**INSTITUTIONEN FÖR SOCIOLOGI
OCH ARBETSVETENSKAP**

PIRATES IN BINARY WATERS

ON COVERT CRIMES AND EDUCATED OFFENDERS

Alexander Knutsson

Abstract

Title
Pirates in Binary Waters: On Covert Crimes and Educated Offenders.

Author
Alexander Knutsson

Supervisor
Charlotta Thodelius

Examiner
Oskar Engdahl

Type of thesis
Master thesis in Criminology, 30 higher education credits

Date
VT 2018

Aims and objectives
In the modern era of digitalization new forms of crime called cybercrime emerged. This study, take a closer look at the efficiency of the routine activity theory (RAT) when applied to one of the most common cybercrimes; software piracy. The aim of the study was to advance the explanatory scope and scientific relevance of RAT in the virtual society. Previous research tends to revolve around theoretical discussions or empirical studies of other cybercrimes, thus not empirically exploring piracy per se.

Method and data
The material consisted of the nationwide survey 'the Swedes and the Internet' (SOI) from 2016 and it was analysed with binary logistic regression. The objective of the SOI is to map, review and present reliable statistics regarding the Swedish populations Internet habits. The reason for choosing binary logistic regression is mainly due to the dependent variable being dichotomous, highly skewed and the distinct lack of multiple layers in the data-set.

Results
The results consist of two binary logistic regressions accompanied by measurements for goodness of fit. In the first regression, each variables individual relationship to piracy was explored. In the second regression, an interaction variable was added containing three of the most impactful variables from the first regression; Internet activity, motivation and knowledge. This study suggests that while the core of RAT remains relevant in cyberspace, further empirical analysis is required. It also suggests that knowledge of the virtual scene is a large contributor to ones' probability of piracy. Contradicting previous findings, this study highlights the importance of including a broader age span when researching piracy.

Keywords
Cybercrime, Cyberspace, Routine Activity Theory, Software Piracy, Virtual Society.

Pirates in Binary Waters
On Covert Crimes and Educated Offenders

Alexander Knutsson

1 Introduction

In the wake of recent years' technological advancement, we have witnessed a rapid expansion of activity within the 'online world' and with it the birth of several virtual platforms' (e.g. Facebook, Tinder and Twitter) that transformed the way we interact with each other and organize our daily lives. The emergence and continued evolution of the so called 'virtual society' have created an arena for new forms of criminal acts that transcend traditional geopolitical jurisdictions. These new forms of crime are more commonly referred to as 'cybercrime' (McQuade III, 2011). One of the most common cybercrimes within the virtual society in present day is 'software piracy' (Britz, 2009).[1] Piracy can be understood as the act of illegal copying of commercially available software (e.g. movies, music or computer programs) to avoid fees and/or whenever an individual creates copies for personal use or distribution (Malin & Fowers, 2009; Higgins & Makin, 2004). Piracy has been a rather popular subject for researchers within the criminological field and as such many have tried to explain this criminal behaviour with traditional criminological theories (see Malin & Fowers, 2009; Higgins & Makin, 2004; Yar, 2005; Hinduja, 2007; Ferraresso et al., 2016; Smallridge & Roberts, 2013). The results from these studies sparked a debate about whether or not traditional criminological theories are equipped with the means to explain these new forms of crime, which begs the question; can piracy be compared to crimes like theft or is this cybercrime more complex than originally anticipated?

1.1 *Previous research*

Piracy has been a popular research subject in recent years, in particular within the criminological field. Consequently, the popularity has resulted in a number of studies where different criminological theories have undergone evaluations in terms of their efficiency and overall usefulness when applied to the cybercrime piracy. Three of the seemingly more popular and applicable criminological theories are Michael Gottfredson and Travis Hirschi's 'general theory about self-control' (1990), Ronald Akers' 'social learning theory' (1977) and Lawrence Cohen and Marcus Felons' 'routine activity theory' (i.e. 'RAT') from 1979. Granted, there are a number of other relevant theories that one might find interesting. Nonetheless, due to the popularity of these theories they will serve as an example of the previous research.

As mentioned, Gottfredson and Hirschi's general theory about self-control (1990) is one of the seemingly more popular theories and as such there have been a number of studies

---

[1] Henceforth when mentioning 'piracy', I'm referring to software piracy.

where the relationship between self-control and tendencies for piracy are explored (see Malin & Fowers, 2009; Higgins & Makin, 2004; Moon et al., 2010). For instance, Jenessa Malin and Blaine Fowers (2009) found that self-control does co-align with adolescents tendencies to commit piracy and could thus conclude that ones' age or maturity may influence ones' level of self-control in a way that makes younger individuals more likely to commit piracy. George Higgins and David Makin (2004) conducted a quantitative study on university students where they concluded that low self-control does indeed correlate with piracy. In addition, they found evidence to suggest that individuals who associate with pirating peers have a mediating effect on the students' tendency for piracy, thus increasing the probability of piracy even further. Although Gottfredson and Hirschi's self-control theory (1990) is one of the more applicable criminological theories for understanding the cybercrime piracy, a potential problem arises when examining the high possibility of organized individuals. These organized users create unauthorized copies and distribute them at a much grander scale than your average user. Consequently, these 'big fish pirates' provide other pirates with access to a considerable range of pirated goods and as such they have more to lose, which requires them to maintain a high level of self-control in order to stay one step ahead of law enforcement and avoid punishment; contradicting the idea that ones' tendencies for piracy is governed by ones' level of self-control.

Another popular theory is Akers' social learning theory (1977). Although the result from this particular theory seems to be somewhat less applicable in comparison with self-control, it has not stopped researchers from examining the relationship (see Morris & Higgins, 2010; Hinduja & Ingram, 2009; Gunter, 2008). In a study by Robert Morris and George Higgins (2010) they evaluated the explained variation of the social learning theory in relation to piracy. They found that the social learning theory can be used to explain a respectable amount of the variation. However, Morris and Higgins (2010) conclude that in order for the social learning theory to adequately explain the cybercrime piracy, improvements and modifications must be made to better suit the digital environment. The problem is linked to the importance of online versus offline peers and there has been mixed results pertaining to this particular problem, some argue that there is a need for modification (Morris & Higgins, 2010) while others claim to have found evidence that supports the equal importance of both online and offline friends in relation to ones' likelihood of piracy (Hinduja & Ingram, 2009). Even if the social learning theory seems to be somewhat applicable to piracy, the inconsistency in the explained variance pose a problem and should be researched upon further in order to thoroughly identify areas that may need modification and thus improve the overall usefulness of the social learning theory in a virtual context.

Cohen and Felons' RAT (1979) and its relationship to cyberspace has been a popular research topic (see Cornish & Clarke, 2003; Yar, 2005; Newman, 2009; Sampson et al., 2010; Leukfeldt & Yar, 2016; Felson & Eckert, 2018). However, some of these studies, such as Majid Yar's article 'the novelty of cybercrime' (2005), are not necessarily conducting empirical testing of RAT's usefulness, but rather discussing the hypothetical use of the theory in a virtual environment. In a recently published book, Felson and Mary Eckert (2018) keeps a similar discussion regarding the crime enhancing factors of cyberspace in relation to a large variance of different cybercrimes including, albeit briefly, piracy. Similarly, Graeme Newman (2009) presents an interesting description of the history and growth of cybercrime in modern society. Although Newman (2009) mentions piracy, the focus of his study is not to specifically explain piracy but rather to provide the readers with a comprehensive overview of cybercrimes as a whole.

Granted, there are studies that empirically test the efficiency of RAT in cyberspace. However, the overwhelming majority of recent studies are examining other cybercrimes such as; computer viruses, phishing, online harassment and consumer fraud, thus not exploring

piracy *per se* (see Holt & Bossler, 2008; Choi, 2008; Pratt et al., 2010; Leukfeldt, 2014; Leukfeldt & Yar, 2016). Supplementary to this, it seems to be a recurring theme amongst the empirical studies to focus on college students which according to numerous reports represents the age group that is most likely to commit cybercrimes (Husted, 2000). In relation to piracy, one could argue that limiting the age scope may be foolish primarily due to the established use of the virtual world within most age groups in modern society (excluding some of the much older generations). In sum, there have been quite a few studies with a theoretical and empirical approach (see Yar, 2005; Newman, 2009; Felson & Eckert, 2018). Although these studies are very interesting, most of them tend to focus on other cybercrimes. Consequently, there is a need for further empirical evaluation of RAT when specifically investigating the cybercrime piracy.

In conclusion, the virtual society that enables cybercrimes like piracy is relatively young and the criminological theories we use to explain this criminal behaviour, such as self-control, social learning and RAT are often much older. Consequently, some of these theories were not developed in a time where the virtual world played such a major part of our everyday life. Needless to say, this does not mean that criminological theories developed before the emergence of the virtual society are substandard theories, but rather that the authors of the past might have published theories that were already modified to fit into a digital context had they been developed during a time of a highly integrated virtual society. Thus, there exists a need to re-evaluate and improve upon previous research in order to increase the scientific relevance and efficiency of these theories within the virtual society that we live in today.

1.2 *Current study*
That being said, the theory that will be under thorough evaluation in this study is Cohen and Felons' RAT from 1979. The purpose of this study is to assess the efficiency of RAT when applied to the cybercrime piracy. The centre of attention in this study will be RAT's concept of 'motivated offenders', mainly due to limitations with the chosen material (e.g. unable to operationalize the concept of 'suitable targets' and 'capable guardians') and the need to re-evaluate the abstract concept of RAT's 'motivation' within the virtual scene. The main hypothesis (H1) is thus to examine if ones' level of activity in the virtual world influences ones' probability of piracy after controlling for other variables. The methodological differences from previous studies will primarily consist of the chosen material and the applied method. This study uses a secondary form of data from an annual nationwide survey in Sweden called 'the Swedes and the Internet' (Davidsson & Findahl, 2016). The original purpose of the survey is to map and review the Swedish populations' Internet habits. As for the method, I have chosen to use 'binary logistic regression' mainly because the dependent variable and many other variables in the data-set are dichotomous and highly skewed (Field, 2013). Therefore, this study differs from previous research of RAT and cybercrime. Primarily because most previous research tend to focus on other forms of cybercrime, use linear logistic regression and target the most likely age group; college students. In contrast, this study's main focus is piracy, the method used is binary logistic regression and the sample size is representative of the Swedish population.

1.3 *Theoretical framework*
RAT was not developed during a time where people were as integrated in the virtual society as we are today and its original purpose was in fact to explain common street crimes like vandalism and theft (Cohen & Felson, 1979). Despite the original purpose, RAT remains relevant, especially within the field of situational crime prevention (see Cornish & Clarke, 2003; Sampson et al., 2010). RAT's continued relevance can be credited to its three core concepts; the 'motivated offender', the 'suitable target' and 'capable guardians' or lack

thereof (Cohen & Felson, 1979). However, much has changed in our society since the theory was first developed. Before I present RAT's three core concepts and how they fit into a digital context, it is necessary to discuss some of the implications tied to the virtual crime scene.

1.3.1 *Crime scene*

Cybercrimes are according to Newman (2009) for the most part new versions of already existing crimes. Although it is easy to understand the sentiment that theft has evolved into cyber theft, the crimes are in fact fundamentally different in ways of execution and the facilitating environment in which the crimes take place. This leads one to think of them as two different forms of crime as opposed to two sides of the same coin. From an historical perspective, crimes that targeted data have existed for a long period of time. Nevertheless, it is not until modern society got dependent on the virtual society that these forms of crime really became worthwhile for the perpetrators (Felson & Eckert, 2018). The introduction of the 'virtual scene' has thus influenced and transformed traditional forms of theft into the new cybercrime known as piracy.

Cyberspace is the virtual catalyst that changed our way of life. However, in the wake of numerous positive conveniences a large number of negatives were developed; including but not limited to new forms of criminal behaviour. Due to society's continuous embrace and dependency of cyberspace the reach of cybercrimes is nowadays a global phenomenon. The continuous expansion of cyberspace has altered the reach of cybercrimes to stretch far into our government agencies, workplace environment and personal home (Felson & Eckert, 2018). The virtual scene is in contrast to the physical world user-friendly, inexpensive and effective. Further, the 'virtual hotspots' (i.e. websites like 'The Pirate Bay') encourage would-be pirates to partake in the pirated goods by designing their piracy websites in a pedagogical manner and providing a form of security for would-be pirates. This 'security structure' consists of a simple 'VIP' and/or 'Trusted' status of some members; this reassures would-be offenders, since one of the major concerns when browsing the Internet is to accidentally download some sort of malware or otherwise vicious programme.[2] Additionally, the publicity of the virtual hotspots increases the availability of the pirated software even further; as a result some of them, like 'The Pirate Bay', have become a household name in Sweden. This publicity factor further enables the would-be pirate, primarily because all they have to do to reach this virtual hotspot is to perform a quick Internet search.

The most apparent problem and challenge for law enforcement with cybercrime is the anonymity provided by cyberspace. Anonymity could arguably be described as twofold in a sense that when ones' browsing cyberspace one is anonymous within the virtual scene. Simultaneously, in the physical world piracy can be described as a 'covert crime' which in short means that the crime takes place behind closed doors (Felson & Eckert, 2018). The ensured anonymity of cyberspace facilitates the transition of would-be offenders to offenders, in primarily two different ways. First, anonymity neutralizes any potential guilt felt by the perpetrator since it usually is neither a clear victim nor human contact involved. Second, anonymity creates the illusion of security, in a sense that ones' actions can go unnoticed by law enforcement and thus evade any potential consequences' of ones' actions. In sum, the virtual crime scene is a complex, abstract scene where thousands- perhaps even millions of people interact and form a steady flow of chaotic binary rivers.

1.3.2 *Motivated offenders*

The existence of the 'motivated offenders' is not overtly analysed by RAT and can be summarized as; "A likely offender was anybody who for any reason might commit a crime.

---

[2] This security structure exists at 'The Pirate Bay' at the time of writing this study.

How this likelihood might vary was avoided since that would bring up the forbidden issue of criminal motivation" (Clarke & Felson, 1993:2). Having said this, RAT does argue that we should not focus on the characteristics of the criminal person but rather shift our focus towards the surrounding activities and routines in our attempts to understand the driving motivation behind criminal behaviour (Cohen & Felson, 1979:589). However, it is important to note that Cohen and Felson (1979) highlighted the importance of the motivated offenders ability to carry out the criminal act; "Each successfully completed violation minimally requires an offender with both criminal inclinations and the ability to carry out those inclinations" (Cohen & Felson, 1979:590). Nowadays people are considerably more active within the virtual world than we were in the past and if recent years are any good indicator of future development we are bound to become even more integrated in the future (Davidsson & Findahl, 2016). Considering that RAT highlights the importance of surrounding activities and above all available opportunities for criminal acts when identifying ones' motivation, it is apparent that the increased activity within the virtual world may have spurred on peoples motivation to commit cybercrimes like piracy.

RAT received some criticism for its rather simplified way of explaining motivation. This was especially apparent in the criticism against the 'pleasure versus pain' notion and its parallels to rational choice theory, i.e. decision making based on seeking fulfilment and simultaneously avoiding potential harm (Paynich & Hill, 2010). In short, human behaviour is more complex and cannot be calculated with such a simple model since we do not commit rational choices by default. This is especially true in crimes of passion where the perpetrator may not think about the immediate reprehension of their actions. Although, to state that humans are, for the most part, rational beings is appropriate, it is problematic to generalize all criminal behaviour as rational when in truth there are plenty of irrational people doing irrational things in this world.

A year before RAT's inception, Kaplan et al., (1978) presented the 'opportunity, target, risk, effort and payoff' model, otherwise known as the OTREP-model. The OTREP-model provides a comprehensive range of factors that may lead to an increased or decreased motivation amongst would-be offenders (Kaplan et al., 1978). The idea that people are governed by something more than just a 'pleasure versus pain' outlook is in my opinion far more realistic. Although OTREP share similar conceptions as rational choice theory, it is a model that tries to explain rational behaviour in a more concrete manner with the inclusion of certain aspects that were not accounted for in RAT. OTREP is in short a model aimed specifically to explain variance in human motivation. One could therefore argue that it should not influence the models relevance whether it is applied in a virtual or physical setting. In this study, OTREP will be used as a tool to supplement the rather weak definition of motivation presented by RAT.

1.3.3 *Suitable Targets*

The 'suitable targets' is according to Cohen and Felson (1979:589-591) people or objects who would put up a low level of resistance for the motivated offender thus, making them easy targets for the perpetrators. The suitability of a target can be broken down into four essential parts represented by the 'VIVA' acronym; value, inertia, visibility and accessibility (Leukfeldt & Yar, 2016).

Value is described as whatever the motivated offender finds valuable, thus assigning value to something or someone will lead to an increased suitability of that target (Leukfeldt & Yar, 2016). Since value is something highly subjective it can take the form of numerous objects, things or even persons. In relation to piracy, a high value target might be the digital files of an unreleased episode of a popular TV show. Value can therefore be understood as a form of 'personal investment' in a sense that, if you are highly invested into a certain TV

show and an unreleased episode pops up at various piracy websites then you are more likely than the un-invested to commit piracy in order to access the material. In short, value can be whatever the person subjectively desire. Cyberspace allows for a virtual setting where the availability of potentially valuable targets is infinite, thus increasing the opportunities of finding something the would-be offender appraises as valuable substantially.

Inertia is described by Cohen and Felson (1979) as the physical premises of said target and whether or not it can be moved efficiently. Inertia can thus be understood as the physical limitations of the suitable target. In the digital world, the physical hindrances are slim, if not non-existent. The targets consist of weightless software with infinite reproduction possibilities and all that is required of you to access these targets is a computer/phone/tablet with Internet access (Yar, 2005). The physical limitations of a motivated offender would thus logically be the lack of a computer/phone/tablet and/or Internet access. Granted, there are people who do not have access to a computer or the Internet. Nonetheless, in this case the overwhelming majority of Swedes' (97 percentages in 2016) have access to both (Davidsson & Findahl, 2016).

Visibility is simply the visibility of the suitable target that the motivated offender wants to access (Cohen & Felson 1979). Traditionally, one might think of medieval food markets where hungry orphans could scout the area and assess the situation before moving in to secure their supply of food and live to fight another day.[3] In the online world the suitable targets are displayed on various pirate websites for the entire world to see. As opposed to the medieval shopkeepers the pirates are not trying to make a profit, in fact they encourage other pirates to access and share the digital goods. This process increases the visibility of the suitable targets even further and facilitates the spread of pirated goods across the globe. Additionally, websites like 'The Pirate Bay' is nowadays a household name in Sweden and many other countries. It is important to note that the increased visibility and recognition by the rest of society has expanded the publics and pirates interest in websites like 'The Pirate Bay'. The popularity factor of these websites attracts new users and increases the overall activity on the website, resulting in an increased availability of pirated goods.

Accessibility is described by Cohen and Felson (1979) as the physical layout of neighbourhoods or other public places and the placement of suitable targets within these locations. In short, the access to the suitable targets should be limited, thus reducing the opportunity for the motivated offenders to strike (Leukfeldt & Yar, 2016). The online world is not restricted in the same manner as the physical world. However, there are some requirements that one needs to achieve before being able to access the suitable targets in the digital environment. A virtual structure is required, such as a functioning operation system, web browsers and in some cases a program that enables torrents to efficiently download and upload (e.g. 'uTorrent'). Although most of these virtual structures are pre-installed and ready to use whenever you purchase a new computer, it is important to remember that they are the digital foundations that enables online life. It is important to recognise that popular piracy websites wants to spread the pirated goods. Consequently, they are typically designed to be pedagogic and easy to use for anyone with basic knowledge of the virtual world, thus increasing the accessibility of the pirated goods even further.

1.3.4 *Capable guardians*

The 'capable guardians' are defined by Cohen and Felson (1979) as either objects or persons' who would prevent the crime in question from ever occurring. Guardianship is not limited to law enforcement; the concept implies that anyone who is present and capable may be able to discourage the motivated offenders from committing the crime (Holt et al., 2016). The police

---

[3] Think Aladdin.

officer strolling down the street in order to interact with the public and maintain order is undoubtedly a capable guardian. However, the everyday guardians such as ones' family, friends, partner or other people of importance are equally if not more capable to fulfil the role of guardian (assuming that they are opposed to the criminal act).

Guardianship in the 'online world' is a tricky concept for a number of reasons. The guardianship of law enforcement in the online world is inadequate; mainly due to the impossible task of monitoring the never ending surge of information. Additionally, even if it was possible to observe and record all activity it would likely be classified as an invasion of privacy. Supplementary to this, the guardianship of others, such as ones' family, friends, partner and other important figures may be limited since piracy is what Felson and Eckert (2018) describe as a 'covert crime'. The private nature of piracy reduces the efficiency of the otherwise capable guardians simply because the crime is typically carried out without their knowledge. Furthermore, piracy is generally not seen as a morally reprehensible crime (Hinduja, 2007; Malin & Fowers, 2009) which may influence ones' likelihood of intervening even if they knew the person was involved in piracy. This is especially true for individuals with no legal responsibility over the pirating individual, such as ones' friends or partners (Holt et al., 2016). In sum, both formal and informal forms of guardianship in the online world are primarily limited by their level of insight, legal- and moral implications.

2 Materials

As mentioned, the data sample used this study is the annual survey the Swedes and the Internet (e.g. 'SOI') published by the Internet foundation of Sweden (Davidsson & Findahl, 2016). SOI represents the Swedish population in the international project called 'World Internet Project' (e.g. 'WIP'). The goal of WIP is to monitor the spread and use of the Internet on an international scale. The purpose of the SOI is thus to map and review the Swedish populations' Internet habits. The survey first launched in the year 2000 and has been held annually since its inauguration. I will be using the data from 2016, because when I requested data for my study that was the most recent and available sample. The sample consists of a secondary form of data, meaning that I was not involved in the process of designing the survey or collecting the data. In addition, any potential personal information of the respondents has already been removed by the SOI; securing the anonymity of all respondents.

As for the selection process, the first year of the survey they initially picked random telephone numbers from the Swedish telephone registry and reached out to roughly ~ 6000 potential respondents. About half of the contacted individuals did not want to partake, leaving them with a sample size of roughly ~ 3000 respondents. They used the first year sample as the foundation for forthcoming surveys, thus reaching out to people who had participated in the previous year to see if they would be interested to partake again. However, each year they had to replace roughly ~ 700 participants due to drop-off. These new participants were gathered in a similar randomized fashion, although they did make sure that they achieved an even distribution of age and sex within the sample (Davidsson & Findahl, 2016). In 2016, the sample size reached a total of 3085 participants ranging from the ages 13 and all the way up to 97.

3 Methods

In this study, I decided to use binary logistic regression for three reasons. First, because the dependent variable and a few of the independent variables can be categorized as dichotomize variables, which in short mean that the variable consists of two valid answers. Binary logistic regression is especially well equipped to deal with dichotomous variables (Field, 2013; Long, 1997). Second, most variables included in the study is highly skewed which makes the otherwise popular approach of a regular linear regression (e.g. 'OLS') somewhat un-suited for

the task. Third, because the sample is gathered through a randomization process across the Swedish population, one could argue that there is a distinct lack of multiple layers, thus rendering multilevel regression unnecessary.

3.1 *Operationalization and descriptive statistics*

The operationalization, or rather, the way in which one try and use data to explain and measure the phenomenon that they seek to understand, is a crucial step in any research. Having said that, operationalization is also tied to the reliability and validity of the study. In short, I want any potential findings to be reliable and thus replicable in a sense that if a similar study was conducted they would get a similar result; this will strengthen the generalizability of the results (Golafshani, 2003). As for validity, one wants to make sure that the measurements used in the study are accurate and more importantly; that the measurements are relevant to the study's purpose and goal (Golafshani, 2003). The questions for each variable discussed below can be found in appendix 1. Supplementary to this, I have added some descriptive statistics to further showcase variable coding, potential drop-off and percentage distribution for each variable.

3.1.1 *Piracy*

Piracy will, unsurprisingly, be the dependent variable in this study. When measuring piracy most of the previous studies tend to use an array of questions regarding ones' attitudes and intentions towards piracy in different situations (see Higgins & Makin, 2004; Holt & Bossler, 2008; Choi, 2008; Malin & Fowers, 2009; Pratt et al., 2010; Leukfeldt, 2014). This makes perfect sense because in general people tend to under-report illegal activities and by all indications piracy is no different (Liang & Yan, 2005). With that being said, unfortunately in this study piracy is not measured with an array of questions primarily because piracy is not the main focus of SOI. Granted, this does not impact the significance or relevance of the study. Nevertheless, it is safe to assume that if an array of questions were used instead of the current question we would have seen a larger percentage of identifiable 'pirates'.

Piracy is measured on a 0 to 5 scale; where zero represents no piracy and five represents several times a day. The variable have for the purpose of this study been recoded into a dichotomize variable, thus separating between the pirates and non-pirates. The main reason for the recoding is simple; the scale of the crime is not of interest but rather why people would commit the crime to begin with. Descriptive statistics reveal that 2846 participants answered the question; this is a drop-off of 239 participants and although this is not a surprise due to piracy being a sensitive subject it is noteworthy. The drop-off is in relation to the total sample size (N_{total} = '3085'), relatively small and should therefore not impact the results. As expected, there is a skewed percentage distribution where roughly ~ 80 percentages of the respondents could be identified as 'non-pirate' and roughly ~ 20 percentages as 'pirates'.

3.1.2 *Internet activity*

Internet activity will be the focal independent variable in this study; because it is my understanding that with a highly integrated virtual lifestyle one is far more likely to discover suitable targets and come across the opportunities to commit piracy. In present day, there are a number of ways to access the Internet, such as through ones' smartphone, tablet and computer. Additionally, you can access Internet in almost any physical environment as long as you have the hardware and adequate Internet connection. This means that piracy can be carried out pretty much anywhere. However, the mere presence of potential capable guardians i.e. people that could interfere, may lead one to be less likely to commit piracy in a public and/or workplace environment. Consequently, in this study, Internet activity will be measured using ones' Internet activity whilst being home for primarily three reasons. First, because

whilst being home the users are free to pursue their own personal interests in the virtual society as opposed to the far more restricted use of Internet in the workplace. Second, because as briefly mentioned above one is less likely to be disturbed by potential guardians thus ensuring ones' privacy. Third, because it is my understanding that our home location is the most common place for most people to access and browse the Internet.

Internet activity is measured on a 0 to 5 scale; where zero represents no Internet activity and five represents Internet activity several times a day. My expectation is that the probability of piracy will increase alongside Internet activity, thus indicating that with an integrated virtual lifestyle ones' probability of piracy increases. To my surprise, the drop-off was 270 participants. This could be explained by the 'I don't know' option available to the respondents, primarily because it is hard to appraise how much time one spends within the virtual world; thus leading to a sense of uncertainty which may explain why some of them resorted to the 'I don't know' option. Nevertheless, the results indicate a highly skewed percentage distribution where the majority of the respondents (roughly ~ 52 percentages) are active several times a day whereas only 0.5 percentages of the respondents claim that they never use Internet whilst being home. This result is expected, primarily because Swedes are in general very integrated and active within the virtual society (Davidsson & Findahl, 2016).

3.1.3 *Legal Alternatives*

Legal alternatives to piracy are available in a larger scale than ever before, although that was not always the case. In the beginning of the 21st century it was often brought up in debates on the 'pro-piracy' side that piracy is the only way for many people to access the software that they need. This could arguably be understood as an attempt to neutralize the act of piracy and shift the blame towards the slow paced evolution of legal alternatives (Sinha & Mandel, 2008; Waldfogel, 2012). Nowadays, there are a number of websites that allows their customers to stream movies and TV shows for a monthly subscription fee. Similarly, there are also a number of programs and/or websites that allows their users to stream music for a monthly subscription fee. Some of the most popular services include; Netflix and HBO for movies and TV shows and Spotify for music. Although these services cannot provide the user with every movie, TV show or song ever created, they offer a legal option for people to access content that they might enjoy. More importantly, it is my understanding or rather preconception that if you are subscribed to some of the legal alternatives available, you are less motivated to commit piracy. Therefore, I concluded that including the 'legal alternatives' as a variable would provide the study with valuable data on the relationship between piracy and the use of legal alternatives available today.

The use of legal alternatives is opted through two straightforward questions that conveniently ask the respondents if they are currently subscribed for any legal service that facilitates the streaming of movies and TV shows and/or music. The reply 'no but I have been before' option, have been recoded into the 'no' category, because previous subscriptions is not of concern in this study but rather if ones' current subscription influences ones' tendencies for piracy. The variables are thus, after recoding dichotomous. Furthermore, descriptive statistics reveal that there is a relatively even percentage distribution; for music roughly ~ 44 percentage and for movies and TV shows roughly ~ 38 percentage of the respondents are currently subscribed to one of the legal alternative available. The drop-off was roughly 240 participants for each question. However, it is likely to be the same respondents who for whatever reason might have skipped or were unfamiliar with the legal alternatives thus resorting to the 'I don't know' option.

3.1.4 *Knowledge*

Knowledge of computers and the virtual world is a crucial trait that allows the pirates to navigate the 'Cyber Sea' in order to reach their destination filled with digital treasure.[4] Knowledge is thus related to ones' ability to carry out piracy, since it is not the physical barriers that restricts digital users but rather their knowledge of the virtual environment (Leukfeldt & Yar, 2016). In the digital world ones' access to the goods is thus primarily limited by ones' level of knowledge of the virtual scene as opposed to physical barriers. Consequently, knowledge is an important factor in the virtual world which is why I have included a variable that measures the respondents' self-proclaimed knowledge of computers and the virtual world. Although self-proclaimed measurement might be somewhat inaccurate at times due to overestimating or underestimating ones' knowledge. Nonetheless, the variable will provide the study with valuable data regarding the relationship between knowledge (i.e. ability) and piracy.

Knowledge is measured using a self-reported level of knowledge on a 0 to 3 scale; where zero represents no knowledge and three represents someone who is very knowledgeable. Descriptive statistics reveal a slightly skewed result where roughly ~ 25 percentage of the respondents identify themselves as individuals with low or no knowledge whereas roughly ~ 75 percentage state that they have a good or very good knowledge. The drop-off was in this case miniscule and thus not worth mentioning.

3.1.5 *Motivation*

Motivation is challenging to operationalize since it is very subjective and thus versatile in nature. RAT purposely avoided discussing this subject since motivation is such a volatile topic (Clarke & Felson, 1993). Although OTREP supplements the motivation aspect of RAT, it is still challenging to find adequate measurements of motivation. With that being said, ones' motivation to commit piracy will be measured with an activity and interest outlook. For instance, if someone is watching movies at their computer on a daily basis it is my understanding that this particular person has a high interest in films. Consequently, this interest may lead to an increased probability of piracy because piracy is one way for the perpetrator to access the material that they seek. Granted, one could be an avid movie watcher without being a pirate, I am simply stating that this interest and/or hobby might lead to an increased desire of the suitable targets available in the virtual environment. Supplementary to this, a high level of activity at ones' computer might lead to an increased exposure of opportunities. Motivation is, in sum, operationalized through two questions that measure ones' level of activity and interest in music and/or movies and TV shows.

Motivation is measured using two questions on a 0 to 5 scale; where zero represents no activity whereas five represents several times a day. The questions are asking the respondents how often they use their computer to either listen to music or watch films / TV shows. The results are very similar; roughly ~ 36 percentages for film and ~ 37 percentages for music state that they never indulge in these activities while being at their computer. Consequently, 64 and 63 percentage of the respondents is consuming films and/or music at their computers. Most of the respondents' who are actively watching at films and TV shows and/or listening to music partake in this activity on a weekly basis (i.e. roughly ~ 21 percentages for film / TV shows and ~ 19 percentage for music). In contrasts, the individuals who partake in this sort of activity several times a day represent the minority; roughly ~ 3 percentage of the respondents watch films / TV shows several times a day, similarly ~ 6 percentage state that they listen to music several times a day whilst being at their computer. The drop-off for both questions are 238 respondents, this is likely due to some respondents either skipping the question entirely or

---

[4] Please excuse the analogy.

simply stating that they don't know how often they indulge in these activities whilst being at their computer.

3.1.6 *Education*

Education is often brought up when discussing deviant behaviour, for instance; Ki et al., (2006) claims that higher levels of education lead to a greater sense of right and wrong. This 'enhanced moral compass' of highly educated people give rise to a harsher view of unethical behaviour like piracy (Ki et al., 2006). However, since the Internet is a crucial element of modern education it is possible that one that has undergone a higher education is more familiar with the virtual scene. Additionally, since a lot of modern universities rely on the Internet to access research material it may lead to an increased exposure of the Internet and thereof opportunities for piracy. Ones' level of education may thus be somewhat of a double-edged sword; in a sense that the increased dependency of the virtual scene within modern education might lead to an unwanted enhancement of the student's ability to carry out cybercrimes like piracy. In an attempt to further investigate this relationship, an education variable has been included in the model.

Education is measured using the respondents self-reported level of completed education complemented with an 'I'm currently a university student' option. The response options range from a scale of 0 to 4; with zero being elementary school and four represents a bachelor's degree at University or higher. Descriptive statistics reveal that roughly ~ 80 percentage of the respondents' graduated high school and of these roughly ~ 19 percentages are currently engaged in University studies. Additionally, 26 percentages state that they have completed a bachelor's degree and/or a higher degree at a University. The drop of was 256 respondents which might be due to the relatively low age of some of the respondents. There may for instance, be a lack of options for students currently engaged in High School studies.

3.1.7 *Income*

Income is another aspect that may influence ones' probability to commit piracy. It is no secret that the increased activity of software piracy in the early 21st century has caused economic losses for the entertainment industry (Bhattacharjee et al., 2003). Although, piracy is not necessarily limited to individuals with 'low income' it is reasonable to assume that people who cannot afford access to the material they seek via legal alternatives may be more motivated to use piracy as an alternative (Waldfogel, 2012). Granted, this would require some form of personal value assigned to the target. However, given how easy some of these targets are to access within cyberspace, the likelihood that a motivated 'low income' would-be offender might commit piracy is very likely.

Income is measured using the combined household yearly income on a scale of 0 to 6; zero representing a yearly household income of 150 000 SEK or less whereas six represents a yearly household income of 750 000 SEK or more. The reason for using this measurement is that I want to avoid labelling individuals who may have a low personal income, when in reality they have a much higher income when combined with their significant other or parents' economic situation. The mean value for income is 3.46, the percentage distribution is relatively even with the exception of the lowest and highest income options. 7 percentage of the respondents have a yearly income of 150 000 SEK or less and surprisingly ~ 22 percentage of the participants earn 750 000 SEK or more each year. The other income categories show similar results with a relatively even distribution of roughly ~ 13-15 percentage in each category. There was no drop-off in this variable.

3.1.8 *Age and sex*

Previous studies typically use college students since they represent the age group most likely to commit piracy according to previous research (Husted, 2000). Similarly, when it comes to the respondents' sex it seems that males are far more likely to commit piracy than their female counterparts (Higgins & Makin, 2004; Liang & Yan, 2005; Felson & Eckert, 2018). Considering the fact that both age and sex seems to influence ones' probability to commit piracy and that they are both available in the data sample, it is appropriate to include these two variables in the study.

Sex is self-proclaimed, with the options being; 'male' or 'female'. Although an 'I don't know' option was included, nearly all respondents choose one of the other two options resulting in a percentage distribution of ~ 52 percent male and ~ 48 percent female.

Age is reported in the form of ones' birth year, which has been recoded and translated into actual years of age at the time of responding to the SOI survey (i.e. 2016-1991=25 years old). The percentage distribution was somewhat expected with a mean of 47.71 years of age (i.e. middle age). The age span ranged from 13 years of age all the way up to oldest participant who was 97 years old. There was no drop-off in this variable.

4 Results

The result will be presented in two sections; the first part (e.g. '4.1') examines the first binary regression, initial interpretations of the regression and the goodness of fit. The second part (e.g. '4.2') examines the same binary regression when adding an interaction variable, thus primarily interpreting potential changes that the interaction variable caused. Lastly, highlights (e.g. '4.3') of the results will be presented to further emphasize the noteworthy findings in the two regressions.

When combining all of the variables above the number of valid participants (i.e. 'N_{valid}') got reduced to 2547 in comparison to the N_{total} of 3085. The drop-off of roughly ~ 17.5 percentages' is likely due to the various reasons mentioned above; in sum, a combination of uncertainty amongst the participants and sensitive questions (i.e. piracy being an illegal activity). Additionally, the 'education variable' would likely have a lower drop-off if a response options like, 'I'm currently a High School student' were implemented. Further, since the age span is so wide some of the youngest participants are likely unaware of their family's economic situation which may lead to an increased likelihood of resorting to the 'I don't know' option when faced with this particular question. Nevertheless, the N_{valid} represents roughly ~ 82.5 percentage of the N_{total} and is still large enough to be considered significant.

One initial way to examine the goodness of fit of the model is to take a closer look at the iteration history; specifically examining the shifts in '-2 Log likelihood' value. In short, the value should ideally become successively lowered with each step of the iteration, since this is one of the earlier indications regarding ones' goodness of fit (Field, 2013). Should the -2 Log likelihood increase instead of decrease it would be a cause for concern. The initial -2 Log likelihood value was 2596.987 and after step six in the iteration the value decreased to 1883.236, thus reducing the initial value by roughly ~ 714. Based on this, I can conclude that the model is initially of a good fit.

4.1 *Binary regression*

The first column of table 1 contains the b-coefficient (also known as log odds), the standard error of the log odds and their significance levels. One should exercise caution when interpreting the results of the first column because these values are, in their initial state, indicators of whether the relationship between the variables has a positive or negative effect. Granted, the significance values cannot be misinterpreted, thus any insignificant values need to be discussed and properly dealt with. Nonetheless, in some cases it makes sense to further

include an insignificant variable due to strong theoretical suggestions. In the second column the calculated odds ratio for each variable is presented. These values are in short, expressions of the increased or decreased odds for one to commit piracy. The value of 1 in the odds ratio should be interpreted as no relationship between the variable and the dependent variable (Agresti, 2015). The odds ratio will not be discussed at great lengths simply because I find the predicted probabilities to be more useful and accurate. In the third and last column the confidence intervals (i.e. 'C.I.') are presented. The C.I. are particularly useful because they represent the intervals where ~ 95 percentage of all samples would fall an infinite amount of samples were tested (Field, 2013). This allows for an increased statistical certainty and confidence when presenting the estimates. Interpreting the C.I. is in short, all about whether or not the C.I. is wide or narrow; if a C.I. contains more than a 1 (e.g. lower = 1.245; upper = 3.425; C.I. = 2.180) one should be concerned since it may not be statistically significant. In contrast, if a C.I. contains less than a value of 1, one can be fairly certain that the variable is statistically significant.

Table 1   **Binary Regression; N=2547**

Variable	B (S.E.)	Exp(B)	95% C.I. for Exp(B)	
			Lower	Upper
Internet Activity	0.391*** (0.106)	1.478	1.201	1.820
Motivation Film	0.282*** (0.046)	1.326	1.210	1.452
Motivation Music	0.025 (0.041)	1.025	0.946	1.110
Legal Alternatives Music (1)	-0.048 (0.134)	0.953	0.733	1.239
Legal Alternatives Film (1)	0.009 (0.127)	1.009	0.787	1.294
Knowledge	0.691*** (0.127)	1.995	1.637	2.431
Education	0.167** (0.053)	1.182	1.064	1.312
Sex (1)	-1.454*** (0.133)	0.234	0.180	0.303
Income	-0.116*** (0.032)	0.891	0.838	0.948
Age	-0.037*** (0.005)	0.963	0.955	0.972
Constant	3.167*** (0.578)	0.042		

*** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$
Source: The Swedes and the Internet 2016.
Comment: 'B' stands for b-coefficient. 'S.E.' stands for standard error. 'Exp' stands for exponential and represents' a math tool for calculating the odds ratio. 'C.I.' stands for confidence interval. The variables ending with '(1)' have had their indicator changed from last to first.

The focal relationship, i.e. the relationship between Internet activity and piracy is according to table 1 positive; supporting the idea that with an increased activity in the virtual world ones' likelihood of piracy is increased. In addition, the relationship is significant at the 0.001 level, thus reinforcing the reliability of the result since it is not a product of chance. The odds ratio

(i.e. (exp(0.391)-1)*100=47.8) indicate that the odds of committing piracy is increased by an average of 48 percentage for each increased step on the scale. Another way to interpret the odds is to interpret the equation SPSS performs for you in the second column; exp(0.391)=1.478, which tells me that one who is active is roughly 1.5 times more likely to commit piracy in comparison to someone who is inactive. The C.I. is narrow with a value of 0.619, thus indicating that the result is statistically significant.

Similarly, the relationship between piracy and motivation film, knowledge, education, sex, income and age all indicate a significant result. In contrast, the relationship between piracy and motivation music, legal alternatives music and legal alternatives film indicate an insignificant result. Although one could potentially argue for the theoretical relevance of the insignificant variables, when further inspecting the values of the b-coefficient, odds ratio and C.I. it is clear that the insignificant variables hold no significant sway over ones' tendencies for piracy.

The variables motivation film, knowledge and education indicate a positive relationship with piracy. The positive relationship reinforces the idea that ones' motivation and knowledge impact ones' tendencies for piracy. Further, the positive result of education contradicts the theory that higher education reduces ones' likelihood to commit illegal acts. On the contrary, it reinforces the idea that modern higher education requires the students to familiarize themselves with the virtual world; leading to an increased exposure and likelihood of piracy.

The variables sex, income and age indicate a negative relationship with piracy. Note that the sex variable had its indicator changed from last to first, i.e. males are coded as 0 and females as 1. At first glance, it may seem that the influence of income and age on ones' likelihood of piracy is miniscule. However, this is because of the vast scale used to report this information, for instance when calculating the odds ratio of the age variable the odds of committing piracy decreases by an average of 3.6 percentages for each aging year; which eventually amounts to a significantly diminished likelihood of piracy.

The C.I. of all the variables are within acceptable range, with the largest value being 0.794 (e.g. 'knowledge') and lowest value being 0.017 (e.g. 'age'). This is good news since this further strengthens the statistical significance of the results from the binary regression.

4.1.1 *Predicted probability*
The predicted probabilities can be either calculated by hand using the 'predicted probability'-formula (see appendix 2) or one can utilize SPSS to calculate the mean predicted probability for each categorical answer. For instance, the mean predicted probability of someone who answered 'No Internet activity whilst being at home' (coded as '0') have a probability of 0.0178 thus roughly ~ 1.78 percentage probability to commit piracy. In contrast, someone who answered 'Internet activity several times a day' have a probability of 0.2872 i.e. ~ 28.72 percentage probability. Based on this, I can conclude that the discreet difference of the focal independent variable 'Internet activity' is 26.94 percentages.

The motivation film variable proved to be one of the most influential variables in terms of increased probability. An avid film watcher (e.g. several times a day) has a probability of 63.95 percentage, whereas someone who does not watch at all has a probability of 7.23 percentage; thus resulting in the discreet difference of 56.72 percentages. Another influential variable is the respondents' self-reported knowledge of the virtual world. A person with low level of knowledge holds a probability of 1.7 percentages. In contrast, a person with a high level of knowledge has a probability of 40.5 percentages, thus resulting in the discreet difference of 38.8 percentages. Similarly, the discreet difference of sex is roughly ~ 21.87 percentages, thus reinforcing the idea that males are, on average, more probable to commit piracy.

As for the education variable, the results indicate that higher educated respondents are on average more probable to commit piracy. Although, there seemed to be stabilization of the probability around 20 to 23 percentages for categories 1 to 3, with the exception being the lowest educated group which had a probability of roughly 13 percentages.

When examining the results from the predicted probabilities of income, a spike of probability seemed to occur in the lowest income category; reporting a probability of 34.3 percentages. However, in all other income categories the probability was relatively stable around roughly 20 percentages; including the highest income category.

Further, when examining the predicted probabilities of age, I found that the most probable age group seems to be respondents between 18 and 28 years of age. All of which contained a probability of at least 40 or above percentages. 22 years of age stands out in particular with a predicted probability of 55.6 percentages. An interesting observation is that it is not until the respondents reaches the age of 60 plus years that the probability drops below 10 percentages, thus indicating that piracy may not be a typical youth crime but rather a crime that is performed throughout most ages, albeit at a diminished rate.

The predicted probability of the insignificant variables e.g. motivation music, legal alternatives music and legal alternatives film will not be reported here since the result is, due to the insignificant values, unreliable and thus misleading.

4.1.2 *Goodness of fit*

Now that the first binary regression and the initial interpretations have been presented, a bivariate correlation analysis can be carried out to further investigate the relationship between the dependent variable and the predicted probabilities generated in the regression. This test will showcase the strength and goodness of fit for the model. The correlation analysis generated a Pearson's-r value of 0.531** significant at the 0.01 level. As a general rule of thumb, a Pearson's-r value of lower than -0.3 or greater than 0.3 is considered a good result assuming, of course, that the correlation is significant and thus not the result of chance (Field, 2013). Having said that, the result from the correlation analysis indicate that the model used is of a good fit for measuring ones' tendencies of committing piracy.

Another way to test the models predictive power and goodness of fit is to perform a 'Receiver Operating Characteristic' (i.e. 'ROC') curve test. This test provides data regarding the models predictive power along with confidence intervals (Agresti, 2015). The ROC curve test of the model generated a value of 0.847*** that is significant at the 0.001 level. Basically, if the confidence interval contains a value of 0.5 or lower ones' model is problematic and there would be cause for concern whereas if the confidence interval contains a value of 0.7 ~ 0.8 or more one can feel reassured that their models predictive power is relevant for the study. This is good news since it further reinforces the validity and reliability of the model.

4.2 *Binary regression with interaction variable*

Based on the predicted probabilities examined in the first binary regression (*see table 1*) it is clear that the variables; Internet activity, motivation film and knowledge is particularly impactful when determining ones' probability for piracy. This is especially visible when measuring the discreet difference of these variables. With this in mind, I will add an interaction variable in the next binary regression consisting of these variables in an attempt to measure the combined effect of the most impactful variables.

The information presented in each column (e.g. column 1, 2 and 3) in table 2 is the same as the information presented in table 1. Additionally, in an attempt to avoid repetition, the interpretations of table 2 will primarily consist of changes caused by the interaction variable on the included variables as well as the interaction variable by and of itself. Note that when interpreting the interaction variable and the variables included within the interaction (e.g.

motivation film, knowledge and Internet activity) one should focus their attention towards changes in the significance of the b-coefficient, the odds ratios and lastly the C.I.

Table 2   **Binary regression with interaction variable; N=2547**

Variable	B (S.E.)	Exp(B)	95% C.I. for Exp(B)	
			Lower	Upper
Internet Activity	0.364*** (0.113)	1.438	1.152	1.795
Motivation Film	0.200 (0.041)	1.222	0.944	1.582
Motivation Music	0.024 (0.041)	1.024	0.945	1.109
Legal Alternatives Music (1)	-0.047 (0.134)	0.954	0.733	1.241
Legal Alternatives Film (1)	0.011 (0.127)	1.011	0.788	1.298
Knowledge	0.619*** (0.148)	1.857	1.390	2.480
Education	0.169** (0.054)	1.184	1.066	1.315
Sex (1)	-1.456*** (0.133)	0.233	0.180	0.302
Income	-0.115*** (0.032)	0.891	0.838	0.948
Age	-0.037*** (0.005)	0.963	0.955	0.972
Interaction	0.007 (0.011)	1.007	0.986	1.029
Constant	2.874*** (0.721)	0.056		

*** p < 0.001; ** p < 0.01; * p < 0.05
Source: The Swedes and the Internet 2016.
Comment: 'B' stands for b-coefficient. 'S.E.' stands for standard error. 'Exp' stands for exponential and represents' a math tool for calculating the odds ratio. 'C.I.' stands for confidence interval. The variables ending with '(1)' have had their indicator changed from last to first. The 'Interaction' variable represents the computed interaction of the variables; knowledge * motivation film * Internet activity.

First of all, the interaction variable is insignificant; this result indicates that the correlation between the focal relationships (e.g. Internet activity → piracy) is stronger than the relationship of the combined effect accumulated by the interaction variable (Fields, 2013). The value of the odds ratio (e.g. '1.007') further reinforces the idea that there is no significant relationship between the interaction variable and the piracy (Agresti, 2015). In addition, the C.I. of the interaction is narrow containing a value of 0.043; thus indicating that the result would, despite its insignificance, fall within this range 95 percentage of the time if I pulled an infinite amount of samples (Field, 2013).

The b-coefficient value of the variables Internet activity and knowledge remained significant at the 0.001 level. This indicates that the relationship these two variables have with piracy is stronger than the combined effect of the interaction variable. Although the values shifted slightly downwards for both, the change was close to miniscule. When examining the C.I., I noticed that knowledge contained a value of 1.090 which is an increase from the

previous value of 0.794. This change is particularly noteworthy because as stated above, if a C.I. contains more than a 1, one should be concerned. In this case, the C.I. does, albeit slightly, contain more than a 1. However, since the C.I. is only slightly above the 1 mark (i.e. 0.09 above), I interpret this to be of no significant concern. In contrast and somewhat surprisingly, the outcome of the third variable 'motivation film' indicates an insignificant b-coefficient value. This indicates that the combined effect of the interaction variable was in fact stronger than the effect of motivation.

Lastly, in regards to the predicted probabilities and goodness of fit; the model is essentially the same, thus producing the same predicted probability values and goodness of fit measurements as generated in the first binary regression. This is as expected since no brand new variable was added into the model, i.e. the interaction variable does not significantly change the measurements of the models overall usefulness and significance but rather illuminates some of the internal relationships in between the chosen independent variables.

4.3 *Highlights*
The first binary regression provided valuable data regarding each independent variable and its relationship with piracy. In particular, both variables measuring the use of legal alternatives were insignificant. Similarly, the music driven motivation variables also produced insignificant results. In contrast, all other variables, i.e. Internet activity, motivation film, knowledge, education, sex, income and age provided significant result and behaved more or less as expected. The focal relationship remained strong, although the variables motivation film and knowledge indicated a very strong correlation towards ones' tendencies for piracy; this was particularly clear when comparing the discreet difference in predicted probability.

In an attempt to illuminate the internal relationships and to further test the strength of the focal relationship an interaction variable was constructed containing three of the most impactful variables; knowledge, motivation film and Internet activity. The result from the second binary regression provided the study with valuable information regarding some of the more impactful variables relationships to each other and their combined effect. Nonetheless, the output indicated an insignificant value for the interaction variable, which in short means that the focal relationship is stronger than the accumulated effect of the interaction. Further, two of the included variables, i.e. Internet activity and knowledge remained significant with only slight changes in value. The third variable, i.e. motivation film indicate an insignificant relationship, it would thus seem as if ones' motivation is mediated by a number of factors, including but not limited to ones' level of knowledge and Internet activity.

5 Discussions
In the introduction of this study I posed the question; can piracy be compared to crimes like theft or is this cybercrime more complex than originally anticipated? Given that RAT was originally developed to explain common street crimes like theft (Cohen & Felson, 1979) the purpose and overarching goal of this study was to evaluate the efficiency of RAT when examining a similar crime within a virtual environment. The result suggests that, in order to adequately explain piracy one needs to include additional factors, thus indicating that piracy is more complex than traditional theft.

5.1 *RAT in binary waters*
The insignificance of motivation music was somewhat unexpected since music is historically one of the most pirated goods on the Internet (Ki et al., 2006). However, due to the increased accessibility of music on free legal websites like 'YouTube' it is possible that one would not need to resort to piracy in order to access the music that they seek. The 'easy access' may sway peoples' motivation to go the extra mile required to commit piracy. In contrast, films are

not as accessible, at least not in a similar free of charge fashion, which may increase peoples probability to commit piracy in order to access the films or TV shows. Although the initial result suggested that motivation film is a strong contributor of peoples' probability to commit piracy, the significance of this result decreased drastically when examined alongside the interaction variable.

The intentionally vague and broad 'non-definition' (e.g. it could be anything) of motivation presented in RAT is problematic. The oversimplified and vague description makes it usable in almost any situation. However, due to the oversimplified and vague description, the usefulness of RAT's motivation is limited and difficult to empirically measure. Although the combined effect of ability, activity and interest used in this study served its purpose, it would be reasonable to assume that if future studies were to work in symbiosis with a more tangible theory the practical relevance of RAT would increase substantially. That said, an example of such a theory is Wortley et al., (2008) 'theory of situational prompts, pressures, permissions and provocations'. The implementation of Wortley's et al., (2008) theory would likely improve the practical use considerably. In addition, this adaptation would ideally provide future empirical studies with a more practical approach to different aspects of situational motivation.

Even if I was not able to empirically test the effects of 'suitable targets' or 'capable guardians' (or the lack thereof) due to limitations in the material, the concepts are discussed from a theoretical standpoint; primarily illuminating some of the strengths or weaknesses that these concepts face when applied to a virtual setting. For instance, target suitability can typically be broken down into four essential parts represented by the VIVA-acronym; value, inertia, visibility and accessibility (Leukfeldt & Yar, 2016). Given that most of the physical limitations are more or less non-existent within the virtual world the suitability of a virtual target is primarily dependent on the subjective value, visibility and accessibility. Piracy websites (e.g. The Pirate Bay) have over the course of the last decade become 'virtual hotspot' for pirates to visit in order to access pirated material. These websites broadcast numerous targets on a global scale, thus advertising the suitable targets to the maximum amount of motivated offenders available at all times. In sum, the concept of suitable targets by RAT is, despite its fixation of physical restrictions, useful when theoretically analyzing suitability within a virtual environment.

Due to the global scale of piracy, the presence of capable guardians is very limited; formal guardians such as law enforcement struggle to keep up with the never ending surge of information. In contrast, informal guardians are, arguably better suited to fulfill the role of guardian. However, since piracy is a typical covert crime (Felson & Eckert, 2018) that is generally not viewed as morally reprehensible (Hinduja, 2007; Malin & Fowers, 2009) the efficiency of the informal guardians decrease drastically. It would thus seem that guardianship is limited by ones' level of insight, legal- and moral implications.

Having said that, the results of this study further suggests that the central core of RAT, i.e. the idea that criminal behaviour originates from peoples routines and activities are not without its merits. This core idea, opted through Internet activity, remained significant in the initial- and second binary regression. Thus, I feel the need to emphasize that while there is room for improvements, the core of RAT remains relevant.

5.2 *RAT and the importance of knowledge and education*
In line with previous findings by several studies (see Husted, 2000; Holt & Bossler, 2008; Choi, 2008; Pratt et al., 2010; Leukfeldt, 2014; Leukfeldt & Yar, 2016), the results indicate that the age span most likely to commit piracy fall within 18 to 28 years of age. However, based on the result it is apparent that a person's probability to commit piracy does not decrease drastically when crossing this 'most likely' threshold (i.e. above 28 years and

beyond). The results would further suggest that while the ages of 18 to 28 are amongst the most likely to perform this crime it would be counterproductive to claim that adjacent age groups are neither worthy nor relevant to include in ones' study, seeing as they too are highly probable to commit piracy. In consideration of the results it would seem as if piracy is more tied to the concept of generations than originally anticipated; in a sense that middle-aged people who were part of the earlier days of piracy remains active today (albeit at a somewhat decreased rate). The probability of the older generation contradicts previous conceptions of piracy as a typical youth related crime and it would therefore be interesting to examine this relationship further, perhaps tied to Jack Katz concept of 'sneaky thrills' (1988). In short, sneaky thrills are explained by Katz (1988) as a repeatable illegal act with little to no resistance (e.g. easy to carry out). The sneaky thrill is not driven by economic desires but rather as an outlet to experience something exciting; consequently, the offenders often experience a euphoric thrill if said crime is successful. Considering the ease and moral gray area of piracy, it is understandable if some individuals commit piracy in order to gain excitement in their everyday life.

The relationship between ones' sex and probability of piracy are consistent with previous findings (see Higgins & Makin, 2004; Liang & Yan, 2005; Felson & Eckert, 2018). Based on the result of this study, males are on average roughly ~ 22 percentages more probable to commit piracy than their female counterparts. The discreet difference in probability between males and females could potentially be explained by the difference in Internet activity on different technological devices; females are, on average, spending more of their Internet time on their smartphones whereas males spend less time on their smartphone and more on the computer (Davidsson & Findahl, 2016). Granted, it is not impossible to commit piracy on a smartphone. Nonetheless, it is reasonable to assume that piracy is a typical computer based crime due to the taxing amount of memory required to download certain files.

Contradictory to previous theoretical claims that a higher education generally reduces peoples tendency to commit immoral and illegal acts (Ki et al., 2006), the results suggest that piracy has the opposite effect; i.e. the probability to commit piracy actually increased with higher education. This result reinforces the idea that the digitalization and dependency of the virtual scene in modern education may lead to an unintentional increase in ability and exposure of the virtual society as a whole and thereof lead to increased opportunities for piracy.

The most unique contribution of this study is the impact of knowledge. The result suggests that piracy is gated behind a knowledge barrier, thus indicating that in order to commit this particular cybercrime a basic understand of the virtual world is more or less required; in part to navigate the virtual scene to find suitable targets but also to evade unwanted consequences. For instance, some users may take protective measurements like enabling a 'virtual private network' (i.e. 'VPN'). The VPN is in short, a tool that allows users from Sweden to appear as if they are in Brazil or somewhere else on the globe; this tool provides protection from any onlookers and further illustrates that cybercrime surpasses traditional geopolitical jurisdictions. The importance of knowledge should thus not be underestimated. However, it is important to note that while individual knowledge is important; the virtual hotspots, i.e. piracy websites, wants to distribute the pirated goods and as a result they are constantly making adjustments to increase their user-friendliness, thus bridging the gap and reducing the knowledge required to partake in the pirated goods.

The results also suggest that ones' yearly household income does not significantly impact ones' probability to commit piracy, although the absolute lowest income category was an exception. When examining the results, I found that while the lowest income category held a probability of roughly 30 percentages all the other categories (including the very highest

income category) held a probability of roughly 20 percentages on average. The widespread use of piracy in all income categories indicate that piracy may be more related to white-collar crime than previously anticipated. The term 'white-collar' originates from Edwin H. Sutherland's presidential address from 1940. In short, Sutherland highlighted criminal behaviour patterns amongst individuals' part of the upper-levels of society and since the result suggests that individuals of all income levels commit piracy at similar rates, it would be beneficial to include elements of white-collar crime in future studies.

5.3 *Study limitations*

The limitations of this study are primarily related to the chosen material and method. As mentioned, the goal of SOI is to map, review and present reliable statistics of the Swedish populations Internet habits; it is thus not a survey specifically developed to measure the sensitive subject of cybercrimes. Although, SOI does ask the respondents about their piracy habits, most previous studies tend to use an array of questions where they identify the respondents' attitudes and intentions towards piracy in different scenarios (see Higgins & Makin, 2004; Holt & Bossler, 2008; Choi, 2008; Malin & Fowers, 2009; Pratt et al., 2010; Leukfeldt, 2014). Even if the results are significantly large enough to perform this study, it would be fair to say that if an array of questions were used, the percentage of pirates would increase. Similar limitations tied to the different purpose and overarching goal of the SOI and this study include; measurements of motivation, the suitability of the virtual targets and impact of capable guardians. Despite these limitations, the findings of this study remain significant and more importantly, provides the criminological field with new information regarding the relationship between piracy and the included independent variables.

Furthermore, binary logistic regression is not without its faults. One of the most obvious drawbacks is that the output and thus result is presented in the form of odds and probabilities (Field, 2013). This may be problematic since the results may seem more abstract and vague in comparison with the more confident presentation of other methods. However, one could argue that there is value in the abstract presentation of results in binary logistic regression because it does not necessarily lead to the stigmatization of certain behaviour patterns. For instance, even if an individual is very likely to commit piracy due to their behaviour patterns, it is not guaranteed that they will commit piracy. This gentle approach is in my opinion an asset that is particularly useful within the social sciences since we are, after all, analysing unpredictable human behaviour.

5.3 *Future research*

This study has shed light on some of the strengths and weaknesses of the traditional criminology theory RAT when applied to the cybercrime piracy. More importantly, the results from this study contradict the stereotypical image of the 'pirate', thus identifying previous conceptions as misleading or even false. The contributions of this study could be explored further in a larger study; preferably with material more in line with the core concepts of RAT and noteworthy contributions. This rings especially true for the concepts 'suitable targets' and 'capable guardians' since I was not able to empirically test these concepts in this study due to limitations with the chosen material.

Considering the rate of advancement in technology and digital dependency by modern society it is very likely that cybercrimes will continue to increase and evolve. Therefore, it is crucial that the criminological field dedicate time and funding to further examine and explain human behaviour in this abstract virtual world. Even though there has been an increased interest in cybercrimes and cyberspace in general over the past decade, criminology and the social sciences still has much to learn about human behaviour in a virtual context.

Acknowledgments

References

Akers, R. L. (1977). Deviant behavior: A social learning approach.

Agresti, A. (2015). Foundations of linear and generalized linear models. John Wiley & Sons.

Britz, M. T. (2009). Computer Forensics and Cyber Crime: An Introduction, 2/E. Pearson Education India.

Bhattacharjee, S., Gopal, R., & Sanders, G. (2003). Digital music and online sharing: Software piracy 2.0? *Communications of the ACM, 46*(7), 107-111.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies*, *16*, 41-96.

Davidsson, P., & Findahl, O. (2016). *Svenskar och Internet 2016*. Internetstiftelsen i Sverige.

Edick, C. (2015). The golden age of piracy: Can open-source democracy redefine citizenship for the internet age? *Harvard International Review, 36*(4), 7-9.

Felson, M., & Eckert, M. (2018). Introductory criminology: The study of risky situations (1st ed.).

Ferraresso, R., Porter, Jeremy, Sung, Hung-En, & Trimbur, Lucia. (2016). Gender Roles, Social Control and Digital Piracy: A Longitudinal Analysis of Gender Differences in Software Piracy among Korean Adolescents,ProQuest Dissertations and Theses.

Field, Andy (2013) *Discovering Statistics Using IBM SPSS Statistics*. London: Sage Publications Ltd (916 pages) (4th edition)

Greene, William H. 2012. *Econometric analysis*. Boston: Pearson.

Golafshani, Nahid. (2003). Understanding reliability and validity in qualitative research. (Report). *The Qualitative Report, 8*(4), 597-606.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Gunter, W. (2008). Piracy on the High Speeds: A Test of Social Learning Theory on Digital Piracy among College Students. *International Journal of Criminal Justice Sciences, 3*(1), 54-68.

Holt, T., & Bossler, A. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior,30*(1), 1-25.

Holt, Thomas J, Reyns, Bradford W, Henson, Billy, & Fisher, Bonnie S. (2016). Guardians of the Cyber Galaxy. *Journal of Contemporary Criminal Justice, 32*(2), 148-168.

Higgins, G. E., & Makin, D. A. (2004). Self-control, deviant peers, and software piracy. *Psychological reports*, *95*(3), 921-931.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. Ethics and Information Technology, 9(3), 187-204.

Hinduja, S., & Ingram, J. (2009). Social learning theory and music piracy: The differential role of online and offline peer influences. *Criminal Justice Studies, 22*(4), 405-420.

Husted, B. (2000). The Impact of National Culture on Software Piracy. *Journal of Business Ethics, 26*(3), 197-211.

Kaplan, H., O'Kane, K., Lavrakas, P. J., & Hoover, S. (1978). *CPTED Final report on commercial demonstration in Portland, Oregon* [Mimeo]. Arlington, VA: Westinghouse Electric.

Leukfeldt, E., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280.

Leukfeldt, E. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Liang, Z., & Yan, Z. (2005). Software piracy among college students: A comprehensive review of contributing factors, underlying processes, and tackling strategies. *Journal of Educational Computing Research*, *33*(2), 115-140.

Long, J. S. (1997). *Regression Models for Categorical and Limited Dependent Variables*. Advanced Quantitative Techniques in the Social Sciences Series. London: Sage Publications (7th edition)

Malin, J., & Fowers, B. J. (2009). Adolescent self-control and music and movie piracy. *Computers in Human Behavior, 25*(3), 718-722.

Moon, Byongook, Mccluskey, John D., & Mccluskey, Cynthia Perez. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice, 38*(4), 767-772.

Morris, R. G., & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. Journal of Criminal Justice, 38(4), 470-480.

McQuade III, S. (2011). Cybercrime. *The Oxford Handbook of Crime and Public Policy,* The Oxford Handbook of Crime and Public Policy.

Newman G.R. (2009) Cybercrime. In: Krohn M., Lizotte A., Hall G. (eds) Handbook on Crime and Deviance. Handbooks of Sociology and Social Research. Springer, New York, NY.

Katz, J. (1988). Seductions of crime: Moral and sensual attractions in doing evil.

Ki, E., Chang, B., & Khang, H. (2006). Exploring Influential Factors on Music Piracy Across Countries. *Journal of Communication, 56*(2), 406-426.

Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *The Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Paynich, R., & Hill, B. (2010). *Fundamentals of crime mapping*. Sudbury, Mass.: Jones and Bartlett.

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, *23*(1), 37-51.

Sinha, R. K., & Mandel, N. (2008). Preventing digital music piracy: the carrot or the stick?. *Journal of Marketing*, *72*(1), 1-15.

Smallridge, J. L., & Roberts, J. R. (2013). Crime specific neutralizations: An empirical examination of four types of digital piracy. *International Journal of Cyber Criminology, 7*(2), 125-140.

Sutherland, E. H. (1940). White-collar criminality. *American sociological review*, *5*(1), 1-12.

Yar, M. (2005). The Novelty of 'Cybercrime'. *European Journal of Criminology, 2*(4), 407-427.

Waldfogel, J. (2012). Copyright Research in the Digital Age: Moving from Piracy to the Supply of New Products. *American Economic Review,102*(3), 337-342.

Wortley, R., Mazerolle, L., & Ebooks Corporation. (2008). *Environmental criminology and crime analysis.* (Crime Science Series). Cullompton: Willan Publishing.

Table 3   **Variable questions**

Variable	*Question Code*	*Information about all questions:*
Piracy	V73L	https://www.iis.se/docs/SOI2016vux.pdf
Internet Activity	V43A2	
Motivation Film	Q224_1	
Motivation Music	Q221_1	
Legal Alternatives Music (1)	V86C3B	
Legal Alternatives Film (1)	V86C3C	
Knowledge	V40A	
Education	Q27	
Sex (1)	Q25	
Income	Q28	
Age	Q26	

Appendix 2

Formula 1 **Predicted probability**

$$\frac{e^{\alpha + \beta 1 x1 + \beta 2 x2 + ... + \beta k xk}}{1 + e^{\alpha + \beta 1 x1 + \beta 2 x2 + ... + \beta k xk}}$$