Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals

Jim A.M. Schiks [a,b,*], Steve G.A. van de Weijer [a], E. Rutger Leukfeldt [a,b]

[a] Netherlands Institute for the Study of Crime and Law Enforcement, Amsterdam, the Netherlands
[b] The Hague University of Applied Sciences, The Hague, the Netherlands

ARTICLE INFO

Keywords:
Intellectual capabilities
Cybercrime
Perpetrators
Computer trespassing

ABSTRACT

In our highly digitalized society, cybercrime has become a common crime. However, because research into cybercriminals is in its infancy, our knowledge about cybercriminals is still limited. One of the main considerations is whether cybercriminals have higher intellectual capabilities than traditional criminals or even the general population. Although criminological studies clearly show that traditional criminals have lower intellectual capabilities, little is known about the relationship between cybercrime and intelligence. The current study adds to the literature by exploring the relationship between CITO-test scores and cybercrime in the Netherlands. The CITO final test is a standardized test for primary school students - usually taken at the age of 11 or 12 - and highly correlated with IQ-scores. Data from Statistics Netherlands were used to compare CITO-test scores of 143 apprehended cybercriminals with those of 143 apprehended traditional criminals and 143 non-criminals, matched on age, sex, and country of birth. Ordinary Least Squares regression analyses were used to compare CITO test scores between cybercriminals, traditional criminals, and non-criminals. Additionally, a discordant sibling design was used to control for unmeasured confounding by family factors. Findings reveal that cybercriminals have significantly higher CITO test scores compared to traditional criminals and significantly lower CITO test scores compared to non-criminals.

1. Introduction

Cybercriminals abuse the possibilities of information technology (IT) within our highly digitalized society to commit criminal offences. Recent victim surveys show that cybercrime has become a common crime (Statistics Netherlands, 2018, 2020). There has been considerable debate in the psychological and criminological community about definitions, concepts and classifications of cybercrimes and cybercriminals (see, for an overview, McGuire, 2020), but usually two types of cybercrimes are distinguished: ‘cyber dependent crimes’ and ‘cyber enabled crimes’ (McGuire & Dowling, 2013). The first category contains ‘new’ types of offences that target IT, such as hacking databases with credit card credentials and taking down websites or networks. The second category includes traditional crimes in which IT plays an important role in the modus operandi of the criminals. Examples include internet fraud and cyber stalking. Moreover, crimes where IT does not play a substantial role for the commission of the offense (e.g., violence, burglary and theft) are referred to as traditional crimes in this article.

Despite the rise of cybercrime, research into cybercriminals is still limited (for an overview see Holt & Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019). Consequently, there are various fundamental questions regarding cybercriminals on which we do not have an answer yet. Are we, for example, dealing with a new type of offender with different characteristics and motives, or with the same old offenders who simply moved their criminal activities online? And are there differences between the characteristics of cyber enabled offenders and cyber dependent offenders? There are studies that suggest that some type of cybercrime offenders have different characteristics compared to traditional offenders (Fötinger & Ziegler, 2004; Randazzo et al., 2005; Chiesa et al., 2009; Bachmann & Corzine, 2010; Leukfeldt et al., 2010; Moon et al., 2010; Aransiola & Asindemade, 2011; Schell & Melnychuk, 2011; Turgeman-Goldschmidt, 2011; Holt et al., 2012; Leukfeldt & Stol, 2012; Weulen-Kranenbarg et al., 2018a). For example, cybercriminals are suggested to be younger, more often men, less often from ethnic minority groups and to have a higher socioeconomic status than traditional offenders (Leukfeldt, 2017). However, the majority of these studies are explorative in nature and suffer from significant methodological limitations (Leukfeldt, 2017; Maimon & Louderback, 2019). This

* Corresponding author. Netherlands Institute for the Study of Crime and Law Enforcement, PO Box 71304, Amsterdam, 1008 BH, the Netherlands.
E-mail address: jschiks@nscr.nl (J.A.M. Schiks).

https://doi.org/10.1016/j.chb.2021.106985
Received 1 March 2021; Received in revised form 16 July 2021; Accepted 15 August 2021
Available online 18 August 2021

has a major impact on our understanding of cybercriminals. Furthermore, recent studies show the intertwinement of financially motivated cybercrimes and traditional street crimes in the Netherlands (Leukfeldt & Roks, 2020; Roks et al., 2020). This suggests that there may be less or no differences between these types of cybercrime offenders and traditional offenders.

One of the key debates in cybercrime offender research, is whether or not cybercriminals have higher intellectual and technical capabilities compared to traditional criminals or even the general population (Holt & Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019). With regard to traditional criminals, previous criminological studies consistently show that lower intellectual capabilities are associated with an increased risk for criminal behavior (Ellis & Walsh, 2003; Frisell et al., 2012; Schwartz et al., 2015; Jacob et al., 2019). In contrast with these findings, cybercriminals - and especially offenders that commit highly technical cybercrimes such as hacking - are often assumed to have a high level of intelligence, problem solving capabilities and being motivated by the intellectual challenge rather than simply earning easy money (Rogers, 2006; Chiesa et al., 2009; Koops, 2010; Bachmann, 2011; Jordan, 2017). On the other hand, the availability of online tools on underground markets enable less intelligent people to commit high tech crimes as well (UNODC, 2013; Chan & Wang, 2015; Décary-Hétu & Giommoni, 2017). Nevertheless, empirical research into the intellectual capabilities of cybercriminals is scarce. The few studies that exist focus on the level of education of cybercriminals or their high school performance (see, for example Turgeman-Goldschmidt, 2005; Lu et al., 2006; Leukfeldt et al., 2010; Holt & Bossler, 2012; Chan & Wang, 2015).

The current study addresses this gap in literature by exploring the relationship between CITO (Central Institute for Test Development) final test scores and cyber-dependent crime in the Netherlands. The CITO final test is a standardized test for primary school students in their last year, usually taken at the age of 11 or 12, which plays a significant role in the admission of students to secondary schools (Bartels et al., 2002; Statistics Netherlands, 2021). The test consists of different components such as language and mathematics and test scores have been shown to have a high positive correlation with IQ-scores at ages 5, 7, 10 and 12, respectively (Bartels et al., 2002). In this study, CITO test scores of cyber-dependent criminals who engaged in computer trespassing will be compared with the scores of traditional criminals and non-criminals.

2. Review of the literature

2.1. *Intellectual capabilities and crime*

Decades of research from multiple disciplines has identified a firmly established relationship between cognitive abilities (often measured in terms of IQ-scores) and criminal behavior. More specifically, individuals with lower IQ-scores have been found to be more likely to engage in crime (Hirschi & Hindelang, 1977; Moffitt et al., 1981; Jolliffe & Farrington, 2004; Rushton & Templer, 2009; Frisell et al., 2012; Beaver et al., 2013; Schwartz et al., 2015). The relationship between IQ and criminal behavior has been found to be stronger for both repeat offending and violent crimes (Donnellan et al., 2000; Guay et al., 2005; Kennedy et al., 2011; Frisell, 2012). In addition, the association between IQ and criminal behavior has been found both in studies that rely on officially recorded and on self-reported crimes, although the relationship seems to be attenuated for self-reported crimes (Boccio et al., 2018; Moffitt & Silva, 1988).

Less is known, however, about the mechanisms behind this relationship. A possible explanation for an effect of intellectual capabilities on criminal behavior is that individuals with lower intellectual capabilities are less likely to anticipate the consequences of their actions and to understand the suffering of others (Moffitt et al., 1993; McGloin et al., 2004; Guay et al., 2005). Others often proposed an indirect effect by suggesting that IQ affects the likelihood of delinquent behavior through its effect on school-related factors such as school performance and school adjustment problems (Hirschi & Hindelang, 1977; Ward & Tittle, 1994; Mõttus, Guljajev, Allik, Laidra, & Pullmann, 2012). The association could also be spurious rather than causal, when some underlying factors have an influence on both IQ as on criminal behavior. Several studies have shown that the relationship between IQ and criminal behavior remains significant after controlling for potential confounding factors such as socioeconomic status, parental characteristics and ethnic background (Hirschi and Hindelang, 1977; Rushton & Templer, 2009; Frisell, 2012), which is in line with a causal relationship. However, when unmeasured confounders are not controlled for, a spurious relationship cannot be ruled out. For example, genetic factors could be a source for hidden bias since Tielbeek et al. (2017) found a moderate negative genetic correlation between educational attainment and antisocial behavior. The current study will use a discordant sibling design to control for all (unmeasured) factors shared within families (i.e., genetic and shared environmental factors) that might confound the relationship between IQ and criminal behavior.

2.2. *Cybercriminals: educational attainment, school performance and intelligence*

To the best of our knowledge, there have not been any studies that directly measured the intellectual capabilities of cybercriminals. In this section, studies on the educational attainment and high school performance of cybercrime offenders are discussed. These studies examined different populations: general cybercrime offenders (i.e. both cyber-dependent and cyber-enabled), only cyber-enabled offenders or only cyber-dependent offenders.

For the general cybercrime population, studies showed diverse results (Lu et al., 2006; Marcum et al., 2012; Chan & Wang, 2015; Odinot et al., 2017). For example, Lu et al. (2006) compared the educational attainment of 18.784 Taiwanese cybercrime suspects with traditional crime suspects. They concluded that cybercrime attracts better educated persons, because the majority of cybercrime suspects in their study were senior high school or college students. However, organized-cybercrime suspects in the Netherlands were suggested to be a diversely educated group (Odinot et al., 2017) and sentenced cybercrime offenders in the United States had an average high-school educational level (Marcum et al., 2012). Chan and Wang (2015) even noted – based upon descriptive statistics in two related Chinese studies – that educational levels of Chinese cybercrime offenders were lower than expected (Chan & Wang, 2015).

For cyber-enabled offenders, most studies suggested that their educational attainment was not higher than in other populations (Leukfeldt et al., 2010; Leukfeldt & Stol, 2012; Kerstens & Stol, 2012). In the Netherlands, a study of Leukfeldt et al. (2010) analyzed data about 54 suspects of online child pornography and showed that these suspects did not have significant different educational levels compared to the general population. In addition, Leukfeldt and Stol (2012) showed that 170 suspects of online fraud did not differ significantly from suspects of traditional fraud. Both studies were based upon data that was retrieved from the Dutch police. Furthermore, Kerstens and Stol (2012) conducted surveys amongst 6.299 Dutch teenagers and found that those who attended a higher level of secondary education – ranging from lower general secondary education to pre-university education – had a lower likelihood of committing online marketplace fraud and involvement in cyberbullying. Contrary to these findings, Moon et al. (2010) showed that – based upon surveys amongst 2751 South-Korean students – students with poorer educational performance were more likely to engage in both illegal downloading and illegal use of another's identity online than students with a higher educational performance.

With regard to cyber-dependent offenders, studies indicated that these offenders completed a relative high level of education (Stambaugh et al., 2001; Turgeman-Goldschmidt, 2005; Chiesa et al., 2009; Bachmann, 2011; Harbinson & Selzer, 2019). Studies into educational levels of self-reported hackers, for example, concluded that these hackers were highly educated (Turgeman-Goldschmidt, 2005; Chiesa et al., 2009; Bachmann, 2011). These studies were based upon interviews with 54 Israelian hackers (Turgeman-Goldschmidt, 2005) and surveys amongst 124 hackers at the ShmooCon convention in Washington (Bachmann, 2011) and 502 hackers from different countries that were approached during the Hacker's Profiling Project (Chiesa et al., 2009). In addition, Stambaugh et al. (2001) stated that, based upon interviews with 123 law enforcement officials in the United States, many hackers were college students and usually intelligent. Furthermore, Harbinson and Selzer (2019) showed, in their study into convicted cyber-dependent offenders in the United States, that 38,3% of the cyber-dependent offenders in their study had a high school diploma and 32,4% had a bachelor's degree or higher. The authors argued that these levels of education were higher than found in studies among traditional offenders.

Finally, two studies investigated the relationship between school performance and cybercrime in the United States (Holt et al., 2012; Marcum et al., 2014). Holt et al. (2012) examined the relationship between students' grades on their report card and different types of cyber deviance in a sample of 518 students. The authors found no significant relationship of students' grades with media piracy, pornography, and hacking. Software piracy was positively correlated with higher grades and harassment was negatively correlated with higher grades of students. In addition, a study of Marcum et al. (2014) showed that as the GPA of 1617 high school students increased, students were more likely to participate in hacking activities.

To conclude, previous studies showed mixed results with regard to the educational attainment and school performance of cybercrime offenders, although cyber-dependent offenders seem to have a relatively high level of education. However, most of the studies report descriptive statistics, are based upon anecdotal evidence or do not make statistical comparisons between cybercriminals and traditional criminals. In addition, it is unclear whether educational attainment and high school performance are valid parameters for measuring intellectual capabilities of cybercriminals, because some studies indicate that hackers have more problems at school (Stambaugh et al., 2001; Chiesa et al., 2009). For example, hackers are suggested to be less motivated, less disciplined, not attending regularly and dropping out as they experience school as easy, boring and not stimulating (Chiesa et al., 2009). This suggests that hackers have more potential in terms of intellectual capabilities than their educational attainment and high school performance indicates. The current study will test this by comparing CITO test scores - which are highly correlated with IQ scores (Bartels et al., 2002) – of Dutch cybercriminals with those of traditional offenders and non-offenders. Moreover, the CITO test scores of cybercriminals will be compared with those of their non-offending siblings, in order to control for unmeasured confounders which are shared within families (i.e., genetic and shared environmental confounders). Our study therefore overcomes limitations of previous studies that did not make statistical comparisons or measured educational attainment and school performance instead of intellectual capabilities. The research question is two-fold: Do cybercriminals have different intellectual capabilities than traditional offenders and non-offenders? And to what extent can the association between cybercrime offending and intellectual capabilities be explained by unmeasured familial factors?

3. Methods

In order to gain insight into the intelligence of cybercriminals, data from Statistics Netherlands about criminal records and CITO test scores were used. These data include information on all Dutch citizens from several sources, which can be linked through an anonymized identification number.

The criminal records include all criminal cases that were registered by the Dutch public prosecutor's office between 2001 and 2018. In these years, 1161 individuals were at least once prosecuted for computer trespassing. Computer trespassing is defined by Dutch law as gaining unauthorized access to a computerized system (article 138 ab of the Dutch Penal Code), and is therefore a type of cyber dependent crime. It is important to note that the data do not provide information about the outcome of the criminal cases. The registered persons are officially only marked as a suspect of a crime. This means that the police has closed their police investigation and found enough evidence to send the case to the Public Prosecutor. It is, however, unknown if the persons in our data actually have been convicted.

Furthermore, the data of Statistics Netherlands included all test scores of children who took the CITO test between 2006 and 2018. Among the cybercriminals, 143 (12,3%) took this test between these years and they were included in the analytic sample of this study. They were born between 1993 and 2005 and were on average 21.10 years old in 2018 (S.D.: 3.10). Moreover, the large majority of them were male (83.22%) and born in the Netherlands (95.57%). Two comparison groups were constructed by matching these 143 cybercriminals to 143 traditional criminals (i.e., who were prosecuted for any crime other than computer trespassing) and 143 non-criminals with the same year of birth, sex and country of birth. These persons in the control groups were randomly selected out of all individuals with a certain combination of these background characteristics. The traditional criminals were most often prosecuted for violent offences, property offences, and/or public order offences, while traffic offences and drugs offences were less prevalent and weapon offences were rare.

In additional analyses, the cybercriminals were also compared to their non-offending full siblings, in order to control for unmeasured familial confounders. As discussed in the literature overview, the causality of the association between IQ and criminal behavior has been debated and it has been suggested that the relationship is spurious. By controlling for all (unmeasured) familial factors, this study will give a better estimate of the causal effect of IQ on cybercrime offending. In our study, the sibling which was most close in age to the cybercriminal was selected in 60 cases, while the remaining cybercriminals did not have a sibling or did not have a non-offending sibling who took the CITO test between 2006 and 2018.

3.1. Measurements

The dependent variables in the analyses were based on the CITO test scores. As mentioned before, the CITO final test is a standardized test that primary school students in the Netherlands take in their last year, around age 12 (Bartels et al., 2002). The CITO test consists of 290 multiple-choice questions divided over four different intellectual skills (Statistics Netherlands, 2021): Language (100 questions), Mathematics (60 questions), Information Processing (40 questions) and World Orientation (90 questions). The part about World Orientation, however, is not mandatory and does, therefore, not influence the final score. Moreover, the questions on Information Processing have, since 2015, been integrated with the modules Language and Mathematics. Students' performances on the mandatory questions result in a standardized score between 501 and 550. Every year the scores on the CITO final test are equalized in order to be able to compare the standardized scores over time (e.g., the level of performance associated with a score of 540 in 2010 is comparable to the score of 540 in 2018; Statistics Netherlands, 2021). These standardized scores were the main dependent variable in our analyses. Additionally, also the performance on the Language, Mathematics and Information Processing questions were analyzed in separate regression models by using the percentile ranks as dependent variables.

The main independent variable in this study was a categorical variable indicating whether a sample member was a cybercriminal, a traditional criminal or a non-criminal. Due to the use of officially registered data, not all criminal behavior is measured and it might be possible that the non-criminals in our sample in fact did commit crime but were never arrested and sanctioned for it. Nevertheless, this group will be referred to as non-criminals for the sake of readability. Moreover, household size, household income, and parental educational level were included as control variables as they may affect both criminal behavior and test scores. Household size was measured as the number of children in a family, i.e. the sample member and his/her full-siblings. Household income was measured in the year in which the sample member took the CITO test and is indicated by quintiles, ranging from 1 (low) to 5 (high). Parental educational levels were measured separately for fathers and mothers and divided in three categories: low (i.e., primary school, prevocational education), medium (i.e., secondary education, vocational education) and high (i.e., higher education: bachelor, master, PhD). Household income and parental education were included as categorical variables in the analyses. For these variables, an additional category was constructed for all individuals with a missing value.

3.2. Analyses

First, ANOVA was used to compare CITO test scores between cybercriminals, traditional criminals, and non-criminals. Next, Ordinary Least Squares regression analyses were used to test whether these differences were still significant after controlling for the control variables. Additionally, a discordant sibling design was used to control for unmeasured confounding by family factors. In this design, a within-family comparison was made between cybercriminals and their full-sibling that was closest in age. By comparing siblings within families, rather than unrelated individuals, this method controls for all unmeasured shared family environments and partly for genetic confounding, since siblings share 50 percent of their genes (D'onofrio et al., 2013).

4. Results

Table 1 shows the descriptive statistics of all variables which were used in the analyses. The 429 sample members had an average score of 531.72 (S.D.: 9.80) on the CITO final test. Their average percentile ranks on the language, mathematics and information processing parts of the test were, respectively, 38.16 (S.D.: 26.88), 46.44 (S.D.:28.14) and 42.49 (S.D.: 29.42). Moreover, the average household size of those included in the sample was 2.50 (S.D.: 1.21). Among those with valid scores, most sample members had a father with a middle education level, a mother with a low educational level and were in the fourth income quintile.

Table 1
Descriptive statistics.

	Mean/N(%)	S.D.
Dependent variables		
CITO final test score	531.72	9.80
Percentile rank language	38.16	26.88
Percentile rank mathematics	46.44	28.14
Percentile rank information processing	42.49	29.42
Independent variable		
Type of criminal		
Cybercriminals	143 (33.3%)	
Traditional criminals	143 (33.3%)	
Non criminals	143 (33.3%)	
Control variables		
Household size	2.50	1.21
Education father		
Low	64 (14.92%)	
Middle	83 (19.35%)	
High	64 (14.92%)	
Missing	218 (50.82%)	
Education mother		
Low	104 (24.24%)	
Middle	97 (22.61%)	
High	55 (12.82%)	
Missing	173 (40.33%)	
Income quintile		
1 (Low)	21 (4.9%)	
2	61 (14.22%)	
3	44 (10.26%)	
4	80 (18.65%)	
5 (High)	76 (17.72%)	
Missing	147 (34.27%)	

The results of the ANOVA showed that the three groups differed significantly on their CITO test scores ($F(2, 426) = 20.90$, $p < .001$) as well as on the modules on language ($F(2, 426) = 217.44$, $p < .001$), mathematics ($F(2, 426) = 15.60$, $p < .001$) and information processing ($F(2, 426) = 19.11$, $p < .001$). In Fig. 1 the average test results of the three groups in our sample are displayed. The results in Fig. 1a show that cybercriminals have an average CITO score of 531.29, which is significantly ($p < .05$) higher than traditional criminals (528.38) but significantly lower ($p < .001$) than the non-criminals (535.50). Fig. 1b, c and 1d show the average percentile ranks of sample members for the parts on language, mathematics and information processing within the CITO test. On all three parts, cybercriminals have significantly lower percentile ranks (37.48, 45.30 and 41.92, respectively) than the non-criminals (47.53, 55.95 and 54.23, respectively) and higher percentile ranks than traditional criminals (29.48, 38.07 and 32.69, respectively, although the difference on mathematics was not statistically significant.

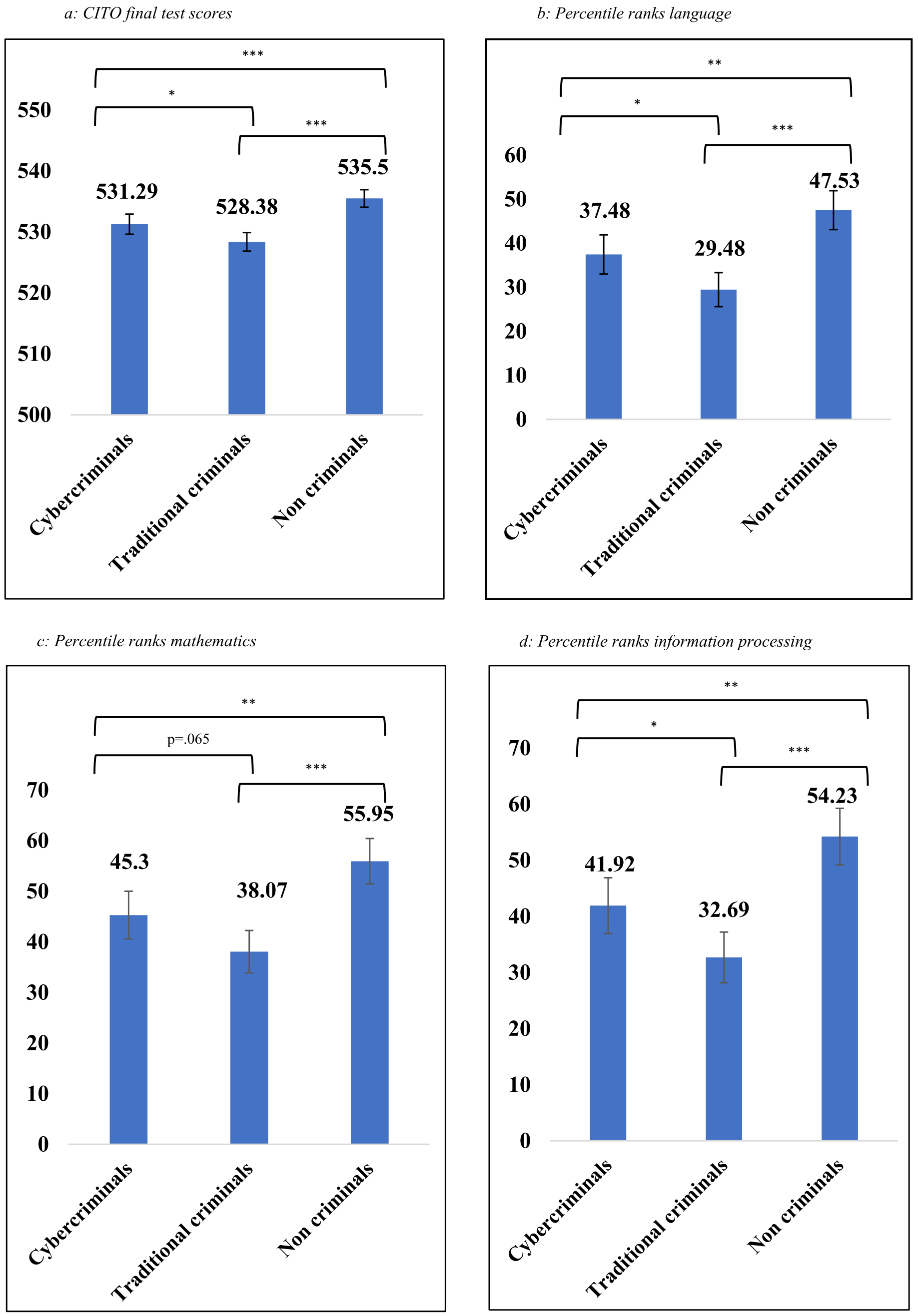
The results of the OLS regression analyses are presented in Table 2. Model 1 shows that cybercriminals score 2.5666 points higher compared to traditional criminals ($p < .05$) and 3.042 points lower than non-criminals ($p < .01$), after including control variables. The same patterns were found in Model 2 to 4 in which the percentile ranks for the modules on language, mathematics and information processing were predicted. Model 2 illustrates that traditional criminals' percentile rank for language is significantly lower than that of cybercriminals ($B = -6.272$; $p < .05$), while the percentile rank of non-criminals is significantly higher ($B = 7.159$; $p < .01$). The results of Model 3 show that the cybercriminals have a 6.883 higher percentile rank for mathematics than the traditional criminals ($p < .05$), and a 7.659 lower percentile rank for mathematics than the non-criminals ($p < .05$). The largest differences were found for the percentile ranks for the module on information processing: traditional offenders have a 9.638 lower percentile rank ($p < .01$) and non-criminals a 8.649 ($p < .05$) higher percentile rank compared to cybercriminals.

Moreover, the associations of the control variables with the test scores and percentile ranks were not significant in most cases. Household size only had a significant negative relation with the percentile rank on language ($B = -3.118$; $p < .01$), while a high educational level of the father was only significantly associated with the percentile rank for information processing ($B = 11.979$; $p < .05$). A high educational level of the mother, on the other hand, was significantly and positively related to all outcomes except the percentile rank for information processing. Finally, sample members in the highest income quintile had a significantly higher percentile rank for language than those in the lowest income quintile ($B = 13.230$; $p < .05$).

Table 3 shows the results of the discordant sibling designs in which cybercriminals were compared with their non-offending full-siblings. The results show that these non-offending siblings have better overall CITO test scores ($B = 3.386$; $p = .105$), as well as higher percentile ranks for the modules on language ($B = 10.596$; $p = .071$), mathematics ($B = 7.526$; $p = .209$) and information processing ($B = 15.482$; $p < .05$), compared to the cybercriminals. Nevertheless, only the within-family comparisons on the percentile rank for information processing was significant. The fact that most comparisons were not significant, however, seems to be the consequence of the reduced statistical power due to the lower sample size, since the effect sizes in Table 3 are similar or even larger than those found in the OLS regression analyses (Table 2). This suggests that unmeasured family confounders do not seem to explain the relationship between cybercrime offending and CITO test scores.

5. Discussion

The aim of the present study was to gain more insight into the intellectual capabilities of cybercriminals by comparing them with


a: CITO final test scores

b: Percentile ranks language

c: Percentile ranks mathematics

d: Percentile ranks information processing

Fig. 1. a: CITO final test scores. b: Percentile ranks language. c: Percentile ranks mathematics. d: Percentile ranks information processing.

traditional criminals and non-criminals as well as to their own siblings. Thereby, this study contributes to the limited body of knowledge about differences between cybercriminals and traditional criminals. In order to do this, a unique dataset was used, which contains both CITO test scores, criminal records and additional background information about individuals in the Netherlands. CITO test scores have been empirically shown to be highly correlated with IQ-scores (Bartels et al., 2002) and therefore provide valuable insights into intellectual capabilities of cybercriminals. The results show that cybercriminals who engaged in computer trespassing have significantly higher CITO test scores compared to traditional criminals and significantly lower CITO test scores compared to non-criminals. The same differences in scores apply to specific parts of the CITO test such as mathematics, language and information processing. In addition, observed differences in CITO test scores were similar or even larger after controlling for unmeasured family confounders, although these differences were not significant due to the decreased sample size.

5.1. Theoretical and practical implications

The findings of this study have important theoretical implications. Due to the limited amount of research into cybercriminals, it is debated whether and how cybercriminals differ from traditional criminals (Holt & Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019). Studies suggest that cyber-dependent offenders are generally highly educated and have a high level of intelligence and problem solving capabilities (Turgeman-Goldschmidt, 2005; Rogers, 2006; Chiesa et al., 2009; Koops, 2010; Bachmann, 2011; Jordan, 2017). Nevertheless, the results in these studies are often descriptive in nature and lack statistical comparisons with groups of traditional offenders. Moreover, as it has been suggested that hackers experience more problems and are less motivated at school (Stambaugh et al., 2001; Chiesa et al., 2009),

Table 2
OLS regression analyses.

	Model 1: CITO final test score			Model 2: percentile rank language			Model 3: percentile rank mathematics			Model 4: percentile rank information processing		
	B	S.E.	P	B	S.E.	P	B	S.E.	P	B	S.E.	P
Type of criminal												
Cybercriminals	(ref.)			(ref.)			(ref.)			(ref.)		
Traditional criminals	−2.566	1.092	0.019*	−6.272	3.032	0.039*	−6.883	3.227	0.034*	−9.638	3.452	0.006**
Non criminals	3.042	1.083	0.005**	7.159	3.006	0.018*	7.659	3.120	0.017*	8.649	3.436	0.012*
Household size	-.634	.384	0.099	−3.118	1.065	0.004**	.360	1.134	0.751	-.136	1.209	0.910
Education father												
Low	(ref.)			(ref.)			(ref.)			(ref.)		
Middle	1.627	1.527	0.287	2.104	4.239	0.620	1.297	4.512	0.774	9.374	4.830	0.053
High	2.409	1.705	0.158	4.059	4.732	0.391	3.529	5.037	0.484	11.979	5.390	0.027*
Missing	1.048	1.364	0.443	1.761	3.785	0.642	3.137	4.028	0.437	7.761	4.307	0.072
Education mother												
Low	(ref.)			(ref.)			(ref.)			(ref.)		
Middle	.470	1.341	0.726	2.251	3.723	0.546	1.579	3.963	0.691	1.442	4.281	0.736
High	4.593	1.636	0.005**	9.816	4.540	0.031*	14.314	4.832	0.003**	9.147	5.170	0.078
Missing	2.529	1.236	0.041*	6.298	3.430	0.067	5.291	3.650	0.148	7.423	3.906	0.058
Income quintile												
1 (Low)	(ref.)			(ref.)			(ref.)			(ref.)		
2	−4.141	2.324	0.075	−5.478	6.450	0.396	−7.662	6.865	0.265	−13.720	7.047	0.052
3	.918	2.458	0.709	6.298	6.824	0.357	6.483	7.263	0.373	-.941	7.463	0.900
4	.786	2.324	0.735	6.793	6.451	0.293	3.723	6.866	0.588	1.829	7.072	0.796
5 (High)	2.546	2.342	0.278	13.230	6.499	0.042*	6.979	6.918	0.314	3.933	7.127	0.581
Missing	−1.572	2.158	0.467	1.275	5.990	0.832	−3.570	6.375	0.576	−4.057	6.670	0.543
Constant	530.666	2.427	0.000***	35.545	6.735	0.000***	38.302	7.168	0.000***	33.812	7.474	0.000***
N	429			429			429			390		
Adj. R	0.1634			0.1439			0.1151			0.1526		

Note: *p < .05; **p < .01; ***p < .001. Age, sex and country of birth were not included as control variables since the groups were matched on these variables.

Table 3
Discordant sibling designs.

	Model 1: CITO final test score			Model 2: percentile rank language			Model 3: percentile rank mathematics			Model 4: percentile rank information processing		
	B	S.E.	P	B	S.E.	P	B	S.E.	P	B	S.E.	P
Type of criminal												
Cybercriminal	(ref.)			(ref.)			(ref.)			(ref.)		
Non-criminal Sibling	3.386	2.054	0.105	10.596	5.750	0.071	7.526	5.929	0.209	15.482	6.861	0.029*
Gender (1 = male)	5.172	2.722	0.062	6.374	7.859	0.421	22.609	7.855	0.006**	28.908	9.741	0.005**
Age	0.588	0.493	0.238	1.065	1.363	0.438	1.782	1.423	0.216	0.551	1.676	0.744
Constant	516.386	10.425	0.000***	14.274	28.527	0.619	−5.773	30.086	0.849	9.312	36.607	0.800
N (Individuals)	**120**			**110**			**120**			**92**		
N (Families)	**60**			**55**			**60**			**46**		

Note: *p < .05; **p < .01; ***p < .001. Household size, household income, parental education and country of birth were not included as control variables as these are shared between siblings.

educational attainment and school performance at high school might not be the best indicators of the intellectual capabilities of hackers. The findings of the current study show that cyber-dependent offenders who engaged in computer trespassing already have more intellectual capabilities compared to traditional offenders at age 12, before they start with secondary education. Our study, thus, suggests that the characteristics of offenders of cyber-dependent crimes differ from those of traditional offenders and that they are not simply traditional offenders who have started to commit their crimes online. More empirical work comparing other characteristics of cybercriminals and traditional criminals needs to be done to further explore this issue. In addition, although cybercriminals in our study have higher intellectual capabilities than traditional criminals, our findings indicate that both traditional criminals and cybercriminals have lower intellectual capabilities than non-criminals. This is in line with previous research about the relationship between IQ and crime, showing that criminals have lower intellectual capabilities than non-criminals (Hirschi & Hindelang, 1977; Beaver et al., 2013; Frisell et al., 2012; Jolliffe & Farrington, 2004; Moffitt et al., 1981; Rushton & Templer, 2009; Schwartz et al., 2015). Our results further suggest that differences in intellectual capabilities between cybercriminals and non-offenders could not be explained by unmeasured familial confounders, which offers further evidence for a causal link between IQ and criminal offending. However, most of our results in the discordant sibling analyses were insignificant due to the decreased sample size and, thus, statistical power, and the results of these analyses should therefore be interpreted with some caution.

The differences between cybercriminals and traditional criminals found in this study also have practical implications, for example for correctional services and rehabilitation programs. It is known that offender treatment must be matched with the learning styles of offenders in order to effectively reduce recidivism (Andrews et al., 1990). The program should be adjusted to the intellectual and social capabilities of the offender (van der Laan, 2004). Consequently, correctional services and rehabilitation programs should adapt assignments, therapies and approaches to the higher intellectual capabilities of cybercriminals in comparison to traditional offenders. For example, participants of Hack_Right – an alternative criminal procedure for young Dutch cybercrime offenders – indicate that assignments they had to carry out at probation service were too easy, while the technical assignments they completed at cybersecurity companies during the intervention were more interesting and challenging (Schiks et al., 2021). In line with this reasoning, shaping practices such as coordinated vulnerability disclosure – where hackers who find a vulnerability in an IT-system can report that vulnerability to the IT-system's owner – can play an important role in influencing the decision-making process of cybercriminals to use their competences for legal purposes (Weulen Kranenbarg et al., 2018b). There could be an important role for teachers and parents to recognize the strengths of technically skilled individuals during (early) adolescence and to provide these individuals with opportunities to use their skills appropriately. This can be essential to prevent people from committing cybercrimes.

5.2. Limitations

Besides the strengths of this study, there are also some limitations that need to be discussed. First, the sample of this study consists of cybercriminals who are detected by law enforcement agencies. Although the association between IQ and crime has been found in both studies that rely on officially recorded and self-reported crimes (Moffitt & Silva, 1988), research also shows that offenders who have relatively high IQ scores are more likely to avoid arrest than offenders who have the same amount of self-reported crimes and relatively lower IQ scores (Boccio et al., 2018). This suggests that it is possible that those who were in the non-criminal group of our analyses, may actually have been involved in crime but have never been arrested and sanctioned as a consequence of their higher intellectual capabilities. If this is the case, our analyses overestimate the difference in intellectual capabilities between non-criminals and criminals due to the use of officially registered crime data. In addition, the police lacks investigative capacities and knowledge to effectively investigate cybercrime (Boekhoorn, 2019; Holt et al., 2019), which reduces the chance for cybercriminals to get caught. Therefore, the most intelligent criminals may even have a smaller chance to be arrested for their cybercrimes than for their traditional crimes, and are not included in the cybercriminal group. This may reinforce the effect of detection bias on the relationship between cybercrime and intellectual capabilities, meaning that differential apprehension may be an alternative explanation for the results in our study. Consequently, differences in intellectual capabilities between cybercriminals and traditional criminals may be larger than suggested and differences between cybercriminals and non-criminals may be smaller. Future studies can overcome this detection bias by conducting research based on self-reporting data. Intellectual capabilities and the commission of (cyber)crimes can be measured with questionnaires, to see whether self-reported cybercriminals possess more intellectual capabilities than this study suggests.

Second, only cybercriminals who have taken a CITO test between 2006 and 2018, and were born between 1993 and 2005, are included in the sample. As a result, cybercriminals in this study are younger than the average cybercriminal in the data of Statistics Netherlands. Therefore, the results of this study might not be representative for all cybercriminals.

Finally, the sample consists of individuals who are suspects of computer trespassing, which involves gaining unauthorized access to a computer system. This could be a high tech hack which requires a lot of IT-knowledge, but could also be someone who still knows his or her ex-partners' account password. Based on the data in this study, no distinction could be made between these types of hacks which require different levels of technical capabilities. However, it can be expected that differences in intellectual capabilities may exist between these types of offenders. Future studies should also further explore differences in intellectual capabilities between different types of cybercrimes. As cyber-enabled crimes are more similar to traditional crimes than cyber-dependent crimes, it can be expected that the characteristics of its perpetrators, including intellectual capabilities, also are more similar to those of traditional offenders. On top of that, research in different countries and larger datasets are necessary to further validate the results of this study.

5.3. Conclusion

The current study provides a strong indication that differences exist between intellectual capabilities of cybercrime offenders and traditional offenders. More empirical research is needed to both validate the differences in intellectual capabilities and to explore other characteristics in which cybercriminals might differ from other offenders. This is not only essential to guide theory, but also to guide criminal justice organizations and other institutes to deal with cybercrime effectively.

Credit author statement

J.A.M. Schiks: Conceptualization, Writing – original draft, Investigation, Writing – review & editing, S.G.A. van de Weijer: Conceptualization, Methodology, Writing – original draft, Writing – review & editing, E.R. Leukfeldt: Conceptualization, Supervision, Writing – review & editing

Funding

This work was supported by the Dutch Research Council (NWO) grant number 451-16-014.

References

Andrews, D. A., Zinger, I., Hoge, R. D., Bonta, J., Gendreau, P., & Cullen, F. T. (1990). Does correctional treatment work? A clinically relevant and psychologically informed meta-analysis. *Criminology, 28*(3), 369–404.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759–763.

Bachmann, M. (2011). Deciphering the hacker underground: First quantitative insights. In T. J. Holt, & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 144–168). New York: Information Science Reference.

Bachmann, M., & Corzine, J. (2010). Insights into the hacking underground. *The Future Challenges of Cybercrime, 5*, 31–41.

Bartels, M., Rietveld, M. J., Van Baal, G. C. M., & Boomsma, D. I. (2002). Heritability of educational achievement in 12-year-olds and the overlap with cognitive ability. *Twin Research and Human Genetics, 5*(6), 544–553.

Beaver, K. M., Schwartz, J. A., Nedelec, J. L., Connolly, E. J., Boutwell, B. B., & Barnes, J. C. (2013). Intelligence is associated with criminal justice processing: Arrest through incarceration. *Intelligence, 41*(5), 277–288.

Boccio, C. M., Beaver, K. M., & Schwartz, J. A. (2018). The role of verbal intelligence in becoming a successful criminal: Results from a longitudinal sample. *Intelligence, 66*, 24–31.

Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging.* Den Haag: Boekhoorn: Den Haag: Politie & Wetenschap.

Chan, D., & Wang, D. (2015). Profiling cybercrime perpetrators in China and its policy countermeasures. In R. G. Smith, R. Cheung, & L. Y. C. Lau (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 206–221). London: Palgrave Macmillan.

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers: The science of criminal profiling as applied to the World of hacking.* New York: CRC Press.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. *Crime, Law and Social Change, 67*(1), 55–75.

Donnellan, M. B., Ge, X., & Wenk, E. (2000). Cognitive abilities in adolescent-limited and life-course-persistent criminal offenders. *Journal of Abnormal Psychology, 109*(3), 396–402.

D'onofrio, B. M., Lahey, B. B., Turkheimer, E., & Lichtenstein, P. (2013). Critical need for family-based, quasi-experimental designs in integrating genetic and social science research. *American Journal of Public Health, 103*(S1), S46–S55.

Ellis, L., & Walsh, A. (2003). Crime, delinquency and intelligence: A review of the worldwide literature. *The Scientific Study of General Intelligence*, 343–365.

Fötinger, C., & Ziegler, W. (2004). *Understanding a hacker's mind: A psychological insight into the hijacking of identities.* Krems: Donau-Universität Krems.

Frisell, T., Pawitan, Y., & Långström, N. (2012). Is the association between general cognitive ability and violent crime caused by family-level confounders? *PloS One, 7* (7), Article e41783.

Guay, J.-P., Ouimet, M., & Proulx, J. (2005). On intelligence and crime: A comparison of incarcerated sex offenders and serious non-sexual violent criminals. *International Journal of Law and Psychiatry, 28*(4), 405–417.

Harbinson, E., & Selzer, N. (2019). The risk and needs of cyber-dependent offenders sentenced in the United States. *Journal of Crime and Justice, 42*(5), 582–598.

Hirschi, T., & Hindelang, M. J. (1977). Intelligence and delinquency: A revisionist review. *American Sociological Review, 42*(4), 571–587.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378–395.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society, 29*(8), 906–921.

Jacob, L., Haro, J. M., & Koyanagi, A. (2019). Association between intelligence quotient and violence perpetration in the English general population. *Psychological Medicine, 49*(8), 1316–1323.

Jolliffe, D., & Farrington, D. P. (2004). Empathy and offending: A systematic review and meta-analysis. *Aggression and Violent Behavior, 9*(5), 441–476.

Jordan, T. (2017). A genealogy of hacking. *Convergence, 23*(5), 528–544.

Kennedy, T. D., Burnett, K. F., & Edmonds, W. A. (2011). Intellectual, behavioral, and personality correlates of violent vs. non-violent juvenile offenders. *Aggressive Behavior, 37*(4), 315–325.

Kerstens, J., & Stol, W. (Eds.). (2012). *Jeugd en Cybersafety: Online slachtoffer- en daderschap onder Nederlandse jongeren*. Den Haag: Boom Lemma Uitgevers.

Koops, B. J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), *Transnational criminology manual* (pp. 735–754). Oisterwijk: Wolf Legal Publishers.

Laan, P. H., & Van Der. (2004). Over straffen, effectiviteit en erkenning. De wetenschappelijke onderbouwing van preventie en strafrechtelijke interventie. *Justitiele Verkenningen, 30*(5), 31–48.

Leukfeldt, E. R. (Ed.). (2017). *Research agenda: The human factor in cybercrime and cybersecurity*. The Hague: Eleven International Publishing.

Leukfeldt, E. R., Domenie, M. M. L., & Stol, W. P. (2010). *Verkenning cybercrime in Nederland 2009. Den Haag: Boom Juridische uitgevers*.

Leukfeldt, E. R., & Roks, R. A. (2020). Cybercrimes on the streets of The Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior*, 1–12.

Leukfeldt, E. R., & Stol, W. P. (2012). De rol van internet bij fraudedelicten. *Justitiele Verkenningen, 38*(1), 108–120.

Lu, C. C., Jen, W. Y., Chang, W., & Chou, S. (2006). Cybercrime & cybercriminals: An overview of the Taiwan experience. *Journal of Computers, 1*(6), 11–18.

Maimon, D., & Louderback, E. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*(1), 191–216.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by Juveniles. *Deviant Behavior, 35*(7), 581–591.

Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2012). Incarceration or community placement: Examining the sentences of cybercriminals. *Criminal Justice Studies, 25* (1), 33–40.

McGloin, J. M., Pratt, T. C., & Maahs, J. (2004). Rethinking the IQ-delinquency relationship: A longitudinal analysis of multiple theoretical models. *Justice Quarterly, 21*(3), 603–635.

McGuire, M. (2020). It ain`t what it is, it`s the way that they do it? Why we still don`t understand cybercrime. In E. R. Leukfeldt, & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 3–28). London & New York: Routledge.

McGuire, M., & Dowling, S. (2013). Chapter 1: Cyber-dependent crimes. In *Home office Research report, 75* (pp. 4–34). Cyber crime: A review of the evidence.

Moffitt, T. E., Caspi, A., Harkness, A. R., & Silva, P. A. (1993). The natural history of change to intellectual performance: Who changes? How much? Is it meaningful? *Journal of Child Psychology and Psychiatry, 34*(4), 455–506.

Moffitt, T. E., Gabrielli, W. F., Mednick, S. A., & Schulsinger, F. (1981). Socioeconomic status, iq, and delinquency. *Journal of Abnormal Psychology, 90*(2), 152–156.

Moffitt, T. E., & Silva, P. A. (1988). IQ and delinquency: A direct test of the differential detection hypothesis. *Journal of Abnormal Psychology, 97*(3), 330–333.

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice, 38*(4), 767–772.

Mõttus, R., Guljajev, J., Allik, J., Laidra, K., & Pullmann, H. (2012). Longitudinal associations of cognitive ability, personality traits and school grades with antisocial behaviour. *European Journal of Personality, 26*(1), 56–62.

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & Poot, C. J. de (2017). *Organised Cybercrime in The Netherlands. Empirical findings and implications for law enforcement*. The Hague: WODC.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Pittsburg: Carnegie Mellon Software Engineering Institute.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97–102.

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2020). The digitized opportunity structure of street offending. *British Journal of Criminology*, 1–20.

Rushton, J. P., & Templer, D. I. (2009). National differences in intelligence, crime, income, and skin color. *Intelligence, 37*(4), 341–346.

Schell, B. H., & Melnychuk, J. (2011). Female and male hacker conferences attendees: Their autism-spectrum quotient (AQ) scores and self-reported adulthood experiences. In T. J. Holt, & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 144–168). New York: Information Science Reference.

Schiks, J. A. M., van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2021). *Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right*. Den Haag: Politie & Wetenschap.

Schwartz, J. A., Savolainen, J., Aaltonen, M., Merikukka, M., Paananen, R., & Gissler, M. (2015). Intelligence and criminal behavior in a total birth cohort: An examination of functional form, dimensions of intelligence, and the nature of offending. *Intelligence, 51*, 109–118.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2001). *Electronic crime needs assessment for state and local law enforcement.* Washington: National Institute of Justice.

Statistics Netherlands. (2018). *Safety Monitor 2017 [Veiligheidsmonitor 2017]* (The Hague: Statistics Netherlands).

Statistics Netherlands. (2020). *Safety Monitor 2019 [Veiligheidsmonitor 2019]* (The Hague: Statistics Netherlands).

Statistics Netherlands. (2021). *Citotab: Characteristics Participants Final Test Primary Education [Citotab: Kenmerken Deelnemers Eindtoets Basisonderwijs]*. https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen/microdatabestanden/citotab-kenmerken-deelnemers-eindtoets-basisonderwijs.

Tielbeek, J. J., Johansson, A., Polderman, T. J., Rautiainen, M. R., Jansen, P., Taylor, M., & Posthuma, D. (2017). Genome-wide association studies of a broad spectrum of antisocial behavior. *Jama Psychiatry, 74*(12), 1242–1250.

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

Turgeman-Goldschmidt, O. (2011). Between hackers and white-collar offenders. In T. J. Holt, & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 18–37). New York: Information Science Reference.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime. Draft-February 2013*. New York: United Nations.

Ward, D. A., & Tittle, C. R. (1994). IQ and delinquency: A test of two competing explanations. *Journal of Quantitative Criminology, 10*(3), 189–212.

Weulen Kranenbarg, M., Holt, T. J., & van der Ham, J. (2018b). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science, 7*(1), 1–9.

Weulen Kranenbarg, M., Ruiter, S., van Gelder, J. L., & Bernasco, W. (2018a). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology, 4*(3), 343–364.