Hacking for the Thrill of it: An Analysis of Hacker Traits and Characteristics

By Jacob John Williams, 15008632

Abstract

The hacker is the modern boogeyman. Given the rise of the value of data and the increase in the use of devices in our everyday life, its no surprise that this is the case, that a person with the right knowledge and mindset can breach our privacy or interrupt our work. This paper aims to look at the psychology of those who partake in hacking and those who identify as hackers by reviewing papers published in recent years, split into three categories: the characteristics they show, the disorders common among them, and their overall rationale.

1.0 Introduction

In recent years the definition of hacker has broadened, changing from that of a person with a wide area of computing knowledge to that of something more sinister. Broadly speaking, the modern hacker is synonymous with that of the Cyber-Criminal, where people used to respect those who they would deem hackers, they are now seen as the bogeyman of the world of modern computing. The evolution of its meaning is not surprising, with the ever increasing value of data and the importance of infrastructure it is only logical that those with the ability to take it all down would be feared.

But with the broadening of its definition, it has boiled over to the point of drastic generalisations, where anyone with a degree of computing skill or utilising tools relating to those that hackers might use are held suspect, as demonstrated in a poster released by the *West Midlands Regional Organised Crime Unit* (2020) where they inform that children using TOR, Virtual Machines, Kali Linux, WiFi Pineapple, Discord, and Metasploit are open for reasonable suspicion despite the fact that they are multifaceted tools. The most blatant among it being Discord, who describes itself as *"Freeware VoIP application… designed for video gaming communities"*.

Most of the suspicions surrounding hackers are generalisations which stem from mostly negative portrayals in media, those with more skill in IT may be cause for suspicion because they may know how to use malicious tool sets, or those with a keen interest in tools that could be used maliciously would only have such an interest because their objective is malicious. The goal of this paper is to explore what makes a hacker, observing what the modern hacker may look like, what characteristics they might display, how they view themselves, and if suspecting those with a background in computing disciplines is reasonable or not.

2.0 Literature Review

There are numerous areas of research surrounding the psychology of hackers, these being characteristics hackers tend to display; how hacker groups operate; how hackers and hacker groups view each other; why hackers do what they do; and the occurrence of mental illness in hackers. For the sake of space and brevity the methods utilised in studies may only be summarised with the focus being to critique the methodology and review the results.

2.1 Hacker Characteristics

A study by Siegfried-Spellar and Treadway (2014) polled students at a large university in America via questionnaire. The sample of their study was a broad, containing an equal amount of students across the disciplines and genders, they achieved a 66% response rate. The questionnaire contained questions designed to question students on

behaviours that Siegfried-Spellar and Treadway (2014) found to be *"Computer Deviant Behaviour",* they formulated these by condensing the categories proposed by *Roger et al (2006)* and broadening their scope. The questionnaire also utilised the Five Factor Model Rating Form (FFMRF) to identify individual cognitive differences such as Neuroticism, Extraversion, Openness to Experience, Agreeableness, and Conscientiousness.

Interestingly, after performing a statistical analysis of their results there was found firstly to be no difference in the degree majors of computer deviants and non-computer deviants, which could imply that suspecting those with computer literate degrees to be more likely to be hackers is a false flag. This could however be skewed by the fact that Siegfried-Spellar and Treadway (2014) included Cyber Bullying as part of their study, and whilst it certainly is relevant to their study, it is not typically considered to be a hacker behaviour and therefore makes it more difficult to interpret these results in the context of this study. Another conclusion made was that statistically there was no significant difference between the personality traits of hackers and non-hackers, the only identifiable minor correlation being that hackers tend to score lower on agreeableness, meaning they were more antagonistic. The only major identifiable trend was a clear correlation between virus writing and low internal moral values. The primary criticism of this study is drawn from its methodology, questionnaires are good at creating a quantitative analysis but generally bad at creating a qualitative analysis, we know from this study that hackers don't tend to display antisocial behaviour, so why is it then that they do what they do? Another, perhaps pedantic criticism of questionnaires is that they make it easier for the subject to exaggerate or lie, this is only preventable by changing the methodology all together.

The reverse side of the coin to this study is a Study by Steinmetz (2015), who performed overt participant analysis leading to interviews with a British hacker group referred to as "Union Hack". Steinmetz also performed content analysis on ten years worth of issues of a hacker magazine called "2600: The Hacker Quarterly". This study reinforces what was developed by Siegfried-Spellar and Treadway (2014), from observing Union Hack Steinmetz (2015) derived numerous personal characteristics that make the hacker, these being: *"The Hacker Mentality, Skill, Ownership, Hacking as a Guild, Commitment, Journey Over Destination, Experience, and Acts of Transgression".* The hacker mentality is typically what one might expect, it is an

orientation towards problem solving and unconventional thinking. In the other characteristics, Steinmetz (2015) frequently likens hacker to that of Craftsmen, and draws numerous interesting parallels. Rather than the typical isolationist view, Steinmetz (2015) looks at the characteristic of Skill from a more social angle, seeing Skill as more of a development rather than something innate. Steinmetz refers to a quote from Farr (2008) *"Most people… are newbies… In a few Mondays… a few of these newbies will start contributing ideas of their own and be recognised by their peers"*, this works against the typical narrative that hackers are introverted, antisocial people in the same way that Siegfried-Spellar and Treadway (2014) did. This social aspect is drawn out again in the characteristic of *"Hacking as a Guild"*, once again being likened to that of a craftsman. Steinmetz (2015) observes the lower apprentices / *"script kiddies"* being taught by the masters / *"hackers".* Whilst conducting interviews Steinmetz also found that multiple participants had learned their skills through other hacker groups or online forum groups. Given this evidence one has to wonder how the typical view of hackers became that of the antisocial deviant, given that there is an obvious social aspect to it, could it be that the general lack of face to face contact or the internet disconnect aspect of it is what has caused people to draw these conclusions? From the outside in the hacker in their bedroom seems isolated, but in reality they are more connected than most. One could also argue that the narrative stems from the comparison of hackers to thieves, even Steinmetz (2015) does this when reviewing skill by drawing parallels with Sutherland (1939) with *"No one is a professional thief unless he is recognized by others"*, but this parallel seems rather forced since hacker groups tends to have more of a social function beyond simply recognition for ones feats.

Another study by *Cayubit et al (2017)* examined 43 male computer hackers in a Q-analysis. The results of this study were different to that of the previous two, it identified hackers of three personality types. The first being superiority, which views hacking as the pursuit of accomplishment, generally viewing hacking in a positive light, and using hacking to gain a sense of fulfillment. The second is exploitative, characterized by feeling that hacking was a way to take advantage of others, the main drive being to acquire things for free and socialize. The third is Opportunistic, where they see hacking as a way to satisfy immediate needs; an opportunity to satisfy curiosity; when the need arises, hacking is a tool for revenge.

Q-analysis can often suffer from having leading questions or statements that direct participants towards a certain answer even they do not subjectively believe said answer. After reviewing the statements in the study, one can confirm this is not the case, each is tailored to acknowledge that what is being sought is the opinion of the participant.

This study is contributes towards our question by creating a degree of separation between the two studies and the general narrative. Cayubit et al (2017) identifies the type of hacker we learn about from Siegfried-Spellar and Treadway (2014) and Steinmetz (2015) in the Superiority hacker, but then also identifies the stereotypical hacker in the Exploitative. This does however throw some of the previous observations away, since Cayubit et al (2017) identifies the social aspect in the Exploitative hacker, and only for the sake of personal gain. It could be that the previous two studies were deceived by their participants, or that *Cayubit et al* (2017) didnt associate for various types of socializing, either way it can be assumed that this area would require more study in order to identify possible degrees of separation. A final parallel is between the Opportunistic personality type and the more hedonistic identity thieves and virus writers identified by *Siegfried-Spellar and Treadway* (2014).

2.2 Disorders in Hackers

The previous studies explore many different aspects of a hackers characteristics, but do little to analyse correlations between hackers and disorders. The closest we get is an analysis of various values and hedonism by *Siegfried-Spellar and Treadway* (2014) but these aren't defining factors of disorders.

Ledingham and Mills (2015) analysed a noticeable rise in reported cases of Autism and Aspergers Syndrome among arrested cybercriminals. They conducted a questionnaire that reflected the intent to inform law enforcement about Autism and Aspergers syndrome, and polled them based on their departments definitions of Cybercrime and their conduct towards mental health. The questionnaire found that despite the reported rise most cybercrime divisions do very little to check the mental health of incoming offenders, and that there is no official recorded number for the rise in cases despite being reported so, this means the reported rise in reality has no factual basis and is based on either self-diagnoses or an unofficial diagnoses.

Siegfried-Spellar et al (2015) conducted a follow up study to the 2014 study this time looking for those on the Autistic spectrum among computer deviants, the study used a similar questionnaire to that of *Siegfried-Spellar and Treadway (2014)* and continued using the adapted form of *Roger et als (2006)* CCI-R as well as an AQ scale for identifying Autism. 275 students completed the questionnaire and only 2 (0.01%) produced an AQ at or above the cut-off, suggesting no relation between being on the Autistic Spectrum and cyber-deviant behaviour. The conclusions from these studies should come as no surprise, as typically those on the autistic spectrum are law abiding citizens (Ledingham and Mills, 2015).

2.3 Rationale

Hackers are usually stereotyped into two groups, those that do what they do for fun and the opposite, who do what they do for the sake of ideology. A study by *Woo et al (2004)* studied a sample of 770 compromised and defaced webpages and performed content analysis to derive the reason the hacker did what they did. The study separated into two categories, Pranksters and Militants. Of the 770 webpages, 71% were found to be defaced by pranksters and 23% by militants. Whilst the pranksters are most certainly still malicious, what they do is merely done for the thrill of it, to brag about skill or impress people, possibly leading into the one of the characteristics identified by Steinmetz (2015) where to become a hacker you have to be recognised by other hackers. Similarly, the Pranksters seem like they would fit into Cayubit et als (2017) Superiority category, since they don't tend to display any malicious reasoning and merely do it for the accomplishment. Following this logic, one could fit Woo et als (2004) Militant hackers into Cayubit et als (2017) Exploitative category, they do what they do to actively attack people, its malicious inside and out.

Silic and Lowry (2019) also make observations about not only hackers rationale towards what they do, but also how they cope with the emotional by-product of what they do such as fear, guilt, and thrill. The study involved interviews with 16 identified black hat hackers found through one of the researchers, who was a white hat hacker.

Silic and Lowry (2019) found throughout their interviews that the black hat hackers all conducted forms of Cognitive Distortion, which involved convincing themselves that no real harm is done and as a result what they are doing is not particularly immoral. They also partook in a cognitive tactic referred to as shunting, where you only think about the positive aspects of an act in order to put aside fear that may arise from it. Furthermore, most of the black hats agreed that they didn't have any fear of consequences because the risks are low are what risk there are they take into consideration when

calculating their plan. Silic and Lowry (2019) believe that the hackers seemingly rational calculation of risk may not be as rational as they believe, but they are merely convincing themselves of such in order to alleviate fear. Another method was a possession of a Plan B, which would be performed in case something goes wrong. Silic and Lowry (2019) found these plans to be fairly basic and not particularly well thought out, but acknowledges that management of a Plan B scenario is *"important for nerve management… reduces the psychological discomfort associated with uncertainty".*

This study once again fits interestingly with Cayubit et als (2017) study, with most of the hackers seeming to fit into the Superiority category, they don't seen anything wrong with what they are doing, they are merely demonstrating their skill, and they have little fear of getting caught, whether the concept of cognitive distortion fits well with the Superiority category however is debatable, but Cayubit et al (2017) make little reference to such concepts in any of their categories.

Silic and Lowry's (2019) study presents an interesting parallel to Steinmetz's (2015) study, where Steinmetz found the hackers studied to be fairly grounded and reasonable, the hackers studied by Silic and Lowry (2019) seems to be more psychologically charged. This is probably due to the context of the two studies, Silic and Lowry (2019) are looking for these rationales, where as Steinmetz (2015) is studying the idea of hackers and their communities. Alternatively, this could be the stark contrast between those who operate in communities and those who operate isolated, but this would require further research.

3.0 Conclusion

The aim of this study was not to make a statement about what sort of people hackers are, and neither was its aim to determine whether hackers are forces for good or evil. It was merely to expand upon the knowledge of what those in the field of Cyber Security already assume, that hackers can be good, evil, and there are numerous shades of grey. The terms of White, Black, and Grey hat hackers have existed for numerous years, despite this there is often very little distinction as to who exactly these three are, and that was the purpose of this study, to give examples of those who fall into the different categories of hackers.

From this study we know that it is folly to assume that those in Computer based discipline's are more likely to be hackers, since Siegfried-Spellar and Treadway (2014) found no clear correlation between the two in a broad study. Furthermore, Steinmetz (2015) shows us that even those who partake in the hacker community aren't necessarily bad people and in some cases are drawn to the community, despite the stereotype of hackers been antisocial or lone wolves. This isnt to say the stereotype doesn't hold ground however, since Silic and Lowry (2019) displayed the lonesome malicious black hat hacker and how they tend to deal with the consequence of what they do.

To try and prove that hackers are White, Black, or Grey hat is fruitless, all have different rationales, positive and negative characteristics. It could be wise to view the three as points on a spectrum, which would justify how hackers can be generally good people but still perform socially immoral acts.

Another purpose of this paper was to enlighten those who know little about hackers, and assume that all of them are particularly bad people, or that all of those in computing disciplines are worthy of suspicion. Hackers are not the bogeyman, and even when they do bad things they could be trying to do them for a good meaning.

This field does require further study, particularly in the distinctions, one would think it would be interesting to draw the spectrum of the different rationales of hackers and what sort of person sits at either end.

4.0 References

Cayubit, R.F.O.C., Rebolledo, K.M.R., Kintanar, R.G.A.K., Pastores, A.G.P., Santiago, A.J.A.S. and Valles, P.B.V.V. (2017) A Cyber Phenomenon: A Q-analysis on the Motivation of Computer Hackers. *Psychological Studies* [online]., pp. 386-394. [Accessed 15 February 2020].

Farr, N. (2008). *'The Hacker Perspective'.* 2600: The Hacker Quarterly, 25: 26–8.

Hayward, K. (2004). *City Limits: Crime, Consumer Culture and the Urban Experience.* Oxfordshire: Taylor & Francis.

Ledingham, R.L. and Mills, R.M. (2015) A Preliminary Study of Autism and Cybercrime in the Context of International Law Enforcement. *Advances in Autism* [online]. 1 (1), pp. 2-11. [Accessed 15 February 2020].

Rogers, M.K.R., Seigfried, K.S. and Tidke, K.T. (2006) Self-reported Computer Criminal Behavior: A Psychological Analysis. *Elsevier: Digital Investigation* [online]. 3, pp. 116-120. [Accessed 14 February 2020].

Steinmetz, K.F.S. (2015) Craft(y)ness: An Ethnographic Study of Hacking. *The British Journal of Criminology* [online]. 55 (1), pp. 125-145. [Accessed 16 February 2015].

Seigfried-Spellar, K.C.S.S. and Treadway, K.N.T. (2014) Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. *Deviant Behaviour* [online]. 35 (10), pp. 782-803. [Accessed 14 February 2020].

Siegfried-spellar, K.C.S.S., O'Quinn, C.L.O. and Treadway, K.N.T. (2015) Assessing the Relationship Between Autistic Traitsand Cyberdeviancy in a Sample of College Students. *Behaviour and Information Technology* [online]. 34 (5), pp. 533-542. [Accessed 25 February 2020].

Silic, M.S. and Lowry, P.B.L. (2019) Breaking Bad in Cyberspace: Understanding Why and How Black Hathackers Manage Their Nerves to Commit Their Virtual Crimes. *Information Systems Frontiers* [online]. [Accessed 25 February 2020].

Sutherland, E.H.S. (1939) *The Professional Thief.* Chicago: University of Chicago Press.

WMROCU & NCA (2020) What is on a child's computer? [Poster] . *West Midlands Regional Organised Crime Unit* [online]. Available from: https://i.imgur.com/YJ4LemS.png [Accessed February 21, 2020].

Woo, H.J.W. and Dominick, J.D. (2004) Hackers: Militants Or Merry Pranksters? a Content Analysis of Defaced Web Pages. *Media Psychology* [online]. 6 (1), pp. 63-82. [Accessed 15 February 2020].

WCT = 3157
RWC = 313
WCT - RWC = 2844

5.0 Appendices

ROCU and NCA Informative Poster.