Cyber-offenders versus traditional offenders

An empirical comparison

Marleen Weulen Kranenburg
Chapter 5

Cybercrime versus traditional crime: empirical evidence for clusters of offences and related motivations*

* This chapter was submitted as: Weulen Kranenburg, M. (under review). Cybercrime versus traditional crime: empirical evidence for clusters of offenses and related motivations.
Abstract

Cybercriminal opportunities are increasing, but it is unknown to what extent the rise in these opportunities has resulted in distinctly different types of offenders with different motivations. In this study this question will be addressed by examining to what extent cyber-dependent offenders can be distinguished from traditional offenders, and identifying clusters of cyber-offences and traditional offences. In addition, it will be explored which motivations for offending the offenders provide and to what extent a specific cluster distinguishes itself from the other clusters by specific motivations. The analyses will be based on a survey among a high risk sample of adult cyber-offenders and traditional offenders (N = 508) registered by the Dutch public prosecutors' office. The principal component analysis identified seven clusters of crimes, four clusters that include only cybercrimes and three clusters that only include traditional crimes. This indicates that cyber-offenders can be distinguished from traditional offenders. In addition, cybercrimes can be distinguished from traditional crimes by almost all motivations. The cybercrimes are mostly committed out of intrinsic motivations, which means that committing the crime is in itself rewarding. Financial motivations are almost absent for cybercrime. Differences between cybercrime clusters are mainly found in extrinsic motivations, the extent to which the external consequences of committing a crime are rewarding. The results will be compared to the existing theoretical and limited empirical literature on cybercrime.

Keywords
cyber-dependent crime motivations,
cybercrime clusters traditional crime clusters comparison
5.1 Introduction

The prevalence of cyber-dependent crimes\(^1\) (for a detailed description of these crimes, see next section) is increasing (e.g., Grabosky, 2017; White, 2013) and it has been claimed that more and more cyber-offenders started to commit these crimes for financial gain, while increasingly less offenders commit them out of intrinsic motivations, driven by internal rewards (e.g., Chan & Wang, 2015; Grabosky, 2017; Holt & Kilger, 2012; Kshetri, 2009; Provos, Rajab, & Mavrommatis, 2009; Smith, 2015; White, 2013). These claims, however, are mostly based on the observation that opportunities for financial cybercrime have increased. Empirical offender-based studies on the relative importance of different motivations for cyber-dependent offending are almost absent. Similarly, it is unknown to what extent the increase in cybercriminal opportunities has resulted in distinctly different types of offenders with different motivations. Nevertheless, while cyber-offenders could theoretically be very different from traditional offenders, the existing empirical literature has focused on either cyber-offenders or traditional offenders, without comparing them. Lastly, for cyber-offenders the theoretical literature has indicated some offender typologies based on skills and motivations, but empirical evidence for these is also lacking.

In this study, these gaps in the literature will be addressed, first by examining to what extent cyber-dependent offenders can be distinguished from traditional offenders, and analysing which clusters of cyber-offences and traditional offences are generally committed by the same offenders. Second, it will be explored which motivations for offending the offenders provide and to what extent the clusters can be distinguished from the others by these motivations. The analyses will be based on data from a survey among adult cyber-offenders and traditional offenders (N = 508) registered by the Dutch public prosecutors’ office.

5.1.1 Cyber-dependent crime

Different names and definitions for cybercrime are used in the literature, but in general a distinction is made between cyber-enabled and cyber-dependent crime (e.g., Furnell, 2002; Gordon & Ford, 2006; McGuire & Dowling, 2013; Wall, 2001; Zhang et al., 2012). Cyber-enabled crime refers to traditional crime in which Information Technology (IT) is used in the commission of the crime, for example, online fraud, stalking, harassment, and so on. This study, however, focuses on cyber-dependent crime, for example, hacking, web defacement, malware use.

---

\(^1\) In this paper ‘cyber-dependent crime’ and ‘cybercrime’ will be used interchangeably to refer to these crimes.
and so on. These crimes cannot be committed without using IT, and therefore are theoretically very different from all other crimes. IT is the key element, as these crimes completely take place in a digital context and require IT-skills. It is unclear to what extent cyber-dependent offending can empirically be distinguished from all other types of offending. Offenders may combine cyber-offences and traditional offences, as some have argued that offenders combine different types of cybercrime or cybercrimes and traditional crimes, because those crimes can be part of a sequence of crimes, that are part of one modus operandi (Alleyne, 2011; Stephenson & Walter, 2012).

Some hypothetical distinctions within the overall category of cyber-dependent crimes have also been described. These distinctions are usually based on the way these crimes are committed. McGuire and Dowling (2013), for example, distinguished intrusions into computer networks (i.e., hacking), disruption or downgrading of computer functionality and network spaces (i.e., malware and denial-of-service (DoS) attacks), and spamming. These could all be further used for other means like stealing personal data. Hacking could additionally be used for defacing websites or as the start of a DoS attack, for example. Similarly, malware could be used for deleting files or crashing systems. In contrast, Kirwan and Power (2013) described infiltration, defacements, and DoS attacks as types of hacking, but malware as a different category. They theorised that malware is a form of vandalism, with motivations similar to traditional vandalism. Limited empirical evidence for such distinctions has been found in interviews with hacker conference attendees, which have indicated that phishers, spammers and virus coders are different from hackers (Bachmann & Corzine, 2010).

5.1.2 Typologies of hypothetical offenders and motivations
In addition to the hypothetical offence clusters that are based on the way crimes are committed, discussed above, some theoretical literature has distinguished hypothetical types of offenders based on their perceived motivations and skills. Most of this literature is about hackers (e.g., Alleyne, 2011; Dalal & Sharma, 2007; Kilger, Arkin, & Stutzman, 2004; Kirwan & Power, 2013; Rogers, 2000, 2006), but some articles also include other types of cyber-offenders (e.g., Furnell, 2002; Ibrahim, 2016; Nykodym et al., 2005; Parker, 1983; Wall, 2001). The hacker taxonomy of Rogers (2000, 2006) is well known and often cited. Rogers identified nine hypothetical hacker categories based on skill level and motivation (i.e., revenge, financial, curiosity, notoriety). He argued that this model can be used to show interactions and relative importance of motivations for different types of hackers and show progression of skill and motivation over time.
As Morris (2011) showed, the literature on offender categories and motivations discussed above is largely based on assumptions and anecdotal evidence. Empirical evidence for different types of cyber-offenders and their motivations is almost non-existent. The assumed motivations are generally based on the outcome of a crime. For example, if the victim suffers financial loss, the offender is often assumed to be motivated by financial gain (e.g., Kilger, 2011; Kilger et al., 2004; Leukfeldt, Lavorgna, & Kleemans, 2016; McGuire & Dowling, 2013; Randazzo et al., 2005; Tcherni et al., 2016). However, even if a crime causes financial loss, it may be motivated by other factors such as revenge and multiple motivations may underlie involvement in the attack (e.g., Holt & Kilger, 2012; National Cyber Security Centre, 2016; Rogers, 2006; Seebruck, 2015). Therefore, it can be more informative to study the different criminal offences that are generally committed by the same offenders and identify to what extent different motivations play a role in those offences.

When combining the existing theoretical literature (e.g., Chan & Wang, 2015; Chiesa, Ducci, & Ciappi, 2008d; Grabosky, 2017; Holt & Kilger, 2012; Kshetri, 2009; Provos et al., 2009; Smith, 2015; White, 2013), it could be concluded that intrinsic motivations are most important for cybercrime, while extrinsic motivations are less important, and financial motivations are argued to be becoming more important. For intrinsically motivated crimes, committing the crime is in itself rewarding. Intrinsic motivations are, for example, learning something from hacking into an IT-system, or acting out of curiosity, for the challenge, because it feels good, or to see how far one can go in misusing a system. Extrinsic motivations are committed because the external consequences of committing that crime are rewarding. Extrinsic motivations are, for example, impressing others, delivering a message, wilfully damaging something that belongs to somebody else, or when you act out of revenge, anger or to bully someone. In comparison to traditional crime, Grabosky (2000, 2001) and Grabosky and Walkley (2007) claimed that most motivations for committing crimes are similar, but the intellectual challenge of defeating a complex system is probably unique for cybercrime. Nevertheless, empirical evidence on the extent to which these different or similar motivations are important and prevalent is scarce.

5.1.3 Empirical evidence on motivations

The limited empirical work done so far mostly focused on identifying all possible motivations for cyber-offending. In the Hacker Profiling Project (Chiesa et al., 2008a), for example, it was found that the worldwide online survey data of 216 hackers could identify different types of criminal hackers, that were also identified in the theoretical literature, with the following motivations: curiosity, learning,
selfishness, anger, it is the in thing to do, media attention, prove power, financial gain. A decade before this project, Taylor (1999) already interviewed hackers\(^2\) and identified six motivations: feelings of addiction, urge of curiosity, boredom with the educational system, feelings of power, peer recognition, and political acts. In one way or another, these are the motivations that are identified in the existing theoretical and empirical literature.

In line with the theoretical literature, there is empirical evidence for the relative importance of intrinsic motivations. Holt (2007), for example, showed in interviews and analyses of hacker forums that most hackers have a desire to learn and act out of curiosity. Similarly, studies showed that some hackers keep looking for new challenges. Their motivation is based on breaking a tougher system every time, thereby improving their skills (e.g., VoiskOUNsky & Smyslova, 2003; Woo, 2003).

Nevertheless, some types of cybercrime seem to be mostly intrinsically motivated while others are not. For example, Gordon and Ma (2003) compared their sample of criminal hackers to their previous work on malware writers and found that while most hackers are self-motivated and self-centred, virus writers are mostly motivated by peer recognition. In research on DoS attacks and web defacements, content analyses identified hacktivism, religiously motivated offenders or other types of motivation in which the offender tries to make a statement or deliver a message (Denning, 2011; Holt, 2009b). But, in contrast, in their analyses of web defacements, Woo et al. (2004) showed that only a few are politically motivated, as the majority are just simple pranks.

In addition to intrinsic motivations, some literature has suggested the importance of impressing others. On online forums, for example, hackers may gain status and respect (e.g., Holt, 2007; Nycyk, 2010). However, as these studies are based on forum posts they only reflect the perceived motivations of people who actually post on these forums. In addition, it is possible that the social status is not the initial motivation for offending, but only a motivation to talk about it on a forum afterwards (Jordan & Taylor, 1998). For example, Woo (2003) showed that intrinsic and extrinsic motivations are not mutually exclusive. While hacking may be intrinsically rewarding, the status that a hacker receives as a result of it is extrinsic. Yet, the intrinsic motivation was the initial motivation. Similarly, based on a literature review, and debriefs with young cyber-offenders known to the National Crime Agency of the United Kingdom, the NCA concluded that the challenge and

---

\(^2\) It should be noted that not all literature about hackers is necessarily only about offenders. Hacking can be part of a completely legitimate profession.
accomplishment of cyber-offending is the main motive, but proving oneself to peers was important (National Crime Agency, 2017a, 2017b). In that study, financial gain was generally not a motive or only a secondary motive.

In 1999, financial motivations were not identified by Taylor (1999), but more recent studies too indicate that hacking is rarely committed for financial gain (Holt & Kilger, 2012; Turgeman-Goldschmidt, 2008). There have been studies based on Dutch criminal case files about the increase of financial motivations, but those yielded contradictory conclusions. A report of the Dutch police (Bernaards, Monsma, & Zinn, 2012), for example, showed that challenge or status is no longer an important motivation, while financial motivation is, in addition to ‘delivering a message’ through hacking or DoS attacks, and simple fun. In contrast, Leukfeldt et al. (2013) could not verify the shift from ‘hacking for fame’ to ‘hacking for fortune’. Some commit it for profit, but revenge and curiosity were important motivations as well. They argued that this is because nowadays hacking could be committed by everyone and as a result more general motivations like revenge are getting more important. In contrast, based on interviews with Israeli hackers Turgeman-Goldschmidt (2008) argued that most hackers have a not-for-profit motivation and this will not change even given the fact that the nature of cybercrime constantly changes. In addition, some empirical evidence has suggested that young offenders are mostly intrinsically motivated, while later in their career most older offenders shift to committing crimes for financial gain (Bachmann, 2011; Bachmann & Corzine, 2010; Xu et al., 2013), although the opposite has also been found (Fotinger & Ziegler, 2004).

### 5.1.4 Justifications or neutralisations

It should be clear that examining motivations after a crime is committed is to some extent asking the offender’s justification for offending (e.g., Bernasco, 2010b; Taylor, 1999; Yar, 2005b, 2013b). In retrospect it is not possible to reliably identify the motivations at the moment the crime was committed. Therefore, it is worth mentioning research on neutralisation techniques (Sykes & Matza, 1957) and justifications. Some neutralisation techniques that have been found among cyber-offenders are denial of victim (e.g., Morris, 2011; Turgeman-Goldschmidt, 2009), denial of injury (e.g., Chua & Holt, 2016; Morris, 2011; Turgeman-Goldschmidt, 2009), denial of responsibility (e.g., Chua & Holt, 2016; Hutchings & Clayton, 2016) and condemnation of the condemners (e.g., Turgeman-Goldschmidt, 2009). These seem to indicate that the digital context of cybercrimes makes it easy to deny the impact of a crime, as the consequences are not directly observable.
More useful in relation to motivations, however, may be that Turgeman-Goldschmidt (2009) found that most interviewed Israeli hackers also appeal to higher loyalties and self-fulfilment, which means they say to have committed the crimes because they want to keep learning and because they want to do the impossible. This is in line with the more intrinsic motivations mentioned in the literature as well. Based on the same interviews, Turgeman-Goldschmidt (2011) also argued that hackers cannot be compared to white-collar offenders as they generally do not commit their crimes for financial gain or out of extrinsic motivations or neutralisations. Appeals to higher loyalties have also been found among malware users (Chua & Holt, 2016) and booters (Hutchings & Clayton, 2016), who generally also say they do not provide their services for financial gain. Similarly, 127 criminal hackers who were interviewed at Defcon say they believe their actions serve a higher goal and improve security (R. Young et al., 2007).

5.1.5 The current study
With survey data of adult cyber-dependent offenders and traditional offenders (N = 508) registered by the Dutch public prosecutors’ office, this study addresses two research questions. First, it will be examined which clusters of crimes can be identified empirically, by studying which self-reported crimes are often committed by the same offender and to what extent cyber-dependent offending co-occurs with traditional offending. Second, it will be examined which motivations or justifications the offenders provide for the different crime clusters and by which motivations the crime clusters can be distinguished from the others. The goal of this paper is not to identify new motivations, but to build on the motivations that have already been identified in the literature and examine to what extent these motivations are related to the different cybercrime clusters that can be identified among a known offender population.

This study thereby contributes to the literature by, first, empirically assessing assumptions about the co-occurrence of different types of cyber-dependent crime and traditional crime and comparing different clusters of cybercrime with traditional crime clusters on the motivations provided by offenders. Second, it will address an understudied population of adult offenders in the Netherlands, which will shed light on the motivations of cyber-offenders who have been in contact with the justice system in the past.
5.2 Data and methods

5.2.1 Sample and procedure
The 2000-2013 Public Prosecutor's Office's database was used to select all 1,100 suspects of cyber-dependent crimes in that period and a random sample of 1,127 traditional suspects. Suspects of cyber-dependent crime were oversampled in order to include a maximal number of this type of offences in the sample, and thus to maximise the amount of variation in measured crime types. A purely random sample would likely not have resulted in a sufficient number of cyber-offenders. It should be stressed that this procedure does not affect the results of regression and principal component analysis outcomes. It should further be noted that both cyber-dependent and traditional suspects received the same survey and were asked to self-report on both their cyber-offending and traditional offending. Thus, both groups could self-report both types of crime.

The 928 cybercrime suspects and 875 traditional suspects who had a valid mailing address and had not passed away, received an invitation letter in the summer of 2015 for participation in an online survey. The letter included a web link and unique password, information on the 50 euro incentive voucher for full participation, the scope and content of the survey, and the option to complete the survey on paper or through a Tor Hidden Service Website. Further details on selection procedure, confidentiality, and a consent form were provided on the first page of the survey.

The aim was to have equal samples of cybercrime and traditional suspects, but response rates were higher in the cybercrime sample. Therefore, only traditional sample respondents received reminder letters after two and four weeks. After six weeks 268 cybercrime suspects (28.88%) and 141 traditional suspects (16.11%) had completed the full survey. To increase the number of traditional suspects in the sample, exactly the same procedure was used to invite a new random sample of 781 traditional suspects. After another six weeks 268 cybercrime suspects (28.88% response rate) and 270 traditional suspects (16.30% response rate) completed all questions relevant for this paper.

---

3 Communication with this type of website is completely encrypted and less easy to trace. Three traditional sample respondents completed the survey on paper and three cybercrime sample respondents completed it through the Tor Hidden Service website.
5.2.2 Measures

Self-reported offending

Dichotomous variables were created based on self-report questions about thirteen cyber-dependent crimes and eleven traditional crimes (1 = committed the crime at least once in preceding twelve months). Cybercrime questions were based on the Dutch National Cyber Security Centre (2012) list of cyber-dependent crime and the Computer Crime Index of Rogers (2001) and included: guessing passwords, other hacking, digital theft, damaging data, defacing websites or online profiles, phishing, DoS attacks, spamming, taking control over IT-systems, intercepting communication, malware use or distribution, selling data, and selling credentials. Traditional offences were based on Svensson et al. (2013) and Dutch criminal law and included: vandalism, burglary, carrying a weapon, using a weapon, stealing, threats, violence, selling drugs, tax fraud, insurance fraud, and buying or selling stolen goods.

Motivation

For each different crime reported by a respondent, respondents were asked to indicate on a 5-point scale (totally disagree - totally agree) about nine motivations which were applicable the last time they committed that crime. These nine motivations were based on both theoretical and empirical literature and included four intrinsic motivations, four extrinsic motivations and financial motivation. Intrinsic motivations (IM) were: ‘boredom / curiosity / excitement’ (IM1), ‘fun / felt good’ (IM2), ‘challenging / educational’ (IM3), and ‘see how far I could go’ (IM4). Extrinsic motivations (EM) were: ‘damage something’ (EM1), ‘revenge / anger / to bully’ (EM2), ‘put things straight / deliver a message’ (EM3), and ‘impress others / gain power’ (EM4). Financial motivation (FM) was formulated as ‘to earn something with it’. In the analyses dichotomous variables (1 = agree) indicate if the respondent agreed or totally agreed that a motivation was applicable when committing the crime.

5.2.3 Analytical strategy

Thirty of the respondents had missing values on one or more of the offending variables (5.58%) and were excluded from the analyses. For the first research question, the remaining sample (N = 508; 77.95% male; \( M_{\text{age}} = 37.16 \) years) was used for the principal component analysis in which it was examined which clusters of crimes were present in the data. Based on the highest factor loading in the pattern matrix, each crime type was assigned to one of the crime clusters.

For the second research question, only respondents who self-reported at least one crime (N = 153) were used in the analyses on motivations. Together these respondents committed 420 different offences (on average 2.75 per offender). Coincidently
exactly half of these were traditional crimes and half were cybercrimes. As offenders could indicate for each different crime which motivations were applicable, each offender-crime combination was analysed as a different observation, while correcting for intra-individual correlation by using clustered analyses. After inspecting prevalence rates of different motivations per crime cluster, multivariate probit models with each motivation were used to examine which crime clusters were statistically significantly different from each other in the extent to which the motivation played a role in committing those crimes. Estimating nine separate models for each motivation would result in stochastically dependent estimates for the different crime clusters, therefore multivariate probit models were used (for STATA, see Cappellari & Jenkins, 2003) to gain efficient parameter estimates that are not stochastically dependent.

5.3 Results

5.3.1 Offending clusters

The principal component analysis with oblique rotation indicated seven factors with an eigenvalue above one. Based on the highest factor loading in the rotated pattern matrix in Appendix A, all crimes were assigned to one of the seven crime clusters\(^4\). The clusters and their prevalence rates are summarised in Table 5.1. It shows that there is a distinction between cyber-offending and traditional offending, as the analyses indicated four clusters that included only cyber-dependent crimes and three clusters that included only traditional crimes. No cluster included both cybercrime and traditional crime.

The cybercrime clusters seem to be based on crimes that are functionally related as they can be part of the same modus operandi and/or crimes that require a similar environment or skill set. For example, for hacking and related crimes (C1), you first have to hack into a system to steal data from it. Similarly, before you intercept communication, you need to take control over an IT-system (C3) and you can use malware to steal data and credentials that you can sell (C4). The internet related offences ($\chi^2$) generally take place by using the internet, while the other crimes are more based on IT-systems, hence the internet-related crimes share an environment and skill set. In line with Bachmann and Corzine (2010) this indicates differences between phishers, spammers, virus coders, and hackers.

\(^4\) It should be noted that some crimes also load on another cluster, as they have another factor loading above 0.30. For clarity of the interpretation and the further analyses on motivations, the highest factor loading is used to assign each crime to only one cluster.
Table 5.1.
Prevalence rates of crime clusters and underlying offences in sample

<table>
<thead>
<tr>
<th>Cybercrime</th>
<th>N</th>
<th>% 1</th>
<th>Traditional crime</th>
<th>N</th>
<th>% 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guessing password</td>
<td>30</td>
<td>7.14</td>
<td>Tax fraud</td>
<td>35</td>
<td>8.33</td>
</tr>
<tr>
<td>Digital theft</td>
<td>27</td>
<td>6.43</td>
<td>Stolen goods</td>
<td>22</td>
<td>5.24</td>
</tr>
<tr>
<td>Hacking</td>
<td>24</td>
<td>5.71</td>
<td>Insurance fraud</td>
<td>15</td>
<td>3.57</td>
</tr>
<tr>
<td>Damaging data</td>
<td>20</td>
<td>4.76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C1: Total hacking and related</strong></td>
<td>101</td>
<td>24.05</td>
<td><strong>T1: Total white-collar</strong></td>
<td>72</td>
<td>17.14</td>
</tr>
<tr>
<td>Defacing</td>
<td>30</td>
<td>7.14</td>
<td>Vandalism</td>
<td>19</td>
<td>4.52</td>
</tr>
<tr>
<td>Phishing</td>
<td>15</td>
<td>3.57</td>
<td>Burglary</td>
<td>6</td>
<td>1.43</td>
</tr>
<tr>
<td>DoS</td>
<td>8</td>
<td>1.90</td>
<td>Using a weapon</td>
<td>5</td>
<td>1.19</td>
</tr>
<tr>
<td>Spam</td>
<td>5</td>
<td>1.19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C2: Total internet related</strong></td>
<td>58</td>
<td>13.81</td>
<td><strong>T2: Total vandalism</strong></td>
<td>30</td>
<td>7.14</td>
</tr>
<tr>
<td>Taking control</td>
<td>19</td>
<td>4.52</td>
<td>Stealing</td>
<td>26</td>
<td>6.19</td>
</tr>
<tr>
<td>Intercepting communication</td>
<td>11</td>
<td>2.62</td>
<td>Threats</td>
<td>24</td>
<td>5.71</td>
</tr>
<tr>
<td><strong>C3: Total control over IT-systems</strong></td>
<td>30</td>
<td>7.14</td>
<td>Violence</td>
<td>23</td>
<td>5.48</td>
</tr>
<tr>
<td>Malware use or distribution</td>
<td>11</td>
<td>2.62</td>
<td>Carry a weapon</td>
<td>20</td>
<td>4.76</td>
</tr>
<tr>
<td>Selling data</td>
<td>6</td>
<td>1.43</td>
<td>Selling drugs</td>
<td>15</td>
<td>3.57</td>
</tr>
<tr>
<td>Selling credentials</td>
<td>4</td>
<td>0.95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C4: Total malware and selling</strong></td>
<td>21</td>
<td>5.00</td>
<td><strong>T3: Total criminal life-style</strong></td>
<td>108</td>
<td>25.71</td>
</tr>
<tr>
<td>Total number of crimes (both cybercrime and traditional crime)</td>
<td>420</td>
<td>100.00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1: percentage of total number of crimes

For traditional crime, crimes in the first cluster are white-collar crimes (T1). The second cluster mainly includes vandalism, but also burglary and using a weapon. These are the least common crimes and only three of these offenders did not commit vandalism. Hence, it is called vandalism (T2). The third cluster is a mix of crimes that often occur in a criminal life-style (T3).

5.3.2 Motivations

Each time the prevalence rates of motivations by crime cluster are discussed in the following sections, these rates can be found in Table 5.2 The documentation on the significance of differences in motivations between clusters can be found in Appendix B.
**Intrinsic motivations cybercrime**

In line with most literature, the prevalence rates (Table 5.2) indicate that for all cybercrime clusters intrinsic motivations are most important. ‘Boredom / curiosity / excitement’ (IM1) is the most prevalent motivation for all cybercrime clusters. ‘Challenging / educational’ (IM3) is just as often indicated as a motivation for control over IT-systems (C3). That is also an important motivation for hacking and related crimes (C1), while ‘fun / felt good’ (IM2) is the second most important motivation for internet related crimes (C2) and malware and selling (C4). The comparison models (Appendix B) show only two statistically significant differences in intrinsic motivations. First, when comparing hacking and related crimes (C1) to internet related crimes (C2) offenders more often (marginally significant) indicate ‘boredom / curiosity / excitement’ (IM1). Second, for malware and selling (C4) compared to control over IT-systems (C3) offenders more often indicate ‘fun / felt good’ (IM2).

**Table 5.2.**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N</td>
<td>%¹</td>
<td>N</td>
<td>%¹</td>
<td>N</td>
<td>%¹</td>
<td>N</td>
</tr>
<tr>
<td>IM: Intrinsic motivations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM1: Boredom / curiosity / excitement</td>
<td>38</td>
<td>37.62</td>
<td>13</td>
<td>22.41</td>
<td>8</td>
<td>26.67</td>
<td>8</td>
</tr>
<tr>
<td>IM2: Fun / felt good</td>
<td>13</td>
<td>12.87</td>
<td>12</td>
<td>20.69</td>
<td>3</td>
<td>10.00</td>
<td>5</td>
</tr>
<tr>
<td>IM3: Challenging / educational</td>
<td>25</td>
<td>24.75</td>
<td>9</td>
<td>15.52</td>
<td>8</td>
<td>26.67</td>
<td>4</td>
</tr>
<tr>
<td>IM4: See how far I could go</td>
<td>16</td>
<td>15.84</td>
<td>7</td>
<td>12.07</td>
<td>5</td>
<td>16.67</td>
<td>3</td>
</tr>
<tr>
<td>EM: Extrinsic motivations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EM1: Damage something</td>
<td>5</td>
<td>4.95</td>
<td>5</td>
<td>8.62</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>EM2: Revenge / anger / to bully</td>
<td>7</td>
<td>6.93</td>
<td>12</td>
<td>20.69</td>
<td>1</td>
<td>3.33</td>
<td>1</td>
</tr>
<tr>
<td>EM3: Put things straight / deliver message</td>
<td>17</td>
<td>16.83</td>
<td>12</td>
<td>20.69</td>
<td>3</td>
<td>10.00</td>
<td>0</td>
</tr>
<tr>
<td>EM4: Impress others / gain power</td>
<td>8</td>
<td>7.92</td>
<td>4</td>
<td>6.90</td>
<td>1</td>
<td>3.33</td>
<td>1</td>
</tr>
<tr>
<td>FM: Financial motivation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FM1: Earn something</td>
<td>3</td>
<td>2.97</td>
<td>3</td>
<td>5.17</td>
<td>1</td>
<td>3.33</td>
<td>1</td>
</tr>
</tbody>
</table>

¹: percentage of all crimes of this crime cluster for which the offender indicated this motivation as true. As respondents could indicate more than one type of motivation as true or all motivations as not true for each crime, these percentages do not add up to 100.
Financial motivations cybercrime
In contrast to claims in the theoretical literature, but in line with most previous empirical work, financial motivations (FM) are almost absent for all cybercrime clusters, even for malware and selling crimes (C4). Therefore, there are no statistically significant differences between cybercrime clusters on financial motivations.

Extrinsic motivations cybercrime
In line with claims in the literature, extrinsic motivations are less prevalent for cybercrime than intrinsic motivations. Nevertheless, most statistically significant differences between cybercrime clusters can be found in these extrinsic motivations. ‘Damage something’ (EM1) is never indicated as a motivation for control over IT-systems (C3) and malware and selling (C4), while it is indicated a few times for hacking and related crimes (C1) and internet related crimes (C2), which is a statistically significant difference. Similarly, ‘put things straight / deliver a message’ (EM3) was never indicated for malware and selling (C4), while it was quite often indicated for other cybercrime clusters and therefore this statistically significantly distinguished malware and selling (C4) from all other cybercrime clusters. Especially for the internet related crimes (C2) this is in line with previous research (Denning, 2011; Holt, 2009b). But, in line with Woo et al. (2004), ‘revenge / anger / bully’ (EM2) is just as often indicated as a motivation for internet related crimes (C2) and this statistically significantly distinguishes those crimes from hacking and related crimes (C1) and control over IT-systems (C3). In contrast to suggestions in the literature, ‘impress others / gain power’ (EM4) is not often indicated for any cybercrime, but for hacking and related crimes (C1) and internet related crimes (C2) this is marginally significantly more often indicated compared to control over IT-systems (C3).

Comparison cybercrime traditional crime
In contrast to claims of Grabosky (2000, 2001) and Grabosky and Walkley (2007), the results show that cybercrime does not only distinguish itself from traditional crime by challenge-related motivations, but also by other motivations. Only, the motivation ‘see how far I could go’ (IM4) is indicated a few times for all crime clusters, both cybercrime and traditional crime, and therefore does not differ statistically significantly between any of the clusters in the comparative models. For all other intrinsic, extrinsic and financial motives, statistically significant differences are observed between cybercrime and traditional crime.
While intrinsic motivations are relatively more common for cybercrimes, extrinsic motivations are relatively more often indicated for traditional crimes. The most important differences are observed for white-collar crimes (T1), followed by the criminal life-style crimes (T3). This supports the findings of Turgeman-Goldschmidt (2011) that hackers cannot be compared to white-collar offenders. For white-collar crimes (T1) the financial motivation (FM) is by far the most important and it is statistically significantly more common compared to all other crime clusters, both cybercrime and traditional crime. In addition, compared to the cybercrimes the financial motivation (FM) is also more common for the other traditional crime clusters, but this difference is only statistically significant for criminal life-style crimes (T3) compared to hacking and related (C1), internet related (C2) and control over IT-systems (C3) crimes.

For intrinsic motivations, most differences can be found for the motivation ‘boredom / curiosity / excitement’ (IM1) that is much more common for the cybercrime clusters, especially compared to the white-collar crimes (T1) and to a lesser extent compared to the criminal life-style crimes (T3). The difference is only once marginally significant for vandalism (T2) compared to hacking and related crimes (C1). But for white-collar crimes (T1) it is a statistically significant or marginally significant difference compared to all cybercrime clusters. For criminal life-style crimes (T3) it is statistically significant compared to hacking and related crimes (C1) and malware and selling (C4).

Additionally, as claimed by Grabosky (2000, 2001) and Grabosky and Walkley (2007) ‘challenging / educational’ (IM3) is a common motivation for hacking and related crimes (C1) and control over IT-systems (C3), while it is not common for traditional crime. This difference is statistically significant for hacking and related crimes (C1) compared to white-collar crimes (T1), and criminal life-style crimes (T3) and marginally significant for white-collar crimes (T1) compared to control over IT-systems (C3). Interestingly, similar to internet related crimes (C2) and malware and selling (C4) ‘fun / felt good’ (IM2) is quite common for white-collar crimes (T1) and vandalism (T2). However, it is not common for control over IT-systems (C3), hence this difference is statistically significant for white-collar crimes (T1) and marginally significant for vandalism (T2). This is the only difference between cybercrime and vandalism (T2) for intrinsic motivations.

For extrinsic motivations, ‘put things straight / deliver a message’ (EM3) was never indicated for malware and selling (C4) and rarely for control over IT-systems (C3). As this is an important motive for vandalism (T2) and criminal life-style crimes
(T3), and to a lesser extent for white-collar crimes (T1), this difference is statistically significant between malware and selling (C4) and all traditional clusters and marginally significant between criminal life-style crimes (T3) and control over IT-systems (C3). Similarly, ‘damage something’ (EM1) is never indicated for C3 and C4, and although it is also not very common for traditional crimes, it is still statistically significantly more common for all traditional crimes compared to C3 and C4. Interestingly, ‘damage something’ (EM1) is statistically significantly more often a motive for vandalism (T2) compared to hacking and related crimes (C1), while it is less often a motive for white-collar crimes compared to internet related crimes (C2).

‘Revenge / anger / bully’ (EM2) is a quite common motivation for vandalism (T2) and very common for criminal life-style crimes (T3). As it is only a quite common motivation for internet related crimes (C2) while almost absent for the other cybercrimes, it differs statistically significantly between the criminal life-style crimes (T3) and the other tree cybercrime clusters (C1, C3, C4). Additionally, as it is very uncommon for control over IT-systems (C3) it is statistically significantly different between C3 and vandalism (T2). In contrast, as it is an important motivation for internet related crimes (C2) and almost absent for white-collar crimes (T1), this difference is also statistically significant. Lastly, ‘Impress others, gain power’ is not very common for all crimes, but marginally significantly more common for vandalism (T2) and criminal life-style crimes (T3) compared to control over IT-systems (C3) and malware and selling (C4).

**Comparison motivations between traditional crimes**

As this paper focusses on cybercrime in comparison to traditional crime, results for traditional crimes will be discussed briefly, but documentation on all statistically significant differences can be found in Appendix B. While the different cybercrime clusters are mostly committed out of intrinsic motivations and show differences based on extrinsic motivations, there is a lot more variation in motivations between the traditional crime clusters. White-collar crimes (T1) have a mostly financial motivation, while vandalism (T2) and criminal life-style crimes (T3) show a somewhat mixed picture. Even though the prevalence rates show that intrinsic motivations are more common for vandalism (T2), while extrinsic motivations are more common for criminal life-style crimes (T3), there is no statistically significant difference between the motivations of these two traditional crime clusters.

Only the white-collar crimes (T1) show statistically significant differences with the other two crime clusters, but only in financial and extrinsic motivations. The most important difference is that financial motivations are much more common, but
some extrinsic motivations are less common for white-collar crimes (T1) compared to the other two. ‘Damage something’ (EM1) and ‘revenge / anger / bully’ (EM2) are statistically significantly or marginally significantly more common for the other traditional crimes (T2 and T3). In addition, ‘put things straight / deliver a message’ (EM3) is very common for criminal life-style crimes (T3) and therefore statistically significantly distinguishes those from the white-collar crimes. Lastly, ‘impress others / gain power’ (EM4) is not very common for all traditional crime clusters and therefore shows no statistically significant differences.

5.4 Conclusion and discussion

In this paper some gaps in the literature on cybercrime have been addressed, by using self-report data from the understudied population of adult cyber-offenders and traditional offenders registered by the Dutch public prosecutors’ office. First, it was examined to what extent cyber-dependent offenders can be distinguished from traditional offenders, by analysing which clusters of cyber-offences and traditional offences are often committed by the same offender. Second, using these clusters it was explored which motivations the offenders provided for committing those crimes and to what extent these clusters can be distinguished from the others by these motivations.

With regard to the first objective, it was found that cyber-dependent crimes form a distinct group of offences that rarely co-occur with traditional crimes. This is in line with the hypothetical distinction between traditional crimes and cyber-dependent crimes. The hypothetical assumption in theoretical literature, that cyber-dependent crimes could be part of the same modus-operandi as traditional crimes, could not be verified with this data, but three out of the four cybercrime clusters appeared to be crimes that are part of the same cyber-modus operandi. These three clusters were hacking and related crimes, control over IT-systems and malware and selling crimes. The internet related crimes were more likely clustered together because they require the same skills set, as, unlike the others, they mainly take place on the internet instead of on specific IT-systems. To some extent this is in line with hypothetically distinguished cyber-dependent crime clusters as described in the theoretical literature (Bachmann & Corzine, 2010; McGuire & Dowling, 2013).

With regard to the second objective, it was found that intrinsic motivations were most important for all cybercrime clusters. This is in line with the empirical literature. Additionally, the comparative analyses showed that although there is
some variation in the relative importance of different intrinsic motivations for the different cybercrime clusters, these can hardly be used to differentiate between the different cybercrime clusters. In contrast to suggestions in the theoretical literature, however, very little offenders indicated they committed their cybercrimes for financial gain, even for crimes where they sold data or credentials. Offenders indicated that these are still mostly committed out of boredom, curiosity or excitement or other intrinsic motivations. Thus these offenders, who have been in contact with the police earlier in their offending career, have not shifted to offending for financial gain. This is in contrast to some literature that suggests that later in their career offenders shift to financial motivations (Bachmann, 2011; Bachmann & Corzine, 2010; Xu et al., 2013).

While the intrinsic motivations seem to indicate that internet related crimes are more comparable to malware and selling crimes, the extrinsic motivations actually distinguish control over IT-systems and malware and selling from hacking and related crimes and internet related crimes. While offenders of the latter crimes quite often indicate extrinsic motivations for these crimes, especially for internet related crimes, they virtually never indicate such motivations for control over IT-systems or malware and selling. Additionally, the internet related crimes seem to be distinguished from all other cybercrime clusters as they are most often committed out of extrinsic motivations, especially out of revenge anger or to bully someone. In line with arguments of Leukfeldt et al. (2013) these may be crimes that are easier to commit and therefore more general motivations, like revenge, are more important. In addition, most of these crimes are more visible to others than the other cybercrimes and can potentially be committed on a large scale, which increases their usefulness for extrinsically motivated offending.

In contrast to empirical evidence based on forums, in this offender sample the cybercrimes were generally not committed initially to impress others or gain power. At the moment a cybercrime is committed, there may generally be no one around to show off to. Some offenders may brag about it online afterwards, but apparently most of them do not start committing the crime for status. As discussed by Jordan and Taylor (1998) the status and rewards received from online friends may stimulate future offending, but may not provide an initial motivation for offending. This could reduce the usefulness of prevention strategies that are based on the assumption that offenders will stop committing crimes if it does not result in more status.
The comparisons between cybercrime and traditional crime showed a lot of differences in motivations between cybercrime and traditional crime clusters. Most importantly, as financial motivations are almost absent for all cybercrimes, this distinguishes them from the white-collar crimes, which is in line with Turgeman-Goldschmidt (2011). Additionally, that is also an important difference between the cybercrimes and criminal life-style crimes, but criminal life-style crimes can also be distinguished from cybercrimes by showing more extrinsic motivations. It should be noted, however, that internet related crimes, and to a lesser extent hacking and related crimes, are more similar to traditional crimes in their motivations, especially in their extrinsic motivations, than control over IT-systems and malware and selling crimes. This may indicate that the latter crimes are more specialised and technical in nature, which potentially results in more distinctly different offenders and motivations.

With respect to intrinsic motivations, cybercrimes can be distinguished from traditional crimes, especially as they are largely committed out of boredom, curiosity or excitement or because it is challenging or educational. It should be noted, however, that vandalism is quite similar to cybercrimes in intrinsic motivations. Nevertheless, when looking at extrinsic motivations, there are a lot of differences between the cybercrimes and vandalism. Therefore the results cannot completely verify the hypothetical claim of Kirwan and Power (2013) that cybercrime, specifically malware use, is similar to vandalism and therefore has similar motivations.

These results provide useful information for both investigation and prevention. First, these results could be used after a cybercrime has occurred, to assess the possible chain of crimes that were committed and the underlying motivations of the offender, based on empirical data instead of only hypothetical assumptions. Second, as motivations for cybercrime are not similar to traditional crimes and more intrinsic, this offers new opportunities for crime prevention that may not have been very useful for traditional crimes. For example, if offenders who have been in contact with the police still mainly commit their crimes out of boredom, curiosity or excitement, or for the challenge or educational aspect, helping convicts to find legal daily activities that can satisfy these needs may be more useful to prevent re-offending for cybercrime than for traditional crime. The skills needed to commit these cybercrimes are actually skills that can be used in legitimate daily activities.
Even though the results and implications address an important gap in the literature on cybercrime, the sample and method also have their limitations. First of all, like most research on crime and criminals, there is a dark number and the sample could be selective. The sample is based on respondents who have been in contact with the police in the past. This high risk sample was necessary to find two comparable groups of cybercrime and traditional offenders and find a sufficient number of cyber-dependent offenders, who are less prevalent in the general population than cyber-enabled offenders. Nevertheless, when using these results, it should be kept in mind that these are the clusters of crimes and related motivations that are reported by offenders who have been in contact with the police and have subsequently continued committing crime. Therefore, these clusters and related motivations may be different among first offenders or offenders who are able to avoid the long arm of the police.

As discussed in the introduction an important limitation of asking offenders about their motivations after they committed a crime, is that it may only show their justifications for offending, instead of the actual motivation at the moment they were committing the crime. In addition, offenders may choose to report a more socially accepted motivation as curiosity or challenge and not report their financial motivation, for example. However, the prevalence rates of reported financial motivations were very high for white-collar crimes, which may indicate that respondents did not feel the urge to only report socially accepted motivations in this study.

Even though it is challenging to study motivations for committing crimes, it is important to examine those motivations as they may guide us to possible prevention methods as discussed above. Most criminological research on both cybercrime and traditional crime just assumes the existence of motivated offenders and research on cybercrime assumes that motivations for cybercrime are similar to motivations for traditional crime. The analyses in this paper have empirically shown the large differences that exist between cybercrime and traditional crime clusters.
## 5.5 Appendix A: Pattern matrix principal component analysis

<table>
<thead>
<tr>
<th></th>
<th>Factor</th>
<th>Factor</th>
<th>Factor</th>
<th>Factor</th>
<th>Factor</th>
<th>Factor</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td><strong>(α=0.75)</strong></td>
<td>(α=0.62)</td>
<td>(α=0.60)</td>
<td>(α=0.74)</td>
<td>(α=0.63)</td>
<td>(α=0.66)</td>
<td>(α=0.59)</td>
<td></td>
</tr>
<tr>
<td><strong>Cybercrime</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>factor C1</td>
<td>0.70</td>
<td>0.03</td>
<td>-0.08</td>
<td>0.10</td>
<td>0.08</td>
<td>-0.09</td>
<td>0.07</td>
</tr>
<tr>
<td>factor C2</td>
<td>0.77</td>
<td>-0.10</td>
<td>0.14</td>
<td>-0.03</td>
<td>-0.11</td>
<td>0.07</td>
<td>0.05</td>
</tr>
<tr>
<td>factor C3</td>
<td>0.65</td>
<td>0.18</td>
<td>-0.13</td>
<td>0.35</td>
<td>-0.18</td>
<td>-0.06</td>
<td>0.06</td>
</tr>
<tr>
<td>factor C4</td>
<td>0.65</td>
<td>0.05</td>
<td>0.07</td>
<td>0.10</td>
<td>0.12</td>
<td>0.03</td>
<td>-0.09</td>
</tr>
<tr>
<td><strong>Traditional</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>crime factor T1</td>
<td>0.00</td>
<td>0.77</td>
<td>0.09</td>
<td>0.09</td>
<td>-0.27</td>
<td>0.06</td>
<td>-0.02</td>
</tr>
<tr>
<td>crime factor T2</td>
<td>0.07</td>
<td>0.63</td>
<td>-0.02</td>
<td>-0.06</td>
<td>0.22</td>
<td>0.09</td>
<td>-0.03</td>
</tr>
<tr>
<td>crime factor T3</td>
<td>-0.01</td>
<td>0.71</td>
<td>0.12</td>
<td>-0.03</td>
<td>0.11</td>
<td>-0.14</td>
<td>0.08</td>
</tr>
<tr>
<td><strong>Defacing</strong></td>
<td>0.08</td>
<td>0.19</td>
<td>-0.01</td>
<td>0.03</td>
<td><strong>0.83</strong></td>
<td>0.03</td>
<td>0.08</td>
</tr>
<tr>
<td><strong>Intercepting communication</strong></td>
<td>0.21</td>
<td>0.13</td>
<td>-0.04</td>
<td><strong>0.66</strong></td>
<td>0.34</td>
<td>-0.11</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Vandalism</strong></td>
<td>0.09</td>
<td>0.14</td>
<td>0.29</td>
<td>0.07</td>
<td><strong>0.37</strong></td>
<td>0.26</td>
<td>-0.23</td>
</tr>
<tr>
<td><strong>Burglary</strong></td>
<td>-0.06</td>
<td>0.20</td>
<td>0.22</td>
<td>0.25</td>
<td><strong>0.63</strong></td>
<td>-0.12</td>
<td>0.09</td>
</tr>
<tr>
<td><strong>Using weapon</strong></td>
<td>0.04</td>
<td>0.02</td>
<td>0.02</td>
<td>0.12</td>
<td><strong>0.71</strong></td>
<td>0.18</td>
<td>0.19</td>
</tr>
<tr>
<td><strong>Stealing</strong></td>
<td>0.35</td>
<td>0.25</td>
<td>0.14</td>
<td>-0.08</td>
<td>0.05</td>
<td><strong>0.40</strong></td>
<td>-0.14</td>
</tr>
<tr>
<td><strong>Threats</strong></td>
<td>-0.01</td>
<td>-0.05</td>
<td>0.02</td>
<td>0.07</td>
<td>-0.10</td>
<td><strong>0.75</strong></td>
<td>0.11</td>
</tr>
<tr>
<td><strong>Violence</strong></td>
<td>-0.01</td>
<td>0.12</td>
<td>-0.15</td>
<td>-0.10</td>
<td>0.35</td>
<td><strong>0.54</strong></td>
<td>0.28</td>
</tr>
<tr>
<td><strong>Carry weapon</strong></td>
<td>0.10</td>
<td>-0.17</td>
<td>0.20</td>
<td>0.00</td>
<td>0.25</td>
<td><strong>0.50</strong></td>
<td>-0.26</td>
</tr>
<tr>
<td><strong>Selling drugs</strong></td>
<td>-0.04</td>
<td>0.35</td>
<td>-0.24</td>
<td>0.05</td>
<td>0.08</td>
<td><strong>0.54</strong></td>
<td>-0.06</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>-0.14</td>
<td>-0.02</td>
<td>0.14</td>
<td>0.48</td>
<td>-0.11</td>
<td>0.15</td>
<td><strong>0.55</strong></td>
</tr>
<tr>
<td><strong>Selling data</strong></td>
<td>0.43</td>
<td>0.01</td>
<td>-0.04</td>
<td>-0.11</td>
<td>0.04</td>
<td>-0.08</td>
<td><strong>0.64</strong></td>
</tr>
<tr>
<td><strong>Selling credentials</strong></td>
<td>-0.01</td>
<td>0.05</td>
<td>0.18</td>
<td>0.03</td>
<td>0.27</td>
<td>0.09</td>
<td><strong>0.70</strong></td>
</tr>
</tbody>
</table>

Note: pattern matrix with oblique rotation, results with varimax rotation indicated the same classification of crimes (results available upon request)
### 5.6 Appendix B: Evidence for significant differences in motivations between clusters

These tables are based on clustered (respondent-crime) multivariate probit models. The underlying parameter estimates are available upon request.

Dark grey areas show comparisons between a specific cybercrime and a specific traditional crime cluster, while light grey areas show comparisons between a specific cybercrime and another cybercrime cluster, or a specific traditional crime and another traditional crime cluster.

+ indicates more common for crime cluster in left column compared to crime cluster in upper row
– indicates less common for crime cluster in left column compared to crime cluster in upper row

+++/- – – p < .001; ++/- – p < .01; +/- p < .05; (+)/(-) p < .10 (two-tailed)

<table>
<thead>
<tr>
<th>IM1: Boredom/curiosity/excitement</th>
<th>IM3: Challenging/educational</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 (+)</td>
<td>C1 +</td>
</tr>
<tr>
<td>C2 (–)</td>
<td>C2 (–)</td>
</tr>
<tr>
<td>C3 (+)</td>
<td>C3 (+)</td>
</tr>
<tr>
<td>C4 ++</td>
<td>C4 ++</td>
</tr>
<tr>
<td>T1 –</td>
<td>T1 –</td>
</tr>
<tr>
<td>T2 (–)</td>
<td>T2 (–)</td>
</tr>
<tr>
<td>T3 –</td>
<td>T3 –</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IM2: Fun/felt good</th>
<th>IM4: See how far I could go</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>C1</td>
</tr>
<tr>
<td>C2</td>
<td>C2</td>
</tr>
<tr>
<td>C3</td>
<td>C3</td>
</tr>
<tr>
<td>C4</td>
<td>C4</td>
</tr>
<tr>
<td>T1</td>
<td>T1</td>
</tr>
<tr>
<td>T2</td>
<td>T2</td>
</tr>
<tr>
<td>T3</td>
<td>T3</td>
</tr>
</tbody>
</table>
### EM: Extrinsic motivations

#### EM1: Damage something

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>+++</td>
<td>+++</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>+++</td>
<td>+++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>–</td>
<td>+++</td>
<td>+++</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>+</td>
<td>+++</td>
<td>+++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>+++</td>
<td>+++</td>
<td>(+)</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EM3: Put things straight/deliver a message

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>+++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>+++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>+++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>+</td>
<td>+++</td>
<td>(+)</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>(+)</td>
<td>+++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EM2: Revenge/anger/to bully

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>++</td>
<td>(+)</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### EM4: Impress others/gain power

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>(+)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>(+)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>(–)</td>
<td>(–)</td>
<td>(–)</td>
<td>(–)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>(+)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>(+)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### FM: Financial motivation

#### FM: Earn something

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3</td>
<td>+</td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References
References


References


