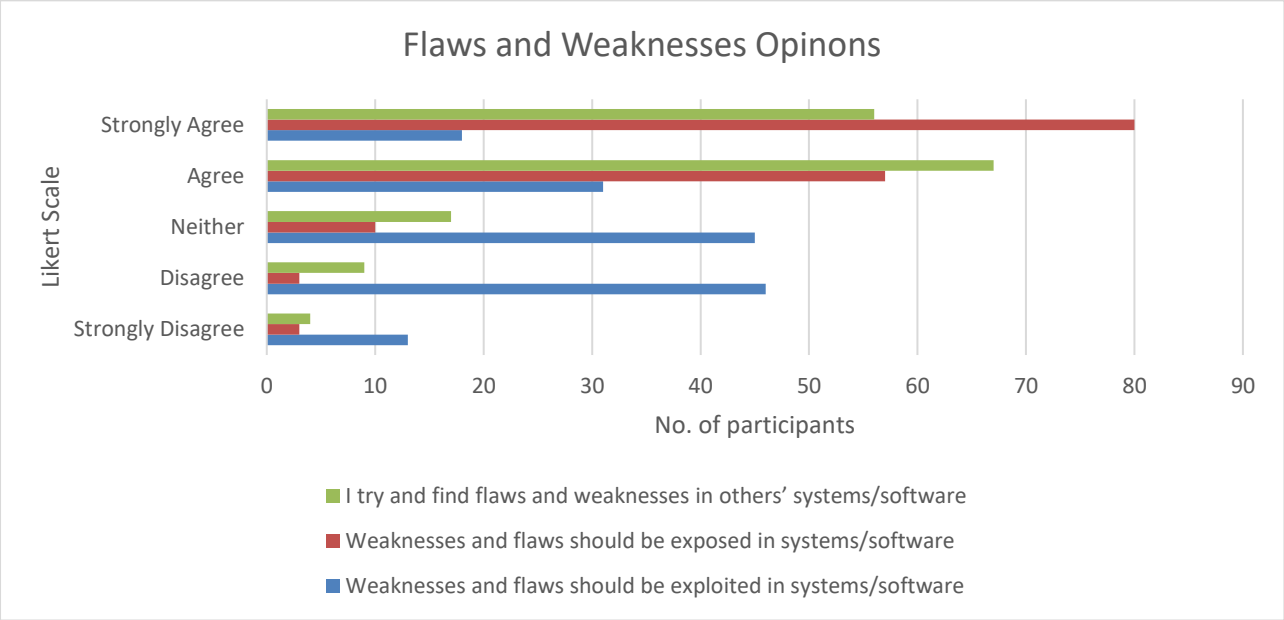

Figure 15: Study 1: Flaws and Weaknesses

At the request of many participants, the basic results of the survey were shared with these communities. This was well received, and it is believed this action alone encouraged group members to interact with the researcher further. The results have also been used as an initial discussion point in interviews.

5.3.3 Analysis

Analyses were performed on two types of variables: nominal (categories with no intrinsic order, e.g. a concept or engaging in a behaviour) and ordinal (categories with a clear order, e.g. Likert Scale). The analyses were conducted to find relationships between the variables and the self-identification as a hacker. Some ordinal variables were evenly distributed, but others such as age or years of experience required transformation. Initially these were grouped as evenly as possible, however, for the sample to be valid in the statistics test, the groups were condensed. Chi-square analyses examined the relationships between nominal variables.

Crosstabulation: Hacker Identity and Age

		Age group (Years)		
		16-35	36+	Total
Hacker	No	33	12	45
	Prefer not to say	16	4	20
	Yes	56	17	73
Total		105	33	138

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.372[a]	2	.830
Likelihood Ratio	.374	2	.829
N of Valid Cases	138		

a. 1 cells (16.7%) have expected count less than 5. The minimum expected count is 4.78.

One cell had an expected count less than five (16.7%); there was no significant relationship between age and whether or not the participant defined themselves as a hacker, with p = .830. However, this suggested another hypothesis: it is experience rather than age that matters in relation to hacking. To test this, the number of years' experience were grouped together. As there was no simple way to divide this equally, it was loosely based on the expected time to proficiency when learning a new language (Eaton, 2011), and then further grouped in pairs to ensure a valid count.

Crosstabulation: Hacker Identity and Years of Experience

		Years of Experience			
		1-5 Years	6-15 Years	16+ Years	Total
Hacker	No	40	7	3	50
	Prefer not to say	13	10	1	24
	Yes	30	33	16	79
Total		83	50	20	153

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	24.385[a]	4	.000
Likelihood Ratio	25.883	4	.000
N of Valid Cases	153		

a. 1 cells (11.1%) have expected count less than 5. The minimum expected count is 3.14.

The Chi-square test for association was conducted between hacker self-identification and years of experience in hacking. There was a statistically significant association between hacker identification and years of experience, p = .000, however one expected cell frequency was less than five (11.1%), meaning the results must be interpreted with caution.

Crosstabulation: Hacker Identity and Forum Membership

Count

		Hacker Forum Membership		
		Yes	No	Total
Hacker	No	32	17	49
	Prefer not to say	12	3	15
	Yes	71	6	77
Total		115	26	141

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.436[a]	2	.001
Likelihood Ratio	14.376	2	.001
Linear-by-Linear Association	14.320	1	.000
N of Valid Cases	141		

a. 1 cells (16.7%) have expected count less than 5. The minimum expected count is 2.77.

The Chi-square test for association was conducted between hacker self-identification and whether the participants was a member of a hacking related forum. There was a statistically significant association between hacker self-identification and forum membership, p = .001 but again one expected cell frequency was less than five (16.7%).

Whilst these results do not explain the relationships between the variables, the statistical significance supports the qualitative findings within the research. The number of possible subcategories or choices, such as the 5-point Likert Scale, and relatively small number of participants (for a quantitative study) limited the statistical analysis that was possible with this data. Further

analytical tests were conducted on the variables; however, the low cell counts made these results invalid.

5.4 Discussion

There are many more users registered on the forums than submitted responses to this survey; however, given the private nature of the communities, these results were very encouraging. Although not probing deeply into the group processes, this survey yielded some interesting considerations. Comments on the survey have reinforced that there are many users across different sites that are interested and encourage such research; this emphasises the significance and importance of social psychological research and human factors within cyber security. By demonstrating an understanding and respect for the hacking communities' perspective, including use of appropriate terminology and acknowledging potential security weaknesses in the methodology, members were more willing to be participants. Whilst there were still elements of online abuse directed at the researcher, it was far less than expected and interspersed with other forum members defending the survey and recruitment post, citing the explanations given and the understanding of the community[9].

Whilst the majority of the participants fit the broad "hacker" stereotype of being young and male, the data suggests that the groups are not as young as often stated. The subsequent data suggests that this is where the accuracy of media portrayals end. In many areas and cultures, age is associated with wisdom due to having had more experience; this, however, is not as applicable in the case of hacking. The use and development of technology mean that it is often younger people who are more involved and computer literate, although this gap is slowly closing. The fact that it is years of experience, not age, that has the relationship with the hacker self-identification supports the participant observations that age is not used to judge ability; whilst someone may know more through more experience, a person in their 20s who has been hacking since they were 10 will know more than someone in their 40s who only recently became interested. Forum membership was also related to whether the participant defined themselves as a hacker or not; this will be discussed further in Chapter 7.

[9] "The research is very clear, it's been approved by a university, he explains it all, this was done respectfully. There is no "hey gaiz! Coolio Wow Bang, it's just a questionnaire. IPs are explained. I agree with the well thought out response about hacktivism and that most hacking is legal. Answer/ don't answer but let the rest of us get on with it." Response to the hostile remarks on the call for participants thread.

The use of this data, in conjunction with the other studies, has allowed for methodological triangulation, creating a more accurate image of the hacker community. The sample size was better than anticipated for this study. It is believed to be relatively representative of the communities, although more participants described themselves as being on the “White” side of the hacking spectrum. Access to Black-hat hackers was not expected, but as there are often links and overlap with cybercriminals, it seemed unlikely that this portion of the community would volunteer information about themselves.

There is the possibility that there were intentional respondent errors in the data; the false submissions were removed, and if there were other false responses, the data given was inconspicuous from the genuine responses. Some surveys were not completed, but it was felt, given the nature of the community, any information was valuable. Equally it is possible that there were some different understandings of some terms, but this was minimised through the forum observations, using the jargon and terms as accurately as possible.

Chapter 6: Study 2 - Qualitative Interviews

This section describes the background to this study, explaining the qualitative methodology of this data collection in greater detail, as well as specifying the interview responses and data analysis. The limitations of this research are identified in the conclusion section.

The data from this study has been examined and checked to confirm initial interpretations. The long engagement with the respondents as well as the triangulation in data collection (with the survey responses) adds to the credibility of these interview responses.

6.1 Background

Continuing from the participant observations and using the results Study 1, the researcher put out a call for participants, stating the need to interview people involved in the hacking community as part of this investigation. As this was an exploratory study in an emergent area, there was no prior theory or hypotheses to test, the researcher used a semi-structured interview approach, addressing the key aims of this research: the hacker social identity; group processes; relevance to informed use and cybersecurity. The interviews used a set of questions with follow-up questions to explore answers in further detail. For ethical approval, participant information sheets, and participant set questions, please see Appendix 9.1.4.

6.2 Method

Semi-structured unrepeated interviews were conducted with the volunteers from March 2017 to January 2018. Participants were initially self-selected; individuals who had identified themselves as hackers or being involved in InfoSec (information security) volunteered for a confidential interview in this study, following the researcher's talks at hacking related events. To recruit further participants, the researcher made appeals on the forum boards, and approached various individuals who had identified themselves as hackers or being actively involved in hacking and InfoSec communities. This was done in person at hacking conventions, and online via Twitter and forums. If individuals were interested in the research and willing to be interviewed, they were sent the full participant information sheet and the set of questions; it was explained that the interview was semi-structured, and subsequent questions would be asked if applicable. If they were happy with the information and the scope of the questions, an appointment was made to conduct the interview at a convenient time.

Interviews were carried out via the participants' preferred mode of communication, as approved by Bournemouth University ethics board. Thirteen of the interviews were remote, one was conducted in person at the participant's request. The remote modes of communication included Skype, email, Pidgin Instant Messenger, and Discord Instant Messenger. At the beginning of each interview the participant was asked if the conversation could be recorded, if applicable. All participants completing a spoken interview gave permission for the interview to be recorded. They were all asked to confirm that they had read the participant information sheet and understood the purpose of the research. They were asked to confirm that they had read and agreed to the participant statements. Once this was done the interviews began. The interviewer asked participants how they became involved in hacking, how they would describe a "hacker", and their experiences or examples of trust in their community behaviour (for the initial set of questions please see Appendix 9.1.4.1). Participants were prompted to give concrete examples of trust activities. The interview ended by asking participants how they felt about the future of hacking and the related communities. The spoken interviews lasted between 40 to 120 minutes, although there was no time limit given; participants were asked if it was permissible to record the interview, all agreed. Where the participant had elected to use email or messaging, the interview was continuous until all questions and sub-questions had been addressed. At the end of the interview, participants were again asked to confirm that they consented to their data being used in this study.

6.2.1 Participants

Fourteen participants were interviewed, twelve males and two females. They were recruited via forums, hacking related conventions, word of mouth, and Twitter. Recruits were informed that the study aimed to investigate how group processes and social identity within online hacking communities affect the members at individual and group levels. All participants either identified themselves as hackers or had an active interest and participated in the community (see Table 11). From the answers given, the researcher assigned a position on the black-white-hat scale if the participant did not self-categorise themselves. To protect the individual's identity and encourage involvement no geographical or personal information was requested from the participants. Some participants gave their age, other ages are approximated from information given by the participants. The majority were white and western, with P13 claiming to be Russian. This is entirely possible as they were recruited to the study by a fellow participant who knew them only through online forums but this cannot be confirmed. Participants reported a range of technical computing skills from basic to advanced; the majority of participants currently work in information security related jobs. Others emphasised that their skill set was more related to the human aspect of hacking, for example social engineering. All interviews were recorded and transcribed in English. Where appropriate participants

were asked to clarify if English was their first language. Those who were not native English speakers are denoted by the * symbol next to their participant number.

Participant	Gender	Age	Scale	Level	Self-Defined Category
P1	Male	50s	White-hat	Expert	Former Hacker/Security Practitioner
P2	Male	70s	Neutral	Expert	Technologist
P3	Male	50s	White-hat	Expert	Security Practitioner
P4	Female	40	White-hat	Novice	Security Education
P5	Male	50s	Grey-hat	Expert	Former Hacker/Security Practitioner
P6	Male	Unknown	White-hat	Expert	Hacker/Security Practitioner
P7	Female	40s	White-hat	Expert	Hacker
P8	Male	30-40s	White-hat	Expert	Hacker/Security Practitioner
P9*	Male	40s	White-hat	Novice	Security Enthusiast
P10	Male	25-35	Grey-hat	Expert	Social Engineer
P11	Male	40s	White-hat	Expert	Former Hacker/Security Practitioner
P12*	Male	20-30s	White-hat	Mid	Penetration Tester
P13*	Male	Unknown	Black-hat	Mid	Black-hat
P14	Male	20s	White-hat	Novice	Security Enthusiast

Table 11: Study 2: Participant details.

As with the other data collection studies in this research, there was no criteria for or barrier to any one participating; two participants did question whether they would be able to help in this research due to their lack of experience. It was explained that their insights as a novice member, or "n00b", were also valuable.

6.3 Results

Given the different modes of data collection, both written and spoken, qualitative thematic analysis (Braun and Clarke, 2006) was deemed the most appropriate technique to use. The focus on the content ensured a more accurate analysis of the data, even if the collection method varied (spoken, versus written, remote versus face to face). Within this research the decision was made to use deductive thematic analysis to continue to build the group of themes within the data, informed by observations and data from Study 1. This however led to a combined objective and emergent analysis approach; there were some apparent pre-figured themes, with categories of interest being social identity and group related behaviour. Emergent thematic analysis was employed as appropriate to develop a fuller representation as it is acknowledged that these pre-figured categories are broad and subjective concepts, and that there is a lack of detailed psychological research involving hackers that does not pre-define them as criminals. This supported the decision to use thematic analysis, allowing the researcher this flexibility.

Before beginning the thematic analysis, the overall word frequency results were examined, from all interviews. Figure 16 demonstrates the most frequently used words by size; this has been included for illustrative purposes only, as an example of the language used across the interviews. Further analysis of specific words and language used was not conducted, as verbal interviews were far longer than written ones, which would give greater emphasis to those participants' views and potentially skew the results.

Figure 16: Study 2: Word Frequency Cloud (all participants)

The data were coded in NVivo software. In the first stage of analysis word counts were used to find the most mentioned words or concepts; where there was significant meaning ascribed to the words and it related to something important to the overall research question (Braun and Clarke, 2006), these were used as key words to begin developing categories (see Table 12).

Key words	Sources	References
Hacking	14	190
Hacker	14	188
Information	14	101
Defcon	8	94
Online	13	93
Group	14	86
Hackers	13	76
Community	14	73
Computer	12	70
Mindset	8	59
Curious	11	45
Identity	8	25

Table 12: Study 2: Interview Key Words

With these initial categories, coding of the interviews began. Where necessary, new categories were created; some of these categories overlapped with each other and were examined further to see if the categories were sufficiently distinct, otherwise they were merged; for example, hacking/hacker/hackers were all separately identified as key words but merged into a single category.

Having identified key concepts across the interviews the researcher also performed open coding, identifying hacker definitions, behaviours, and attitudes in the interview transcripts. Once there were clear and clarified code definitions, from both the researcher coding and the word count query, similar or related concepts were clustered into themes.

Themes	Description	Keywords
To Hack (verb)	General hacking constructs; relevance of information sharing, privacy, security	Hacker(s) Information Anonymity Privacy Security
Hacker Identity	What are hacker traits? Emphasis on mode of thinking, curiosity, influence of subcategories	Mindset/Mentality Curiosity Learning Subcategories
Community	Group behaviours; online and offline aspects of the community; meeting other hackers – trust; conferences	Groups Online Offline (DefCon) Trust

Table 13: Study 2: Interview Themes

The relationships between the thematic categories were examined using a semantic approach, looking for patterns in reported experiences and concepts. The themes were refined during the writing process: To Hack; Hacker Identity; and Community. Within these themes keywords and ideas were discussed by participants, demonstrating their experiences and understanding of the community. The semantic approach was chosen in order to allow comparison between the quantitative and qualitative data sets in terms of concepts, their importance to the participants, and their perceived meanings (Braun and Clarke, 2006).

6.3.1 "To Hack"

One of the first things that was evident in the interviews, is that hacking was definitely used as a verb. In order to be a hacker, you had to be active and want to "do". The opening question at the beginning of the interviews asked the participant to describe what they understood a hacker to be. As mentioned in Chapters 1 and 2, "hacker" is currently used in many different ways, despite its original meaning, with participants having diverse opinions on the term. The word "hacker" itself was acknowledged to have been perjorised by various parties, such as the media and politicians, meaning there is often no distinction between the different types of hacking carried out. Whilst some participants felt this had irrevocably taken the word 'hacker' from the community, others felt that there was a legitimate basis for this use of the term:

> *"What I do is no different from what the criminals that we call hackers do. The only difference is I do it on commission and with permission."* (P5)

Some felt that the standard definition, of "an unauthorized computer user" (P14), was sufficient and to try and give more detailed meaning to the concept of a hacker was to unnecessarily complicate it. Nine of the participants however felt that this description did not convey the depth and breadth of knowledge that one should have to be a hacker. They expressed the need for a hacker to be informed, not just on coding or technology, but also with regards to important elements such as anonymity, online privacy and above all information security.

Information

In their answers, the participants addressed the need for and the use of information within hacking communities, although the responses were less varied than expected. According to the participants the clear aim of anyone interested in this community is to gain knowledge, to learn more: for a "pure" hacker, information was currency and valued beyond money. However, there was a homogeneity in the ways they discussed information being used. It was relatively binary in that information on hacking and being shared by hackers was good; information being collected by an

out-group was negative, as they felt it would be used against them in some way, either to encroach further on their privacy, or to perpetuate the negative stereotypes of hackers.

There was also a certain level of distrust and paranoia regarding out-groups or individuals who wanted to gain personal information. Those that expressed this clearly appeared to feel vindicated by the revelations such as those in the Snowden files (Ball, 2013), and the extent of government surveillance:

"I've always been very aware of the value of information to people and information about people to others, and the fact that it's very much a manifestation of information is control. Most people for a long time thought I was paranoid…I've always been deeply interested in privacy and identity. I've maintained a very, very small information footprint deliberately…it occurred to me that there was benefit in maintaining your privacy and being aware of what information was available to the world about you and who held that information…I also avoid photographs for the same reason. It's all about identity." (P5)

Whilst P5 went to further lengths to ensure their privacy, other participants also expressed scepticism about the use of their information, and what information was given back to the general public:

"We're already in a new cold war and you can tell that there is an ongoing cyber war between US/Russia/China." (P12)

Five participants discussed how the lack of knowledge and information led to fear-based reactions to technology; for four of them, part of their motivation in being involved with hacking communities was to combat this, often through education to the general public.

"I think people maybe my age, I mean I'm 40, so people of maybe my age and above like, certainly my parents, they use tech[nology] but they quite suspicious of it" (P4)

The remaining participant although involved in the hacking community and conferences did not mention education, just stating her suspicion and distrust:

"I worry for our future…it seems every time I turn around someone in government is trying to pass some legislation on tech that they don't understand…Those who don't understand shouldn't try to make rules for everyone else. I think there is far too much ignorance in the general public as well, with propaganda delivery via social media like Facebook, they can influence the hearts and minds of people who are indifferent, ignorant or apathetic into believing that hacking or hackers are all criminals and that certain technology needs to be regulated in order to satiate their fears on terrorism and national surveillance. I just don't trust the general public or my government." (P7)

Whilst it was mentioned in a different context, another participant made a similar statement with the sentiment of uninformed individuals and groups creating the laws and norms:

> *"I think we have too many laws on the books regarding hacking or computer work, written by people who don't understand hacking or computer work."* (P1)

Anonymity

There was a general consensus that anonymity was being eradicated online; although not mentioned by all participants, the ones who did discuss anonymity regarded this eradication unanimously as a negative.

> *"If someone is anonymous, society becomes a meritocracy judged on skills and ability, not who you are related to or what school's you went to… online the sense of anonymity allows me to be more open."* (P10)

> *"The key point of anonymity is, you can only be judged based on what you are putting forward."* (P8)

The idea of a meritocracy is a central concept in hacking communities, where it is not important who you are, but more what you can do. The latter part of P10s statement is an element of benign online disinhibition as described by Suler (2004), supporting the idea that these communities serve that positive purpose for their members. There was a participant who had a different view to the group norm on anonymity, stating:

> *"Everything I do is legal and there is no need for anonymity… I wouldn't trust anyone on the internet and I wouldn't work with someone that I don't know…I don't believe in anonymity to be honest. I guarantee you that there is always a way to track someone…The whole concept of the internet is similar to the enigma machine; it's broken, but why would they tell you that?"* (P12)

Whilst this participant was still not regarding anonymity as a negative, by stating that they didn't "believe" in anonymity, as well as the reasoning for not needing it, they are expressing another distrustful sentiment against the out-group, "them", in this case meaning law enforcement agencies. This was also mentioned by another participant, stating:

"We live within this denial bubble of believing that we are relatively anonymous, we're not anonymous in the street, London has how many cameras? 100,000 in Chicago or more." (P2)

Privacy and Security

Contrary to expectations, privacy was not as prevalent as anonymity in participant answers, with eight participants mentioning it explicitly. Where it was discussed, it was regarded as important but broken or even already gone from the internet. The majority felt that personal privacy was a personal responsibility, although six participants observed that this was impossible due to the amount of data routinely collected on all internet users through every transaction, and the data breaches from large corporations.

All of the participants mentioned security and discussed its role in the online world, as well as hacking communities. Three were not unaware or uninterested in security but made no specific mention of how they approached it. Overall the consensus was that security is too often an afterthought when programmes and apps are being developed, and it is not something that can be added retrospectively. Opinion was negative as to whether this would change in the future, as it was pointed out, security is rarely the main goal or aim in development.

It became apparent that there are two broad but distinct approaches to personal privacy within the hackers. The first was to protect your privacy simply by not putting personal details online. This was used to varying degrees, some taking it very seriously allocating time and modifying resources to ensure the smallest possible online footprint. The second approach was to be "open" – not make attempts to hide identity or links to the offline world. Whilst this was not to the extent of self-doxing (revealing their own real-life identity), there was no "secret" life; the logic behind this was that if there is no interesting challenge, those inclined to find personal details would look for a more interesting target. Others felt that as companies had all their data anyway, and these companies were at far greater risk of being breached or hacked, their personal privacy and data was beyond their control to secure. Therefore, beyond basic safety, no additional precautions were taken.

6.3.2. Hacker Identity

An aspect of the hacking identity that was mentioned by eight participants was the existence of the "hacker mindset". Even if those words, or similar ones were not explicitly said, the majority expressed the feeling that there were certain types of thinkers who were more likely and able to be accomplished hackers.

"It's down to self-definition, if you're think you're a hacker…it's not for anyone else to tell you otherwise…It's got to start with the mindset" (P5)

"Radically different kinds of thinkers willing to explore a very complex space in order to see what [technology] can be made to do" (P2)

"Playing with tech, making things do what they shouldn't – it's a way of thinking, but it's difficult to decide if you have it" (P3)

"What makes me a hacker is not necessarily a skill set but a mentality – I want to understand something, how it works, not the limitations," (P8)

Other common hacker traits described included curiosity, passion and obsession. Four of the participants questioned if those with the hacking mindset were more prone to autistic or antisocial characteristics as well, based on personal experiences and interactions. All mentions of the hacker mindset were either offered as a statement of fact or as a positive aspect; while not necessarily better than those without, it was regarded as something that cannot be taught or tested, it is either present or not. The idea of arrogance was also brought up, with one participant consciously stating when talking that they were not trying to be arrogant in their comments, more presenting what they believed to be fact. This necessity for arrogance or confidence in the community was supported by the comments of others:

"You want to show off, you want to demonstrate to your community or to your peers how good you are. And, because we are not talkative, we hackers [chuckles], we need to demonstrate that with fact. We deface a website without breaking it, just to show how good we are" (P9)

"Hacker is an honourable title like Dr and Sir" (P12)

Curiosity and Learning

The word "curiosity", or a synonym, was mentioned 45 times in all; whilst this is not the highest mention rate of a term or concept, the context of its use made it a key term within these interviews. Curiosity and learning were portrayed by participants as the building blocks of hacking, positive aspects that were necessary in order to fully realise the potential of the technology, individuals and the community.

"It's the guy who breaks things to understand them, to remix them, to transform them. It's a creation. It's a creative act, being a hacker. It's not a destructive one." (P8)

"People without curiosity, I'd call "script kiddies"…[It's about] being curious, when something breaks and instead of going "oh no", going "huh?"" (P10)

"My first experience was around 16 years ago, mostly out of curiosity. I had my own computer, since I was 5 (more than 2 decades ago) and one day I found a "hacking" forum with challenges, similar to {Forum}." (P12)

"When my son was little, we would give him things like we have an old DVD player. I'd say, "Take it apart, and figure out what part makes the DVDs read." Just give him a screwdriver and tell him to take it apart and sit there and tinker with it and figure out how the thing worked. That to me is a hacker. He wasn't trying to destroy all DVDs. He was trying to figure out how this thing worked so he can understand it a little bit better." (P11)

"Kind, innovative, creative, passionate, obsessive work" (P12)

Again, participants emphasised that the curiosity was a constructive trait in hacking, not a negative or destructive impulse. When it is employed destructively, participants no longer regarded it as hacking, but as the separate subcategory of cracking, which supports the assertions of Raymond (2011, see appendix 9.2.2).

Subcategories

The different subcategories of hacker were discussed and acknowledged, some agreeing with the literal "black", "grey" and "white" -hat view, others arguing that it could not be that simple, and that an individual may 'wear' all of these "hats" in a single day.

"I don't think the "hacker" is a singular identity" (P5)

Several participants acknowledged that this was the case for themselves, although they each offered a justification for donning an alternative "hat", for example, finding an exploit in a system without the legal owner's permission, but disclosing it privately or not at all. The researcher was aware that the participants were predominantly involved in white-hat or InfoSec activities rather than black-hat, however, they continued the cynical tone, even when describing their own subcategories.

"A Blackhat hacker is a hacker. A Grey-hat hacker is a hacker who fudges the truth…A whitehat hacker is someone who put the truth down somewhere and forgot where." (P12)

"I wouldn't say its necessarily definitely Black-hat or White-hat unless you start with your intent…I know a guy who wrote a programme for stealing credit card numbers. Okay well that's a

Black-hat hacker. He ended up going to jail for it… When I think of "hacker" though I still get the, you know, you think of the Chinese, or the North Korea." (P1)

Some participants felt strongly that the subcategories surrounding hacking were highly important to differentiate the types, especially with the pejoration of the word "hacker" in mainstream media to signify criminal. Others felt, whilst the labels might be of use, they did not portray an accurate account of the community and its members.

"While I may be elite in one aspect, I'm still a skid in others. Ultimately we as a community, we've all got a variety of hats in our past… I'm always being a good guy, but good guys and hacking don't necessarily go together well… I miss this other half of potential identity that I now know I could have, but I don't feel yet comfortable to move into… it makes you think how it is also difficult to understand where you are on the hacker scale." (P8)

"There is no such a thing as an ethical hacker. As a hacker, there's the ethical thing, or the unethical thing." (P9)

*"They [subcategories of hacking] can also be misused and typecast a person, sometimes inaccurately or derogatorily." (*P7)

"With skiddie - It used to be an insult. It was like "yo' mama" jokes when we were kids…they're not ashamed of it because well, in fact, now if you're a skiddie you could still download 50 tools and hack the living crap out of a website without much skill." (P11)

"As humans we really have a hardcore dedication to categorizing things. However, the field of computers is so broad that I don't feel there's any way to use those types of categories and apply them globally." (P8)

The self-awareness of the heterogeneity of the communities continues to support the idea that not only is a single hacker identity is impossible, but it also allows participants and community members to select different subcategories to simultaneously suit and justify their methods, as well as incorporating the self-concept that best suits the morals and ideals expressed.

6.3.3 Community and groups

It appeared unanimous amongst participants that the community was an incredibly important part of being a hacker; most mentions were very positive, and criticisms were tongue-in-cheek, but also emphasising that this community is a community of individuals. As stated in Chapter 2, this can be interpreted as a western cultural view; these comments could not necessarily be generalised to the

global hacking communities. The sense of belonging expressed supports the positive use of the online world in order to find a social group that you identify with (Bernstein et al, 2011; Tanis and Postmes, 2005):

"You find your group and it's like home," P1

Again, the theme of meritocracy was important, with participants stating in a neutral fashion that the community is not there to coddle members, but to encourage and develop an individual's abilities.

"The hacking community doesn't care about you. So, you can come if you want…Your Wi-Fi doesn't work, I'll just make a joke out of you, I won't help you, I don't care about you [laughs], and it's not in a bad way." (P9)

In order to be accepted by the community, time, effort and application of knowledge needs to be demonstrated; this is what many believed constitutes the acceptance of the community:

"*Someone who says "I'm the best hacker in the world"…that's not a determination you get to make. That's something the community makes"* (P1)

"The interesting bit, I believe, of this community, is that you don't know if you belong to it. [Is that] a nice [community]? You do not know." (P8)

Regardless of the negative or positive aspects of the community, the continued participation with these communities was summarised by a participant simply stating:

"The people are good people. " (P7)

Online

The online and offline divide within hacking communities was stronger than expected. Whilst all participants were active in both spheres, some had a clear preference for staying online:

"I don't need to know someone's real life name or where they live or what they do for a living…as far as I am concerned they are their online nick name. Some of us, are more our persona then we are our name. We have spent more time behind the computer screen being our persona, done more significant things as the persona" (P10)

There was also a strong awareness of the fact that the online world is still relatively young, and as such, communities are still developing in their behaviours:

"Its new, it doesn't have thousands of years of best practices and behaviour…there is no etiquette." (P10)

Whilst this statement is true to a point, there are obvious accepted social norms within the groups, but the online sphere is regarded as a place for those that otherwise might feel like outsiders:

"There's people in minority groups like LGBTQ and stuff like that they find -- and also like the autistic – because I do a lot of my work based around people I suspect are unsafe - They find Twitter and online forums an excellent way of communicating and having community because they can't necessarily do that face to face. I wonder also if that's a side of things with InfoSec as well." (P4)

Offline

With offline interaction, the main space used are hackerspaces or conventions and events such as DefCon. Some participants expressed concern that this changed the hacker community in a fundamental way:

"The 'hacking culture' has moved or actually never, perhaps left the shadow in a way. The moment you come in the light, you're in a way bastardizing the idea" (P9)

"I'm not generally there to socialize. A lot of the people they're actually there primarily for socializing and the beer, and the information content is almost secondary to them, I'm not. I'm generally late arriving. I'm not there to make a profile for myself or to be seen by people. I'm there to learn or to listen mostly. For the most part, I don't socialize with people." (P5)

The researcher however also emphasises that these events were also seen as an entirely positive aspect of the communities, continuing to support work by Coleman (2010) on the importance of these conventions and meetings.

"The original idea, that is actually original idea why I started going to DEF CON, just for inspiration. You go to DEF CON as a festival, not as a conference." (P9)

"I wish I'd discovered it sooner, it's perfect." (P4)

Not only does it allow human interaction, but it reinforces the bonds created online.

*"It's also odd because people will call me my online nick[name] when I'm in real life. They'll just talk to me like they'll call me ******. I've had to learn to get used to, not just my real name but my fake name to"* (P11)

Trust

All participants agreed that trust on the internet was not a straightforward concept. Some stated their thoughts very plainly:

"Trust? Lmao. This is internet I don't trust shit." (P13)

However, when questioned further P13 acknowledged that he did assume other registered members would abide by community rules and to complete any tasks assigned on forums. Others seemed to feel that you could build relationships online, but the important element was always online security, requiring effort and constant vigilance to maintain your privacy or anonymity. If an unknown user wanted information, most agreed they would happily provide it (some with the addendum that the unknown user must show an effort to have found knowledge on their own), and they in turn would trust information if it came from someone who had shown evidence of understandable and logical thinking in the past.

"If somebody comes up and asks a legitimate question, I want to see that they have put effort in first." (P6)

"I attempt to not trust anything anybody says and let them prove it." (P8)

Three participants were very protective of their identity, making an effort in online and offline interactions to maintain a strict level of privacy. One took this as far as having a stockpile of custom smartphones with various online elements disabled; others used professional and private mobile phones and computers. All participants made a clear distinction between personal and private information; however, one participant said he made no effort to hide details such as his home address, as if the information is available, no one would make a game out of finding it.

"Biggest problem these days, not only for hackers but for humans…I don't trust anyone even in my real life, I'm always suspicious…if you want my trust it means you want to "take advantage" of me." (P12)

P12 went on to say that this "taking advantage" included the researcher's relationship with participants, but in the context of academic research they felt it was a justified exercise.

6.4 Discussion

As with the other data sets in this research, there is an obvious gender imbalance in the sample; again, this is argued to be representative of the gender imbalance in this field, where men are said

to outnumber women by a margin of approximately nine to one (Executive Women's Forum, Frost and Sullivan and (ISC)^2, 2017). As far as the information was available, the participants were white and western, in part due to the location of the researcher and the conferences attended.

The "hacker" social identity is currently as fluid as it has ever been; however, what is apparent from this study is that for those involved in this community, there is a lot of positivity behind this identity. They emphasise the creativity and learning involved within their communities; indeed, a key element for the participants in the hacker mindset was the desire to know more and not accepting that everything was already known. Those with white-hat or InfoSec involvement were the ones who talked more about the community and the need to be active in making the spaces constructive; although many said that the word "hacker" was not reclaimable, their actions and the language they used suggested that they were still willingly and actively promoting hacker related activities for the benefit of increasing awareness and improving education within the general population.

There was some anecdotal evidence of cognitive dissonance displayed, with older hackers discussing the former use of grey or black hat tactics; they emphasised however this was either youthful experimentation, or prior to laws being enacted regarding computer misuse. Evidence of conformity to group norms is presence, with an observable influence, but generally a positive one, that discourages elements groupthink, promoting thought and discussion.

When applying Social Identity Theory (SIT) to this data, it was broken down into three broad stages:

> 1) Categorisation: Individuals observe and define the appropriate behaviour for the group,
> 2) Social Identification: Individual adopts the group identity, creating their "in-group",
> 3) Social Comparison: Compare in-group with others ("out-groups"), often to emphasise positive characteristics of the in-group (Turner, 1975).

With these stages defined this way it is easier to see where participants see themselves in terms of their adoption of the social identity of hacker. For example, participants from Study 1 (Chapter 5) who participated in the survey but did not define themselves as hackers would be in stage 1. All participants in Study 2, the interviews, had identified themselves as hackers or as having a part of the group identity. Two participants stated they did not feel they were hackers, based on their lack of knowledge and experience, but were drawn to the community and identity through interest. A further two participants expressed belief that they were a hacker due to elements of the "mindset", but were uncertain if they truly qualified, due to again lacking skills in coding or experience. From their answers, there was no evidence that another member of the community had expressed the opinion that they did not belong, it was their own judgement. The remaining 10 participants seemed

comfortable defining themselves as hackers, often assigning to themselves a subcategory; the participants who identified themselves as InfoSec all acknowledged that past behaviour had included grey or black hat behaviours.

In contrast, when examining the data in relation to Social Categorisation Theory (SCT) there was less evidence of this being applicable. SCT posits that individuals categorise themselves into their chosen groups, and that categorisation leads them to adopt group norms in order to achieve social acceptance; this then becomes their salient identity and they are the representative of that social identity (Turner et al, 1994). As discussed in the previous paragraph, all participants had categorised themselves, but their interviews showed more evidence of speaking for themselves than acting as a group representative. Although there was stereotyping of other groups, they also presented the stereotypes of their own groups and displayed attempts at balanced observations.

Participants all shared a cautious approach to trusting others online, stating that the other unknown person had to meet certain criteria (such as knowledge and constancy). They all demonstrated awareness of the risks of putting their own personal information on the internet but responded differently; some felt it should not be online, others felt if all information was available it would discourage people from looking for it as a form of entertainment. Two participants mentioned that it seemed irrelevant what they did with their personal data as it would be collected by companies who were at risk of attack and so their data could be stolen and shared even if they followed all correct protocol. None of the participants displayed evidence of an online disinhibition effect; those who actively tried to maintain complete anonymity reported responsibility for and awareness of their online actions, whether in practice or theory. The occasional mention of arguing or provoking someone online was described as “not worth it” or immature; this was recognised as being in conjunction with wanting to maintain their online identity and reputation. It is recognised that the participants were already showing trust by agreeing to participate in the research.

There was a distinct bias within the sample towards those involved in information security, or “white-hat” hacking, not least because those involved in criminal activity are far less likely to participate in academic research. Further investigation and analysis are needed in order to clarify whether the participants views on the subcategories of hackers is affected by how they categorise themselves; this would suggest similar ingroup/outgroup processes as found in offline behaviour. Although there was not the obvious snowball effect that had been hoped for, at the end of interviews, 6 participants mentioned that they had done their own background check on the researcher, through both the online presence and asking others within the hacking communities.

There was also ample evidence of progression in mental health concerns and discussions within the community coming to the fore. Mental health was discussed openly at two of the conferences attended, one as part of a conference presentation, discussing the presenter's personal journey, and struggles with depression. There were other factors, but he noted that his solitude, in always being in front of the computer both alleviated and worsened his condition. One of the participants recruited via Twitter first came to the researcher's attention when they messaged the researcher; it was entirely unconnected to this research, but they had seen some tweets from another account and were concerned for the person's wellbeing. Because of this they were messaging people that followed the account, in the hopes of finding someone who knew the person in an offline capacity and could therefore check they were ok through a mode of communication other than Twitter. There has also been the formation of support groups:

"Geared for information security professionals who have mental health issues or behavioural health issues. I work there more as a counsellor, but also doing some research" (P8)

An element that was notable by its absence was any reference to the concept of the hacker ethic. This had been a central theme for hackers throughout the decades (Levy, 2010) and so it was a surprise that it was not mentioned. One participant did mention Levy's book, and his [the participant's] romanticised view of the 1960s hackers, but not any of the underlying concepts that "made" them hackers. It is believed that this could be evidence of the divergence away from the traditional definition, which has in the media become associated with the criminalised use of the word "hacker", or possibly more associated with hacktivists. There were however personal morals and ethics discussed, which appear to be in line with the general "hacker" stance reported in Study 1, Chapter 5.

The feelings surrounding the lack of informed law making in terms of computing and hacking were an interesting result. The researcher asserts there is a potential link to the attitudes reported in Young et al (2007), where hackers seemed unconcerned about breaking laws. Young et al (2007) attributed this to the perception that attribution was unlikely, and therefore the hackers believed they would not be arrested or prosecuted. Whilst all the participants in this study emphasised the legitimacy of their hacking actions, it is suggested that the lack of trust in those making the laws contributes to the cognitive dissonance of hackers, reinforcing the self-image of positive deviants (Turgeman-Goldschmidt, 2005).

Chapter 7: Study 3 - Survey 2

This chapter details the methods, analysis, and results of the third and final data collection study carried out.

7.1 Background

This Study was conducted as the final data collection for this research, with the aim of augmenting the previous two studies, and with the results supporting or opposing the conclusions of the previous observations and studies. The survey strategy introduced concepts and keywords from Study 2, but with a similar quantitative design to Study 1. Following on from the pilot survey and Study 1 (see Chapter 5), further websites and forums with relevant users and discussions were identified. Some websites were no longer used, as they had not wanted to participate in the research, and this consensus was respected by the researcher.

197 full and partial responses were submitted; a further 143 responses were started but not submitted so were not included in the study. As none of the questions were compulsory the partial responses were accepted. This does mean there was a fluctuation in the number of participant responses per question.

7.2 Method

As with Study 1, the survey was carried out using Qualtrics. Included in the recruitment posts was information about the study, the site hosting the survey and the researcher. It was recommended that readers, to help keep IP addresses private, used Tor Browser or a VPN connection. Again, previous approaches to these communities have led to the potential participants demanding details of the research, including ethical considerations, which were provided. To minimise the uncertainty of genuine or false information, as well as exaggeration or boasting, the questions were designed to be simple opinion on widely used terms and shared beliefs, rather than asking questions about individual experience or skill.

7.3 Results

The online survey recorded 197 submitted responses over the course of two months, shared across thirty websites and subreddits. Throughout the survey and recruitment there were no repercussions from posting this survey (despite the inclusion of the researcher's university and topic, which made the researcher easy to find online). Feedback and responses on the forums covered the entire range

of possibilities; confirmations of completion, polite and impolite refusals, and users who made clear their disapproval of the research and the presence of the researcher. Four forums banned the researcher's account entirely and deleted the recruitment post. Due to the anonymisation there is no way of knowing if anyone from these websites completed the survey.

As with the previous studies, the demographic of the participants was as anticipated: predominantly male and under 35. It is worth noting that this study only asked for the age group rather than the participants' actual age – this resulted in no missing data for this question, compared to Study One where 15 participants chose not to answer.

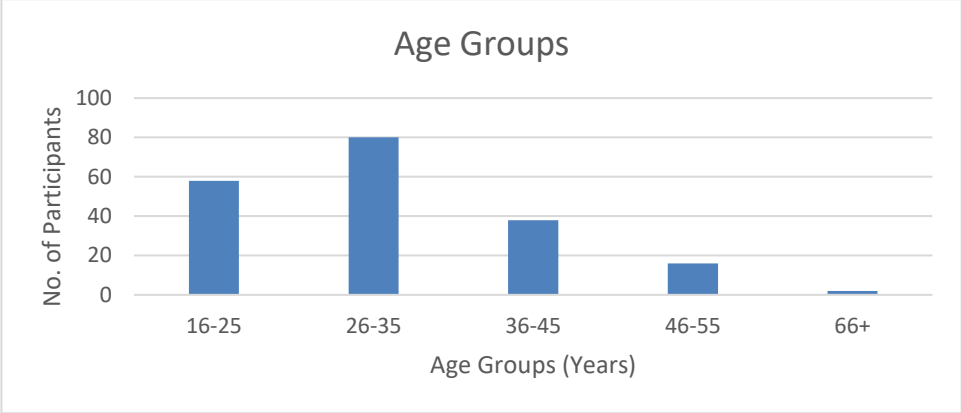

Figure 17: Study 3: Participant Age Groups

Whilst the percentage of transgender participants was smaller in this survey (see Figure 18), they were believed to be genuine responses – in part due to comments from a member of that community on one of the recruitment threads, commending the inclusion of transgender as an option. It was also mentioned by interview participants that transgender individuals are an active part of the hacking community, although there is currently no data to suggest that this is more common than in other social communities.

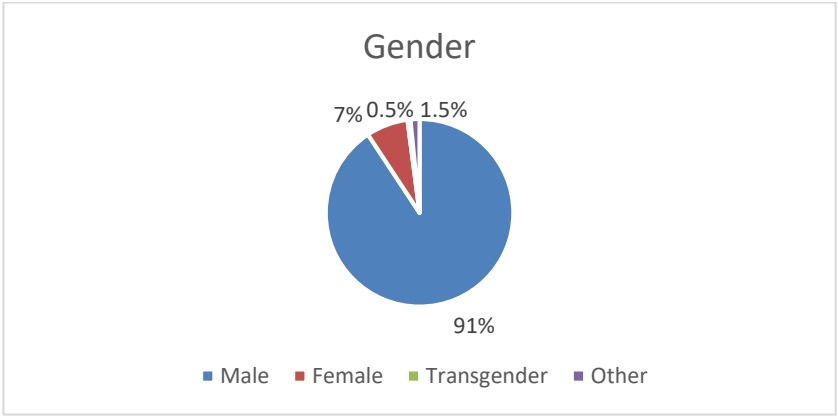

Figure 18: Study 3: Participant Gender

For this survey, instead of asking the participants to confirm if they consider themselves hackers, they were instead asked to just put themselves straight into hacking subcategories (Table 14). Participants were allowed to select more than one sub-category to which they considered themselves to be a part of. This greatly increased the responses in subcategory compared to Study 1 (see Chapter 5), and aligns more with the interview participants, some of whom were uncertain that they could call themselves a hacker; the researcher believes that it is possible for individuals to identify with a hacking subcategory even if they might hesitate to unambiguously state themselves as a hacker.

Category	**%**	**No. of Participants**
I consider myself a White-hat hacker	38%	73
I consider myself a Black-hat hacker	4%	7
I consider myself a Grey-hat hacker	26%	50
I consider myself a cracker	6%	11
I consider myself a script kiddie	6%	11
I consider myself an elite hacker	2%	4
I consider myself a cyberpunk	6%	11
I consider myself a hacktivist	6%	11
I am involved in InfoSec	60%	116
I disagree with these categories	7%	14
Other	9%	17

Table 14: Study 3: Selection of hacking sub-category

In comparison to Study 1 (Chapter 5), the number of self-identified White-hat hackers was higher, but the overwhelming majority identified themselves as being involved in InfoSec (information security). This is regarded as being a White-hat profession, so it is possible that the shift in participant demographic was an influence; this occurred through the snowball effect of recruitment, following participation and attendance and hacking and security related conferences (see Chapter 4).

As in the first survey, Study 1, participants were given the opportunity to comment on the subcategories, or offer their own interpretation of their identity:

Participant Comments
“Program analysis (deeper than cracker)”
“A hacktor” [Subcategory unknown to the researcher; possibly a reference to the bug bounty offered by the Tor browser]
“I'm a software engineer that has to learn about security in order to write robust applications.”
“I am enthusiastic about InfoSec and considering a career in it”
“More than one of these”
“I am in the business of creating compelling events.”
“Incident response”
“Not affiliated with these groups”
“Current InfoSec student”
“Classic Social Engineer”
“more of Hardware person with” [Incomplete sentence].
“R+D” [Research and Development]
“Security enthusiast”

Table 15: Study 3: Full Participant comments on subcategories

The number of participants in the Black/Grey/White-hat hacking categories was of particular interest, given that it is very unclear how people distinguish themselves from one “hat” to another. As such, part of Study 3 attempted to identify any patterns in how the Black/Grey/White-hats have placed themselves on a scale, from 0-100, with 0 being entirely Black-hat methods, which it stated in the survey were assumed to be illegal and/or unethical; 100 was entirely White-hat methods, stated to mean completely legal and/or ethical. They used a sliding button to position themselves on this scale.

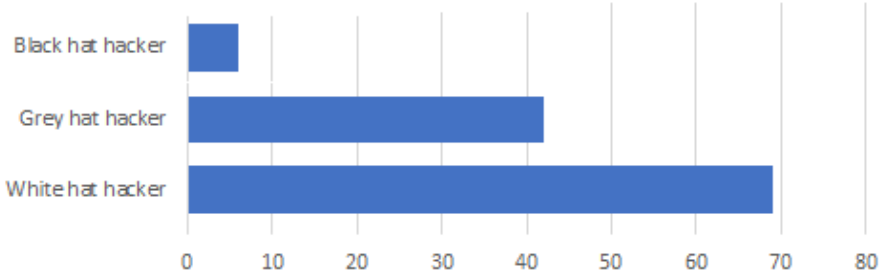

Figure 19: Study 3: Participant Black/Grey/White-hat Self-Identity

Whilst there were many more self-identified Grey and White-hat hackers than Black-hat, there was still a good spread across the scale, although there were more positioned towards the White-hat end for the obvious reason that there were more White-hat participants. The mean average of all responses (n=91) was 79.

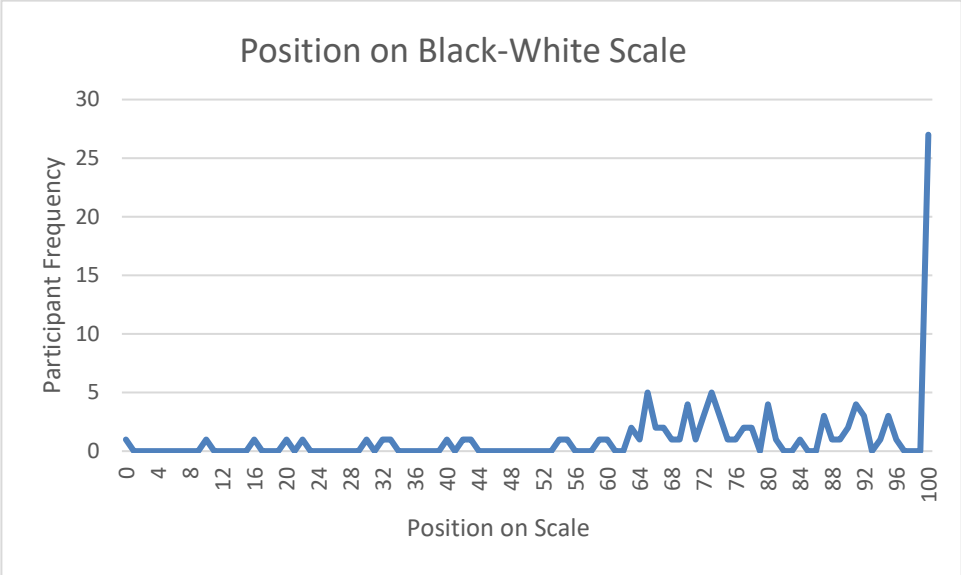

Figure 20: Study 3: Participant Placement on Black-White Hacking Scale

On Figure 20, the participant frequency was given on the vertical axis, showing how many participants had defined themselves as on that point on the scale; for example, more participants placed themselves at 100 (purely White-hat) on the scale than any other position. It should be noted that the scale the participants saw did not show the numbers of the position, to prevent people from rounding up or down to the nearest 10.

The next part of the survey addressed the concept of trust within these communities, i.e. how different posts and approaches on the forums receive different reactions (see Chapter 4). Although from observing the forums it appears largely predictable which type of posts will receive more positive or negative reactions, there is a lack of empirical data regarding trust and trusting behaviours within online communities. As discussed in Chapter 2, online trust is defined as an "attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited" (Corritore, Kracher, and Wiedenbeck, 2003, cited in Beldad et al, 2010:860). With this in mind a selection of statements were taken from forum posts and interview transcripts, in some cases with minor modifications for the sake of privacy or ease of understanding. Mistakes in grammar or spelling were not corrected unless it affected the legibility or comprehension of the statement.

Participants were asked to rate statements, again using a scale from 0-100, on the following criteria:

1. Genuine - how sincere (high) they believed the statement or request to be.
2. Trustworthy - how honest (high) they believed the statement or request to be.
3. Author's integrity - how moral or ethical (high) they felt the statement or request was.
4. Personal response - if they felt positive (high) or negative (low) about the statement.

These criteria were selected based on signs and signals used to develop or judge trust online (see Chapter 2.4). These categories were used to examine if there was a relationship between an individual personal response with the level of trust in a statement. It was believed that evidence of curiosity and commitment to learning would be more trusted or appreciated by these communities, with the expression of hacker concepts as way of signalling the shared hacker identity, which can prompt trusting behaviour (Tanis and Postmes, 2005). This was examined by using statements that could be viewed both positively and negatively, according to the traits and thoughts observed from the previous studies.

The success of these categories is further discussed in the following section, 7.5. Categories 1 (Genuine) and 3 (Author's Integrity) were included as other potential indicators regarding individual perception and subsequent trusting behaviour, and to allow evidence of fluctuation in rating on different criteria. This was done as a measure to ensure the same answer was not submitted for every criteria and statement. The main interest in these results lay with the level of Categories 2 and 4 in relation to each other, as well as the different influences on Category 2 within the different statements. It was anticipated that the level of Trust (honesty – Category 2) perceived would be highly correlated to the personal response (Category 4); if participants thought the statement was truthful, and rated high, the personal response rating would also be high. The mean and median averages were both included in the results; the mean, in order to have a better measure of central rating, and the median to account for the potential influence of outlying responses.

Statement 1 (Open Source Statement): "Open source doesnt mean you can ask the author for anything and hes obliged to deliver if you cant read/write source code thats not my problem"

	Criteria	Scale Response (Overall Mean)	Scale Response (Median)	No. of participants
1	Genuine (sincere)	76.04	81	184
2	Trustworthy	67.69	74	178
3	Author's Integrity	56.88	58	181
4	Personal response	58.17	65	178

Table 16: Study 3: Statement 1 Results

The combined response to the genuine and trustworthy criteria was positive, with integrity and personal response being more neutral. As well as the scale response, participants were able to comment on the statement, and these supported the scale responses; there were 19 positive comments that supported this statement, agreeing that the attitude was reasonable, 11 neutral, and 7 that were negative. The majority agreed with the statement but in the neutral and negative comments participants felt that it was not well phrased and came across as unpleasant. There were also comments about the poor punctuation; this had intentionally been left by the researcher, as with some of the other statements, to see if it was relevant to participants.

Statement 2 (Resources Statement): "I'm quite comfortable with dissecting network protocols, xss, sql injection, and etc. but I've never been able to do the low level stuff like buffer overflows, or reverse engineering assembly. Where is a good place to start with this type of hacking? What are some good resources on these specific kinds of hacking?"

	Criteria	Scale Response (Overall Mean)	Scale Response (Median)	No. of participants
1	Genuine (sincere)	82.02	86.00	187
2	Trustworthy	76.10	79.00	178
3	Author's Integrity	77.16	79.00	178

4	Personal response	74.82	80.50	180

Table 17: Study 3: Statement 2 Results

Both the mean and median response to this statement were very positive in all criteria. Overall there were 21 positive comments that were pleased and would answer to encourage this sort of request on forums. There were 5 neutral, and 4 negative comments, mostly implying that the author could simply do a search for this information.

Statement 3 (Booty Pics Statement): "have no clue how to hack or anything about it so can someone give me a step by step tutorial on how to get an instagram password tryna see booty pics and crap they post on it"

	Criteria	Scale Response (Overall Mean)	Scale Response (Median)	No. of participants
1	Genuine (sincere)	46.26	46.00	180
2	Trustworthy	20.90	6.00	184
3	Author's Integrity	7.91	0.00	187
4	Personal response	9.36	0.00	186

Table 18: Study 3: Statement 3 Results

The reaction to this statement was very negative, as was anticipated. There was some confusion over the use of the Genuine criteria, but the majority appeared to have rated the Genuine criteria to mean the individual sincerely wanted help to access Instagram accounts, regardless of how they felt about such a request. This was supported by the comments, only 1 positive comment was left, with that participant stating at least the author was honest about their intentions. There were 7 neutral comments, and 21 negative comments, some calling the author a skid (script kiddie), but many lamenting the fact that there was no real interest in learning about hacking, despite the Author's presence on the hacking forum.

Statement 4 (Government Statement): "If you are working for a government you are told what to do therefore how can you truly be a hacker."

#	Criteria	Scale Response (Overall Mean)	Scale Response (Median)	No. of participants
1	Genuine	47.11	50.00	177
2	Trustworthy	41.75	36.50	166
3	Author's Integrity	38.59	34.00	164
4	Personal response	27.70	21.50	172

Table 19: Study 3: Statement 4 Results

This statement was also ranked quite negatively. This was the only statement to receive no positive comments from the participants, with 10 neutral and 20 negative comments. These comments generally criticised the naiveite and the Black-hat stereotype assumed in the statement.

Statement 5 (Mindset Statement): "Everyone started as a beginner, no one can say "I'm a hacker and you're not" - it's about self-definition."

#	Criteria	Scale Response (Overall Mean)	Scale Response (Median)	No. of participants
1	Genuine	76.78	81.50	180
2	Trustworthy	72.35	76.00	170
3	Author's Integrity	73.74	78.50	172
4	Personal response	70.21	76.00	170

Table 20: Study 3: Statement 5 Results

Despite the high average rating for this statement, the comments were quite divided – 13 were positive, 10 neutral, and 7 negative. The criticisms were not that the participants disagreed with the idea of the mindset, but they argued that the self-definition of self as a hacker was only valid if it could be backed up by ability and the endorsement of others with the ability. Most positive comments were related to inclusivity and welcoming individuals to the community.

Statement 6 (Limitations Statement): "What makes me a hacker is not necessarily a skill set but a mentality – I want to understand something, how it works, not the limitations"

#	Criteria	Scale Response (Overall Mean)	Scale Response (Median)	No. of participants
1	Genuine (sincere)	84.45	92.00	185
2	Trustworthy	82.33	88.50	180
3	Author's Integrity	80.84	89.00	180
4	Personal response	82.82	93.00	177

Table 21: Study 3: Statement 6 Results

This statement received the highest rating of all, with 20 positive comments and 8 neutral. There were only 2 negative comments, who disagreed with the mentality aspect. Overall comments suggested this was a positive and good approach to hacking and learning.

The final question listed 5 hacker traits that had been mentioned in both the previous survey and the qualitative interviews, and asked participants to rank them in order of importance (Figure 21). There was also an "other" option if they felt that something important had been missed.

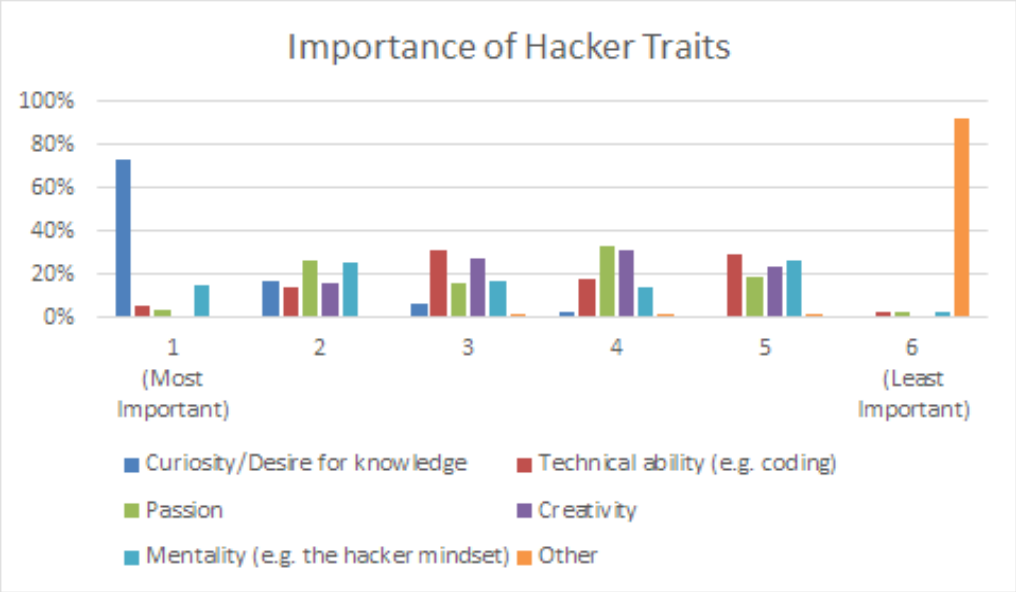

Figure 21: Study 3: Importance of Hacker Traits

It is evident that curiosity or the desire for knowledge is indisputably ranked as the most important trait by the participants, with technical ability only being ranked as the third most important

attribute. The remaining traits were relatively equal in their importance. The category of Other received 24 suggestions, including perseverance, social skills, and community or friends. For the full list of Other, see Appendix 9.1.5.1.

7.4 Analysis

The demographic data continues to support the results from the previous studies, whilst still demonstrating the inaccuracy of the stereotypes surrounding the age of those involved with hacking.

To examine the participant positioning on the Black-White Hacking Scale data further (see Figure 20), the data points were divided into the subcategories. From Figure 22 it is evident that there is large overlap between Grey and White-hat positions; this may be due in part to the fact that participants could select more than one of the three subcategories. When the participant has self-identified themselves as one or more subcategory, the data point is shown in each subcategory (with the colour dot representing the "hat" identity). For example, one participant identified themselves as Black, Grey, and White-hat, but placed themselves at 16 on the scale. Another, a Grey and White-hat hacker who despite self-identifying as a Grey-hat, still positioned themselves at 100, indicating they felt they had purely White-hat approaches to hacking. There are other examples, but it is harder to distinguish, due to the clustering of the data. A subsequent study would be interesting to examine whether this is related to what participants felt to be the salient identity, or acknowledgement of a mixture of hacking methods, or if this was an example of cognitive dissonance within the community (see Chapter 8 for further discussion).

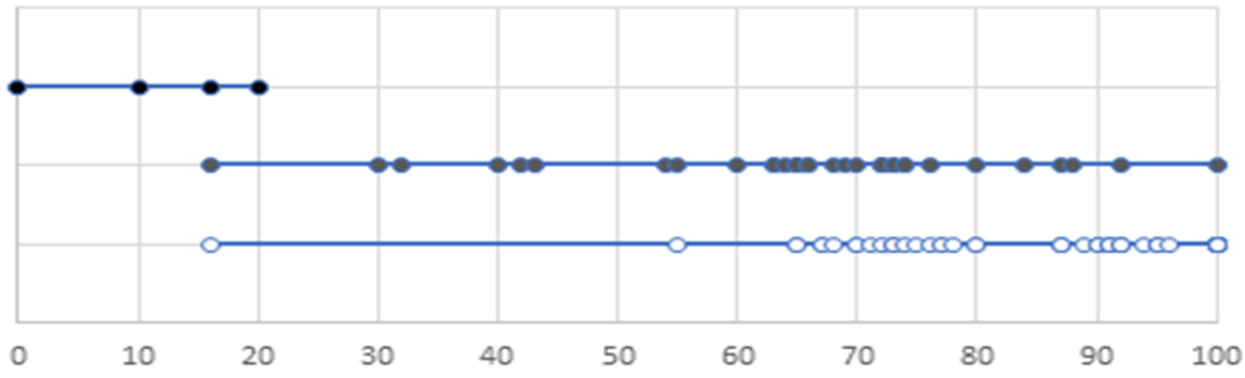

Figure 22: Study 3: Participant Black/Grey/White self-identification placement on scale

After the main survey questions were completed there were two final questions relating to feedback on the survey. The first question asked the participants reason for completing the survey: it received 118 responses. A brief content analysis was completed, with the same initial steps as conducted on the interview data in Chapter 6, with the word frequency displayed in a word cloud (Figure 23). Basic coding into nodes confirmed that the main motivation given was in order to help the researcher, or to improve research about the community (Table 22).

Figure 23: Study 3: Participant Motivation Word Cloud

Participant Motivation	Percentage coverage
Bored / Procrastinating	11%
Curiosity	8%
Wanted to help (researcher/research/community)	51%
Nonsense comment	2%
Saw post/link to the survey	28%
Total	**100%**

Table 22: Study 3: Participant Motivation

There were a number of thoughtful and interesting comments which have been included below. The researcher felt that these comments were a fair representation of the community that participated in this study, acknowledging again the predominance of Whitehat and InfoSec self-categorised participants. The participants took the time to express their thoughts, wanting to emphasise again the positive aspects of these communities and encourage further research into them.

"I have spent the better 4/5 of my life in and around these communities. Having started as an admitted miscreant, albeit wishing to "do no harm", I actively began to try to

lead people to constructive, ethical careers. I have found some truly unique and amazing opportunities through this community and have been able to influence some important aspects of the world as a result. I think it's important to understand how people arrive at self-directed discovery and the degrees to which that understand can and should influence everything from policy to design to recruiting."

"Put a footnote in your thesis that the Cult of the Dead Cow assisted with your research."[10]

"I grew up as a "hacker", exploring networks and technology just to learn and understand it. I never did damage and I never stole (money, data, etc), but those were my own personal ethical choices. I now work as an information security consultant for government and private entities, assessing security programs and technical controls. It's some of the most fun I've ever had in my career, and I'm very fortunate. Whenever I can contribute and give back to the community, I try and do so. This felt like a good opportunity to have my perspective registered in a meaningful way (vs just ranting on Twitter.) So thank you."

"Being a hacker has a "stigma" about it and the more actions we can take to educate people about hacking and hackers the better off we will be. I hope in the future people don't look at hackers as dangerous or as weirdos we are just normal people and most of us want to help."

"I want to help people see that the word "Hacker" does not mean criminal. The vast majority of hackers are here to help people and to make the internet and the world in general a better and more secure place. :)"

As with the previous studies, the feedback given emphasised the support both for the communities and for research that can help de-stigmatise the group.

The second feedback question asked if there were any additional comments the participants wanted to make about the survey, which received 60 comments. Again, for illustrative purposes the word frequency was examined and displayed in a word cloud (Figure 24).

[10] The comment refers to an infamous USA based hacker group established in 1984; it cannot be ascertained whether or not the statement is true.

Figure 24: Study 3: Survey Feedback Word Cloud

In contrast to the previous comments, the feedback (Table 23) often contained more than one sentiment; as such, the comment was coded into more than one category. One of the most common comments was that there had been confusion regarding the use of a sliding scale with the statements. This is discussed further in 7.5.

Participant Feedback	Percentage coverage
To provide additional information	31%
Engaged in the research/community	29%
To give survey feedback	31%
Expression of gatekeeping	1%
Negative comment	11%
Neutral comment	28%
Positive comment	28%

Table 23: Study 3: Participant feedback

7.5 Discussion

The data from this study supports the conclusions drawn from the participant observations, Studies 1 and 2; the demographic remains consistent and there is continued evidence that the hacking community wants to embody a positive and productive social identity, whilst individuals self-identify themselves as belonging to multiple subcategories. One of the main conclusions of this study is that the self-categorisation does not lead to the participants appearing to exclude themselves from another subcategory; participants were confident in selecting more than one of the subcategories, even if the selection seemed at odds to another identity group, such as the Black/Grey/White-hat selection. In Study 2 the participants discussed the fact that “hacker” was not a single identity and it

was misleading to propose otherwise, and an individual may wear the different "hats". The data shown in Figure 22 and Table 24 support this.

Hacker subcategory	Study 1 (No. of participants)	Study 3 (No. of participants)
I consider myself a White-hat hacker	30	73
I consider myself a Black-hat hacker	7	7
I consider myself a Grey-hat hacker	39	50
I consider myself a cracker	3	11
I consider myself a script kiddie	5	11
I consider myself an elite hacker	5	4
I consider myself a cyberpunk	14	11
I consider myself a hacktivist	10	11
I am involved in InfoSec	-	116
I disagree with these categories	9	14
Other	10	17

Table 24: Summary of Hacker Subcategorization

In this study there was an issue with the data reliability in one section: the use of the sliders on the statement questions caused confusion. It was designed in this manner to allow a more precise response to the statements, with the intention of enabling more depth to the data; however, the feedback suggests that participants would have found the use of a Likert-scale clearer. It is accepted that in any future studies, a Likert-Scale may be able to produce more generalisable data. The average of responses however were useful in indicating the signs and symbols that participants responded positively or negatively to; for example, the level on personal opinion was close to the level of perceived honesty (trustworthiness) they expressed toward the statement for four of the six statements (see Table 25).

Statement	Median Trustworthy Rating	Median Personal Response Rating	Divergence
1 – Open Source	74	65	-9
2 – Resources	79	80	+1
3 – Booty Pics	6	0	-6
4 – Government	36	21	-15
5 – Mindset	76	76	0
6 – Limitations	88	93	+5

Table 25: Study 3: Median Trustworthy/Personal Responses

The high divergence in ratings were for Statement 1: although participants agreed with the statement itself, the feedback suggested that the phrasing should have been more courteous, and the poor grammar was commented on. Statement 4 was arguably the most contentious statement, both in the results and the feedback given; it is believed this explained the divergence between the

two ratings. The perception of honesty (trustworthy criteria) appeared to be strongest when the statement aligned to personal views and the salient subcategory identity; for example, the statement about the government may have been more popular in a sample that contained more Black-hat hackers rather than InfoSec, who are employed by legitimate companies and government agencies. Statements 3, 5, and 6, regarding the resources request, the hacker mindset and the attitudes towards limitations were the most positive; it is suggested that this is because these statements express positive and prevalent concepts within the hacker identity for these communities.

The consistency in hacker traits is evident: learning and curiosity are highly desirable traits within the hacker identity, regardless of the subcategory. It is also argued that knowledge is used as a basis for trust within these communities; therefore, the more active and established a member is, especially if they share and contribute knowledge, the more they are trusted within the community. This supports the work of Zhang et al (2015) which suggested that dedicated members can progress through stages of the hacking social identity, having to actively participate and demonstrate value, or the potential to bring value, to the group in order to be trusted.

Chapter 8: Discussion

This research was designed to investigate the hacker identity, as well as the influence of group processes on individuals within hacker communities. This thesis had the aim of exploring whether having this advanced understanding could lead to improvements for cybersecurity and online safety, as well as looking at improving awareness of the non-criminal element to hacking and promoting informed behaviour online for those involved in hacking communities and the general public.

8.1 Research Overview

The aims and objectives set out in Chapter 1 will be addressed individually and followed by further discussion of the most salient points. One of the themes to emerge from the analysis of all the data was that there is definitely a shared hacker identity but the central ideas of what constitutes a hacker have developed over time and will continue to do so. As with all social identities, there are divides in how the subgroups define themselves. The fluidity of the hacker social identity means that group identities changes along with the rest of the world, and this researcher suggests that the link to technology and the pace at which that transforms means that the hacker identity has evolved, and changes faster than a purely offline or traditional identity might.

Currently the broad hacker community, (excluding the cybercriminal community within), strives to position its social identity to be a positive one. These findings are consistent with previous research; for example, Madarie (2017) states that intellectual challenge and curiosity were the strongest motivators for participating in hacking, and there was an awareness of the social acceptability as a motivation; the interview results in Chapter 6 support this. Turgeman-Goldschmidt (2008) found that hackers find ways to establish their identity as a positive, regardless of the legality and severity computer related offences they may have committed. This presence of cognitive dissonance appears in some sections of the hacking community to promote positive social behaviours (as discussed in Chapters 4 and 6).

The application of Social Identity Theory (Tajfel, 1974) to understand the data shows there are evident stages that members of the community progress through (see Chapter 6); the resulting effect on self-esteem of belonging to a respected group is clear, assuming the member has made it into the third stage of social comparison. Because hacking is a contested area, however there is the apparent influence of cognitive dissonance. Hacking is regularly portrayed in the media as a combination of positive and negative traits. A hacker can be heroic, criminal, deviant, anti-establishment (Coleman, 2014; Merck, 2015) all at the same time, and this complexity within the

identity leads to individuals categorising themselves into multiple subcategories, in order to justify and understand their own beliefs and behaviours. The data from this research suggests that by labelling oneself as both black and white -hat, or somewhere in between, individuals can justify their methods, and align them to their personal beliefs.

The findings of this research offer examples and areas for improvement of online research methodologies as well as reinforcing the importance of social psychological research and human factors within cybersecurity. The results are beneficial to those wanting to conduct their own online research in challenging or sensitive areas, as well as those interested in online behaviour and hacking related topics.

8.1.1 Hacker Social Identity

1) Ascertain how accurate and reliable the hacker social identity is currently. This includes analysis of the hacker subcategories according to Social Identity Theory (SIT) and Social Categorisation Theory (SCT).

There is a loose international "hacker" identity, and although it has its own regional variances, key elements remain globally. Whilst some individuals have moved away from the traditional hacker ethic followed by groups such as the CCC (see Chapter 2), importance is still placed on certain traits: curiosity; the desire to learn; the desire to improve; using logic and evidence. In some ways the overlap between white-hat hackers and InfoSec professionals has meant that this subcategory had adopted a more business orientated stance. Members of this subcategory emphasise the legitimacy of their actions. In groups such as DefCon, locally, at the conference, and online, the consensus suggests that hacking is no longer exclusively for the rebellious fanatics, and that hackers are positive members of the general public, having their families and careers, a more rounded work-life balance than the trail-blazing obsessives from the 1960s (Levy, 2010). There is a pervasive belief in western society that as individuals grow older they become more politically conservative, but it is argued that this is not necessarily due to age, but to the societal changes that the different generations have experienced (Tilley, 2015). It is suggested by the researcher that this could in fact be an explanation for the changes to the hacker identity; computers are not only mainstream but often essential for everyday life in the Western world. It is therefore little wonder that the once edgy and niche counter-culture has also become mainstream and popular.

The research findings are comparable with those of Young, Zhang and Prybutok (2007) although it is again acknowledged that this research did not knowingly access the criminalised hackers. In their paper Young et al state that hackers perceive high value from engaging in illegal hacking activities and consider their behaviour morally right within their social context (2007). They also stated that

whilst the sanctions are severe if caught, many hackers believe the likelihood of being arrested is low, concluding that technological detection and defences should be improved, rather than more laws; however, in the decade since the research by Young et al (2007), there is evidence that there has been an evolution to the hacker beliefs. Participants in this research reported a high awareness of the risk of detection and prosecution within the hacking community, which for some had the direct effect of altering their hacking behaviours or finding a role or employment that allowed them to legitimately use their skills and knowledge. Even those who may not act completely as a "white-hat" reported participating in bug bounties and responsible disclosure of flaws and weaknesses in computer systems (Chapter 5). Unfortunately, the nature of the data does not provide evidence on the potential influence of any criminal elements in hacking related communities which may have been more prevalent in Young et al's study; see section 8.4 for further discussion.

Within the communities there are still the strong status signals related to confidence; those who know they are skilled in their area and have proven themselves tend to have a more open attitude and this has led to the more supportive elements growing (see Chapter 4). It is possible that those who are still less experienced or insecure in their ability are more likely to exhibit gatekeeping and proposing challenges towards the less experienced. There was also still the 'anti-authority impulse' present (Kirwan and Power, 2013; Levy, 2010), with this being an expression of intergroup behaviour towards "outsiders" rather than the subcategories within the hacker identity.

8.1.2 Group processes

2) Assess the level of awareness within hacking communities of the potential influences in online groups, especially in vulnerable members, and examples of informed behaviour online.
3) Determine to what extent there is an observable effect of group process within hacking communities. Processes considered include group norms, influence, groupthink, conflict, and trust.

The second research aim in this study was regarding the influence on individual behaviour of the group processes. It was apparent in forum discussions that there were slow changes to attitudes and mindset, referred to as stage two within SIT. The adoption of the group identity and relevant social norms appeared to be part of the appeal of participating with these communities, with many citing the meritocracy of hacking communities as commendable as an influence, supporting the work of Zhang et al (2015). The hacking cycle requires that individuals prove their worth, do research, show effort in order to be accepted; once they are accepted, they adopt this behaviour with subsequent new comers.

From the observations detailed in Chapter 4 there was limited evidence of manipulation of trust or use of group process observed in fora. Those that went looking for grey or black hat related activities doubtless found them, but there was equally the information available for learning and skills that did not necessitate criminal activities. The influence of the group appeared strong in offline settings, but these were generally positive community conventions with the aim of responsible and informative disclosure. This of course could be due to the fact that black-hat or cybercriminal communities do not hold such events, for the obvious reason of entanglement with law enforcement.

The behaviour of the in-group vs out-group was interesting; initially the researcher expected higher conflict between the subcategories, for example, black-hats vs white-hats as the in-groups and out-groups. However, the more serious divisions seemed to mostly occur within subcategories, with disagreement over definitions. The overall view appears to be that one's self-identified category is mostly a personal decision; if you want to discuss your subcategory, then, in true hacker spirit, other community members will want logical and empirical evidence that your definition is accurate and not subject to personal bias. As discussed in Chapter 7, the most contentious area for this is the grey/white -hat divide. The exception to this seems to be cybercriminals; there was the impression that those who were not motivated by illicit financial gain looked down on those who used hacking tools to scam and ransom. It is not regarded as skilful, and therefore not true hacking. Others however felt that making money is a fact of life, therefore why should they not use their skills and knowledge over others. When this sentiment was voiced, there was a degree of superiority and a lack of sympathy or empathy expressed for potential victims; if someone doesn't learn enough to defend themselves, that's their problem, and they can be taken advantage of.

The researcher observed that regardless of their subcategory, individuals categorised themselves in the "hacker" in-group, rather than their subcategory, and the out-group was the government or law enforcement, or even the general public who were not informed (see Chapter 6). This was especially interesting given the government and security companies trying to be more encouraging of "ethical" hackers – as is the community – than they were even 20 years ago. Despite this shared desire for better security and technological advancement, the hacker community seems still suspicious and untrusting of these out-groups (Chapters 4 & 6; Kirwan and Power, 2013; Levy, 2010). Although government and security companies offer legitimised ways to use hacking skills, they are criticised by the hacking community for not fully understanding the standards required and have to an extent become their own subcategory of InfoSec professionals. As such this group has more presence in their own community and in the offline context. Whilst individuals appear to be comfortable categorising themselves as both InfoSec and white-hat (see Table 24 and data from Chapter 7) if the

hacking community perceives the out-group trying to encroach on a private community it does not welcome the intrusion. This is in part believed to be the difference between teaching sites and forums online; at the teaching sites, InfoSec and White-hat crossover is never seen as a problem, but in the more general fora it is less accepted, often with a separate section for those only interested in white-hat techniques.

Originally this research anticipated that more data would be obtained regarding hacktivism. In fact, this was one of the smallest subcategories that the community openly identified with (Chapter 5 & 7). It is suggested by the researcher that following the high-profile exploits of Anonymous and Lulzsec the methods and channels for hacktivism have vastly changed, supporting the conclusions of Coleman (2015). There is evidence that hacktivism is becoming either less widespread or less reported on in the western world, although still used effectively in Africa (Solomon, 2017), with protests moving increasingly against corporations rather than governments (Postill, 2014). What were common tactics, such as DDoS attacks, are not now used in the same way, which again could be attributed to the arrest and prosecution of those involved in the Paypal14 attacks (see Chapter 2). There has been a realisation among online communities that the role of anonymity has changed; there is evidence that it is still assumed in “lulz attacks”. The latest example of this was the “swatting” death in the USA, when a hoax call after an online dispute led to the fatal police shooting of a man (The Guardian, 2018), but this appears to be restricted to “skids” or “wannabes” from sites such as 4chan or gaming related fora, rather than those individuals invested in hacking communities.

Within the community that was accessed for this research, the influence of group dynamics appears to not be directed towards encouraging attacks, but more towards promoting a positive self identity for the individual and the communities.

8.1.3 Cybersecurity

4) Clarify the relevance of hacking related activity for cybersecurity development. Is there potential to develop mitigation and prevention techniques from cyberattacks? Is there evidence of a strong link between hacking communities and cyberattacks?

A clear desire within the hacking community is for improved security, but not at the further cost of privacy online. In the communities that engaged with the researcher there was an obvious overlap between the InfoSec, white-hat, and grey-hat subcategories. The use and acceptance of grey-hat techniques in improving security is self justified by the community as long as the results are defined and consistently productive. In terms of mitigation and prevention, the researcher believes a positive step forward would be to acknowledge the evident distinction between cybercriminals and hackers. Whilst there is a recognised overlap between these identities, the traits and motivations are

starkly divergent. The observations and data from this research suggest that hacking communities rarely engage in large scale cyberattacks, although the black-hat subcategory is still active in scamming and cracking activities. By de-stigmatising the hacking communities, the knowledge and mitigation techniques would be more easily disseminated through the general population, including for example sensible but achievable approaches to personal security; increased awareness of one's online footprint; and accepting that there is no method that enables 100% security online. This dissemination has the additional benefit of assuring victims of cyberattacks or scams, helping them to understand that it is not necessarily their "fault", but to be vigilant and incorporate best practices for online safety.

8.2 Key contributions to knowledge

The main contributions to knowledge from this research are to the fields of psychology and cybersecurity. For psychology, this research demonstrates the validity of applying social psychological theory to online contexts, strengthening and emphasising the significance of the distinction between online and offline social contexts. Whilst Social Categorisation Theory was not as applicable to the individuals involved in this research, the Social Identity Theory showed relevance. The main distinction however was that the third stage of SIT did not necessarily lead to negative intergroup comparison or any intergroup conflict in this context; it is possible there needs to be an adaptation of social psychological theories in order to fully allow their application to positive online communities, not only to toxic ones. This research also attempted to provide a different perspective on cyber events than has previously been taken and as such expanded cyber-psychological knowledge through the participant observation method (see Chapter 4). With regards to cybersecurity this research has and will continue to highlight the importance of recognising the social psychology present in cyber incidents and investigations. Discussions and sharing of knowledge about the influence and importance of human factors and human-computer interaction leads to improved security concepts and safer communities for individuals interested in hacking. It is hoped that this trend will continue within hacking and security communities, to improve the design and application of technology and hence contribute to the overall security of the internet.

The hacker social identity, discussed in section 8.2.1, as well as leading to the formation of the community and subcategories, has unmistakeable motivation that drives the majority of members: the importance of curiosity and learning. The emphasis within hacker communities to educate and improve oneself is a major positive factor, which also makes the community more accessible: they welcome those who want to learn, whether it's in learning to code, improving hacking skills, or even as in the case of the researcher, examining the community itself. This research provides evidence

that, although difficult to access, hacking communities will work and support endeavours to improve individuals, communities, and technology. All members have their own preference and priorities, but the overwhelming picture is that knowledge is important and should be found and shared. This does not mean that there is no element of gatekeeping with in the community, it is clear that the members are very wary of strangers who are not seriously interested. The communities are very factual, and require evidence of effort and commitment, but if these criteria are met they are often willing to help. This is an observation that overlaps with many of the qualities that were evident in the initial era of hacktivism, that were cited as a motivation: to help people and provide information and evidence to improve real world situations. Whilst hacktivism has changed significantly in the last 15 years, this is still a distinct priority within hacking communities.

For the hacking communities themselves, there is the hope that this research, in conjunction with previous studies (Madarie, 2017; Zhang, 2015), can prevent them from continuing to be marginalised and stereotyped. By proving the communities to be positive and engaged, this may help to further develop and provide legitimate channels of communication with academics, companies, and governments. There is also evidence that suggests these results will help vulnerable group members (Chapters 4 and 6), giving them confidence in identifying their role and position within the community, as well as raising awareness on the potential for manipulation from their own groups. It is believed that this would help to avoid another "Paypal 14" situation where individuals were taken advantage of through group processes (see Chapter 2 for full details). Even during the period of this research, more of the conferences and communities have openly discussed the effects of imposter syndrome, the prevalence and needs of those with autism in the community, mental health issues – including depression, which is especially commendable in a male dominated environment (see Chapter 4, section 4.3.5). The hacker community is acknowledging to itself the importance of psychology and human factors, not just in how they help improve their hacks, but in how they can support and work with each other as a community, regardless of the "hat" they wear.

8.3 Reflections and Limitations

Whilst the researcher acknowledges that there are hackers who do engage in cybercrime, this was not the focus of this research; as such no strong attempt was made to recruit individuals from this area. This is evident in the results but was a conscious decision. Aside from often not fitting into the theorised "hacker identity", the financial motivation of cybercriminals highlights a significant difference to other hackers' motivation, regardless of their identification as Black-hat (illegal/immoral techniques), Grey-hat (mixed), or White-hat (legal/moral techniques). There are instances where individuals argued their tactics or techniques were not always "White-hat" but

because the motivation and consequences from the actions were, they still self-identified as White-hat or example, those involved in social engineering or penetration-testing might use Black–hat skills to test the security of a program. Cracking forums, which commonly are based around black-hat and illegal activities, were included in the early searches, and the researcher posted on them. As discussed in Chapter 4, the researcher's account was subsequently banned on four cracking forums and her threads removed. This was taken as an obvious sign that this section of the community did not want to be involved, and it was felt if there were individuals who were interested, they would be able to find the researcher on other forums with relative ease. Initial contact had been made and members of the forums had the opportunity to follow up if they wished.

Whilst the participant observation was primarily to ensure an understanding of people from their own frames of reference, experiencing reality as they experience it (Corbin and Strauss, 2008), this was not possible in relation to underground fora involved in cybercrime. It would have taken a vast amount of time and resources to gain meaningful insight, which would have necessitated that observation of the other areas of hacking, which are often overlooked, would have suffered. Because of this, and because of concerns for security around the researcher and participant data, the cybercriminal aspect of hacking communities was not investigated. Where there were obvious illegal or criminal related threads and discussions on the hacking fora, this was included in the participant observations (see Chapter 4).

This research resulted in far more qualitative data than anticipated, partly through changes in design, led by the data collected through observations and Study 1 (Chapter 4 and 5), and partly because even with the quantitative surveys, the community respondents wished to give thoughts and opinions, which cannot be wholly quantified. As with all qualitative research, this means the analysis and interpretations of the data are subjective to a degree; objectivity was a necessary factor in the design of the surveys and the interview questions, but there are some subjective factors that could not be avoided. There was an awareness of potential influence from the researcher in the form of confirmation bias. This research has always emphasised the positive identity within hacking communities, as well as the desire to combat the negative stereotypes. As such the reflexive process was a key part of each study in order to confirm to the researcher that negative aspects of the community were not being overlooked or excluded. There is also the acknowledgement that the cybercriminal element is probably less likely to respond to research of this type, while the pro-information spreading hackers are more likely to be interested and participate.

Another factor that could influence this research was the researchers' gender. As stated in Chapter 1 this research did not focus on gender-related issues within the hacking communities, although the

presence is acknowledged in the literature review (Chapter 2). It was felt that the inclusion of gender as a key variable would diminish the importance of the role of social identity, shared by male, female, and transgender participants. Therefore, the scope of this research purposefully avoided addressing such issues; female and transgender participants were in the minority, any comments on this from participants were included as part of the investigation of the social identity. With all online posts and surveys, comments made it apparent that participants believed the researcher was male. This was not corrected, but equally the researcher identity was not hidden if they wished to find her. It is challenging to judge the impact of the researcher with complete certainty, but it is strongly believed that results from observations and the interviews would have been significantly different had the research been carried out by a male with more technical knowledge. It is impossible to say in what ways the data would have been affected but it is believed that there are positives to the research being conducted by a non-technical female. Initially the limited technical knowledge on the part of the researcher was a concern, as a hindrance to gaining access and interest from the hacking community members. With the benefit of hindsight, in combination with the researcher's gender it is believed that this limit of knowledge may have in fact allowed further access. Computer, technology, and hacking related fields are competitive and male dominated (Brooke, 2018), and the approach of a technical minded male would have been a less obvious intrusion; however, the researcher believes this would also have inspired different reactions from the male participants, in the sense of viewing a male researcher as a challenger or competitor in some form. With the researcher however, as she deferred to the participants, on both their personal experiences and hacking knowledge, it is believed there was a calmer disposition. This was especially noticeable in interviews where the participant was an older male, there was an air of mentorship that made it seem that they were more willing to talk openly (Ragins, 1999) about aspects that may have been over looked otherwise, such as mistakes made by the participant while developing their skills.

8.4 Future Studies

This research was exploratory in terms of methodology, attempting to find the most efficient and effective ways to contact and question hard to reach and secretive online communities. It is intended that the methods used can be developed into a comprehensive guide for procedures for others to use. This research will continue to be disseminated to academics, hackers, and the general public, to educate and inform on cyber-safety and emphasise that hacking is not in itself a crime nor only done by criminals. Hacking has helped to develop new technologies and encourages new ways of thinking. This positive approach to hacking, combined with the consideration of human factors should also be applied to current education in the UK; lessons in coding and computer science are

growing rapidly, as is the encouragement to become involved in these fields. It is believed this could be achieved through further co-operation with government agencies to ensure that school curricula involve not only the practical aspects but also the issues of social responsibility and the risks of engaging in cybercriminal activities. In this form it is hoped that this research could help a new generation of those interested in hacking, not only from finding a community to help them grow in ability, but also to make informed choices on what they do with the abilities they learn.

A recommended approach to this area is to continue promoting research into developing a better understanding of why people become involved in hacking. Whilst motivations have long been a research topic, there is evidence to suggest that the motivation becomes a more significant factor after the individual has found and adopted a social identity. It would be interesting to examine, in a subsequent study, the link between the motivation for hacking involvement and what participants felt to be their salient hacker identity, as these were observed to be fluid rather than static; it is recommended that this is also investigated for examples of cognitive dissonance within the community. The ways in which individuals' online collectives are treated and cyberattacks are dealt with are currently very harsh, with those who are merely reporting issues and vulnerabilities in a responsible way being arrested (Osborne, 2016; Siqi, 2016; Zetter, 2014). It is hoped that the evidence of the positive aspects of hacking communities can be disseminated to prevent the knee-jerk reaction against "hacks" that are actual productive rather than destructive.

The development of a global internet policy should remain an aim, despite the obvious difficulties in achieving a global consensus across different states and cultures. This researcher emphasises that such policies need to be developed in conjunction with those who have knowledge and insight into technology and hacking communities. This supported by the participants, who expressed concerns that laws and regulations were being made by those who did not understand the technologies and techniques invovled. Legitimate organisations such as Electronic Frontier Foundation focus on informing the general public and organisations, whilst stating the value of privacy and anonymity online. The information and attitudes towards security can be applied to public and workplace settings, to encourage individuals to adopt better approaches to managing Cybersecurity threats, such as not opening links in phishing emails or disclosing sensitive information that could be used in an attack.

Future work needs to continue to engage with these diverse and multifaceted communities. As noted throughout this research, the common and negative stereotype of hackers equating to criminal is misleading and overly simplistic. By developing an informed and mutually respectful

relationship with such communities there is the potential for knowledge exchange that could be used to address at least some of the societal challenges related to cybersecurity.

8.5 References

Adams, T. (2018). “Facebook’s week of shame: the Cambridge Analytica fallout”. *The Guardian*, retrieved August 28, 2018, from https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence

Allport, G.W. (1954). *The Nature of Prejudice*. Cambridge MA: Perseus Publishing.

Anderson, B. (1983). *Imagined communities: reflections on the origin and spread of nationalism*. London: Verso.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M. & Savage, S. (2013). “Measuring the cost of cybercrime”. In *The economics of information security and privacy,* 265–300.

Attrill, A. (Ed) (2015). *Cyberpsychology*. Oxford: Oxford University Press.

Bacharach, M. & Gambetta, D. (2001). “Trust in signs”. *Trust in society*, Vol. 2, 148-184.

Ball, J. (2013). “How the Snowden leak is changing the tech landscape”, *The Guardian*, retrieved March 13, 2017 from https://www.theguardian.com/world/2013/dec/02/snowden-leak-tech-privacy-nsa-gchq-surveillance

Barak, A., Boniel-Nissim, M. & Suler, J. (2008). “Fostering empowerment in online support groups”. *Computers in Human Behavior*, 24(5), 1867-1883.

Barber, R. (2001). “Hackers profiled—who are they and what are their motivations?”. *Computer Fraud & Security*, 2, 14-17.

Beenen, G., Ling, K., Wang, X., Chang, K., Frankowski, D., Resnick, P. & Kraut, R. E. (2004). “Using social psychology to motivate contributions to online communities”. In *Proceedings of the 2004 ACM conference on Computer supported cooperative work*, 212-221.

Beldad, A., De Jong, M. & Steehouder, M. (2010). “How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust”. *Computers in human behavior*, 26(5), 857-869.

Benjamin, V. & Chen, H. (2012). “Securing cyberspace: Identifying key actors in hacker communities”. In *Intelligence and Security Informatics (ISI)*, 2012 IEEE International Conference 24-29.

Benjamin, V., Zhang, B., Nunamaker Jr, J.F. & Chen, H. (2016). "Examining hacker participation length in cybercriminal Internet-relay-chat communities". *Journal of Management Information Systems*, 33(2), 482-510.

Bernstein, M.S., Monroy-Hernández, A., Harry, D., André, P., Panovich, K. & Vargas, G.G. (2011). "4chan and/b: An Analysis of Anonymity and Ephemerality in a Large Online Community." In *ICWSM,* 50-57.

Bissett, A. & Shipton, G. (1999). "An investigation into gender differences in the ethical attitudes of IT professionals". *ETHICOMP99*, Rome.

Blue, V. (2016). "The hysterical hacking headlines of Def Con 24". *Engadget,* retrieved August 30, 2016, from https://www.engadget.com/2016/08/12/def-con-2016-hysterical-headlines-mainstream-media/.

Bojarski, K. (2015). "Dealer, Hacker, Lawyer, Spy: Modern Techniques and Legal Boundaries of Counter-cybercrime Operations." *The European Review of Organised Crime,* 2-2, 25-50.

Brambilla, M., Sacchi, S., Pagliaro, S. & Ellemers, N. (2013). "Morality and intergroup relations: Threats to safety and group image predict the desire to interact with outgroup and ingroup members." *Journal of Experimental Social Psychology*, 49(5), 811-821.

Branscombe, N.R. & Wann, D.L. (1994). "Collective self-esteem consequences of outgroup derogation when a valued social identity is on trial." *European Journal of Social Psychology*, 24(6), 641-657.

Branzei, O., Vertinsky, I. & Camp, R.D. (2007). "Culture-contingent signs of trust in emergent relationships". *Organizational behavior and human decision processes*, 104(1), 61-82.

Braun, V. & Clarke, V. (2006). "Using thematic analysis in psychology". *Qualitative research in psychology*, 3(2), 77-101.

British Psychological Society (2017). "Ethics Guidelines for Internet-mediated Research". Retrieved January 18, 2018, from: https://www.bps.org.uk/files/ethics-guidelines-internet-mediated-research-2017pdf

Brooke, S. J. (2018). "Breaking Gender Code: Hackathons, Gender, and the Social Dynamics of Competitive Creation". *Hackathon Workshop 2018*, retrieved June 12, 2018, from http://hackathon-workshop-2018.com/

Brown, R. (1988). *Group processes: Dynamics within and between groups*. Oxford: Blackwell.

BruCon (2018). Retrieved August 15, 2018, from https://www.brucon.org/2018/conference/

Castellan, N.J. (2013). *Individual and group decision making: current issues*. Psychology Press.

Castells, M. (1996). *The network society*. Oxford: Blackwell.

Chandler, A. (1996). "The Changing Definition and Image of Hackers in Popular Discourse." *International Journal of the Sociology of Law*; 24-2: 229-251.

Chantler, N. (1996). *Profile of a computer hacker*. Florida: Infowar.

Chapman, G.B. & Johnson, E.J. (2002). "Incorporating the irrelevant: Anchors in judgments of belief and value". *Heuristics and biases: The psychology of intuitive judgment*, 120-138.

Chiu, C.M., Hsu, M.H. & Wang, E.T. (2006). "Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories". *Decision support systems*, 42(3), 1872-1888.

Cialdini, R.B., Borden, R.J., Thorne, A., Walker, M.R., Freeman, S. & Sloan, L.R. (1976). "Basking in reflected glory: Three (football) field studies." *Journal of personality and social psychology*, 34(3), 366.

Coleman, G. (2010). "The hacker conference: A ritual condensation and celebration of a lifeworld". *Anthropological Quarterly*, 47-72.

(2011). "Hacker politics and publics". *Public Culture*, 23(3 65), 511-516.

(2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books.

(2015). "Epilogue: The State of Anonymous", chapter in *Hacker, hoaxer, whistleblower, spy: The Many Faces of Anonymous*, Verso books, 401-461.

Collister, L.B. (2017). "Transformative (h)activism: Breast cancer awareness and the World of Warcraft Running of the Gnomes". *Transformative Works and Cultures*, 25.

Corbin, J. & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. 3rd Edition, London: SAGE Publications.

Crews, C.W. (2007). "Cybersecurity and Authentication: the marketplace role in rethinking anonymity–before regulators intervene." *Knowledge, Technology & Policy*, 20(2), 97-105.

Davis, K. & James, C. (2013). “Tweens' conceptions of privacy online: implications for educators”. *Learning, Media and Technology*, 38(1), 4-25.

Denning, D.E. (2011). “Cyber conflict as an emergent social phenomenon”. In *Corporate hacking and technology-driven crime: Social dynamics and implications*, 170-186. Hershey, PA: IGI Global.

Dobusch, L. & Schoeneborn, D. (2015). “Fluidity, identity, and organizationality: The communicative constitution of Anonymous.” *Journal of Management Studies*, 52(8), 1005-1035.

Doney, P.M., Cannon, J.P. & Mullen, M.R. (1998). “Understanding the influence of national culture on the development of trust”. *Academy of management review*, 23(3), 601-620.

Douglas, M. & Wildavsky, A. (1983). “Risk and culture: An essay on the selection of technological and environmental dangers”. California: University of California Press.

Dupont, B., Côté, A-M., Savine, C., Décary-Hétu, D. (2016). “The ecology of trust among hackers.” *Global Crime,* 17-2: 129-151.

Eaton, S. E. (2011). “How Long Does it Take to Learn a New Language?” Retrieved March 15, 2017, from https://drsaraheaton.wordpress.com/2011/02/20/how-long-does-it-take-to-learn-a-new-language.

Economist (2016). “The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise”, *The Economist Intelligence Unit*, retrieved June 12, 2018, from https://www.eiuperspectives.economist.com/technology-innovation/cyber-chasm-how-disconnect-between-c-suite-and-security-endangers-enterprise-0/article/protecting-brand%E2%80%94cyberattacks-and-reputation-enterprise

Eurostat (2018). *Educational attainment statistics,* retrieved March 15, 2018, from http://ec.europa.eu/eurostat/statistics-explained/index.php?title=Educational_attainment_statistics#Level_of_educational_attainment_by_age

Executive Women’s Forum, Frost & Sullivan and (ISC)^2 (2017). “The 2017 Global Information Security Workforce Study: Women in Cybersecurity”. Retrieved June 8, 2018, from https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

Farrell, S. (2016). “TalkTalk counts costs of cyber-attack”. *The Guardian*, retrieved March 13, 2017, accessed at https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave.

Festinger, L. (1950). “Informal social communication”. *Psychological review*, 57(5), p.271.

(1962). *A theory of cognitive dissonance (Vol. 2)*. Stanford University Press.

Fogel, J., & Nehmad, E. (2009). “Internet social network communities: Risk taking, trust and privacy concerns”. *Computers in Human Behaviour*, 25, 153-160.

Fötinger, C.S. & Ziegler, W. (2004). “Understanding a hacker’s mind–A psychological insight into the hijacking of identities”. Danube-University Krems, Austria: *RSA Security*.

Fox, N.J. (2004). “Qualitative data analysis”, *Health and Social Care Research*. Sheffield: University of Sheffield.

Goode, L. (2015). “Anonymous and the Political Ethos of Hacktivism”. *Popular Communication*, 13-1, 74-86.

Greenburg, A. (2014). “What is the dark web?” *Wired.com*, retrieved March 13, 2017, from https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

Guardian (2018). “Suspect in Kansas 'swatting' death charged with involuntary manslaughter”, *The Guardian*, retrieved June 12, 2018, from at https://www.theguardian.com/us-news/2018/jan/13/suspect-kansas-swatting-death-charged-involuntary-manslaughter

Halbert, D. (1997). “Discourses of danger and the computer hacker”. *The Information Society*, 13(4), 361-374.

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA: IGI Global.

Hampson, N.C. (2012). “Hacktivism: A new breed of protest in a networked world”. *Boston College International & Comparative Law Review*, 35, 511.

Hanna, P., Vanclay, F., Langdon, E. J., & Arts, J. (2016). “Conceptualizing social protest and the significance of protest actions to large projects”. *The Extractive Industries and Society*, 3(1), 217–239.

Harris-McKoy, D. & Cui, M. (2013). “Parental control, adolescent delinquency, and young adult criminal behavior.” *Journal of child and family studies*, 22(6), 836-843.

Hay, C., Meldrum, R. & Mann, K. (2010). “Traditional bullying, cyber bullying, and deviance: A general strain theory approach.” *Journal of Contemporary Criminal Justice*, 26(2), 130-147.

Hewstone, M. & Jaspars, J.M.F. (1982). “Intergroup relations and attribution processes.” *Social identity and intergroup relations*, 99, 133.

Hogg, M.A., Abrams, D., Otten, S. & Hinkle, S. (2004). “The social identity perspective: Intergroup relations, self-conception, and small groups”. *Small Group Research*, 35(3), 246-276.

Hong, Y.S. & Kim, D.K. (2011). “Structural relation of juvenile stress, self-esteem, self-control and cyber delinquency: Testing a sex difference”. *Korea Youth Research Association*, 18(1), 127-148.

Hornsey, M.J. & Hogg, M.A. (2000). “Subgroup relations: A comparison of mutual intergroup differentiation and common ingroup identity models of prejudice reduction”. *Personality and Social Psychology Bulletin*, 26(2), 242-256.

Hornsey, M.J. (2008). “Social identity theory and self-categorization theory: A historical review”. *Social and Personality Psychology Compass*, 2(1), 204-222.

Howard, J.A. (2000). “Social psychology of identities”. *Annual review of Sociology*, 26(1), 367-393.

Hsu, C. L., & Lin, J. C. C. (2008). “Acceptance of blog usage: The roles of technology acceptance, social influence and knowledge sharing motivation”. *Information & Management*, 45(1), 65-74.

Hu, C., Zhao, L. & Huang, J. (2015). “Achieving self-congruency? Examining why individuals reconstruct their virtual identity in communities of interest established within social network platforms”. *Computers in Human Behavior*, 50, 465-475.

Janis, I.L. (1972). *Victims of groupthink: a psychological study of foreign-policy decisions and fiascoes.* Oxford, England: Houghton Mifflin.

Joiner, R., Gavin, J., Brosnan, M., Cromby, J., Gregory, H., Guiller, J., Maras, P. & Moon, A. (2013). “Comparing first and second generation digital natives' Internet use, Internet anxiety, and Internet identification”. *Cyberpsychology, Behavior, and Social Networking*, 16(7), 549-552.

Joinson, A.N. (2007). “Disinhibition and the Internet”. In J. Gackenbach (Ed.), *Psychology and the Internet: Intrapersonal, interpersonal, and transpersonal implications*, 2nd ed., San Diego, CA, US: Academic Press, 75-92.

Jordan, T., & Taylor, P. (1998). “A sociology of hackers”. *The Sociological Review*, 46(4), 757-780.

Kahneman, D., Lovallo, D. & Sibony, O. (2011). “Before you make that big decision”. *Harvard Business Review*, 89(6), 50-60.

Kirwan, G. & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Cambridge: Cambridge University Press.

Kozinets, R.V. (2015). *Netnography: redefined*. London: SAGE Publications.

(2010) *Netnography*. London: SAGE Publications.

Krapp, P. (2005). "Terror and play: or what was hacktivism?". *Grey Room*, 70-93.

Kubitschko, S. (2015). "The Role of Hackers in Countering Surveillance and Promoting Democracy". *Media and Connection*, 3-2: 77-87.

Lampe K. V., & Johansen, P. O. (2004). "Organized crime and trust: on the conceptualization and empirical relevance of trust in the context of criminal networks," *Global Crime*, 6, 2.

Landreth, B. & Rheingold, H. (1985). *Out of the inner circle: a hacker's guide to computer security.* Bellevue, Washington: Microsoft Press.

Lapidot-Lefler, N. & Barak, A. (2015). "The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors?". *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 9(2).

Leach, D.K. (2009). "An Elusive "We" Antidogmatism, Democratic Practice, and the Contradictory Identity of the German Autonomen". *American Behavioral Scientist*, 52(7), 1042-1068.

Levy, S. (2010). *Hackers: Heroes of the computer revolution*. Sebastopol, CA: O'Reilly.

Madarie, R. (2017). "Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers". *International Journal of Cyber Criminology*, 11(1).

Marcella, A. J. (1999). *Establishing trust in virtual markets*. Altamondate Springs, Florida: Institute of Internal Auditors.

Marques, J.M. & Paez, D. (1994). "The 'black sheep effect': Social categorization, rejection of ingroup deviates, and perception of group variability." *European Review of Social Psychology*, 5(1), 37-68.

Mayer, R.C., Davis, J.H. & Schoorman, F.D. (1995). "An integrative model of organizational trust." *Academy of Management Review*, 20(3), 709-734.

McMahon, C. (2016). "Cyber-Psychology: The Key to Securing the Human Element in Your Organization". *Info Security Magazine,* retrieved April 14, 2016, from https://www.infosecurity-magazine.com/magazine-features/cyberpsychology-securing-human/.

Media Insight Project (2016). “A new understanding: What makes people trust and rely on news,” *The American Press Institute*, retrieved June 12, 2018, from https://www.americanpressinstitute.org/publications/reports/survey-research/trust-news/single-page/

Merck, M. (2015). “Masked men: hacktivism, celebrity and anonymity”. *Celebrity studies*, 6(3), 272-287.

Meyers, C., Powers, S., & Faissol, D. (2009). “Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches”. *Lawrence Livermore National Laboratory*, 7, 1-22.

Milan, S., & Atton, C. (2015). “Hacktivism as a radical media practice” in Atton, C. (Ed), *The Routledge Companion to Alternative and Community Media*, 550-560. Oxon: Routledge.

Milner, R. M. (2013). “ Hacking the Social: Internet Memes, Identity Antagonism, and the Logic of Lulz.” *The Fibreculture Journal*, 22.

Mitchell, A. (2005). “A Leet Primer”, Tech News World, retrieved August 26, 2018, from https://www.technewsworld.com/story/47607.html

Moore, R. (2005). *Cyber crime: Investigating High-Technology Computer Crime*. Cleveland, MI: Anderson Publishing.

Nail, P.R. (1986). “Toward an integration of some models and theories of social response”. *Psychological Bulletin*, 100(2), 190.

Narayanan, A. (2013). “What happened to the crypto dream?, part 1.” *IEEE Security & Privacy*, 11(2), 75-76.

National Crime Agency (NCA) (2016). “Cyber crime: Preventing young people from getting involved”. National Crime Agency. Retrieved January 18, 2017, from http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved

Nisbett, P. (2018). “Steelcon 2018”, *Paul Nisbett Blog*, retrieved August 24, 2018, from https://paulnisbett.com/steelcon-2018-the-annual-trip-to-sheffield-that-keeps-getting-better

Nissenbaum, H. (2004). “Hackers and the contested ontology of cyberspace”. *New Media & Society*, 6(2), 195-217.

O'Brien D. (2004). "Life Hacks: Tech Secrets of Overprolific Alpha Geeks". Presentation *at O'Reilly Emerging Technology Conference*, San Diego, USA.

Olsen, P. (2013). *We are Anonymous*. London: Random House.

Onorato, R. S. & Turner, J. C. (2004). "Fluidity in the self-concept: The shift from personal to social identity". *European Journal of Social Psychology*, 34, 257-278.

Osbourne, C (2016). "Security researcher arrested for disclosing US election website vulnerabilities", ZdNet.com, retrieved January 18, 2017, from https://www.zdnet.com/article/security-researcher-arrested-for-reporting-us-election-website-vulnerabilities/

Oxford English Dictionary (2012). Oxford: Oxford University Press.

Packer, D.J. (2009). "Avoiding groupthink: Whereas weakly identified members remain silent, strongly identified members dissent about collective problems". *Psychological Science*, 20(5), 546-548.

Papadimitriou, F. (2009). "A nexus of Cyber-Geography and Cyber-Psychology: Topos/''Notopia" and identity in hacking." *Computers in Human Behavior,* 25, 1331–1334.

Pfleeger, S.L., & Caputo, D. (2012). "Leveraging behavioral science to mitigate cybersecurity risk". *Computers and Security*, 31, 597-611.

Pingdom (2012). Pingdom website, retrieved June 13, 2018, from https://royal.pingdom.com/2012/04/24/irc-is-dead-long-live-irc/

Postill, J. (2014). "Freedom technologists and the new protest movements: A theory of protest formulas". *Convergence: The International Journal of Research into New Media Technologies*,20-4, 402-418.

Postmes, T. & Brunsting, S. (2002). "Collective action in the age of the Internet: Mass communication and online mobilization". *Social Science Computer Review*, 20(3), 290-301.

Postmes, T. & Spears, R. (2002). "Behavior online: Does anonymous computer communication reduce gender inequality?". *Personality and Social Psychology Bulletin*, 28(8), 1073-1083.

Power, A., and Kirwan, G. (Eds) (2014). *Cyberpsychology and New Media: A thematic reader*. New York: Psychology Press.

Preece, J., & Maloney-Krichmar, D. (2005). “Online communities: Design, theory, and practice.” *Journal of Computer-Mediated Communication*, 10(4).

Ragins, B. R. (1999). “Gender and mentoring relationships”. In G. N. Powell (Ed.), *Handbook of gender in organizations* (347–370). Thousand Oaks, CA: Sage.

Raymond E. (1996). *The New Hacker's Dictionary*. USA: MIT Press.

(2001). “How to become a hacker”, *Cathedral and the Bazaar,* retrieved June 18, 2017 from http://www.catb.org/esr/faqs/hacker-howto.html

Reddit (2018). Organisation website, retrieved August 24, 2018, from https://www.redditinc.com/

Reicher, S.D., Spears, R. & Postmes, T. (1995). “A social identity model of deindividuation phenomena”. *European Review of Social Psychology*, 6(1), 161-198.

Reid, E. M. (1996). “Communication and community on Internet Relay Chat: Constructing communities”. In P. Ludlow (Ed), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, 397-411. Sabon: MIT Press.

Rid, T. & Buchanan, B. (2015). “Attributing cyber attacks”. *Journal of Strategic Studies*, 38(1-2), 4-37.

Rogers, M. (2003). “The psychology of cyber-terrorism” In Silke A. (Ed.), *Terrorists*, *Victims and Society*: *Psychological Perspectives on Terrorism and Its Consequences,* 75–92. London: Wiley and Sons.

(2011). “The psyche of cybercriminals: A psycho-social perspective”. In *Cybercrimes: A multidisciplinary analysis,* 217-235. Berlin: Springer.

Rosenzweig, R. (1998). “Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet.” *The American Historical Review*, 103(5), 1530-1552.

Scheuerman, W.E. (2016). “Digital disobedience and the law”. *New Political Science,* 38-3, 299-314.

Schimke, D., Stoeger, H. & Ziegler, A. (2007). “The relationship between social presence and group identification within online communities and its impact on the success of online communities”. In *International Conference on Online Communities and Social Computing,* 160-168. Berlin: Springer.

Schrock, A.R. (2016). “Civic Hacking as data activism and advocacy: A history from publicity to open government data”. *New Media and Society*, 1-19.

Seebruck, R. (2015). “A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.” *Digital Investigation*, 14, 36-45.

Shah, D.V., Kwak, N. & Holbert, R.L. (2001). ““Connecting" and "Disconnecting" With Civic Life: Patterns of Internet Use and the Production of Social Capital”. *Political Communication,* 18-2, 141-162.

Shankar, V., Urban, G.L. & Sultan, F. (2002). “Online trust: a stakeholder perspective, concepts, implications, and future directions”. *The Journal of Strategic Information Systems*, 11(3-4), 325-344.

Sherif, M. (1956). “Experiments in group conflict”. *Scientific American*, 195(5), 54-59.

Shiau, W. L. & Luo, M. M. (2012). “Factors affecting online group buying intention and satisfaction: A social exchange theory perspective”. *Computers in Human Behavior*, 28(6), 2431-2444.

Short, J., Williams, E. & Christie, B. (1976). *The social psychology of telecommunications*. London: Wiley.

Siqi, C. (2016). “Helpful hacker forums close after arrest for revealing vulnerabilities”, Global Times, accessed January 28, 2017, from http://www.globaltimes.cn/content/1001271.shtml

Skibell, R. (2002). “The myth of the computer hacker”. *Information, Communication & Society*, 5(3), 336-356.

Smith, A.D. & Rupp, W.T. (2002). “Issues in cybersecurity; understanding the potential risks associated with hackers/crackers”. *Information Management & Computer Security*, 10(4), 178-183.

Smith, J.R. & Hogg, M.A. (2008). “Social identity and attitudes”. *Attitudes and Attitude Change*, 337, 360.

Solomon, R. (2017). “Electronic protests: Hacktivism as a form of protest in Uganda”. *Computer Law & Security Review*, 33(5), 718-728.

Spears, R. & Postmes, T. (2015). “Group identity, social influence, and collective action online”. *The Handbook of the Psychology of Communication Technology*, 23-46. Oxford: Wiley.

Stets, J.E. & Burke, P.J. (2000). “Identity theory and social identity theory”. *Social Psychology Quarterly*, 224-237.

Stryker, S. & Burke, P.J. (2000). “The past, present, and future of an identity theory.” *Social Psychology Quarterly*, 284-297.

Sturgis, P., Patulny, R., Allum, N. & Buscha, F. (2012). “Social connectedness and generalized trust: a longitudinal perspective”. *ISER Working Paper Series*, 19, 1-23.

Suler, J. (2004). “The online disinhibition effect”. *Cyberpsychology & Behavior*, 7(3), 321-326.

Sun, N., Rau, PP-L., & Ma, L. (2014). “Understanding lurkers in online communities: A literature review”. *Computers in Human Behavior,* 38, 110–117.

Tajfel, H. (1974). “Social identity and intergroup behaviour”. *Information (International Social Science Council),* 13(2), 65-93.

Tanczer, L.M., 2016. “Hacktivism and the male-only stereotype”. *New Media and Society,* 18-8, 1599-1615.

Tanis, M. & Postmes, T. (2005). “A social identity approach to trust: Interpersonal perception, group membership and trusting behaviour”. *European Journal of Social Psychology*, 35(3), 413-424.

Tarrant, M. & North, A.C. (2004). “Explanations for positive and negative behavior: The intergroup attribution bias in achieved groups”. *Current Psychology*, 23(2), 161-172.

Taylor, P.A. (2005). “From hackers to hacktivists: speed bumps on the global superhighway?” *New Media & Society*, 7(5), 625-646.

Teo, T.S.H., Limb, V.K.G., & Laia, R.Y.C. (1999). “Intrinsic and extrinsic motivation in Internet usage.” *Omega,* 27-1, 25–37.

Terrion, J. L., & Ashforth, B. E. (2002). “From ‘I’to ‘we’: The role of putdown humor and identity in the development of a temporary group.” *Human Relations*, 55(1), 55-88.

Thomas, J. (2005). “The moral ambiguity of social control in cyberspace: a retro-assessment of the ‘golden age’of hacking”. *New Media & Society*, 7(5), 599-624.

Tilley, J. (2015). "Hard Evidence: do we become more conservative with age?", *The Conversation,* retrieved 24 August 2018, from https://theconversation.com/hard-evidence-do-we-become-more-conservative-with-age-47910

Travaglino, G.A. (2014). “Social sciences and social movements: the theoretical context”. *Contemporary Social Science*, 9(1), 1-14.

Tsohou, A., Karyda, M. & Kokolakis, S. (2015). “Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs”. *Computers & Security*, 52, 128-141.

Tu, C.H. & McIsaac, M. (2002). “The relationship of social presence and interaction in online classes”. *The American Journal of Distance Education*, 16(3), 131-150.

Tu, C.H. (2002). “The relationship between social presence and online privacy”. *The Internet and Higher Education*, 5(4), 293-318.

Turgeman-Goldschmidt, O. (2005). “Hackers' accounts hacking as a social entertainment”. *Social Science Computer Review*, 23(1), 8-23.

Turkle, S. (1984). *The second self: computers and the human spirit*. New York: Simon and Schuster.

(1999). “Cyberspace and Identity”. *Contemporary Sociology,* 28-6, 643–648.

Turner, J. C. (1975). “Social comparison and social identity: Some prospects for intergroup behaviour”. *European Journal of Social Psychology*, 5(1), 1-34.

(1985). “Social categorization and the self-concept: A social cognitive theory of group behaviour”. In E. J. Lawler (Ed.), *Advances in Group Processes* (Vol. 2, 77-122) Greenwich, CT: JAI Press.

Turner, J. C., & Oakes, P. J. (1986). “The significance of the social identity concept for social psychology with reference to individualism, interactionism and social influence.” *British Journal of Social Psychology*, *25*(3), 237-252.

Turner, J. C., Oakes, P. J., Haslam, S. A., & McGarty, C. A. (1994). “Self and collective: Cognition and social context”. *Personality and Social Psychology Bulletin*, 20, 454-463.

Tynan, D. (2016). “The state of cybersecurity: we’re all screwed”. The Guardian, retrieved August 26, 2016, from https://www.theguardian.com/technology/2016/aug/08/cyber-security-black-hat-defcon-hacking.

Uitermark, J. (2017). “Complex contention: Analyzing power dynamics within Anonymous”. *Social Movement Studies*, 16(4), 403–417.

V for Vendetta. (2005). [film] United States of America: Andy Wachowski, Larry Wachowski, James Mcteigue.

Van Lange, P.A. (2015). “Generalized trust: Four lessons from genetics and culture”. *Current Directions in Psychological Science,* 24(1), 71-76.

Vegh, S. (2002). “Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking”. *First Monday*; 7-10.

Voiskounsky, A.E. & Smyslova, O.V. (2003). “Flow-based model of computer hackers' motivation”. *CyberPsychology & Behavior*, 6(2), 171-180.

Wang, Y.D. & Emurian, H.H. (2005). “An overview of online trust: Concepts, elements, and implications”. *Computers in Human Behavior*, 21(1), 105-125.

Wellman, B., Haase, A.Q., Witte, J. & Hampton, K. (2001). “Does the Internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment.” *American Behavioral Scientist*, 45(3), 436-455.

Whitehead, T. (2016). “British teenager suspected of being a mystery hacker who stole CIA boss emails”. The Telegraph, retrieved August 24, 2016, from https://www.telegraph.co.uk/news/uknews/crime/12154592/British-teenager-suspected-of-being-a-mystery-hacker-who-stole-CIA-boss-emails.html

Wolfradt, U., & Doll, J. (2001). “Motives of Adolescents to use the internet as a function of personality traits, personal and social factors”. *Journal of Educational Computing Research,* 24-1, 13–27.

Xu, K., & Lombard, M. (2017). “Persuasive computing: Feeling peer pressure from multiple computer agents.” *Computers in Human Behavior*, 74, 152-162.

Young, R., Zhang, L. & Prybutok, V.R. (2007). “Hacking into the minds of hackers”. *Information Systems Management,* 24(4), 281-287.

Zajácz, R. (2013). “WikiLeaks and the problem of anonymity: A network control perspective”. *Media, Culture & Society*, 35(4), 489-505.

Zand, D.E. (1972). “Trust and managerial problem solving”. *Administrative Science Quarterly*, 229-239.

Zelda Capital (2009). “The History of the Triforce”, *Zelda Capital*, retrieved September 30, 2016, from http://www.zeldacapital.com/triforce.php

Zetter, K. (2014). “Teen Reported to Police After Finding Security Hole in Website”, *Wired,* retrieved September 30, 2016, from https://www.wired.com/2014/01/teen-reported-security-hole/

Zhang, X., Tsang, A., Yue, W.T. & Chau, M. (2015). “The classification of hackers by knowledge exchange behaviors.” *Information Systems Frontiers*, 17(6), 1239-1251.

9. Appendices

9.1 Complete Surveys and Ethics Approval

9.1.1. Pilot Survey Ethical Approval

Bournemouth University

Research Ethics Checklist

Reference Id	12275
Status	Approved
Date Approved	01/06/2016

Researcher Details

Name	Helen Thackray
School	Faculty of Science & Technology
Status	Postgraduate Research (MRes, MPhil, PhD, DProf, DEng)
Course	Postgraduate Research
Have you received external funding to support this research project?	No

Project Details

Title	Anonymous Online Hacking
Proposed Start Date of Data Collection	29/05/2016
Proposed End Date of Project	21/09/2018
Original Supervisor	John McAlaney
Approver	John McAlaney

Summary - no more than 500 words (including detail on background methodology, sample, outcomes, etc.)

9.1.1.1 Pilot Study Questions and Results

1. Please indicate your gender:

Answer:	Number of participants
Male	39
Female	3
Transgender	2
Other	3

2. Please indicate your ethnicity:

Answer:	Number of participants
African	0
Caribbean	0
Caucasian	35
South Asian	1
Latino/Hispanic	2
Middle Eastern	1
Mixed	4
Other	4

3. Please indicate your geographical region:

Answer:	Number of participants
Africa	2
Asia	2
Australasia/Oceania	2
Europe	15
North America	26
South America	0

4. Please indicate the level of education completed:

Answer:	Number of participants
Up to age 16/17 years	5
Up to age 18/19 years	8
Some college/university, no degree	14
Bachelor's degree (or equivalent)	13
Postgraduate degree (e.g. Masters, Doctorate)	3
Other	4

5. Have you ever accessed the computer or system without admission?

Answer:	Number of participants
Yes	26
Yes, but with permission	14
No	6
I don't know	1

6. What is your main motivation in remaining anonymous online?

Answer:	Number of participants
Privacy	18
Security	6
Freedom of expression	16
Honesty within the community	3
Other	4

7. What is your main motivation for participating in hacking activities?

Answer:	Number of participants
Money	3
Curiosity	26
Activism	3
Entertainment	6
Security	3
Other	6

8. How would you define yourself as a hacker?

Answer:	Number of participants
White-hat	10
Black-hat	1
Grey-hat	14
Script kiddie	11
Hacktivist	6
Other	5

Additional comments:

Participant Comments (Pilot Survey)
Very well done.
Some of the questions [were] restrictive
This is a narrow range of definitions you're cramming us into.
Kind of gay
This survey takes for granted that "hacking" is in some way related to, or specific to, computers. This is not true.
You are mixing definitions (hacker vs cracker). The goal of these questions is not very clear.
This is probably the last place you want to look for genuinely skilled hacker groups. 4chan is probably better, but certainly isn't as active as it used to be in this regard. There are subreddits that have decent attendance of skilled code monkeys that would probably give you good results. But most hacker groups communicate with each other via IRC. As far as your study goes, I think that it's a fantastic idea and that the public NEEDS a better understanding of these people. I wish you the best of luck!
I have aids

I didn't like how the default for the questions was that you were hacking without permission. Hacking is NOT breaking into systems without permission. There are Black-hats but their activities shouldn't define the default of us all.
Could have more options at times. Also few people that are a member of a hacking collective will say that. You might get a number of false positives of script kiddies pretending to be Anon, Lolsec and lizzardsquad.
I support some actions and will devote time to assist. I.e. Running scripts to identify Isis twitter accounts for further action. I also report shitposts and spam to improve the community.

9.1.1.2 Pilot Thread Response

These are the replies to a thread that was posted in a subreddit, asking volunteers to complete the pilot survey, with a link to the questionnaire. The points have been left in to show the (un)popularity of comments (each comment starts with a default 1 point).

Reply1 - 6 points: so then show us some evidence that you are actually a pHd student.

Researcher - 0 points: http://imgur.com/YczTBdl [Link to photo of university student ID with all personal information blocked out]

Reply2 - 2 points: Answering this seems mighty incriminating...

Researcher - 0 points: It's entirely anonymous, it doesn't ask for or record any identifying information.

Reply2 - 2 points: Geographic location, educational history, ethnicity and age help create a profile. Then the survey asks things like 'do you belong to a hacker collective' and 'have you ever hacked a website'.

Tying information like this to an IP address (which I believe Google log to help prevent duplicate entries) could lead to a very unhappy survey taker.

I don't want to sound overly critical but if you are doing a PhD and do require this information, reword your survey. Remember who your target audience is and adapt and adjust accordingly.

Reply3 - 3 points: Or you know... just use tor to answer...

Reply4 - 1 point: that and its a google survey.. The whole thing is 100% not anonymous lol.

Researcher - 0 points: That is a fair point - like I said this is a starting point, I'm trying to build a picture. If this approach is completely insufficient/impractical, then I'll find another way.

However the questions you highlighted - one does not require an answer and the other has "I don't know" as an option.

With the IP address, I had only found statements that they were not captured on the Google forms. Can I ask where your information is from? It's possible that I'm out of date.

Reply5 - 2 points: Nice try...

Reply6 - 1 point: Ask a high suspicious group to dox themselves. What result was expected?

Reply7 - 2 points: Why are there so many so-called "students" asking for surveys on this sub? Seems legit

Reply4 - 1 point: what's in it for me?

Researcher - 1 point: Right this second? Nothing. In the future? Who knows. Maybe a better understanding of a subculture you are a part of, less hysterical media coverage, more sensible legislation...the possibilities...

Reply8 - 1 point: Makes sense.

9.1.2 Participant Observation Ethical Approval

Bournemouth University

Research Ethics Checklist

About Your Checklist	
Reference Id	12516
Status	Approved
Date Approved	06/07/2016 08:48:19
Date Submitted	05/07/2016 16:31:54

Researcher Details	
Name	Helen Thackray
Faculty	Faculty of Science & Technology
Status	Postgraduate Research (MRes, MPhil, PhD, DProf, EngD, EdD)
Course	Postgraduate Research - FST
Have you received external funding to support this research project?	No

Project Details	
Title	Anonymous Online Hacking
End Date of Project	31/08/2017
Proposed Start Date of Data Collection	03/08/2016
Supervisor	John McAlaney
Summary - no more than 500 words (including detail on background methodology, sample, outcomes, etc.)	
See attached document.	

External Ethics Review	
Does your research require external review through the NHS National Research Ethics Service (NRES) or through another external Ethics Committee?	No

Research Literature	
Is your research solely literature based?	No

Human Participants	
Does your research specifically involve participants who are considered vulnerable (i.e. children, those with cognitive impairment, those in unequal relationships—such as your own students, prison inmates, etc.)?	No
Is a DBS check check required?	

Printed On 12/09/2018 18:41:14

9.1.3 Study 1 - Survey Ethical Approval

Bournemouth University

Research Ethics Checklist

About Your Checklist	
Reference Id	12275
Status	Approved
Date Approved	01/06/2016 08:43:59
Date Submitted	30/05/2016 09:59:21

Researcher Details	
Name	Helen Thackray
Faculty	Faculty of Science & Technology
Status	Postgraduate Research (MRes, MPhil, PhD, DProf, EngD, EdD)
Course	Postgraduate Research - FST
Have you received external funding to support this research project?	No

Project Details	
Title	Anonymous Online Hacking
End Date of Project	21/09/2018
Proposed Start Date of Data Collection	29/05/2016
Supervisor	John McAlaney

Summary - no more than 500 words (including detail on background methodology, sample, outcomes, etc.)

The proliferation of cyber-attacks have been attributed or claimed by anonymous online groups. The influence of the group processes, including the role of group cohesion, group conflict and self-identity, is an area that has not been explored. The influence of the group is predicted by social psychological theory, and this research will contribute to this area through studying the processes of these groups, and why individuals join them. An attempt to recruit participants for questionnaires will be made via community board/sharing websites identified from preliminary research. The websites include forums such as Defcon, Reddit, Whyweprotest, Crack Hack, Sinister.ly, and Hackthissite, as these sites discuss hacking and hacktivism from differing perspectives. Whyweprotest is different in that it overtly states that the group does not "support, condone or endorse any illegal activities. If you, as a visitor, have come to WhyWeProtest seeking out such activities (eg: hacking, DDOS, violence, etc.) then you have come to the wrong place." (WWP.com). There are however veteran and new members of Anonymous (the online hacking collective) on the site, meaning that there is some valuable information available. Online surveys will be used to collect data from voluntary participants. Participants' responses will be treated with full confidentiality and the online questionnaires will be completely anonymous. The questionnaires will not ask for any personally identifying information. The posts on the community boards/websites will be in the appropriate format for each website. These posts will provide the project information and a link to the online anonymous questionnaire. Given the general suspicion of Google and its services in relation to personal privacy, a downloadable copy of the questionnaire will be made available. Links to websites that offer temporary email address will be made, to encourage anonymous submission of the survey. The completion and submission of the questionnaire will be taken as consent. Participants will be given the option to provide contact details if they wish to be involved further with the study. A further ethics application will be made for the interviews if this method is successful in recruiting participants. Any personally identifying information will be given voluntarily and will not be used at any point in the study and will be kept entirely confidential. These questionnaires will help investigations into how people feel about their hacking related activities and the groups. It will also offer an insight into the factors that lead to the individual adopting the group identity and facilitate the analysis of the effects (to the individual and the group, online and offline) from assuming that identity. There will be questions about the perspective of the individual on group identity and processes, and their understanding of the risks involved in joining these groups. The findings of this study will allow this project to develop methods of informing individuals on the risks and consequences of being involved in online anonymous communities.

9.1.3.1 Study 1 – Survey 1 Participant Information and Questions

Participant information: This is a very short online questionnaire on hacking. There are 8 questions and it should take approx. 2 minutes.

About the study: This questionnaire is part of a doctoral study investigating group process and identity in anonymous online communities related to hacking. This study has been reviewed and

approved in line with the University's Research Ethics Code of Practice. The data gathered from this questionnaire will be solely used for academic research.

About the questionnaire: The questionnaire is hosted by Qualtrics.com. The website will record IP addresses but no other information. No identifying information is required or requested. The questionnaire contains a combination of questions and statements. It should take approximately 2 minutes to complete. Submission of the questionnaire will constitute consent, allowing the data given to be used in the study. Please note that in order to withdraw at any time you only need to close the browser page, however, once you have completed and submitted the questionnaire we are not able to remove your anonymised responses from the study. All information will be kept strictly confidential. This questionnaire is entirely anonymous, no identifying data is collected. All data relating to this study will be kept for the duration of this project, until December 2018. Only people aged 16 years and above should complete this questionnaire.

About the researcher: I am a PhD student at Bournemouth University (UK). I have attended various hacking conventions including DEFCON24. I am posting this call for participants across different online forums. My personal stance on hacking is neutral, I support organisations that want to keep the internet neutral (e.g. no mass surveillance, protect free speech, right to privacy and anonymity). In my work I argue that hackers are not the same as cybercriminals, but my focus is on group processes online and identity. If you have any questions or would like further information on this study, please email socscisur@tutanota.com. Thank you.

Q1 - Please state your age:

Please indicate your gender:

- (•) Male
- ( ) Female
- ( ) Transgender
- ( ) Other

Q3

Please answer the following statements:

I am a member of a community or forum related to hacking	Yes	No	Prefer not to say
I am a member of a community or forum related to cracking	Yes	No	Prefer not to say

I am a member of a community or forum related to coding	Yes	No	Prefer not to say
I am a member of a community or forum related to information security	Yes	No	Prefer not to say
The forum or community was recommended to me by an offline connection	Yes	No	Prefer not to say
I tell friends and family I am a part of this community or forum	Yes	No	Prefer not to say
I consider myself a hacker	Yes	No	Prefer not to say

Display Q4 if: I consider myself a hacker - Yes Is Selected

Q4 Please select the most applicable statements:

- ☐ I consider myself a White-hat hacker
- ☐ I consider myself a Black-hat hacker
- ☐ I consider myself a Grey-hat hacker
- ☐ I consider myself a cracker
- ☐ I consider myself a script kiddie
- ☐ I consider myself an elite hacker
- ☐ I consider myself a cyberpunk
- ☐ I consider myself a hacktivist
- ☐ I disagree with these categories
- ☐ Other

Q5 Please state how many years you have been an active member:

Q6 Please indicate how you feel about the following statements on privacy:

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Privacy is an important feature of the internet	○	○	○	○	○
Privacy on the internet should be protected	○	○	○	○	○
I take precautions online to protect my privacy	○	○	○	○	○

Q7 Please indicate how you feel about the following statements on anonymity:

	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Anonymity is an important feature of the internet	○	○	○	○	○
Anonymity on the internet should be protected at all costs	○	○	○	○	○
I take precautions online to protect my anonymity	○	○	○	○	○

Q8 Please indicate how you feel about the following statements:

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Online security should take priority over personal privacy	○	○	○	○	○
I try and find flaws and weaknesses in others' systems/software	○	○	○	○	○
Weaknesses and flaws should be exposed in systems/software	○	○	○	○	○

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Weaknesses and flaws should be exploited in systems/software	○	○	○	○	○

9.1.4 Study 2 - Interviews Ethical Approval

Bournemouth University

Research Ethics Checklist

About Your Checklist	
Reference Id	14569
Status	Approved
Date Approved	08/03/2017 17:16:55
Date Submitted	30/01/2017 10:12:16

Researcher Details	
Name	Helen Thackray
Faculty	Faculty of Science & Technology
Status	Postgraduate Research (MRes, MPhil, PhD, DProf, EngD, EdD)
Course	Postgraduate Research - FST
Have you received external funding to support this research project?	No

Project Details	
Title	Hackers gonna hack - Interviews
End Date of Project	30/06/2018
Proposed Start Date of Data Collection	13/02/2017
Original Supervisor	John McAlaney
Approver	Research Ethics Panel
Summary - no more than 500 words (including detail on background methodology, sample, outcomes, etc.)	
See attached document	

External Ethics Review	
Does your research require external review through the NHS National Research Ethics Service (NRES) or through another external Ethics Committee?	No

Research Literature	
Is your research solely literature based?	No

Human Participants	
Does your research specifically involve participants who are considered vulnerable (i.e. children, those with cognitive impairment, those in unequal relationships—such as your own students, prison inmates, etc.)?	No

Printed On 12/09/2018 18:41:23

9.1.4.1 Study 2 - Interviews Participant Information and Set Questions

Participant Information Sheet

Project: Investigating the effect of group processes and social identities within online hacking communities.

You are invited to take part in a research project. Before you decide whether to participate it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. If there is something that is not clear or you would like more information please ask.

This research is being carried out by Helen Thackray, a PhD candidate, supervised by Dr John McAlaney, Senior Lecturer. This research is funded by Bournemouth University, UK. The central aim of this research is to investigate how group processes and social identity within online hacking communities affect the members at individual and group levels. It is believed that by identifying significant elements of the group process within hacking communities, this research could lead to positive developments for both global cybersecurity and those who identify as hackers. The findings of this study will aid future policy decisions regarding the development of a global legal structure for the internet, as well as the ways in which online collectives are treated and cyberattacks are dealt.

You are recruited on an entirely voluntary basis. You are being approached because of your interaction with the researcher, as well as recognition of your experience and position in these communities. There is no obligation to participate.

You will be asked to verbally confirm at the beginning of the interview that you have understood the participant agreement statements and again at the end of the interview, to confirm that you are happy for the information you have provided to be included in the study. During the interview you may withdraw at any time; as no identifying data is collected, the interview is entirely anonymous but once completed the data cannot be withdrawn. Should you wish to withdraw you do not have to give a reason.

This is for an unrepeated individual interview. The interviews are semi structured and should take between 30-90 minutes. These will be conducted via your medium of choice (e.g. Skype or alternative, IRC, instant messenger). You will be expected to answer questions, although thoughts on the topic that are not covered by the questions are welcome. If there is a question you do not wish to answer please say.

It will not be possible to be identified or identifiable in the outputs that result from the research. The interviews will be conducted and recorded (either voice recording or text file, as agreed) on a newly formatted computer. The audio and written recordings made during this research will be used only for analysis and the transcription of the recording(s) for illustration in conference presentations and lectures. No other use will be made of them without written permission, and no one outside the project will be allowed access to the original recordings. Only files related to the study will be stored, with security measures. All information collected during the course of the research will be kept in accordance with the Data Protection Act 1998. You will not be able to be identified in any reports or publications. Completely anonymised data relating to this study will be kept for 5 years on a BU password protected secure network.

Any concerns about the study should be directed to Helen Thackray (hthackray@bournemouth.ac.uk). If your concerns are not answered, you should contact Professor Tiantian Zhang, Deputy Dean for Research and Professional Practice at the Faculty of Science and Technology, Bournemouth University via email to: researchgovernance@bournemouth.ac.uk.

Participant Consent Statement

You will be asked to confirm that you have read and understood this statement and that you consent to the interview being used in this study.

- I have read and understood the participant information sheet for the above research project.
- I confirm that I have had the opportunity to ask questions.
- I understand that my participation is voluntary.
- I understand that I am free to withdraw up to the point of anonymisation when the data are processed and become anonymous, so my identity cannot be determined.
- During the interview, I am free to withdraw without giving reason and without there being any negative consequences.
- Should I not wish to answer any particular question(s), I am free to decline.
- I give permission for members of the research team to have access to the anonymised responses.
- I understand taking part in the research will include being recorded (audio) but that these recordings will be deleted once transcribed.
- I agree to take part in the above research project.

9.1.5 Study 3 - Survey Ethical Approval

Bournemouth University

Research Ethics Checklist

About Your Checklist	
Reference Id	13777
Status	Approved
Date Approved	17/01/2017 11:58:51
Date Submitted	01/12/2016 16:49:05

Researcher Details	
Name	Helen Thackray
Faculty	Faculty of Science & Technology
Status	Postgraduate Research (MRes, MPhil, PhD, DProf, EngD, EdD)
Course	Postgraduate Research - FST
Have you received external funding to support this research project?	No

Project Details	
Title	Hackers gonna hack - Qualtrics Survey
End Date of Project	21/09/2018
Proposed Start Date of Data Collection	05/12/2016
Original Supervisor	John McAlaney
Approver	Research Ethics Panel

Summary - no more than 500 words (including detail on background methodology, sample, outcomes, etc.)

Hacking is a long established element of the internet; in existence for as long as computers. This project aims to bring together key concepts and arguments with regard to the hackers, their role in the cyber world, and identify potential areas of investigation for the future. It is only relatively recently that the importance of psychology has been acknowledged when investigating the cyber world; there is a strong possibility that the role of online communities has been overlooked. The influence of the group processes, including the role of group cohesion, group conflict and self-identity, is an area that has not been explored. The influence of the group is predicted by social psychological theory, and this research will contribute to this area through studying the processes of these groups, and why individuals join them. Online surveys will be used to collect data from voluntary participants. Participants' responses will be treated with full confidentiality and the online questionnaires will be completely anonymous. The questionnaires will not ask for any personally identifying information. The posts on the community boards/websites will provide the project information and a link to the online anonymous questionnaire where the project information will be repeated.The questionnaire will be hosted on Qualtrics, the research company used by the Psychology Department. An individual account has been set up. This company recognises the data as the property of the account holder and does not record information from those who are completing the surveys. Participants will be informed that completion and submission of the questionnaire will be taken as consent. There will be no personally identifying information requested. If any is submitted by participants it will be removed. These surveys will include questions and use of the Likert scale to examine how participants view their hacking related activities and the group identities. It is hoped this will offer an insight into the factors that lead to the individual adopting the group identity and facilitate the analysis of the effects (to the individual and the group, online and offline) from assuming that identity. There will be questions about the perspective of the individual on group identity and processes, and their understanding of the risks involved in joining these groups. The findings of this study will allow this project to develop further methods and questions. Once there have been sufficient submissions on the first set of questions, these will be reviewed and updated using the information gained. Participants will be asked to complete it again, via websites and forums.

Printed On 12/09/2018 18:41:19

9.1.5.1 Study 3 – Survey 2 Participant Information and Questions

This is a short online questionnaire on hacking related communities. There are 21 questions and it should take approx. 5 minutes to complete.

This questionnaire is part of a doctoral study investigating group process and identity in anonymous online communities related to hacking. This study has been reviewed and approved in line with the Bournemouth University's Research Ethics Code of Practice. The data gathered from this questionnaire will be solely used for academic research.

The questionnaire is hosted by Qualtrics.com. The website will record IP addresses but no other information. No identifying information is required or requested.

The questionnaire contains a combination of questions and statements. Submission of the questionnaire will constitute consent, allowing the data given to be used in the study. Please note that in order to withdraw at any time you only need to close the browser page, however, once you have completed and submitted the questionnaire we are not able to remove anonymised responses from the study.

All information will be kept strictly confidential. This questionnaire is entirely anonymous, no identifying data is collected. All data relating to this study will be kept for the duration of this project, until December 2018, and then archived for 5 years on secure BU servers. Only people aged 16 years and above should complete this questionnaire.

If you have any questions or would like further information on this study, please email socscisur@tutanota.com. Thank you.

Q1 Please indicate your age group:

- 16-25
- 26-35
- 36-45
- 46-55
- 56-65
- 66+

Q2 Please indicate your gender:

- Male
- Female
- Transgender
- Other

Q5 Please state how many years you have been involved in hacking related communities:

Q4 Please select the most applicable statements:

- [ ] I consider myself a White-hat hacker
- [ ] I consider myself a Black-hat hacker
- [ ] I consider myself a Grey-hat hacker
- [ ] I consider myself a cracker
- [ ] I consider myself a script kiddie
- [ ] I consider myself an elite hacker
- [ ] I consider myself a cyberpunk
- [ ] I consider myself a hacktivist
- [ ] I am involved in InfoSec
- [ ] I disagree with these categories
- [ ] Other

Display This Question if: I consider myself a White / Black / Grey-hat hacker Is Selected

Q14 If you answered that you consider yourself a Black, Grey, or White-hat hacker, please indicate where you would place yourself on this scale.
Black-hat indicates that you only engage in illegal/unethical hacking.
White-hat indicates that you only engage in legal/ethical hacking.

	Black-hat	Grey-hat	White-hat
Personal position on scale	0----------100		

Q9 The next section will ask you to rate statements on the following criteria:
Genuine - how sincere (high) you believe the statement or request to be.
Trustworthy - how honest (high) you believe the statement or request to be.
Author's integrity - how moral or ethical (high) you feel the statement or request is.
Your personal response - if you feel positive (high) or negative (low) about the statement.

Statements are based on comments from interviews on hacking or popular or unpopular comments

posted on various hacking related forums. Some have been modified for the purpose of data collection.

Q8 Please rate this statement:
"Open source doesnt mean you can ask the author for anything and hes obliged to deliver if you cant read/write source code thats not my problem"

	Low	High
Genuine	0	100
Trustworthy	0	100
Author's Integrity	0	100
Personal response	0	100

Q10 Any further comments on this statement?

Q7 Please rate this statement:
"have no clue how to hack or anything about it so can someone give me a step by step tutorial on how to get an instagram password tryna see booty pics and crap they post on it"

	Low	High
Genuine	0	100
Trustworthy	0	100
Author's Integrity	0	100
Personal response	0	100

Q11 Any further comments on this statement?

Q12 Please rate this statement:
"I'm quite comfortable with dissecting network protocols, xss, sql injection, and etc. but I've never been able to do the low level stuff like buffer overflows, or reverse engineering assembly. Where is a good place to start with this type of hacking? What are some good resources on these specific kinds of hacking?"

	Low	High
Genuine	0	100

	Low	High
Trustworthy	0----------	----------100
Author's Integrity	0----------	----------100
Personal response	0----------	----------100

Q13 Any further comments on this statement?

Q16 Please rate this statement:
"If you are working for a government you are told what to do therefore how can you truly be a hacker."

	Low	High
Genuine	0----------	----------100
Trustworthy	0----------	----------100
Author's Integrity	0----------	----------100
Personal response	0----------	----------100

Q17 Any further comments on this statement?

Q18 Please rate this statement:
"Everyone started as a beginner, no one can say "I'm a hacker and you're not" - it's about self-definition."

	Low	High
Genuine	0----------	----------100
Trustworthy	0----------	----------100
Author's Integrity	0----------	----------100
Personal response	0----------	----------100

Q19 Any further comments on this statement?

Q20 Please rate this statement:
"What makes me a hacker is not necessarily a skill set but a mentality – I want to understand something, how it works, not the limitations"

	Low	High
Genuine	0----------	----------100
Trustworthy	0----------	----------100
Author's Integrity	0----------	----------100
Personal response	0----------	----------100

Q22 Any further comments on this statement?

Q15 Please rate the following "hacker" traits in order of importance:
(1 = most important, 6 = least important)

Curiosity/Desire for knowledge

Technical ability (e.g. coding)

Passion

Creativity

Mentality (e.g. the hacker mindset)

Other

Q23 What was your reason for participating in this survey?

Q25 Do you have any further comments on this survey?

9.1.5.1.1 All Other submissions for Q15 were:

Ability to learn.
ability to tightrope walk
Autism
drugs
ethic
Free Time
Friends/Community

High openness and conscientiousness
Listening
Motivation
Not being an asshole
[Traits] One and two feed into three, four is a given by this point and five is really a combination that comes naturally if you truly embody the other traits.
Panglossian attitude to problem solving
Perseverance "Try Harder"
Perseverance in the face of obstacles
Persistance.
Physical fitness
Sharing knowledge
Social Graces
Social Skills
Some of these overlap
The only thing that matters is taking action and doing things

9.2 Hacker Ethic Examples

9.2.1 The Hacker's Manifesto

By The Mentor (Loyd Blankenship) - January, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...

Or feels threatened by me...

Or thinks I'm a smart ass...

Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

9.2.2 How To Become A Hacker: What is a hacker? (Raymond, 2001)

Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker.

The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music — actually, you can find it

at the highest levels of any science or art. Software hackers recognize these kindred spirits elsewhere and may call them ‘hackers’ too — and some claim that the hacker nature is really independent of the particular medium the hacker works in. But in the rest of this document we will focus on the skills and attitudes of software hackers, and the traditions of the shared culture that originated the term ‘hacker’.

There is another group of people who loudly call themselves hackers, but aren't. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. Real hackers call these people ‘crackers’ and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word ‘hacker’ to describe crackers; this irritates real hackers no end.

The basic difference is this: hackers build things, crackers break them.

If you want to be a hacker, keep reading. If you want to be a cracker, go read the alt.2600 newsgroup and get ready to do five to ten in the slammer after finding out you aren't as smart as you think you are. And that's all I'm going to say about crackers.

9.3 Forum Discussions

The following discussions were copied from relevant threads on various forums related to hacking. All usernames have been changed. Spelling and typing mistakes have not been corrected unless it impeded comprehension, in which case the correction is presented in square brackets.

9.3.1 What is your opinion on Anonymous?

Retrieved 4/11/15 via Tor Browser. Approximate date of original conversation mid-June 2014.

Jupiter: I am going to post an IRC chat log for you to read where I state my opinion. I am Jupiter. We are referencing a thread on 4Chan where Nazism was supported in the name of Anonymous. Or "AnonymouSS" as their sect is called.

<Jupiter> I'm pretty sure it's Nazism.

<Editor> yea, i mean this is not good for us.

<Editor> they are sending wrong messages to people

<Jupiter> Well Anonymous is dead anyways..

<Jupiter> But still

<Jupiter> Why beat a dead horse?

<Editor> why did you say so?

<Jupiter> It's sad.. The one group who actually tried to do good for us and people have to make it look like shit..

<Editor> well you know, there are some things that happened bad. We all have to accept that. But Anonymous is a beginning of new world, a revolution. it won't be dead. it will rise again

<Jupiter> Ooooh. I know what happened. Anonymous used to be for freedom. Then they attacked Pedophiles (the majority of 4Chan). So now 4Chan is trying to trash their name.

<Jupiter> name*

<Editor> well they won't get anything.

<Editor> what people did, was for the good

<Jupiter> They just need to fuck off IMO.

<Jupiter> Why sacrifice future possibilities of doing good in the name of doing one good thing.

<Jupiter> ?

<Jupiter> Fuck.

<Jupiter> ?*

<Editor> you are right, but we don't know what lies in the future. So it is better to fight in the present.

<Jupiter> No it's not. It's not good to fight people that aren't even bad. And trash your reputation as well.

<Editor> the biggest misconception about anonymous is that it is the solution to everything. It is not.

<Editor> but we have to fight at many different things

<Jupiter> What? I never said it was? Dude I've known about Anonymous for a few years now and have followed them. I was around when Par:AnoIA was in business and AnonyOps existed instead of AnonOps. They actually fought for worthy causes. Not indi[vi]dual gray moral breaches.

<Jupiter> Why are we/they/w.e. preoccupied with CP instead of fighting for net neutrality and freedom? Guess what? Now everyone is caught up in this neonazism and CP and no one cares about the rest? Anonymous is dead. We lost. The end. It was a fun ride that I never got to really get on.

<Jupiter> Fucking people had to post shit on Facebook and YouTube and that's what caused this.

<Editor> well i think you are right, FBI can take care of CP. we have to work on our real aim.

<Jupiter> It's too late..

<Jupiter> Half of Anonymous or more is FBI/NSA/CIA CoIntelPro.

<Jupiter> FFS I could be, you could be.

<Jupiter> There's no trust.

<Jupiter> You actually think that this PUBLIC IRC server is any sort of HQ?

<Editor> yea i think you are pointing to Sabu. well that was a shock. Jeremy is in jail.

<Editor> no i don't think it is any sort of HQ. But being anonymous how can we communicate with everyone.

<Jupiter> And you know what? 99.99% of the people here, including myself, can't do shit hacking-wise. We're all just here because we think we're cool and "i r leejun". I'm not. I actually wanted to make a change and learn and do something, but that part of me is gone after seeing the condition of things. Now all this place is is a monitored chat room.

<Editor> i mean the whole structure of anonymous without leadership has some pros and cons. Do you have some suggestions? don't complain. find a solution.

<Jupiter> There's no solution. The feds own everything. EVERYTHING. You can't even trust your own hardware now.

<Jupiter> I don't have the knowledge to invent something either.

<Editor> you can suggest some ideas.

<Jupiter> I know we'd need a closed network of course. But that's impossible without trust. And there can't be trust when 600 million+ people know about the group. And you can't get the word out without letting everyone know.

<Jupiter> Do you understand me though?

<Editor> so you are talking about setting a network in deep web. but people who are not techsavy, how are they going to access. the power of anonymous is in the strength of people. that's why we are strong.

<Jupiter> You don't understand. This is a group labeled TERRORIST. With its being online there has to be high security. It cannot be public. You shouldn't be here if you're not tech-savvy. I shouldn't be here. That's why there were underground sects of Anonymous.

<Jupiter> The business needs to be done any from prying eyes is my point.

<Jupiter> It needs to be hidden.

<Jupiter> Those Anons who are not tech-savvy should be wearing masks and protesting and voting and making change.

<Jupiter> They shouldn't be trying to spice-up their image by looking like a 'cool' hacker.

<Jupiter> And they shouldn't be crying about feminism and CP.

<Jupiter> Yeah CP is a bad thing. Children should not be coerced into that shit. But because of Anonymous' back-story it's something we regretfully have to ignore.

<Editor> i understand, so we can restructure the group. we can make a closed network of hackers for technical operations. and other faction of general public for protest all over the world.

<Editor> and for sometime we will not bother ourselves with CP and other creepy things

<Jupiter> The thing is, if you became an Anon any time after its founding, you're a fraud. You know why? Because you support the bullshit. Anonymous is about freedom and defying the government. Well, that's what it quickly evolved into anyways. It was originally about having fun and trolling

websites and DDoSing bullshit groups like The Church of Scientology. I was too young when it formed.

<Jupiter> Yeah the group needs restructuring. Who is gonna do it? You? Me? I don't know how. Do you? Should we ask one of the feds sitting in #anonops? Maybe we should ask one of the neonazis or the people trying to bring down CP sites.

<Editor> okay Jupiter what exactly are you proposing? Clear it. because brag[g]ing and complaining won't help you, me and anonymous. And anyone can do anything.

<Jupiter> I'm not bragging about anything?

<Jupiter> And you're missing the point. We're beating a dead horse. It's time we move on. Unless you thoroughly no someone in person and you've both developed professional skills in networking and PHP and SQL then I suggest you do nothing. Just wait it out and prepare for something physical in the future.

<Jupiter> know*

<Jupiter> Don't trust strangers.

<Jupiter> Not anymore.

<Jupiter> Things used to be different.

<Editor> okay Jupiter, i will contact some people and we will see what we can do. I am always proud about anonymous that we stand aginst censorship and corrupt people. and it was a very good thing.

<Jupiter> I don't know, man. I just don't know anymore. It's sad and depressing. Maybe one day we'll see it shine again, but don't live on hope.

END

9.3.2 Is happiness a result of choice?

Originally posted 2016.

OP: 1. First of all, what is choice?

2. Is happiness directly related to choice?

3. If 2 is true, does it mean that I and I alone am responsible for my own happiness?

4. If 3 is true, can I be happy no matter what my situation in life is?

5. Finally, if 4 is true, should we refrain from giving to the poor lest they gain a false idea of happiness and come to rely on others for their happiness instead of their own choice.

your thoughts..

Re: Is happiness a result of choice?

Reply1

If you are trying to be philosophical, then consult Mills and Aristotle.

To them, Happiness is the result of an ending, or completion of a purpose. The purpose in their minds is very simple. A fish, swims; a golden retriever, retrieves; and a human, thinks and expands his/her thoughts.

In regards to your questions,

1. what is choice?
-In a basic sense, choice would be your option to do a task that can come to an end. (VERY rough concept, and not that easy)

2. Is happiness directly related to choice?
-Directly if the task comes to an end- then the choice to begin the task caused it; take a dog race for example. "Racing dog, to race." If the dog makes the choice to race, and wins the race, then his/her choice resulted directly in the happiness gained from this end. Indirectly the dog can be forced into the race (he/she has no choice*), and can end up winning, or causing an end to his/her purpose; which leads to happiness.

Ergo, choice is neither directly related or indirectly related to happiness. In essence 'No' is the short answer.

Dogs can experience happiness, but do not necessarily make choices.

3. If for your purposes you believe that 2 is true (which it could be, Do not trust a word that anyone speaks on this matter because no one really knows.), than no, either way I would chose the answer of "No" because the choice of others can make decisions for you and make you come to the 'end' of a purpose. At that end you will experience happiness.

Friend steals a dollar of yours and buys a loto ticket, then gives it to you. You did not make the choice, but if the purpose of buying the loto ticket comes to a complete end (winning), and not a incomplete end (nothing happening), than you would techincally gain happiness from this.

4. Getting away from Mills and Aristotle, I believe that yes, no matter what sitiuation you are in, you can make some happiness come from it. They would disagree and call this pleasure, not happiness.

5. I believe, no we should not refrain from giving to the poor, because some truly do need assistance, some choose to be there by choice, some by the choices of others, and some by misfortune. Mills would say that through utilitarianism the one giving the money, or items, or w/e of your choice, would be the one to gain happiness, while the poor who recieves would only experience pleasure for a short while. However though the concept of money gain to happiness, the purpose of humans to gain money (research shows up to 15,000 dollars then it has no effect on happiness) would cause an increase in happiness as the end of gaining money occurs. So the poor would technically be able to gain happiness as well.

This is merely suggestions of how to interpret this, I mean not to enforce these upon anyone,

Re: Is happiness a result of choice?

Reply1

I mean no offense in my opening statement, merely "choosing" 1 of 2 paths to go, my pure opinion or a philosophical view. Reread it and it sounded a bit forward. My appologies.

Re: Is happiness a result of choice?

Reply2

I think happyness is a state of chemistry in one's brain. I believe that love in a romantic sense is not really love...it is just a state of being high on chemicals in one's brain. I'm not saying i don't like happyness. I love getting high. But still i think Real love is unselfishly sacrificing something for another with no benefit to oneself. For me to make another person happy, even if it causes me pain to do so, is love.

Happiness cannot be confused with purpose and meaning. None of these can be confused with hope. Hope is the knowing that one day things will get better, knowing that one's purpose will be fulfilled. One cannot hope without a purpose, and the purpose must have meaning, and be true.

For us humans to be fulfilled on this earth, we must have a purpose. This purpose must be outside of this world, it cannot be entwined by the reigns of life and death. This purpose can be found by some in a god, for others it can be found by other means. However, the purpose must be real. It must be the truth. If it is not, then it has no meaning. It cannot benefit the individual who strives for it.

Reply1 wrote: If you are trying to be philosophical, then consult Mills and Aristotle.

To them, Happiness is the result of an ending, or completion of a purpose. The purpose in their minds is very simple. A fish, swims; a golden retriever, retrieves; and a human, thinks and expands his/her thoughts.

My Thoughts, which are no better than anybody else's

Reply3:

OP wrote:1. First of all, what is choice?

Choice is the illusion of having multiple paths to follow, when in reality the path you will take is predetermined by the physical properties of your brain.

OP wrote:2. Is happiness directly related to choice?

Although choice does not truly exist, the illusion of choice can cause chemicals in your brain, which can cause happiness, so the concept of choice is related to happiness.

OP wrote:3. If 2 is true, does it mean that I and I alone am responsible for my own happiness?

You are the only person responsible for your happiness, but not the only person who influences it.

OP wrote:4. If 3 is true, can I be happy no matter what my situation in life is?

It is possible to be happy no matter your situation in life.

OP wrote:5. Finally, if 4 is true, should we refrain from giving to the poor lest they gain a false idea of happiness and come to rely on others for their happiness instead of their own choice.

You cannot have a false idea of happiness, because if something makes you happy then it makes you happy. You can believe something will cause you to become happy, and find it does not. However, you cannot at one time think something is making you happy, and, later, think it did not. If it made you happy at one time, then you experienced happiness.

Cesare Pavese wrote:We never remember days, only moments.

Re: Is happiness a result of choice?

Reply4

You have to choose to be happy and then make it happen. YOu can not be happy if you are not going to do anything about it.

Re: Is happiness a result of choice?

Reply5

I want to avoid pushing my spiritual dogma and also nocroing threads But i just wanted to jump in and say that while completely ignoring all rationality to the contrary, I fully beleive that you can simply choose to be happy. When people harp on about something negative for a long enough period of time, I often make the aknowledgement that, that person on some level, as much as they deny it, enjoys being miserable.

Re: Is happiness a result of choice?

Reply6

1. Choice to me, is simply the action you decide to take, simple enough. Although, I imagine some people could be much more philosophical on this topic

2. While happiness isn't related to choice, it is a choice to be happy. People living in the worst situations can be happy by looking at the world through a glass half full type of perspective. That choice of how to view the world around you can be harder for some due to chemical imbalances in the brain causing depression. Nonetheless, it is a choice

3. At the very core of it, yes you are responsible for your own happiness. You can decide how to view the world

4. yes, I've seen homeless people who are the happiest they could be and are thrilled with life. They radiate happiness and share joy. It is incredible

5. no, It is always better to help the poor. While happiness does not completely rely on your financial status, having less stresses in life through sufficient amounts of money help make that path to

happiness easier.

That is my opinion

Re: Is happiness a result of choice?

Reply7

Everyone is the architect of their own happiness. So our hapiness is directly related to our choices and actions.
If you feel unhappy - try to change your life. Any excuses are ridiculous. You can start from small things and alter life for the better.

END

9.3.3 What is your opinion on Anonymous?

Retrieved 4/11/15 via Tor Browser. Approximate date of original conversation mid-August 2014.

Anon3: Anyone can be Anonymous by simply deciding to be, so technically it can't "die", though the name has certainly been stained. They were mislead into focusing on trivial issues (in comparison) and even doing the government's job. However, for those of us who remember the real Anonymous, it will always be a cherished symbol of justice. I am waiting for when they rise again, once they set their priorities straight. If they educate themselves properly, they should be able to prevent the same from happening.

Anon4: According to Anonymous, EVERYONE is a member of Anonymous, whether they do anything/like Anonymous or not. I'm sure there are some neo-nazi anons.

Anon2: Anonymous is a CIA front. Maybe not from the beginning but it is now.

Anon1: I like one type of anonymous and I dislike another type of anonymous,I like the anonymous that fights for justice and human rights,and I dislike those type of anonymous that steal music and give it free in the internet or make pirate games of idea without permission with the dumb excuse "knowledge is free" or "the ideas of a person belong to society".

Anon5: Knowledge and data should be free. Services however, belong in the market.

Anon1: Anon5, exactly.

Anon6: Something new needs to come up in the place of Anonymous. The name has been tainted, and therefore in the oppinion of the public, any and all actions taken by someone calling themselves Anonymous have been tainted as well. This is something important. They used to do good work. Now they have been co[-]opted. Instead of waiting for Anonymous to rise again, why not take where they left off and proceed in a different manner that is more focused on the main goal of information freedom?

Anon7: If I may make a proposal: If Anonymous IS to live on, it needs to be reformed. Like it was mentioned somewhere in the above posts, if the reform is to take place, it needs to be a secret. Ive been wanting to do this reform for quite some time now. Im not proposing doing such a thing here at the I.E, but it needs to happen on a darknet, wether it be Tor or Freenet or an i2p like network.

That might help at keeping a level of secrecy AND keeping out the people who have ruined Anonymous's name.

Also, if this reform wer[e] to happen, Anonymous would need a new alias, at least until we could get shit re-organized. I dont know what it would be though...

Sorry if this kind of catches anyone off guard, or if anyone finds it off topic. Im just trying to make this shit happen. I want it to happen, not just a bunch of people sitting around in IRC and discussing it.

Anon6: @Anon7: What do you think needs to be done and how can we do it?

Anon7: @Anon6

Like I said, if Anonymous is to regain its title of being a feared figure, the first thing would be to root out all of the 12 year old who think they are 1337 because the can DoS someone, and i have a feeling that a good portion of the Anonymous we know today consists of those 12 year olds...

If we could find some of the anons that have been around since at least the Scientology days, maybe we could convince them to help re-organize things...

Also, Anonymous would need to gain support. I think the only way they could actually get anyones attention ATM would be to do something good for net-neutrality, or maybe do something relating to the whole internet fast-lane B.S...I dont know...

Anon6: How many of the original Anons do you think are left. I would imagine a large amount of the first guard would have moved on to other things to stay out of the spotlight, are in jail or have been coopted by the feds.

I do hope that something can be re-built, but like I said in another post, I think it needs to be something under a different name with a better focused philosphy. There is a reason that saying that everyone is Anonymous, even if they never say they are, didn't work. If you open up your structue, sure you become impossilbe to take down in a sense, but you also make it damn hard to operate. There has to be a happy middle ground between completely centralized and vulnurable and completely decentralized and impotent.

I wonder what the middle ground is.

Anon7: @Anon6

Unfortunatly, I think your right about the origional Anons...

I too hope greatly that something else will rise, or Anonymous really gets their shit together and turns things around. As for a middle ground, you would think that the members that are the most involved would have the most influence on the others. Maybe thats the way Anonymous should operate.

Anon8: Anonymous is dead because of edgy 13 years old kids and popularity. Alot of things other than Anonymous died from popularity. Internet and the Internet culture is dead because of popularity. Before that, Internet was full of prodigious, introvert hackers, nerds and scientists.

At the time of the creation of Internet, it was mostly scientific, and most of people attracted by it were those kind of people. Now internet is commercial and for entertainments. It's full of lazy, immature idiots who don't have a clue about how their computer works and don't care that their

constantly being spied on from everywhere. They keep using their popular services, trying to belong to everything because it's cool.

Not a misogynist or anything but i remarked that where there are women and "girl gamers", there is pollution, there are kids and teens, there is shitty unfunny immature content.

Sorry for bad english or if what i say is stupid.. It's my vision of things..

Anon7: @Anon8

I wouldnt say the culture is COMPETELY dead... at least, not in places like here. Now Anonymous? they might as well be.

Anon9: I think Anonymous's image has been destroyed, you can find all type of people in Youtube claiming to be a member and the worst thing is that it's hard to know who are real members and who are not,the real members should do something to stop that problem.

Anon5: The previous genius culture got crowded out by the entertainment culture, think of it like bacteria.

Anon9: What I wonder is if someday Anonymous will rise again?

Anon6: @Anon9: Like I said in a previous comment on this thread, there should come something more co[h]esive than the old Anon. It is time for a complete rethink of the concept. Anything that could be seen as a new rising of Anonymous should be something other than anonymous. The first problem is the videos you talked about in your other comment. The involvment of the group should be seen through the actions that were taken, not some anouncement video on a popular service like some kind of terrorist organization releasing a beheading video. Those videos can be refuted easily. What can't be refuted that easily is the clear concequences of an action taken. Also, to feighn involovement in that kind of system would require something to actually be done, so there wouldn't be a bunch of script kiddies and wanna be "haxors" claiming false membership in somehing they have no way of understanding.

Something new guys. That is what is needed. Time for a new guard to take up position.

Anon9: @Anon6, your right in that opinion. What if we made our own organization?

Anon6: @Anon9: well, we as humans didn't go to the moon by talking the spaceship into taking off. So, all we need to do is actually take actions. As was said before, anyone who does take action would need organize and operate in secret.

Anon9: The error of Anonymous was to make theirselfs popular, and your right about action.

Anon11: Nothing under the sun is new, we face the same evil that the one's before us faced, just through different mean's. Let me share a parable with you. A wise woman who was traveling in the mountains found a precious stone in a stream. The next day she met another traveler who was hungry, and the wise woman opened her bag to share her food. The hungry traveler saw the precious stone and asked the woman to give it to him. She did so without hesitation. The traveler left, rejoicing in his good fortune. He knew the stone was worth enough to give him security for a lifetime.

But, a few days later, he came back to return the stone to the wise woman.

"I've been thinking," he said. "I know how valuable this stone is, but I give it back in the hope that you can give me something even more precious. Give me what you have within you that enabled you to give me this stone."

Sometimes it's not the wealth you have but, what's inside you that others need. IF we all strive within ourselves to make this world a better place,

then it is inevitable that we WILL affect the world a round us. Anon11 out.

Anon8: The guys who started the #AnonymouSS movement are guys from 4chan.org/pol/. A board called Politically Incorrect. They are not hateful or anything, but they think that Jews control the world. They wanted to "redpill" (reveal the truth, take the redpill=have a revelation, learn the truth) people.

Anon6: @Anon11: I like that parable. I am going to have to use that from now on. You speak truth. But, even with the good in us reflecting out, our reach by those means is limited, by space, by seperation, by our deaths. When thinking about the greater good, you must think even beyond your own release from this world. You must have a reach that can far exceed the feeble influence we have as individuals. Sometimes you have to take that good down inside you and broadcast it on a fucking huge antenna.

Anon1: And that's where ideas come in. They can outlive us all. Just like the original Anonymous showed that we can fight back.

Anon12: LOL @ "Anonymous is a CIA front."

Anon7: @Anon12

It very well could be a CIA front. At least, parts of it may be. Think of the LulzSec situation with Sabu. We wont ever really know if it is or isnt for sure, since "everyone is Anonymous".

Anon13: You don;t understand what anonymous is, just like the news doesn't understand it. Anonymous can;t be a CIA front cause you and I are anonymous.

Anon7: My point exactly. Everyone is Anonymous. Whos to say thats limited to CIA?

Anon4: Well, Anonymous certainly isn't what it used to be, that's for sure.

END

9.3.4 State Sponsored Hackers

From the DEF CON Forums, February 2015.

State sponsored hackers:

Opp1: I have seen the above term being used a lot recently and to me it seems to be an oxymoron. Due to the fact if you are working for a government you are told who to target and what to do therefore how can you truly be a hacker. To me a hacker is someone who goes where the mood takes you you look at things that interest you. You shouldn't be told what to do especially by governments.

Opp2: Different people have different definitions for, "hacker." Often, hackers are described by the work they do and the novel solutions they provide which are often non-standard, but effective, and possible, usually through thoroughly understanding the scope of work in-depth. Disagreements which are about the definition of a word, a word that each side chooses to define differently, in ways that are mutually exclusive to other definitions, can't ever be resolved. Effectively, such arguments are over opinion. Arguments over definition are like trying to resolve which flavor of ice cream is best -- there is no single correct answer, and with people that do not like ice cream or are unable to consume it, an attempt to resolve this is itself a loaded question, unless an acceptable answer from them is "none." I would bet that most attendees of DEF CON would accept that a "hacker" can do good or evil or both, and they can work for government, organized crime, private industry or independently or any mix of these.

Opp1: I would agree that the hacker community is a wide and varied one. But the fact that the press use the term hacker to describe anyone who breaks the law on a computer just angers me. So instead of using the term state sponsored hackers. Why not just say government employees. It just seems like scare tactics.

Opp3: Check out this 1985 documentary called "Hackers: Wizards of the Electronic Age." Vintaged documentaries like these are especially awesome, both to see how far things have come, and how the definition of a "hacker" took on a much more optimistic (naive?) meaning back then. There appears to be a consensus in the security community that the word started taking a much darker tone after the release of the 1983 film "Wargames"--where a young Matthew Broderick "hacked" into an American nuclear defense facility and nearly started WW3.

https://www.youtube.com/watch?v=cVCLowi4v7w

END

9.3.5 Ethical Hacking

Retrieved September 2018. Would you describe yourself as a law abiding or ethical hacker and if so how much?

OP: Hello everyone,

I myself want to be an ethical hacker, although I'm sure we all have weird fantasies and a cantenna would be cool to build and I think if your at a school that tracks you I think we all know how that could potentially be misused. Even on clearnet hacker forums, I know for a fact certain people will admit to being a "Black-hat," "Grey-hat," or "White-hat" hacker. Obviously, some script kiddy anon kid would not care about those labels. I am not yet a hacker, but since most of you hackers and non-hackers don't like the labels mentioned above, looking at individuality, how law-abiding and ethical would you say you are on a scale of 0 to 20, just so I can get a good measurement?

I also know for a fact that the vast majority (maybe not all) of the people who admit to this are telling the truth.

Obviously, no one is asking you to admit to specific crimes and I know you are not all bad people or even bad hackers just because legal does not equal ethical, but it would be nice to have a measurement of both in your view.

So, legal = 0 to 20; same for ethical. thanks

Peace everyone.

Thanks for the info.

Best,

OP

Reply1

Quote: " how law-abiding and ethical would you say you are on a scale of 0 to 20"

I could spend hours pulling this question apart, but the most glaring thing wrong with this question can be summarised by me saying "who defines what's legal, who defines what's ethical?".

As someone who is culturally and racially European, I think premarital sex is legal, and yet, this is highly illegal and punishable by imprisonment in Saudi Arabia, and other countries.

So if I have premarital sex, am I committing a crime or not? Why does the fact I am not in Saudi Arabia mean I am not committing a crime. Surely a legal framework is merely an idea and surely not confined to a geo-spatial point? How the hell does that make any sense?

In a similar (and more relevant) vein, if I live in Russia, and Mr Putin gives me a subtle nudge and a wink to indicate that he won't really care if I hack the West, does this make it ethical? It may actually be illegal under a strict interpretation of Russian law, but the highest authority in the land has just told me it is okay, so does that mean it is okay? If I go ahead and hack the West, does this make me unethical, or Putin? Am I suddenly a criminal? What happens if Putin sends me to a country where hacking is allowed - how come I'm a criminal in one country but not a criminal in another when I've done the same thing?

Let me summarise for you. There is no thing as good, there is no thing as bad. There is just stuff that people do and a collective interpretation of those actions that is strictly relevant to a specific cultural-societal-racial-political dynamic.

My answer is 0, because it all means nothing.

Any answer other than 0 is either too localised and affected by local beliefs to be completely irrelevant to your unique perspective, or is simply hypocritical.

Reply2

Hmm - similar to Reply1, I do not have a straight answer for you. I will say that "ethics are subjective."

Legality is a set of rules that society-at-large agrees on, in a democratic setting. Someone, or a group of people, agree that these rules are the guidelines that society should follow; otherwise, systematic punishment should be enforced.

Ethics is the question of what is right and what is wrong. Just because something is law doesn't mean it is "right", which implies that legality doesn't always equal ethical, just as ethical does not always equal legal.

There are different types of ethics that society generally follows, primarily: deontological (rule-based; do what is right to be a good person in society), teleological (goal-oriented, do what is necessary to reach a goal). and virtue ethics (personal views, more or less). I would say that must hackers fall into the latter category: virtue ethics.

With deontological and teleological ethical views, society's rules are considered when acting; people generally want to follow rules or want to do what is necessary to meet their goals, even if other people view their ethics as unethical. These societal rules, though, who decides them? Well, that depends on what type of society you live in: democratic, communist, socialist, etc. As Reply1 said in their USA vs Saudi Arabia example, laws are different everywhere. To follow laws does not mean that you are truly ethical, just as to be ethical does not mean to be truly law-abiding.

For virtue ethics, we take an individualist approach to ethics. We think for ourselves; we ourselves decide "what is right?" and "what is wrong?" Most hackers take this approach, as they are critical and free thinkers.

With all of that said, while it is important to be law-abiding to avoid prosecution, I believe that ethics are always up for debate, even if the action or goal is not exactly legal. This is why I consider myself to be a "Grey-hat" even though I do not consider myself to be a (cyber)criminal, but most people may call me a "White-hat" just because I generally follow laws; however, I will not allow society's national laws to do what I consider to be unethical. If you work for the NSA, and you want to blow the whistle on an unethical operation, is it ethical to blow the whistle, even if it is illegal? Ask Snowden; I'd say that we can also call him a "Grey-hat" under these definitions.

I'll leave off with a question for you: what revolution or uprising in history was legal? If they were illegal, were they ethical?

Reply1

Reply2 Wrote: If you work for the NSA, and you want to blow the whistle on an unethical operation, is it ethical to blow the whistle, even if it is illegal? Ask Snowden; I'd say that we can also call him a "Grey-hat" under these definitions.

Yes, I'd argue that all White-hats are Grey-hats, if we say that one is only truly a White-hat if they follow a code of ethics 100%, which in this case would come down from an industry body, such as (ISC)^2.

Any White-hat could be faced with a scenario where they have to compromise ethics to do the "right" (by virtue) thing, even under an extreme scenario - say if they were being Blackmailed and

owed lots of money to people who were going to harm his family, so for his next Red Team job he decided to actually steal a bunch of PII and company details to sell on the dark web to pay off his Blackmailers. He's done something highly illegal, absolutely unethical according to the industry standards in the extreme... And yet, he may think he did the right thing?

Reply2 Wrote: I'll leave off with a question for you: what revolution or uprising in history was legal? If they were illegal, were they ethical?

Viva la resistance!

A good example here is the Bolshevik Revolution. Yes, they successfully took over the Government relatively peacefully - they took the Tsar and his family and hid them in a shack, meanwhile assumed power. Then they had a decision to make: what to do with the family long-term?

To let them live would leave open the possability of escape, where they could easily rally forces to try take back the country, inevitably leading to armed conflict and loss of human life - how is that a good thing?

To keep his family, including his young son and wife, under guard their entire life would be unfair. Surely better to die than live like that? And surely there would be attempts to rescue them - it would be a massive mission simply to keep their location secret. Again, if they escape, it will almost certainly lead to more loss of life.

So they decided to murder them all.

Legally murder. Ethically suspect? They did what they thought was right. Others thought they were wrong.

There is no objective framework for measuring ethics, just like there are no universal standards for making people accountable to the law, they differ by place, culture, time, etc.

The first step in being truly awake in this world is to realise that laws and ethics do not exist anywhere except inside yourself. It turns out that you can do whatever you want in this life without any consequences, but other people may think you did something wrong. If those people are your family or friends, do you really want to live your life without their love?

Reply3

Ignoring the silly post-modernist and nihilist views expressed in this thread. I think it is safe to say that there are some things that are universally good.

Let's take murder for example. Murder is bad, why? Because i don't want to be murdered. Now Reply1 the radical socialist revolutionary he is might want to murder me. Why should what i want be of more value than what he wants? Well Let's look at it this way, i bet Reply1 doesn't want to be murdered right? So whatever views we hold we both do not want to be murdered. Therefore not murdering is the universally preferable behavior because even murderers don't want to be murdered.

In this sense we derive our ethics from the values that everyone holds. Therefore there is a universal good and a universal evil.

Secondly. The law are just some words on a piece of paper. Therefore the law is meaningless. That is not to say the law is useless, just that if you are going to have a law it should be reflective of a universal set of ethics.

Anyway, i consider myself a Grey-hat. Because what i do might be the right thing, even though the government disagrees.

Reply1

Reply3 Wrote: Therefore not murdering is the universally preferable behavior because even murderers don't want to be murdered.

In this sense we derive our ethics from the values that everyone holds. Therefore there is a universal good and a universal evil.

Doesn't this assume that humans occupy an elevated status over all other forms of conscious life?

Animals don't want to be murdered, in fact their whole biology is developed to increase their chances of survival, and yet the vast majority of humans murder them and believe it is ethical to do so. Given that we are technically and biologically capable of surviving off non-animal food, we can't realistically use our own survival as a justification to murder animals, and even if we could, it wouldn't change the fact that it was still a "bad" action.

If murder is a universal bad thing, I don't understand why it doesn't apply universally, and why this rule doesn't apply to our treatment of creatures with less intelligence than ourselves.

My personal solution to this problem is to argue that there is no universal bad. But I'd be interested to see how you tackle this dilemna, or if you even identity that there is one here.

I think your approach sounds like it falls under the "do unto others" framework. You are right that murderers don't want to be murdered, and that's a good reason to conclude that murder is bad, but people still murder people all the time. If it is universally bad, what are the consequences for that action? If there are no consequences (say, someone murderers his friend but never gets found out his entire life and he's a psychopath so he doesn't have any personal feelings of guilt or moral corruption), isn't the attribution of "bad" entirely irrelevant and ineffective, even if it did theoretically exist? What's the point of "bad" if it doesn't actually result in a tangible effect - or are you just saying that it's a concept we should use to orientate our society and laws around?

Reply3

Reply1 Wrote: Doesn't this assume that humans occupy an elevated status over all other forms of conscious life?

We do. Because we have moral agency. Would you blame a lion for killing a gazelle? No, because lions do not have the brain capacity to have a notion of ethics, they have no moral agency. Therefore any creature that does not have moral agency should not be considered in the same way that humans should be.

Reply1 Wrote: Animals don't want to be murdered, in fact their whole biology is developed to increase their chances of survival, and yet the vast majority of humans murder them and believe it is ethical to do so. Given that we are technically and biologically capable of surviving off non-animal food, we can't realistically use our own survival as a justification to murder animals, and even if we could, it wouldn't change the fact that it was still a "bad" action.

If you disagree with my point about moral agency, go be a vegetarian then.

Reply1 Wrote: If murder is a universal bad thing, I don't understand why it doesn't apply universally, and why this rule doesn't apply to our treatment of creatures with less intelligence than ourselves.

It applies universally to all beings with moral agency.

Reply1 Wrote: My personal solution to this problem is to argue that there is no universal bad. But I'd be interested to see how you tackle this dilemna, or if you even identity that there is one here.

I think your approach sounds like it falls under the "do unto others" framework. You are right that murderers don't want to be murdered, and that's a good reason to conclude that murder is bad, but people still murder people all the time. If it is universally bad, what are the consequences for that action? If there are no consequences (say, someone murderers his friend but never gets found out his entire life and he's a psychopath so he doesn't have any personal feelings of guilt or moral corruption), isn't the attribution of "bad" entirely irrelevant and ineffective, even if it did theoretically exist? What's the point of "bad" if it doesn't actually result in a tangible effect - or are you just saying that it's a concept we should use to orientate our society and laws around?

What does that even mean? "What's the point of "bad" if it doesn't actually result in a tangible effect".

Bad or evil is a classification of someone's actions. But if you are asking what the point is to classify something as evil then i would answer that we humans need a system of classification to protect ourselves and society from harm. In that sense, my concept of ethics is something to build our laws around in my opinion.

Reply1

Our opinions are so diverging there's literally no point continuing to argue them, it's like an atheist trying to argue away someone's religious convictions, or Locke vs Hobbes, Thérèse vs Nietzsche. We're dealing with long-debated opinions that have never been conclusively demonstrated.

And you're right, this is the wrong environment to be arguing these points anyway.

END

9.3.6 When are you a "Hacker"?
Original discussion February 2013.

Post by OP

(Just to put things to the side, I am aware of my post count and what my alias may stereotype me as, deal with it.)

I am somewhat new to the community, but I've done simple, lame things before. (Packet sniffing, mostly.) What level would I have to be at to proclaim myself "Hacker"? This comes into consideration due to there being stereotypes. (Such as, "Skiddie")

(ALSO, I LOVE BRACKETS.)

Post by Reply1

The way I see it, hacking isn't a title or a style. It isn't something you are. It's not about how many missions you've completed or how many posts you have. It's a mind set, the way you look at the world and the web. It's how you use what you have, and get what you want. It's having the tools you need, locked away in your head. Knowing how to test, exploit and execute anything you can wrap your head around. I'm thinking when I can hack I'm a hacker. As it stands now, I'm just a user.

Post by Reply2

Don't you mean you love parenthesis not brackets?

Also you may want to read this: http://www.catb.org/~esr/faqs/hacker-howto.html

---

Post by Reply1

Reply2 wrote: Also you may want to read this: http://www.catb.org/~esr/faqs/hacker-howto.html

Intense. I don't know about OP, but I'm digging the link.

Post by Reply3

First of all, I don't believe in titles. I don't know why, but western people have the urge to call themselves something. That's the reason why most people claim that the hacker movement and the open source movement is originated from America... but that's not true. There were hackers way before, in europe and asia, it's just that they didn't feel the urge to tag themselves with pity titles.

That being said, I only call someone a hacker if he/she is a real professional in a field (not nesseserally in computer science), and he/she is very creative in it.

Post by Reply4

I like how ESR explains it in his essay:

> ESR wrote:
>
> Q: How do I tell if I am already a hacker?
>
> A: Ask yourself the following three questions:
>
> Do you speak code, fluently?
>
> Do you identify with the goals and values of the hacker community?
>
> Has a well-established member of the hacker community ever called you a hacker?

I'm not saying this is a definitive list, or that you must satisfy 100% of some set of attributes, but this is a nice gauge.

Post by Reply5

> *OPwrote: (Just to put things to the side, I am aware of my post count and what my alias may stereotype me as, deal with it.)*

Fair enough :)

> *OPwrote: I am somewhat new to the community, but I've done simple, lame things before. (Packet sniffing, mostly.) What level would I have to be at to proclaim myself "Hacker"? This comes into consideration due to there being stereotypes. (Such as, "Skiddie")*

Personally, I think "hacker" is an attitude, but public opinion would tell you otherwise.

(i also love parentheses)

When ever I'm on a computer in a public place, I'm always bored because i reckon if i did anything i find interesting, people would get suspicious.

(possibly on topic(depends on how you look at it(I even nest mine)))

Reply4 wrote: Oh, that's simple. All you need to do is dedicate many years of your life to studying security.

IF you feel like exchanging ASCII arrays, let me know ;)

Post by Reply6

As far as I am concerned, if you can hack into the pentagon and steal 2 billion dollars to fund your hello kitty collection then you are a hacker.. If you can delete everything in the HLS database, you are a hacker. Finding Google's IP address or getting admin access to a lame ass site nobody uses is not being a true hacker. That is why I'm not a hacker, I'm just good with computers.

“Teach me how to hack!”

"What, like, with an axe?"

Post by Reply5

Reply6 wrote: As far as I am concerned, if you can hack into the pentagon and steal 2 billion dollars to fund your hello kitty collection then you are a hacker.. If you can delete everything in the HLS database, you are a hacker. Finding Google's IP address or getting admin access to a lame ass site nobody uses is not being a true hacker. That is why I'm not a hacker, I'm just good with computers.

So if i do something really hard core and risk prosecution? or is your interpretation based on difficulty?

Post by Reply7

Why does it matter?

Okay, so, I like to do things with computers. I've taken a real shine to networking lately, I've set up two networks in my house for no apparent reason. I've done a lot of the missions here. I've done things with my computer that most people didn't even know was possible. Does that make me a hacker? Yes? No?

I also like working with cattle. It's my job, and has been for as long as I can remember. I'm good at it, between me and my dad we take care of over 300 pairs. Does that make a cowboy? Oh, but wait, I don't wear a cowboy hat. I don't carry around a revolver. And I absolutely suck at roping things.

Shakespeare wrote: A rose by any other name would smell just as sweet

Oh, and by the way, Google's answer [Hyperlink disabled]. Guess I really am a hacker.

Post by Reply6

Reply6 wrote: As far as I am concerned, if you can hack into the pentagon and steal 2 billion dollars to fund your hello kitty collection then you are a hacker.. If you can delete everything in the HLS database, you are a hacker. Finding Google's IP address or getting admin access to a lame ass site nobody uses is not being a true hacker. That is why I'm not a hacker, I'm just good with computers.

Reply5 wrote: So if i do something really hard core and risk prosecution? or is your interpretation based on difficulty?

It's based on being able to do something useful without getting caught.

Post by Reply7

Reply6 wrote: It's based on being able to do something useful without getting caught.

Yes, Reply5, don't you know how useful a Hello Kitty collection is? /joke

What is your definition of useful, Reply6?

Post by Reply3

So... if I do the laundry (which is useful, that's a fact), and no one catches me, then I'm a hacker? :D

And, do you consider deleting the HLS database useful? Let me be the first to congratulate you...

Post by Reply8

Reply7wrote: Oh, and by the way, Google's answer. Guess I really am a hacker.

Google wrote: someone who plays golf poorly

Oh my god, I'm a hacker too!

Post by Reply9

This seems like a silly, semantic question. It's obviously not too silly, because I'm inclined to open my big mouth. I don't understand why it matters other than as a matter of definition. I think the terminology that surrounds hacking is ambiguous to say the least.

I understand the frustrations of a hacker, who, as a programmer, gets confused with kids "hacking" peoples websites to do God knows what.

At the same time, the 99% of the population needs some sort of term to refer to these kiddies. No one says their silly little webpage was "cracked" into. The term English speakers have agreed upon is

"hacked into". The hacker community, by latching on to that very name has set itself up for the very issue it now complains of. You can't everyday people who barely use their personal computers and talk about hacking a few times a year to distinguish the difference between hackers and crackers.

I have, one time only, "hacked" a website and caused it to function differently to the way the person who wrote the script intended it to. According to the hacker community that alone would not earn me any kudos necessarily. That is fine, but how would I explain to my Mom what it was up to?

END