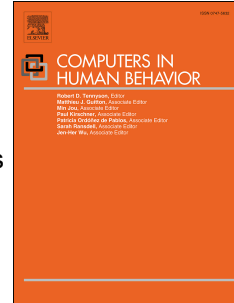


Journal Pre-proof

Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets

Marleen Weulen Kranenborg, Jean-Louis van Gelder, Ard J. Barends, Reinout E. de Vries



PII: S0747-5632(22)00396-X

DOI: <https://doi.org/10.1016/j.chb.2022.107576>

Reference: CHB 107576

To appear in: *Computers in Human Behavior*

Received Date: 15 July 2022

Revised Date: 17 November 2022

Accepted Date: 23 November 2022

Please cite this article as: Kranenborg M.W., Gelder J.-L.v., Barends A.J. & de Vries R.E., Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets, *Computers in Human Behavior* (2022), doi: <https://doi.org/10.1016/j.chb.2022.107576>.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2022 Published by Elsevier Ltd.

Credit Author Statement

Marleen Weulen Kranenbarg: Investigation, Methodology, Original draft preparation, Formal analysis,

Jean-Louis van Gelder: Conceptualization, Methodology, Investigation, Writing-, Reviewing, Editing, Funding acquisition, Supervision

Ard Barends: Writing-, Reviewing, Editing, Formal analysis

Reinout de Vries: Writing-, Reviewing, Editing, Formal analysis

Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets.

1. *Marleen Weulen Kranenborg^a,*
2. *Jean-Louis van Gelder^{b*}*
3. *Ard J. Barends^c*
4. *Reinout E. de Vries^d*
 - a. *Vrije Universiteit (VU) Amsterdam – Department of Criminal Law and Criminology, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands; M.WeulenKranenborg@vu.nl*
 - b. *Max Planck Institute for the Study of Crime, Security and Law - Department of Criminology, Günterstalstraße 73, 79100 Freiburg, Germany; Leiden University, Faculty of Social and Behavioural Sciences; j.vangelder@csl.mpg.de*
 - c. *Leiden University – Department of Criminal Law and Criminology, PO Box 9500, 2300 RA Leiden, The Netherlands; a.j.barends@law.leidenuniv.nl*
 - d. *Vrije Universiteit (VU) Amsterdam - Faculty of Behavioural and Human Movement Sciences, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands; re.de.vries@vu.nl*

* corresponding author

Jean-Louis van Gelder

Max Planck Institute - Department of Criminology

Günterstalstraße 73

79100 Freiburg

Germany

Tel. +49 761 7081 701

j.vangelder@csl.mpg.de

Declaration of interest

The authors declare to have no competing interests.

Acknowledgements

This work was supported by the Netherlands Organisation for Scientific Research (NWO) in the framework of the Cyber Security research program under Grant 12-NROI-058b.

Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets

Abstract

Cyberspace creates opportunities for new forms of crime that may be related to specific personality characteristics of offenders. Few studies have investigated the personality characteristics of cyber offenders. We address this gap by comparing a judicial sample of 261 suspects of cyber-dependent crime, 260 suspects of offline crime, and a community sample of 512 participants on the HEXACO personality domains and their underlying facets. This provides a nuanced picture of the cybercriminal personality and could provide information for prevention and intervention programs. Results indicate that, compared to suspects of offline crime, suspected cyber offenders score significantly lower on extraversion and significantly higher on conscientiousness and openness to experience. Cyber offenders are more similar to community participants on these main personality domains. With regard to the underlying facets, suspected cyber offenders appear to be unique in their relatively high level of diligence. They are more similar to suspected offline offenders on traits that may help them perform criminal activities, such as lower levels of modesty, fearfulness, and flexibility. They are more similar to the community sample, however, on traits that may strengthen their ability or tendency to commit cyber offenses, such as higher levels of patience, perfectionism, and prudence.

Keywords

Cybercrime

Online crime

Offending

Personality

HEXACO domains

HEXACO facets

Journal Pre-proof

1. Introduction

Most types of offline crime (i.e., conventional or traditional crime) have shown a consistent decline over the past decades in the majority of Western countries, including the United States (Morgan & Thompson, 2022), the Netherlands (Akkermans et al., 2022), and the United Kingdom (Office for National Statistics, 2021). Cybercrimes, however, constitute an exception to this development. Both official crime statistics and crime surveys reveal consistent increases in recent years (Akkermans et al., 2022; Federal Bureau of Investigation, 2021; Office for National Statistics, 2021). In the UK, for example, the downward trend in overall crime converts into an upward trend when online fraud and computer misuse are included (Office for National Statistics, 2021).

Offline crimes and cybercrimes also differ in various meaningful ways, in spite of their shared rule-violating and unethical nature and the harm they cause to victims. Cyberspace is a unique context in which interactions have a different nature than in the offline world. For example, offenders and victims do not need to have physical contact in cyberspace, which may lower the threshold for committing cybercrimes (e.g., Suler, 2004). Additionally, cyberspace may require specific skills or characteristics that offline crimes do not (e.g., Gottfredson & Hirschi, 1990; Steinmetz, 2015; Taylor, 1999; Turgeman-Goldschmidt, 2005; Van Der Wagen, 2018). This begs the question whether decades of consolidated knowledge about offender characteristics still apply to this comparatively novel category of offenders. Our goal is to address this question. To do so, we compare the personality characteristics of suspected cyber offenders with those of suspected offline offenders and those of a community sample.¹

¹ It should be noted that the participants in the two judicial samples were suspected of having committed crimes, which means that any given participant in one of these samples may not have been convicted of their alleged crime. We used suspects instead of convicted criminals, as conviction rates for cybercrime are very low—mainly because of evidentiary problems. However, research has shown that generally about 90% of the suspects registered by the

The media often employ stereotypes in their portrayals of cyber offenders, especially the more technically skilled ones, such as criminal hackers. Many of these stereotypes include characteristics reflective of their personalities, such as being socially awkward, loners, computer addicted, etc. (Seigfried-Spellar et al., 2017). Such attribution of specific, personality-related adjectives should come as no surprise. The digital nature of these crimes and the skillsets required to execute them suggest that the characteristics of an individual who is capable of committing them will likely differ from both those of the general population and those of offline offenders. Indeed, our empirical knowledge of offline offenders deviates from such characterizations in important ways: the offline offender tends to be an individual who is driven by quick reward at the expense of considering long-term consequences, has poor self-regulation, has a modest education level and employment records, and leads an irregular lifestyle characterized by histories of drug and alcohol abuse and relationship difficulties (e.g., Farrington & Welsh, 2007; Gottfredson & Hirschi, 1990; but see also Nee et al., 2019).

While previous empirical comparisons between cyber offenders and offline offenders indicate that cyber offenders are unique in that they are less prone to risk factors (e.g., drug use, low self-control) than offline offenders are (Rokven et al., 2018; Weulen Kranenbarg, 2018), research on the personality traits of cybercriminals is largely lacking. Few studies have specifically investigated the personality traits of cyber offenders, with even fewer studies specifically focusing on so-called cyber-dependent offenses, such as hacking (Rogers, Seigfried, & Tidke, 2006; Rogers, Smoak, & Liu, 2006; Seigfried-Spellar & Treadway, 2014; Seigfried-Spellar et al., 2017). Importantly, previous work has relied exclusively on samples of students,

public prosecutor's office are convicted or settle out of court with the public prosecutor (Blom et al., 2005). For the purpose of readability, we will refer to our suspect samples as *offline offenders* and *cyber offenders* in the remainder of this paper.

who may be atypical and may tend to commit less serious cybercrimes. Previous work also has not compared the personality traits of cyber offenders with those of offline offenders. Hence, little is known about the personality traits of cyber offenders and the extent to which it is possible to speak of a cybercriminal personality.

To contribute to this literature, we aim to compare—using the HEXACO personality inventory—the personality traits of a judicial sample of 261 cyber-dependent offenders (the offenses in question are mainly different types of hacking and related criminal behaviors, such as malware use) with those of a sample of 260 offline offenders and those of a community sample of 512 individuals. We compare the three groups on the main HEXACO personality domains as well as on their underlying facets. We discuss differences and similarities between the groups in the light of the existing literature and the nature of the offenses committed by the offender groups.

This article is structured as follows: We start out by reviewing the existing body of research literature on personality traits and offline crime. Subsequently, we discuss the literature, focusing on personality traits and cybercrime. We conclude the introductory section by discussing the present study and our expectations as derived from the literature review. In the Method section, we provide detailed information on our recruitment strategy, how we measured personality traits, and our analytical strategy. In the Results section, we discuss the findings for each HEXACO personality domain separately. In the Discussion section, we review our findings in light of the literature and the nature of the offenses committed by the offender groups. We also discuss strengths and limitations as well as implications for future research and practice. We conclude the article by summarizing our results and their implications for the future.

1.1. Literature review

1.1.1. *Personality and offline crime*

The Big Five (Goldberg, 1990) and Five-Factor Model (FFM) (Costa & McCrae, 1990) of personality assume that the human personality is best described by a handful of broad traits, which are tendencies to show consistent patterns of thoughts, feelings, and actions (McCrae & Costa, 1997). The personality traits incorporated in the Big Five / FFM are openness to experience, conscientiousness, extraversion, agreeableness, and emotional stability (versus neuroticism). Of the Big Five / FFM traits, agreeableness and conscientiousness (and, to a lesser extent, neuroticism or emotionality) emerge as the strongest correlates of antisocial and aggressive behavior in meta-analyses (Jones et al., 2011; Miller & Lynam, 2001). Both conscientiousness and agreeableness are also related to self-control and impulsivity, which have often been studied in relation to criminal behavior (e.g., Caspi et al., 1994; De Vries & Van Gelder, 2013; Gottfredson & Hirschi, 1990; Pratt & Cullen, 2000; Van Gelder & De Vries, 2012, 2014), and similar personality traits have been linked to Antisocial Personality Disorder (Ruiz et al., 2008).

1.1.1.1. *From Big Five to Big Six*

Reanalysis of the original lexical data that were used to uncover the Big Five traits and analyses of data that have since become available have demonstrated the existence of a sixth cross-culturally replicable personality dimension termed *honesty-humility* (Ashton et al., 2004; Lee & Ashton, 2004). A growing body of empirical research indicates that the six-factor model, known by the acronym “HEXACO,” provides a more comprehensive description of personality than its five-factor predecessors (Ashton et al., 2014; De Vries et al., 2016).

The HEXACO and Big Five models are, by and large, isomorphic with respect to three of their dimensions: extraversion, conscientiousness, and openness to experience. They differ in two of their dimensions, with content referring to anger and irritability shifted from Big Five / FFM neuroticism to HEXACO agreeableness and content referring to sentimentality shifted from Big Five / FFM agreeableness to HEXACO emotionality (Ashton et al., 2014). That is, the HEXACO model distinguishes more clearly between internally directed emotions (emotionality; e.g., fearfulness, anxiety) and externally directed emotions (agreeableness; e.g., anger, irritability) (Gaughan et al., 2012; Knight et al., 2018; Lee & Ashton, 2012).

The main difference between the Big Five / FFM and HEXACO models, however, is the addition of the honesty-humility dimension in the latter. This trait refers to individual differences in the tendency to be interpersonally genuine, to be unwilling to take advantage of others for personal gain or to break rules, to avoid fraud and corruption, to be uninterested in status and wealth, and to be modest and unassuming (Lee & Ashton, 2004). The honesty-humility dimension is marked by characteristics largely absent from the Big Five / FFM, such as sincerity, fairness, greed avoidance, and modesty, on the one hand, versus deceitfulness, slyness, greediness, and pretentiousness, on the other (Paunonen & Jackson, 2000)—traits with obvious relevance for the study of crime and unethical behavior (Ashton et al., 2014). Prior research has indeed shown that offline offenders have significantly lower levels of honesty-humility than the general population (Montalto, 2021; Rolison et al., 2013; Ścigala et al., 2022).

By virtue of the inclusion of honesty-humility, the HEXACO model has been shown to outperform five-factor models and to explain incremental variance in a number of important behavioral criteria related to aggression and crime, such as psychopathy, Machiavellianism,

egoism, immorality, pretentiousness, unethical decision making, and employee integrity (Ashton & Lee, 2008; De Vries & Van Kampen, 2010; Gaughan et al., 2012; Lee & Ashton, 2005).

1.1.1.2. Comparing different types of offending

In contrast to the literature discussed above, Miller and Lynam (2001) observed that research on the relationship between personality traits and criminal behavior should differentiate between specific types of offending rather than use broadly defined outcome variables, such as anti-social behavior or crime. For example, Moffitt et al. (2000) compared partner abuse and general crime and found that, while negative emotionality (similar to HEXACO agreeableness) predicted both types of behavior, weak constraint (similar to low self-control or low conscientiousness) was related only to general crime, not to partner abuse. Unfortunately, although there are studies that examine personality traits for specific types of offending, empirical comparisons between a specific type of offending and general offending, such as the one by Moffitt et al. (2000) and a similar comparison by Varley Thornton et al. (2010), are scarce. In the present study, we will contribute to the literature by comparing cyber offenders, offline offenders, and a community sample.

1.1.2. Personality and cybercrime

To be able to compare cyber offenders with offline offenders, it is important to address the existing knowledge on personality of cyber offenders. Although most people use their computers on a daily basis for work purposes, social activities/networking, and entertainment, only few people use their computers to commit cybercrimes. Who are the people who commit these crimes? According to the Situation-Trait-Outcome Activation (STOA) model (De Vries et al., 2016), (1) people tend to select situations that “fit” their personality (situation activation), (2) different traits are expressed in different situations (trait activation), and (3) different outcomes

occur based on the level of traits expressed (outcome activation). With respect to cybercrime, this implies that—based on their personality traits—some people may exploit situations (i.e., online opportunities) in which they can anonymously hack into other computer systems or distribute malware for fun or for personal gain (situation activation). In such situations, they are more likely to express traits that are conducive to their criminal intent (trait activation), which may—or may not—result in outcomes they want (outcome activation; e.g., immaterial or material gain).

Before turning to the traits that may be important to the selection of criminogenic cyber situations and that are activated in situations leading some—but not others—to commit cybercrimes, some limitations of prior research into the relationship between personality and cybercrime should be discussed. The limited number of prior studies on cyber offending relied primarily on small samples, often of undergraduate students. While these studies provided a number of initial insights into the personality characteristics related to cyber offending, most students are probably not involved in serious or sophisticated cyber offending. Students who commit cyber offenses may also differ from the general population of cyber offenders as regards, for example, their educational level and social status. A number of other studies have examined how personality relates to cyber-enabled offending, such as software piracy (Tan et al., 2016) or digital aggression (Kim et al., 2020), or even used a broad outcome variable including a combination of cyber-enabled and cyber-dependent offenses (Palmieri et al., 2021). But when it comes to the personality correlates of purely cyber-*dependent* offending, which is the focus of this study, we were able to identify only a few studies that address this topic.

Perhaps unsurprisingly, the findings of this prior work on cyber-dependent offending do not point in a clear direction. Studies using different types of student samples reveal different

personality characteristics. For example, among information-technology students in the United States, extraversion is negatively related to cyber offending (Rogers, Seigfried, & Tidke, 2006), whereas among liberal-arts students in Canada, there is no significant relationship between extraversion and cyber offending (Rogers, Smoak, & Liu, 2006). A later study by Seigfried-Spellar and Treadway (2014) attempted to overcome the limitations of these earlier studies by differentiating between different types of students and different types of cyber offending. In this study, no significant differences regarding extraversion emerged between non-offenders and students who committed different types of cyber offenses. Furthermore, students who committed any of the cyber offenses were less agreeable (more antagonistic) than non-offenders. Lastly, as a follow-up to these Big Five personality studies, Seigfried-Spellar et al. (2017) used the Elemental Psychopathy Assessment (which is based on Big Five personality traits) to examine the extent to which psychopathy is related to cyber offending. Their results indicate that, similar to individuals who engage in other types of anti-social behavior, cyber offenders score relatively high on psychopathy traits—specifically antagonism, disinhibition, and narcissism.

The limited number of studies and mixed findings of this body of research do not allow us to infer clear hypotheses about the personality of cyber-dependent offenders. Yet several other studies have investigated elements in the behavior of cyber offenders that could be related to personality traits. Below, we link this research to the six HEXACO personality domains and their underlying facets.

1.1.2.1. HEXACO personality domains and facets and cybercrime

In the following, we will consecutively discuss the theoretically and empirically derived relationships of the HEXACO domains—honesty-humility, emotionality, extraversion, agreeableness, conscientiousness, and openness to experience (including some of the underlying

facets) —with cyber offending. With respect to *honesty-humility*, behavior that is unethical, deceitful, sly, and manipulative may be useful for the purpose of exploiting others in cyber settings (e.g., by means of “phishing”). However, research on traits resembling honesty-humility shows mixed results. Whereas Rogers, Smoak and Liu (2006) find that cyber offenders are more exploitive/manipulative than non-offenders, Rogers, Seigfried, and Tidke (2006) find no significant difference in exploitive/manipulative behavior. With respect to the possibility that cyber offenders might be inclined to break ethical rules, Rogers, Smoak and Liu (2006) conclude that cyber offenders tend to have flexible ethical boundaries and do not internalize general norms. Similarly, several other studies also suggest that the morality of cyber offenders is underdeveloped or based on their own (non-conventional) moral values (Seigfried-Spellar & Treadway, 2014; Young et al., 2007). This is further supported by the research on neutralization techniques among hackers (e.g., Chua & Holt, 2016; Hutchings & Clayton, 2016; Morris, 2011; Turgeman-Goldschmidt, 2009) and is also related to the online disinhibition effect (Suler, 2004), according to which individuals are more likely to break ethical rules online than in the physical world. Additionally, Van Der Wagen (2018) suggested that some skilled hackers have a strong sense of self-importance, as they believe they can do things other people are not capable of, and research by Woo (2003) suggests that they possibly also possess some narcissistic traits.

Although the studies mentioned above suggest that cyber offenders score low on honesty-humility and facets such as *modesty*, it should be noted that a number of cyber offenders may not be motivated by financial gain and may instead commit crimes out of curiosity, for the thrill, or because they relish the challenge of breaking into computer systems (Bachmann, 2011; Denning, 2011; Holt, 2007, 2009; Turgeman-Goldschmidt, 2005, 2008, 2011; Van Der Wagen et al., 2016; Voiskounsky & Smyslova, 2003; Weulen Kranenbarg, 2018; Woo, 2003). In contrast to the

present study, research on financially motivated cyber offenders generally analyzes organized cybercrime (Kruisbergen et al., 2018; Lusthaus, 2018). As most cyber offenders in the present study are individual offenders who have indicated that they are not primarily motivated by financial gain (XXX – anonymized reference), they may score higher on the *greed avoidance* facet of honesty-humility compared to other cyber offenders. Nevertheless, even though they may not benefit financially, if they receive intellectual gratification or a boost in social status in their community from committing these crimes, this could still be perceived as personal profit.

In contrast to the honesty-humility domain, there is not much research available on cyber offenders that is related to *emotionality*. As suggested by the online disinhibition effect (Suler, 2004), some researchers have argued that cyber offenders have a lack of empathy towards their victims (Schell & Melnychuk, 2011) or a lack of insight into the consequences for their victims (Morris, 2011; Turgeman-Goldschmidt, 2009). In addition, it has been shown that cyber offenders have a high risk propensity (Bachmann, 2010) and therefore it seems plausible that they score low score on the emotionality domain. Apart from such research suggesting that cyber offenders may score low on some aspects of emotionality, there is not much research that can be used to derive clear hypotheses in the present context.

In relation to the mixed results regarding *extraversion* already discussed above (Rogers, Seigfried, & Tidke, 2006; Rogers, Smoak, & Liu, 2006; Seigfried-Spellar & Treadway, 2014), a number of studies suggest that autism-related traits or other characteristics related to (low) extraversion are more common among technically skilled cyber offenders (Aiken et al., 2016; Harvey et al., 2016; National Crime Agency, 2017; Payne et al., 2019). Some aspects of autism, such as attention to detail and systemization, can be helpful in facilitating cyber-attacks (Schell & Melnychuk, 2011). It should be noted, however, that no research employing rigorous study

designs exists in this area, and existing studies have yielded mixed results (Ledingham & Mills, 2015; Seigfried-Spellar et al., 2015). In addition, many skilled hackers say that they do not agree with this stereotype (which is also the main stereotype used in the media); they argue that they may not have as many conventional social contacts but that their online community is a very important part of their social life in which they learn in interaction with their online peers (e.g., Steinmetz, 2015; Van Der Wagen et al., 2019).

How does cyber offending relate to *agreeableness*? Here, it should be noted that some cyber offenses are committed out of revenge or anger or as so-called hacktivism (Denning, 2011; Holt, 2009; Taylor, 1999; Weulen Kranenbarg, 2021; Woo et al., 2004). DDoS-attacks or website defacements, for example, are often targeted against specific people or organizations. This indicates how critical some cyber offenders are towards others, which may motivate them to commit these crimes and may point to the presence of low agreeableness.

With respect to *conscientiousness*, researchers studying cyber offenders have often argued that cyber offenders work very systematically and need to acquire advanced skills to commit their offenses. Cyber offenders work towards a goal and gain new knowledge along the way (Maimon et al., 2014; Steinmetz, 2015; Van Der Wagen, 2018). Some even experience a state of flow when they are committing their crimes (Voiskounsky & Smyslova, 2003). It is therefore hardly surprising that some studies have found that cyber offenders have a relatively high degree of self-control, which shows relevant overlap with conscientiousness (Bossler & Burruss, 2011; Holt & Kilger, 2008; Weulen Kranenbarg et al., 2019). Conversely, there are also several studies that find that cyber offending is sometimes related to low self-control (Donner et al., 2014; Hu et al., 2013; Marcum et al., 2014; Seigfried-Spellar & Treadway, 2014), especially if skills are learned not through trial and error but by imitating deviant friends (Bossler &

Burruss, 2011; Holt et al., 2012). Additionally, cyber offenders may have a high risk propensity (Bachmann, 2010) and may experience difficulties controlling their behavior because of a computer addiction (Schell & Melnychuk, 2011; Taylor, 1999). For some, once they enter a computer system, the temptation to continue hacking may simply be too strong to overcome, resulting potentially in their misuse of the system (Van Der Wagen, 2018). Overall, it seems that high conscientiousness could be a very helpful personality trait for cyber offenders, but, given that these offenders commit crimes instead of using their skills in a legitimate information-technology-related profession, they may show a tendency towards hedonistic behavior and low self-control.

Lastly, with respect to *openness to experience*, cyber offenders also use their analytic skills to analyze computer systems and find new and innovative ways of using them. Making a system do something it was not meant to do is even part of many definitions of hacking. Cyber offenders can be creative, look for the limits of computer systems, and try to change them. Many are motivated by the challenge of mastering computer systems (Steinmetz, 2015; Taylor, 1999; Turgeman-Goldschmidt, 2005; Van Der Wagen, 2018). These characteristics suggest that cyber offenders may score relatively high on openness to experience.

1.1.3. *The Present Study*

The present study will use a unique sample to investigate the extent to which cyber offenders differ from offline offenders and the general population on the HEXACO personality domains and their underlying facets. Based on the discussion of the literature on both offline crime and cybercrime above, we anticipate that both cyber offenders and offline offenders will score low on honesty-humility and agreeableness. With respect to extraversion, cyber offenders are expected to score lower than offline offenders. Regarding both conscientiousness and openness

to experience, cyber offenders are expected to score higher than offline offenders. It should be noted, however, that we do not expect that these domain-level relationships will necessarily hold for all underlying facets, which is why we will empirically compare both the general domains and the facets.

2. Method

2.1. Sample and procedure

We collected offender data as part of a comparative study on cyber offenders and offline offenders (see XXX – anonymized reference). The data come from a sample of respondents who had been formally suspected of committing either a cyber-dependent crime or an offline crime during the period 2000–2013. We selected this purposive sample with the help of the public prosecutor's office in the Netherlands. The office chose all 928 individuals suspected of committing a cybercrime during this period and a random sample of 875 individuals suspected of committing an offline crime. Afterwards, we invited these individuals to participate in the study by sending them a letter explaining the scope, confidentiality, and anonymity of the study. The letter also informed participants that they would receive a €50 voucher in exchange for their participation.

For the group of suspected cyber offenders, the response rate was 29.42%. For the group of suspected offline offenders, the response rates were much lower. After two reminders, only 150 individuals in the latter group participated in the study. Therefore, we invited another random sample of 781 offline offenders to participate. After again two reminders, 16.04% percent of all offline offenders responded, resulting in a final sample of 280 offline offenders and 273 cyber offenders (77.50% male; $M_{\text{age}} = 36.90$; $SD_{\text{age}} = 13.06$).

For the community sample, we used an ISO-certified online panel dataset, as reported in De Vries and Born (2013). The original dataset contained 525 participants (48.00% male; $M_{\text{age}} = 51.17$ $SD_{\text{age}} = 13.90$), with educational levels varying from low (e.g., only primary school education; 2.1%) to high (e.g., university education; 9.9%) (see De Vries & Born, 2013).

We used response quality screening for the personality questionnaire in this study, as discussed by Barends and De Vries (2019); as a consequence, we removed the data of 37 participants. Specifically, the raw responses to all personality items showed too little variation ($SD \leq .70$) for nine cybercrime participants, nine offline crime participants, and 13 participants from the community sample. After recoding the necessary responses, we used average standard deviations of item responses for the six personality domains to find responses with too much inconsistency (if $SD \geq 1.60$). As a result, we removed the data of two cyber offenders and four offline offenders. Lastly, eight respondents (one cyber offender and seven offline offenders) had a missing value on one of the background variables and we excluded them from the analyses. The final sample included 1033 participants (62.4% male; $M_{\text{age}} = 43.87$ $SD_{\text{age}} = 15.29$).

2.2. Measures

After receiving the invitation letter to participate in the study, the offender groups completed an online survey by logging onto the study website with the details stated in the letter. The first page of the website contained an informed consent form and further details on the purpose and procedure of the study. Next, the survey started by asking about background information, including age, gender, ethnicity, and educational level. This was directly followed by the HEXACO personality questionnaire that we used for this paper.

To measure HEXACO personality, we used the HEXACO Simplified Personality Inventory (HEXACO-SPI; De Vries & Born, 2013), which is designed to be suitable for

respondents with language difficulties and lower educational levels. The HEXACO-SPI contains 96 items that measure the main six HEXACO domains (16 items each) and the underlying 24 facets (four items each). After recoding the responses to reverse-scored questions, we combined the individual items into 24 facet variables and six domain variables. See Table 1 for the correlation matrices of the domain variables and Appendix A for the correlation matrices of the facet variables. See Tables 2 and 3 for the alpha reliability scores per group on the individual facets and domains.

Table 1. Correlation matrix of domain-level variables for full sample, community sample, offline sample, and cyber sample

	H	E	X	A	C	O
H	-	-.01 / -.01 / .03	-.01 / .01 / .07	.20 / .22 / .15	.23 / .31 / .29	-.23 / -.20 / -.19
E	.05	-	-.14 / -.20 / -.21	-.06 / .12 / .02	-.05 / -.01 / -.06	-.09 / -.02 / -.19
X	-.01	-.19	-	.06 / .00 / .12	.24 / .20 / .36	.13 / .04 / -.02
A	.19	.02	.05	-	.11 / .21 / .11	-.04 / -.01 / .05
C	.28	-.01	.24	.15	-	.01 / .07 / -.11
O	-.2	-.08	.06	.00	.01	-

Note. Above diagonal (divided by /): community sample (N = 512) / offline sample (N = 267) / cyber sample (N = 262).

Below diagonal: full sample (N = 1041).

Table 2 includes all domain names and the corresponding codes used in this table.

It should be noted that, in the survey presented to among cyber offenders and offline offenders, we replaced three standard items in the HEXACO personality questionnaire (“I am allowed to break the rules”, “I am above the law”, and “I would rather die than steal”) with three different items from the HEXACO-PI-R questionnaire (Lee & Ashton, 2006), as the standard items demonstrated risk of predictor-criterion overlap. However, as the survey for the community sample included only original items, we excluded these from the facets and Honesty-

Humility domain scores for all three groups. This exclusion resulted in reduced alpha reliabilities (see Tables 2 and 3). The alpha reliability on the Honesty-Humility domain was still adequate ($\alpha = .74$).²

Given that Cronbach alpha is a rather imprecise lower bound estimate of internal consistency reliability (Sijtsma, 2009), we calculated two additional reliabilities. These two reliabilities, the general lower bound (*glb*; Sijtsma, 2009) and omega total (ωt ; Revelle & Zinbarg, 2009), are also lower bound estimates of reliability, but are closer approximations of the true reliability of scales (Revelle & Zinbarg, 2009). These additional reliability estimates of the HEXACO domains and facets for each of the three groups are reported in Table S1 in the online supplement and generally show somewhat higher reliabilities than the Cronbach alpha does. It should be noted, however, that the reliabilities for some facets are below the standard threshold of .70.

2.3. Checking for socially desirable responding

In line with Dunlop et al. (2020), we used extreme response counts to check for social desirability, comparing the medians between the groups ($Mdn_{community} = 6$; $Mdn_{cyber} = 8$; $Mdn_{offline} = 7$). Subsequent Kruskal-Wallis and Mann-Whitney U tests showed that the cyber sample and offline sample did not differ from each other but that both displayed more extreme responses compared to the community sample. In all three groups, these extreme responses are similarly correlated to the personality domains. Applied to the extreme response counts for each domain separately, the tests showed that the cyber sample and offline sample did not differ from each other in the frequency of extreme responses on any of the domains. However, both groups had

² Additional analyses including all items showed very similar results for the comparison between the cyber sample and the offline sample, but the results also revealed important differences in the comparison with the community sample (results available upon request).

significantly more extreme responses on Emotionality, Extraversion, and Agreeableness compared to the community sample. Additionally, the cyber sample participants had significantly more extreme responses on Openness to Experience than the community sample participants.³

To further check the extent to which participants in both offender samples faked their responses, we checked for the general factor saturation of a bi-factor model of the item-level HEXACO data. Such a general factor emerges when people fake their responses and generally does not emerge in standard research settings (Ashton et al., 2020). We checked for this general factor saturation by using McDonald's omega hierarchical (ω_h) and the OmegaSem procedure in the "psych" package in R (Revelle, 2018). Evidence for a general factor would be observed if ω_h was greater than .50 (Arias et al., 2018). However, we found no meaningful indication of a general factor in either the community sample ($\omega_h = .28$) or the combined offender sample ($\omega_h = .37$).

2.4. Analytical strategy

We first compared all three groups on their mean domain scores (Table 2) and additionally ran a multinomial logit model (Table 4) to examine to what extent scores on these six domains were able to predict the group to which a respondent belonged. Furthermore, we compared the means on the facets underlying the domains (Table 3) in order to provide a more complete understanding of the way the groups differed on personality. As background characteristics (such as age and gender) differed between the three groups, we used MANCOVA analyses, including age (and age-squared), gender, ethnicity, and educational level as covariates for the mean comparisons. The MANCOVA procedure is also suitable for unbalanced data, such as the data

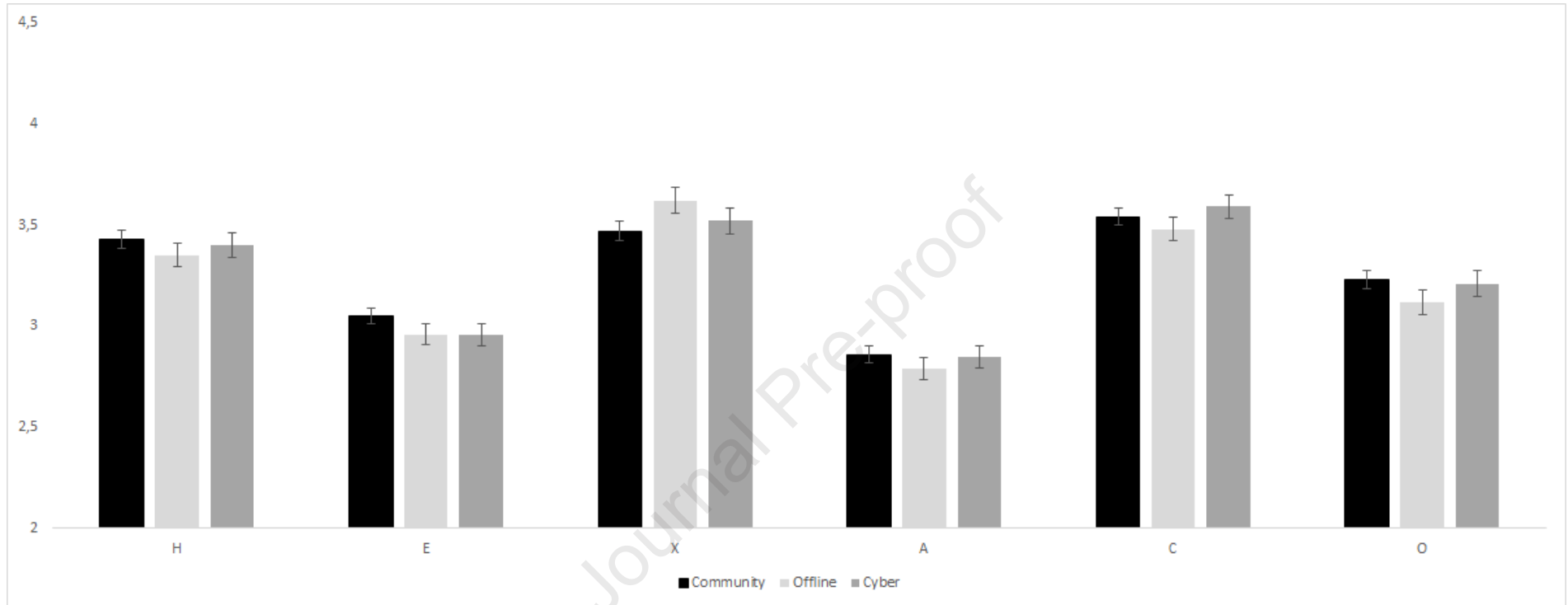
³ Results are available upon request.

used in this study. The means, standard deviations, and test statistics in Tables 2 and 3 have therefore been corrected for differences in these background characteristics. We also controlled for these variables in the multinomial model.

3. Results

As shown in Figure 1 and Table 2, we found the most important domain-level differences between cyber offenders and offline offenders on Extraversion, Conscientiousness, and Openness to Experience. On the domain level, cyber offenders are more similar to community participants than they are to offline offenders. At the facet level, we found many differences on the Conscientiousness facets (Diligence, Perfectionism, and Prudence), and a number of other domain facets, such as Patience and Inquisitiveness, also show interesting differences (see Table 3 and additional figures in the online supplement). It appears that cyber offenders are more similar to offline offenders on facet-level traits that may help them perform criminal activities, but they are more similar to the community sample on characteristics that may strengthen their ability or tendency to commit cyber offenses. The following paragraphs will detail these results for each HEXACO personality domain and the underlying facets.

Figure 1. Mean HEXACO personality domain scores and 95% confidence intervals for the community, offline, and cyber samples



Note: Table 2 includes all domain names and the corresponding codes used in this figure.

Table 2. Domain-level descriptive statistics and tests for mean differences between groups based on MANCOVA

		Community sample ($N = 512$)			Offline sample ($N = 260$)			Cyber sample ($N = 261$)			Test community-offline		Test community-cyber		Test offline-cyber	
		α	M	SD	α	M	SD	α	M	SD	t	Cohen's d	t	Cohen's d	t	Cohen's d
Main HEXACO Domains																
H	Honesty-Humility	.74	3.43	.50	.71	3.35	.48	.71	3.40	.49	-2.03 *	-.16	-0.84	-.07	1.13	.10
E	Emotionality	.78	3.05	.47	.67	2.96	.44	.75	2.96	.45	-2.45 *	-.20	-2.37 *	-.19	0.02	.00
X	Extraversion	.86	3.47	.55	.83	3.62	.53	.85	3.52	.54	3.34 ***	.27	1.05	.08	-2.19 *	-.18
A	Agreeableness	.76	2.86	.46	.74	2.79	.44	.74	2.85	.45	-1.87	-.15	-0.25	-.02	1.56	.13
C	Conscientiousness	.78	3.54	.49	.80	3.48	.46	.78	3.59	.47	-1.60	-.13	1.33	.11	2.86 **	.24
O	Openness to Experience	.80	3.23	.54	.80	3.12	.51	.80	3.21	.52	-2.57 **	-.21	-0.43	-.03	2.05 *	.17

Note. The means, standard deviations, and test statistics are corrected for age, age-squared, gender, ethnicity, and education in MANCOVA.

As a result of missing data on these background characteristics, the N of both offender samples is slightly lower than in Table 1.

* $p < .05$. ** $p < .01$. *** $p < .001$.

Table 3. Facet-level descriptive statistics and tests for mean differences between groups based on MANCOVA

		Community sample ($N = 512$)			Offline sample ($N = 260$)			Cyber sample ($N = 261$)			Test community-offline		Test community-cyber		Test offline-cyber	
		α	M	SD	α	M	SD	α	M	SD	t	Cohen's d	t	Cohen's d	t	Cohen's d
HEXACO Facets																
H1	Sincerity	.66	3.21	.75	.61	3.25	.71	.62	3.32	.73	0.61	.05	1.70	.14	1.10	.09
H2	Fairness	.48	3.60	.78	.47	3.56	.74	.41	3.64	.76	-0.69	-.06	0.71	.06	1.37	.12
H3	Greed Avoidance	.57	3.30	.71	.58	3.17	.67	.63	3.20	.69	-2.45 *	-.20	-1.78	-.14	0.60	.05
H4	Modesty	.33	3.61	.77	.06	3.43	.74	.18	3.43	.75	-2.92 **	-.23	-2.90 **	-.24	-0.06	.00
E1	Fearfulness	.64	3.12	.72	.52	2.90	.68	.58	2.98	.70	-3.94 ***	-.32	-2.41 *	-.20	1.42	.12
E2	Anxiety	.70	3.06	.76	.58	2.93	.72	.60	2.98	.74	-2.13 *	-.17	-1.24	-.10	0.83	.07
E3	Dependence	.78	2.77	.73	.58	2.78	.70	.68	2.71	.71	0.10	.01	-1.13	-.09	-1.22	-.10
E4	Sentimentality	.72	3.24	.74	.61	3.23	.71	.68	3.17	.72	-0.25	-.02	-1.22	-.10	-0.97	-.08
X1	Social Self-Esteem	.79	3.98	.62	.71	4.03	.59	.76	3.97	.60	0.95	.08	-0.34	-.03	-1.26	-.11
X2	Social Boldness	.81	2.93	.86	.70	3.32	.82	.74	3.13	.84	5.82 ***	.47	2.95 **	.24	-2.70 **	-.23
X3	Sociability	.77	3.21	.77	.63	3.35	.73	.71	3.28	.74	2.39 *	.19	1.12	.09	-1.21	-.10

X4	Liveliness	.81	3.78	.77	.76	3.77	.74	.80	3.71	.75	-0.08	-.01	-1.13	-.09	-1.04	-.09
A1	Forgivingness	.61	2.72	.67	.41	2.81	.63	.53	2.78	.65	1.82	.15	1.15	.09	-0.62	-.05
A2	Gentleness	.56	3.13	.62	.49	3.04	.59	.45	3.07	.60	-1.80	-.14	-1.08	-.09	0.66	.06
A3	Flexibility	.59	2.71	.61	.52	2.54	.58	.55	2.59	.60	-3.46 ***	-.28	-2.37 *	-.19	0.99	.08
A4	Patience	.69	2.87	.78	.64	2.76	.74	.68	2.94	.76	-1.84	-.15	1.16	.09	2.92 **	.25
C1	Organization	.82	3.46	.90	.80	3.44	.85	.79	3.52	.87	-0.22	-.02	0.88	.07	1.09	.09
C2	Diligence	.53	3.44	.65	.52	3.47	.61	.56	3.58	.63	0.63	.05	2.73 **	.22	2.10 *	.18
C3	Perfectionism	.74	3.81	.65	.60	3.71	.61	.68	3.82	.63	-2.06 *	-.17	0.15	.01	2.14 *	.18
C4	Prudence	.60	3.43	.65	.62	3.28	.62	.53	3.43	.64	-3.06 **	-.24	-0.10	-.01	2.86 **	.24
O1	Aesthetic Appreciation	.75	3.19	.85	.70	3.02	.80	.71	2.99	.82	-2.48 *	-.20	-2.91 **	-.24	-0.49	-.04
O2	Inquisitiveness	.71	3.63	.81	.77	3.42	.77	.70	3.68	.78	-3.30 ***	-.26	0.77	.06	3.94 ***	.33
O3	Creativity	.67	3.26	.70	.55	3.27	.66	.56	3.33	.68	0.17	.01	1.39	.11	1.21	.10
O4	Unconventionality	.61	2.84	.71	.52	2.77	.67	.68	2.83	.69	-1.28	-.10	-0.08	-.01	1.16	.10

Note. The means, standard deviations, and test statistics are corrected for age, age-squared, gender, ethnicity, and education in MANCOVA.

As a result of missing data on these background characteristics, the N of both offender samples is slightly lower than in Table 1.

* $p < .05$. ** $p < .01$. *** $p < .001$.

3.1. Honesty-Humility

Cyber offenders and offline offenders are similar in their scores on Honesty-Humility, but they both score lower than the community sample on this domain. However, this difference is significant only for offline offenders ($t_{offline}(1020) = -2.03, p < .05$). The multinomial model shows similar results, although it should be noted that the difference between offline offenders and the community sample is here only marginally significant (*Relative Risk Ratio* (RRR) = .67, $p = .06$). With respect to the underlying facets, we again see similar scores for cyber offenders and offline offenders and no significant differences between these two groups. Compared to the community sample, however, both cyber offenders and offline offenders score significantly lower on the Modesty facet ($t_{cyber}(1020) = -2.90, p < .01$; $t_{offline}(1020) = -2.92, p < .01$). Offline offenders also score significantly lower on Greed Avoidance ($t_{offline}(1020) = -2.45, p < .05$) compared to the community sample.

3.2. Emotionality

As with the Honesty-Humility domain, both offender groups are very similar in their scores on the Emotionality domain and its underlying facets, with no significant differences emerging. Again, both cyber offenders and offline offenders score significantly lower on Emotionality than the community sample ($t_{cyber}(1020) = -2.37, p < .05$; $t_{offline}(1020) = -2.45, p < .05$). This result holds in the multinomial model as well. It is mainly driven by the difference between the community sample and the offender groups on the Fearfulness facet ($t_{cyber}(1020) = -2.41, p < .05$; $t_{offline}(1020) = -3.94, p < .001$). Additionally, the offline offenders score significantly lower than the community sample on Anxiety ($t_{offline}(1020) = -2.13, p < .05$).

3.3. Extraversion

In contrast to their patterning on the first two domains, the offender groups clearly differ on the Extraversion domain and its underlying facets. Cyber offenders score significantly lower

than offline offenders on this domain ($t_{cyber}(1020) = -2.19, p < .05$). Additionally, while offline offenders score significantly higher than the community sample on Extraversion ($t_{offline}(1020) = 3.34, p < .001$), cyber offenders do not differ significantly from the community sample ($t_{cyber}(1020) = 1.05, p = .30$). Results in the multinomial model are identical. We also observed these differences at the facet level. Although both offline offenders and cyber offenders score significantly higher than the community sample on Social Boldness ($t_{cyber}(1020) = 2.95, p < .01$; $t_{offline}(1020) = 5.82, p < .001$), cyber offenders still score significantly lower than offline offenders on this facet ($t_{cyber}(1020) = -2.70, p < .01$). Lastly, offline offenders also score significantly higher on the Sociability facet than the community sample ($t_{offline}(1020) = 2.39, p < .05$).

3.4. Agreeableness

With regard to the Agreeableness domain, there are no significant overall differences between the three groups, also not in the multinomial model. However, a difference between cyber offenders and offline offenders do emerge at the facet level. Cyber offenders score slightly higher than the community sample on the Patience facet, while offline offenders score slightly lower than the community sample. Consequently, cyber offenders score significantly higher than offline offenders on Patience ($t_{cyber}(1020) = 2.92, p < .01$). Cyber offenders and offline offenders are similar in their scores on the Flexibility facet, and both score significantly lower than the community sample ($t_{cyber}(1020) = -2.37, p < .05$; $t_{offline}(1020) = -3.46, p < .001$).

3.5. Conscientiousness

Various differences between cyber offenders and offline offenders emerge for the Conscientiousness domain and its underlying facets. As with Agreeableness, cyber offenders score slightly higher than the community sample, while offline offenders score slightly lower than the community sample, resulting in a statistically significant difference between cyber

offenders and offline offenders on Conscientiousness ($t_{cyber}(1020) = 2.86, p < .01$). Results in the multinomial model are identical. In line with these results on the domain level, cyber offenders also have the highest scores on the facets underlying Conscientiousness. Compared to offline offenders, they score significantly higher on three of the four facets: Diligence ($t_{cyber}(1020) = 2.10, p < .05$), Perfectionism ($t_{cyber}(1020) = 2.14, p < .05$), and Prudence ($t_{cyber}(1020) = 2.86, p < .01$). Compared to the community sample, too, cyber offenders score significantly higher on the Diligence facet ($t_{cyber}(1020) = 2.73, p < .01$), showing that they are unique in their high score on Diligence. Offline offenders score lower than the community sample on both Perfectionism ($t_{offline}(1020) = -2.06, p < .05$) and Prudence ($t_{offline}(1020) = -3.06, p < .01$).

3.6. Openness to Experience

Offline offenders are unique in their score on Openness to Experience. They score significantly lower than both cyber offenders ($t_{offline}(1020) = -2.05, p < .05$) and the community sample ($t_{offline}(1020) = -2.57, p < .01$), while cyber offenders and the community sample do not differ from each other ($t_{cyber}(1020) = -.43, p = .67$). Results in the multinomial model are identical. At the facet level, offline offenders score lower on the Inquisitiveness facet compared to both the cyber sample ($t_{offline}(1020) = -3.94, p < .001$) and the community sample ($t_{offline}(1020) = -3.30, p < .001$). In addition, both cyber offenders and offline offenders score lower than the community sample on the Aesthetic Appreciation facet ($t_{cyber}(1020) = -2.91, p < .01$; $t_{offline}(1020) = -2.48, p < .05$).

Table 4. Multinomial logit model predicting group membership based on HEXACO domain scores ($N = 1033$)

Community sample-offline ¹		Community sample-cyber ¹		Offline-cyber ²	
<i>RRR</i>	<i>SE</i>	<i>RRR</i>	<i>SE</i>	<i>RRR</i>	<i>SE</i>

Main HEXACO Domains									
H	Honesty-Humility	.67		.14	.75		.16	1.13	0.24
E	Emotionality	.64 *		.14	.61 *		.14	0.95	0.22
X	Extraversion	1.93 ***		.37	1.08		.21	0.56 **	0.11
A	Agreeableness	.77		.17	.95		.22	1.23	0.29
C	Conscientiousness	.70		.15	1.29		.30	1.85 **	0.41
O	Openness to Experience	.55 **		.11	.82		.16	1.48 *	0.28
Control variables									
	Male	3.87 ***		.83	3.35 ***		.74	0.87	0.21
	Age	.95		.04	.90 **		.04	0.94	0.04
	Age-squared	1.00		.00	1.00		.00	1.00	0.00
Ethnicity (base is native Dutch)									
	First-generation immigrant	.79		.22	.16 ***		.06	0.20 ***	0.08
	Second-generation immigrant	1.07		.27	.50 **		.13	0.47 **	0.12
Education (base is level 4) ³									
	Level 1	7.14 ***		3.36	2.03		1.11	0.28 **	0.12
	Level 2	1.55		.39	.83		.23	0.54 *	0.15
	Level 3	.50 *		.15	.41 **		.12	0.83	0.26
	Level 5	.88		.24	1.38		.36	1.57	0.44
	Level 6	.34 **		.13	.75		.25	2.22 *	0.89
Constant		224.28		390.88	183.83		328.1	0.82	1.43

8

Note.

RRR = Relative Risk Ratio

1: Base outcome is community sample

2: Base outcome is offline sample

3: Level 1: None or primary school;

Level 2: Preparatory secondary vocational education (in Dutch: VMBO);

Level 3: Senior general secondary education (in Dutch: HAVO) or university preparatory education (in Dutch: VWO);

Level 4: Vocational school (in Dutch: MBO);

Level 5: University of applied sciences (in Dutch: HBO);

Level 6: University (in Dutch: WO) or higher, such as PhD.

* $p < .05$. ** $p < .01$. *** $p < .001$

4. Discussion

Differences in the context in which cyber offenders and offline offenders commit their crimes may result in corresponding variation in personality between these groups of offenders.

Nevertheless, the extent to which there is a specific cybercriminal personality is still an open question. Existing research is largely based on small samples, often composed of undergraduate students. Importantly, to the best of our knowledge, prior work has not compared cybercriminal personalities to offline criminal personalities. In this study, we compared a unique, large judicial sample of suspects of cybercrime with a sample of suspects of offline crime and a community sample on their HEXACO personality scores.

Even though both offender groups are made up of crime suspects, results at the domain level show that their personalities differ and that cyber offenders show greater similarities with the community sample than with offline offenders. Only on the emotionality domain are they more similar to offline offenders. On extraversion, conscientiousness, and openness to experience, they differ significantly from offline offenders and are more similar to the community sample. The most important domain-level personality difference between cyber offenders and offline offenders relates to the conscientiousness domain, as cyber offenders score significantly higher than offline offenders and even slightly, though not

significantly, higher than the community sample here. On the honesty-humility domain, the scores of cyber offenders lie in between both groups and do not differ significantly from either, whereas offline offenders score significantly lower on honesty-humility than the community sample (although this difference is only marginally significant in the multinomial model). These findings are largely in line with the expectations outlined in the introduction.

The results at the facet level largely correspond to the results found for the main domains, as offline offenders differ from the community sample on twice as many facets as cyber offenders do. On some facets, we found similarities between cyber offenders and offline offenders. For other facets, however, cyber offenders seem to be more similar to the community sample and, on a few facets, they are clearly different from both groups. Cyber offenders differ from both groups on diligence (a facet of conscientiousness), as they score significantly higher than both offline offenders and the community sample on this facet. The offender samples are similar in their significantly lower score (compared to the community sample) on modesty, fearfulness, flexibility, and aesthetic appreciation. Furthermore, both offender groups score higher than the community sample on social boldness, but cyber offenders are more in the middle (less different from the community sample) on social boldness than offline offenders. In contrast, on four other facets, cyber offenders are similar to the community sample and differ from offline offenders. Specifically, cyber offenders—like the community sample—score significantly higher than offline offenders on patience, perfectionism, prudence, and inquisitiveness.

The facets in which cyber offenders are similar to offline offenders may contribute to their selection of criminal situations and the activation of criminal traits, as cyber offenders—like offline offenders—consider themselves to be superior to others (modesty) and are less prone to experiencing fear (fearfulness). Furthermore, and also like offline offenders, they tend not to compromise or care as much about the opinions of others (flexibility). These

results are in line with research indicating that cyber offenders have a strong sense of self-importance (Van Der Wagen, 2018) and a high risk propensity (Bachmann, 2010).

A notable personality difference we found between cyber offenders and offline offenders, and one that is reflective of the skillsets required to commit cybercrime, relates to conscientiousness. Cyber offenders' tendency to be thorough and pay attention to detail (perfectionism) and be cautious (prudence) is useful for committing cybercrimes (Bachmann, 2010; Bossler & Burruss, 2011; Holt & Kilger, 2008; Maimon et al., 2014; Steinmetz, 2015; Van Der Wagen, 2018; Weulen Kranenbarg et al., 2019; Willison, 2006). Relatedly, cyber offenders appear to be unique (compared to both other groups) in their level of discipline in trying to achieve their goals (diligence). In comparison to offline offenders, they also appear to be more patient and not to lose their temper easily (patience). Lastly, having a curious nature and a tendency to "dig for" information—cyber offenders scored higher on inquisitiveness than offline offenders—may also be helpful in cyber offending. Curiosity has even been found to be one of the main motivations for committing cyber-dependent crimes (Bachmann, 2011; National Crime Agency, 2017; Turgeman-Goldschmidt, 2011; Weulen Kranenbarg, 2021).

4.1. Strengths and limitations

Despite the fact that the samples used in this study are unique in comparison to those used in previous studies, it should be noted that our offender samples also have limitations, mainly because of selectivity. Our findings are limited to suspects of cybercrime and offline crime who have been in contact with the judicial system. Even though this means that offenders in our samples are likely to have committed more serious crimes than those reported by participants in student samples, it also means that they do not represent the entire offender population. In addition, as they are suspects, not all of them will be convicted of their alleged crimes.

Although we collected the cyber offender and offline offender samples in the same manner, there was a difference in response rates. Offline offenders were less inclined to participate and needed more reminders. This may be related to differences in personality traits such as conscientiousness. As cyber offenders score higher on conscientiousness than offline offenders, cyber offenders are also more likely to complete a 96-item personality questionnaire. It is therefore possible that the personality traits measured in both of these offender samples are more similar than those in the full population of offenders. Even though we have no way of knowing the extent to which the different response rates were related to a different selection process for both offender groups, this difference in conscientiousness may suggest that our estimates are conservative and that differences in personality traits are in fact larger in the full population of offenders.

Similarly, data for the community sample were collected for a different purpose. Therefore, community sample participants did not receive exactly the same information about the study. As the offender participants knew that the study was based on a judicial sample, they may have felt a stronger need to give socially desirable answers and present a more positive view on some of their personality characteristics—a possibility consistent with the pattern of extreme response counts. This could also explain why the difference in honesty-humility between the community sample and the offline sample was not as large as expected (Ashton & Lee, 2008; De Vries & Van Kampen, 2010; Gaughan et al., 2012; Lee & Ashton, 2005). Nevertheless, we found no evidence for faked responses, as there was no indication of a general factor in our samples. We did control for background characteristics in order to make the groups more comparable, and we used response quality screening to remove participants who had less reliable or inconsistent answers. This reduces concerns regarding sampling bias, though we acknowledge that such bias cannot be completely ruled out.

4.2. Implications

While many studies highlight the unique nature of cyberspace and the use of stereotypes about cyber offenders is common, surprisingly little empirical research has been conducted into the personality traits of cyber offenders. The present study addressed this gap in the knowledge base and provides a nuanced picture of the personality traits of cyber offenders. It demonstrates that, in general, ideas about the personality characteristics of cyber offenders, which are largely based on qualitative research, can be verified in quantitative research using personality surveys. It also shows that this type of research should focus not only on the main personality domains but also on their underlying facets, as they provide more detailed insights into the unique traits related to this type of criminal behavior. Additionally, as we compared cyber offenders not only to the community sample but also to offline offenders, this study shows how a number of offline-offender personality traits also seem to be necessary traits for committing cybercrime.

Based on these results and the limitations discussed above, further research on the personality traits of cyber offenders is desirable. As the type of cyber offenders apprehended by the police may differ between countries (Lusthaus, 2018), it is important to replicate this study in other countries. In addition, other ways of recruiting offender groups who committed more serious cybercrimes could be explored, but it should be noted that comparisons between such groups and offline offenders may be limited if the two offender groups cannot be recruited in a similar manner. Although serious offender groups provide insights into the most problematic personality traits, research on offending among the general population remains necessary in order to be able to examine the generalizability of these personality traits and to compare different types of offenders and non-offenders by using exactly the same methodology.

As this study analyzed a judicial sample, the results will be mainly useful in understanding and helping convicted or apprehended cyber offenders. It shows that some

elements of intervention programs for offline offenders may be applied to cyber offenders as well—for example, intervention elements that address entitlement and feelings of being superior to others. It also provides evidence for the idea that cyber offenders possess several unique traits that are not necessarily conducive only to crime. Traits such as high conscientiousness are useful in many legitimate professions. As cyber offenders also have technical skills that can be used for good, it is important to focus rehabilitation efforts on the aspects of their personality driving the criminal use of their skills. Therefore, in addition to the research suggestions above, it is important to empirically compare the personality characteristics of cybercriminals with those of normative information-technology professionals who have similar skillsets but use them for legitimate purposes. These insights could further help initiatives such as the Dutch Hack_Right intervention (www.politie.nl, 2018) and the UK Prevent interventions (National Crime Agency, 2017) in order to steer cyber offenders away from crime and offer them legitimate, positive alternatives.

5. Conclusion

In sum, there appears to be a specific cybercriminal personality that is characterized by both conventional and criminal personality traits. In line with the Situation-Trait-Outcome Activation (STOA) model (De Vries et al., 2016), the cyber context seems to require personality traits that enable offenders to take all the tedious and technical steps necessary to prepare for (situation activation)—and commit (trait activation)—these cybercrimes. Still, several criminal personality traits, such as believing oneself to be above the law and having no fear of getting caught, are required in order to be able to victimize others. This study has provided a new and unique comparison, but results should be replicated in other offender and general population samples. Similar comparisons with normative information-technology

professionals could deliver valuable information on how we can steer cyber offenders away from crime.

Journal Pre-proof

References

- Aiken, M., Davidson, J., & Amann, P. (2016). *Youth pathways into cybercrime*. Retrieved from: <https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf>.
- Akkermans, M., Kloosterman, R., Moons, E., Reep, C., & Tummers-van der Aa, M. (2022). *Veiligheidsmonitor 2021* [Safety monitor 2021]. The Hague, The Netherlands: Statistics Netherlands (CBS). Retrieved from: <https://www.cbs.nl/-/media/cbs/veiligheid-en-recht/veiligheidsmonitor-2021.pdf>.
- Arias, V. B., Jenaro, C., & Ponce, F. P. (2018). Testing the generality of the general factor of personality: An exploratory bifactor approach. *Personality and Individual Differences, 129*, 17-23.
- Ashton, M. C., & Lee, K. (2008). The prediction of honesty humility-related criteria by the HEXACO and five-factor models of personality. *Journal of Research in Personality, 42*(5), 1216–1228.
- Ashton, M. C., Lee, K., & De Vries, R. E. (2014). The HEXACO Honesty-Humility, Agreeableness, and Emotionality Factors: A Review of Research and Theory. *Personality and Social Psychology Review, 18*(2), 139–152.
- Ashton, M. C., Lee, K., Perugini, M., Szarota, P., De Vries, R. E., Di Blas, L., ... De Raad, B. (2004). A six-factor structure of personality-descriptive adjectives: Solutions from psycholexical studies in seven languages. *Journal of Personality and Social Psychology, 86*(2), 356–366.
- Ashton, M. C., Xia, X., & Lee, K. (2020). Is there a G in HEXACO? Testing for a general factor in personality self-reports under different conditions of responding. *Personality and Individual Differences, 156*, 109750.

- Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, 4(1), 643-656.
- 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. 105-126). New York: Information Science Reference.
- Barends, A. J., & de Vries, R. E. (2019). Noncompliant responding: Comparing exclusion criteria in MTurk personality research to improve data quality. *Personality and Individual Differences*, 143, 84-89.
- Blom, M., Oudhof, J., Bijl, R. V., & Bakker, B. F. M. (2005). *Verdacht van criminaliteit: Allochtonen en autochtonen nader bekeken* [Crime suspect: a closer look at ethnic minorities and native Dutch]. The Hague, The Netherlands: Wetenschappelijk Onderzoek-en Documentatiecentrum (WODC) & Statistics Netherlands (CBS). Retrieved from: https://repository.wodc.nl/bitstream/handle/20.500.12832/17/ca2005-2-volledige-tekst_tcm28-68014.pdf?sequence=2&isAllowed=y.
- Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: low self-control hackers? In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 38-67). New York: Information Science Reference.
- Caspi, A., Moffitt, T. E., Silva, P. A., Stouthamer-Loeber, M., Krueger, R. F., & Schmutte, P. S. (1994). Are some people crime prone? Replications of the personality-crime relationship across countries, gender, race, and methods. *Criminology*, 32(2), 163-195.
- Chua, Y.-T., & Holt, T. J. (2016). A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. *Victims & Offenders*, 11(4), 534-555.

- Costa, P. T., & McCrae, R. R. (1990). Personality disorders and the Five-Factor Model of Personality. *Journal of Personality Disorders*, 4(4), 362-371.
- Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). New York: Information Science Reference.
- De Vries, R. E., & Born, M. P. (2013). De Vereenvoudigde HEXACO Persoonlijkheidsvragenlijst en een additioneel interstitieel Proactiviteitsfacet [The simplified HEXACO personality questionnaire and an additional interstitial proactivity facet]. *Gedrag & Organisatie*, 26(2), 223-245.
- De Vries, R. E., & Van Gelder, J. L. (2013). Tales of two self-control scales: Relations with Five-Factor and HEXACO traits. *Personality and Individual Differences*, 54(6), 756-760.
- De Vries, R. E., & van Kampen, D. (2010). The HEXACO and 5DPT models of personality: A comparison and their relationships with psychopathy, egoism, pretentiousness, immorality, and Machiavellianism. *Journal of Personality Disorders*, 24(2), 244-257.
- De Vries, R. E., Tybur, J. M., Pollet, T. V., & van Vugt, M. (2016). Evolution, situational affordances, and the HEXACO model of personality. *Evolution and Human Behavior*, 37(5), 407-421.
- Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, 34, 165-172.
- Dunlop, P. D., Bourdage, J. S., de Vries, R. E., McNeill, I. M., Jorritsma, K., Orchard, M., ... Choe, W.-K. (2020). Liar! Liar! (when stakes are higher): Understanding how the overclaiming technique can be used to measure faking in personnel selection. *Journal of Applied Psychology*, 105(8), 784-799.

- Farrington, D., & Welsh, B. (2007). *Saving children from a life of crime: Early risk factors and effective interventions*. Oxford, England: Oxford University Press.
- Federal Bureau of Investigation (2021). *Internet Crime Report 2021*. FBI. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- Gaughan, E. T., Miller, J. D., & Lynam, D. R. (2012). Examining the utility of general models of personality in the study of psychopathy: A comparison of the HEXACO-PI-R and NEO PI-R. *Journal of Personality Disorders*, 26(4), 513-523.
- Goldberg, L. R. (1990). An alternative “description of personality”: The Big-Five factor structure. *Journal of Personality and Social Psychology*, 59(6), 1216-1229.
- Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Palo Alto, CA: Stanford University Press.
- Harvey, I., Bolgan, S., Mosca, D., McLean, C., & Rusconi, E. (2016). Systemizers Are Better Code-Breakers: Self-Reported Systemizing Predicts Code-Breaking Performance in Expert Hackers and Naïve Participants. *Frontiers in Human Neuroscience*, 10, 229.
- Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, 28(2), 171-198.
- Holt, T. J. (2009). *The attack dynamics of political and religiously motivated hackers*. Paper presented at the Cyber Infrastructure Protection Conference, New York, USA.
- 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., & Kilger, M. (2008). *Techcrafters and makecrafters: A comparison of two populations of hackers*. Paper presented at the 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, Amsterdam, The Netherlands.

- Hu, Q., Xu, Z., & Yayla, A. A. (2013). *Why college students commit computer hacks: Insights from a cross culture analysis*. Paper presented at the Pacific Asia Conference on Information Systems (PACIS), Jeju Island, Korea.
- Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior, 37*(10), 1163-1178.
- Jones, S. E., Miller, J. D., & Lynam, D. R. (2011). Personality, antisocial behavior, and aggression: A meta-analytic review. *Journal of Criminal Justice, 39*(4), 329-337.
- Kim, M., Clark, S. L., Donnellan, M. B., & Burt, S. A. (2020). A multi-method investigation of the personality correlates of digital aggression. *Journal of Research in Personality, 85*, 103923.
- Knight, N. M., Dahlen, E. R., Bullock-Yowell, E., & Madson, M. B. (2018). The HEXACO model of personality and Dark Triad in relational aggression. *Personality and Individual Differences, 122*, 109-114.
- Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2018). *Georganiseerde criminaliteit en ICT* [Organized crime and IT]. The Hague, The Netherlands: Wetenschappelijk Onderzoek-en Documentatiecentrum (WODC). Retrieved from:
<https://repository.wodc.nl/bitstream/handle/20.500.12832/203/Cahier-2018-08-volledige-tekst.pdf?sequence=9&isAllowed=y>.
- Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. *Advances in Autism, 1*(1), 2-11.
- Lee, K., & Ashton, M. C. (2004). Psychometric properties of the HEXACO Personality Inventory. *Multivariate Behavioral Research 39*(2), 329–358.

- Lee, K., & Ashton, M. C. (2005). Psychopathy, Machiavellianism, and narcissism in the Five-Factor Model and the HEXACO model of personality structure. *Personality and Individual Differences, 38*(7), 1571-1582.
- Lee, K., & Ashton, M. C. (2006). Further assessment of the HEXACO personality inventory: Two new facets scales and an observer report form. *Psychological Assessment, 18*(2), 182-191.
- Lee, K., & Ashton, M. C. (2012). Getting mad and getting even: Agreeableness and Honesty-Humility as predictors of revenge intentions. *Personality and Individual Differences, 52*(5), 596–600.
- Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. London: Harvard University Press.
- Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System. *Criminology, 52*(1), 33-59.
- 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.
- McCrae, R. R., & Costa, P. T. (1997). Personality trait structure as a human universal. *American Psychologist, 52*(5), 509-516.
- Miller, J. D., & Lynam, D. (2001). Structural Models of Personality and Their Relation to Antisocial Behavior: A Meta-Analytic Review. *Criminology, 39*(4), 765-798.
- Moffitt, T. E., Krueger, R. F., Caspi, A., & Fagan, J. (2000). Partner Abuse and General Crime: How Are They the Same? How Are They Different? *Criminology, 38*(1), 199-232.
- Montalto, M. (2021). *A criminological and psychological approach to criminal offender personality traits* (doctoral dissertation). University of Western Australia. Retrieved from: <https://api.research->

[repository.uwa.edu.au/ws/portalfiles/portal/134249302/THESIS DOCTOR OF PHI
LOSOPHY MONTALTO Michael Mario 2021.pdf](https://repository.uwa.edu.au/ws/portalfiles/portal/134249302/THESIS_DOCTOR_OF_PHI_LOSOPHY_MONTALTO_Michael_Mario_2021.pdf).

Morgan, R. E., & Thompson, A. (2022). *The Nation's Two Crime Measures, 2011–2020*.

U.S. Department of Justice: Bureau of Justice Statistics (BJS). Retrieved from:

<https://bjs.ojp.gov/content/pub/pdf/ntcm1120.pdf>.

Morris, R. G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 1-17). New York: Information Science Reference.

National Crime Agency (2017). *Pathways into Cyber Crime*. Retrieved from:

<https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file>.

Nee, C., van Gelder, J. L., Otte, M., Vernham, Z., & Meenaghan, A. (2019). Learning on the job: Studying expertise in residential burglars using virtual environments.

Criminology, 57(3), 481-511.

Office for National Statistics (2021). *Crime in England and Wales: year ending December 2021*. UK Office for National Statistics. Retrieved from:

<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2021/pdf>.

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior*, 120, 106745.

Paunonen, S.V., & Jackson, D.N. (2000). What is beyond the Big Five? Plenty! *Journal of Personality*, 68(5), 812-835.

- Payne, K.-L., Russell, A., Mills, R., Maras, K., Rai, D., & Brosnan, M. (2019). Is There a Relationship Between Cyber-Dependent Crime, Autistic-Like Traits and Autism? *Journal of Autism and Developmental Disorders*, *49*(10), 4159-4169.
- Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's General Theory of Crime: A meta-analysis. *Criminology*, *38*(3), 931-964.
- Revelle, W. (2018). *Psych: Procedures for Personality and Psychological Research*. Northwestern University, Evanston, Illinois, USA. Retrieved from: [https://CRAN.Rproject.org/package = psych](https://CRAN.Rproject.org/package=psych) Version = 1.8.12.
- Revelle, W., & Zinbarg, R. E. (2009). Coefficients alpha, beta, omega, and the glb: Comments on Sijsma. *Psychometrika*, *74*(1), 145-154.
- Rogers, M. K., Seigfried, K. C., & Tidke, K. (2006). Self-reported computer criminal behavior: a psychological analysis. *Digital Investigation*, *3*(supplement), 116-120.
- Rogers, M. K., Smoak, N. D., & Liu, J. (2006). Self-reported deviant computer behavior: A Big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior*, *27*(3), 245-268.
- Rolison, J. J., Hanoch, Y., & Gummerum, M. (2013). Characteristics of offenders: The HEXACO model of personality as a framework for studying offenders' personality. *The Journal of Forensic Psychiatry & Psychology*, *24*(1), 71-82.
- Ruiz, M. A., Pincus, A. L., & Schinka, J. A. (2008). Externalizing Pathology and the Five-Factor Model: A Meta-Analysis of Personality Traits Associated with Antisocial Personality Disorder, Substance Use Disorder, and Their Co-Occurrence. *Journal of Personality Disorders*, *22*(4), 365-388.
- Rokven, J. J., Weijters, G., Beerthuisen, M. G. C. J., & van der Laan, A. M. (2018). Juvenile Delinquency in the Virtual World: Similarities and Differences between Cyber-

- Enabled, Cyber-Dependent and Offline Delinquents in the Netherlands. *International Journal of Cyber Criminology*, 12(1), 27-46.
- 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.
- Ścigała, K. A., Ruhara, N., Nitschke, J., & Pfattheicher, S. (2022). Honesty-humility and criminal behavior among imprisoned criminal offenders. Pre-print retrieved from: <https://psyarxiv.com/t9r3b/>.
- Seigfried-Spellar, K. C., O'Quinn, C. L., & Treadway, K. N. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour and Information Technology*, 34(5), 533-542.
- Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, 35(10), 782-803.
- Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, 51, 67-73.
- Sijtsma, K. (2009). On the use, the misuse, and the very limited usefulness of Cronbach's alpha. *Psychometrika*, 74(1), 107-120.
- Steinmetz, K. F. (2015). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology*, 55(1), 125-145.
- Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321-326.

- Tan, M. M., Jabar, M. A., Tieng Wei, K., & Sidi, F. (2016). *A preliminary study of personality traits and their influence on software piracy*. Paper presented at 2015 9th Malaysian Software Engineering Conference, Kuala Lumpur, Malaysia.
- Taylor, P. A. (1999). *Hackers: crime in the digital sublime*. London: Routledge.
- Turgeman-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review*, 23(1), 8-23.
- Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2(2), 382-396.
- Turgeman-Goldschmidt, O. (2009). The rhetoric of hackers' neutralizations. In F. Schmallegger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 317-335). New Jersey: Pearson Education.
- 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.
- Van Der Wagen, W. (2018). The Cyborgian deviant: An assessment of the hacker through the lens of actor-network theory. *Journal of Qualitative Criminal Justice and Criminology*, 6(2), 157-178.
- Van Der Wagen, W., Althoff, M., & Swaaningen, R. (2016). De andere 'anderen' [The other 'others']. *Tijdschrift over Cultuur & Criminaliteit*, 6(1), 27-41.
- Van Der Wagen, W., van't Zand-Kurtovic, E. G., & Fischer, T. F. C. (2019). Cyberdaders: uniek profiel, unieke aanpak? [Cyber offenders: unique profile, unique prevention?] The Hague, The Netherlands: Wetenschappelijk Onderzoek-en Documentatiecentrum (WODC). Retrieved from: https://repository.wodc.nl/bitstream/handle/20.500.12832/2432/2974_Volledige_Tekst_tcm28-426136.pdf?sequence=2&isAllowed=y.

- Van Gelder, J.-L., & De Vries, R. E. (2012). Traits and States: Integrating Personality and Affect Into a Model of Criminal Decision Making. *Criminology*, *50*(3), 637-671.
- Van Gelder, J. L., & De Vries, R. E. (2014). Rational misbehavior? Evaluating an integrated dual-process model of criminal decision making. *Journal of Quantitative Criminology*, *30*, 1-27.
- Varley Thornton, A. J., Graham-Kevan, N., & Archer, J. (2010). Adaptive and maladaptive personality traits as predictors of violent and nonviolent offending behavior in men and women. *Aggressive Behavior*, *36*(3), 177-186.
- Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-based model of computer hackers' motivation. *CyberPsychology & Behavior*, *6*(2), 171-180.
- Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: an empirical comparison* (doctoral dissertation). Amsterdam, The Netherlands: Vrije Universiteit (VU) Amsterdam. Retrieved from: <http://dare.uvu.vu.nl/handle/1871/55530>.
- Weulen Kranenbarg, M. (2021). Cyber-dependent crime versus traditional crime: empirical evidence for clusters of offenses and related motives. In M. Weulen Kranenbarg & E. R. Leukfeldt (Eds.), *Cybercrime in context: the human factor in victimization, offending, and policing*. Cham, Switzerland: Springer.
- Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J.-L. (2019). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, *40*(1), 40-55.
- Willison, R. (2006). Understanding the offender/environment dynamic for computer crimes. *Information Technology & People*, *19*(2), 170-186.
- Woo, H.-J. (2003). *The hacker mentality: exploring the relationship between psychological variables and hacking activities* (doctoral dissertation). Athens, Georgia: The

University of Georgia. Retrieved from: https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf.

Woo, H.-J., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*, 6(1), 63-82.

www.politie.nl. (2018). Hack_Right: jonge hackers weer op het rechte pad [Hack_Right: young hackers on the right path]. Retrieved from: https://www.politie.nl/onderwerpen/hack_right.html.

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

Appendix A

Table A1. Correlation matrix of facets.

	H1	H2	H3	H4	E1	E2	E3	E4	X1	X2	X3	X4	A1	A2	A3	A4	C1	C2	C3	C4	O1	O2	O3	O4
H1	-	.44	.30	.19	.08	-.01	-.01	.07	.07	-.11	.08	.11	-.27	.21	-.03	.15	.12	.16	.16	.27	.01	-.07	-.18	-.17
H2	.45	-	.28	.20	.04	-.03	.01	.13	.17	.09	.15	.13	.08	.26	-.03	.17	.11	.21	.22	.27	.14	.04	-.14	-.16
H3	.33	.28	-	.38	.03	.02	-.06	.06	-.04	-.21	-.21	-.02	-.02	.20	-.04	.10	.05	.02	.07	.17	-.04	-.10	-.21	-.03
H4	.19	.22	.37	-	.06	.01	-.04	.02	-.01	-.18	-.02	.03	.00	.18	.11	.09	.09	.02	.08	.16	-.13	-.08	-.27	-.26
E1	.04	-.02	-.02	-.01	-	.23	.22	.16	-.08	-.20	-.06	-.07	-.04	.10	.11	.02	.07	-.22	.12	.22	.10	-.04	-.21	-.22
E2	-.02	-.01	-.03	.03	.22	-	.26	.36	-.22	-.30	-.17	-.44	-.01	-.02	.07	-.25	-.07	-.18	.04	-.05	.08	-.09	-.11	-.11
E3	-.03	-.02	-.12	-.09	.20	.28	-	.27	-.04	-.05	.25	-.19	.06	.07	.14	-.18	-.05	-.19	-.06	-.06	.13	-.13	-.15	-.23
E4	.07	.17	-.02	-.04	.07	.38	.31	-	.06	.00	.11	-.05	.05	.14	.11	-.11	.12	-.04	.17	.02	.22	.03	.02	-.13
X1	.03	.21	-.05	-.02	-.06	-.18	-.04	.12	-	.30	.35	.49	.11	.17	-.04	.18	.15	.20	.16	.16	.04	.08	.09	-.15
X2	-.10	.11	-.18	-.24	-.16	-.27	-.03	.05	.31	-	.48	.33	.04	-.19	-.17	-.04	.09	.23	.02	-.08	.06	.09	.22	.05
X3	.09	.19	-.17	.01	-.04	-.13	.29	.20	.36	.46	-	.34	.11	.03	.03	.00	.11	.17	.03	.00	-.03	-.04	.02	-.19
X4	.09	.14	-.05	-.01	-.04	-.47	-.23	-.04	.47	.36	.30	-	.09	.06	-.05	.15	.19	.31	.13	.12	-.02	.07	.14	-.05
A1	-.06	.12	.00	.04	.00	-.06	.04	.10	.12	.08	.13	.11	-	.28	.24	.28	-.01	-.04	-.03	.01	.05	.06	.03	-.01

A2	.22	.29	.18	.18	-.01	-.03	.00	.14	.21	-.16	.07	.06	.27	-	.30	.43	.09	.01	.10	.27	.09	.04	-.10	-.20
A3	-.09	-.04	-.04	.13	.09	.09	.09	.11	-.04	-.17	.03	-.05	.21	.31	-	.22	.02	-.14	-.03	.07	.04	-.04	-.06	-.16
A4	.19	.15	.09	.12	-.07	-.30	-.26	-.14	.14	-.09	-.04	.18	.25	.42	.21	-	.13	.12	.07	.39	.04	.14	.01	-.07
C1	.11	.15	-.02	.08	.04	-.08	-.04	.11	.14	.11	.16	.21	-.02	.09	.01	.10	-	.22	.30	.29	.00	-.04	-.11	-.27
C2	.15	.19	-.01	-.02	-.24	-.12	-.20	.01	.15	.24	.16	.25	-.10	.02	-.15	.06	.27	-	.34	.23	.06	.23	.16	.03
C3	.14	.27	.03	.08	.05	.06	-.03	.13	.15	.08	.05	.07	.00	.05	-.04	.03	.27	.30	-	.39	.17	.14	.06	-.09
C4	.21	.22	.09	.09	.17	-.08	-.09	-.06	.10	-.10	-.04	.13	-.01	.27	.03	.39	.22	.17	.34	-	.11	.11	-.19	-.29
O1	.00	.13	-.12	-.21	.04	.04	.18	.18	.11	.13	.05	.01	.04	.07	.02	-.04	-.04	.08	.19	.09	-	.38	.23	.17
O2	-.02	.01	-.11	-.12	-.07	-.10	-.12	.05	.16	.07	-.03	.14	.03	.08	-.07	.07	-.05	.27	.12	.16	.39	-	.37	.26
O3	-.17	-.14	-.20	-.35	-.21	-.09	-.07	.02	.07	.28	.05	.16	.04	-.08	-.05	-.02	-.12	.19	.07	-.20	.27	.34	-	.51
O4	-.11	-.17	-.01	-.30	-.21	-.15	-.21	-.15	-.12	.10	-.18	-.03	-.03	-.22	-.18	-.07	-.26	.02	-.13	-.25	.16	.24	.53	-

Note. Table 3 includes all facet-level names and the corresponding codes used in this table.

Above diagonal: full sample ($N = 1041$); below diagonal: community sample ($N = 512$).

Table A2. Correlation matrix of facets.

	H1	H2	H3	H4	E1	E2	E3	E4	X1	X2	X3	X4	A1	A2	A3	A4	C1	C2	C3	C4	O1	O2	O3	O4
H1	-	.38	.24	.16	.11	.00	.05	-.01	.13	-.03	.09	.10	.10	.19	-.06	.04	.09	.19	.13	.24	-.10	-.19	-.18	-.26
H2	.46	-	.27	.20	.09	-.05	.05	.06	.22	.19	.19	.19	.12	.23	-.05	.19	.11	.31	.19	.34	.13	.00	-.10	-.25
H3	.29	.24	-	.31	-.11	.05	-.04	.00	.01	-.21	-.21	-.01	.01	.20	-.17	.12	-.01	.17	.03	.23	-.01	.06	-.14	.05
H4	.17	.13	.39	-	.10	-.06	.07	-.06	.00	-.10	-.01	.07	-.05	.17	-.01	.03	-.02	.09	.04	.16	-.16	.00	-.14	-.21
E1	.09	-.02	.05	-.03	-	.14	.33	.13	-.08	-.11	.06	-.09	.03	.23	.18	.10	.01	-.15	.13	.18	.05	-.10	-.21	-.32
E2	-.04	-.10	-.03	-.07	.21	-	.28	.36	-.28	-.32	-.19	-.50	-.03	-.07	.02	-.29	-.13	-.26	-.02	-.07	.08	-.15	-.13	-.06
E3	-.06	-.03	-.06	-.11	.10	.17	-	.25	-.02	-.06	.26	-.19	.09	.14	.18	-.18	-.05	-.13	-.08	.00	.02	-.19	-.31	-.32
E4	.12	.07	.08	.06	.17	.25	.14	-	-.04	.02	.13	-.15	-.02	.05	.10	-.16	.11	-.08	.13	-.03	.17	-.05	.05	-.13
X1	.09	.10	-.05	.01	-.08	-.20	-.05	.10	-	.26	.26	.47	.11	.21	-.05	.27	.19	.26	.19	.25	.00	.06	.14	-.19
X2	-.17	.03	-.17	-.08	-.21	-.29	-.03	.00	.30	-	.55	.38	.04	-.11	-.14	.14	.17	.24	.05	.10	.12	.09	.08	-.09
X3	.09	.11	-.20	-.01	-.13	-.17	.20	.01	.42	.44	-	.40	.10	.04	.07	.03	.16	.20	.10	.17	-.05	-.10	-.09	-.29
X4	.17	.08	.02	.07	-.11	-.35	-.11	.06	.53	.24	.36	-	.08	.07	-.05	.16	.18	.45	.20	.11	-.05	.12	.17	-.06
A1	.02	.00	-.02	.07	-.07	.14	.12	.11	.08	-.08	.05	.04	-	.40	.23	.37	-.02	.00	-.01	.07	.10	.07	.04	-.04
A2	.19	.21	.18	.14	.06	-.01	.09	.13	.11	-.26	-.02	.08	.22	-	.22	.44	.08	.01	.13	.28	.04	-.03	-.08	-.17

A3	.07	-.03	.01	.12	-.01	.05	.16	.06	-.01	-.14	.04	-.02	.34	.35	-	.13	-.08	-.19	-.08	.01	.00	-.04	.00	-.16
A4	.21	.19	.12	.13	.11	-.11	-.01	.02	.16	-.11	.06	.07	.25	.46	.31	-	.06	.13	.08	.37	.13	.23	.15	-.03
C1	.17	.03	.16	.18	.11	-.04	-.12	.12	.13	.05	.02	.17	.04	.08	.07	.24	-	.16	.29	.31	.04	-.06	-.13	-.33
C2	.16	.18	.02	.08	-.22	-.17	-.19	-.03	.20	.22	.13	.29	.02	.04	-.05	.17	.23	-	.39	.24	.00	.19	.04	-.02
C3	.19	.13	.09	.05	.11	.01	-.13	.23	.16	-.03	-.02	.21	-.07	.11	-.01	.10	.35	.39	-	.40	.05	.08	.05	-.10
C4	.39	.25	.15	.19	.23	-.08	-.09	.13	.21	-.09	-.04	.15	.03	.24	.13	.41	.35	.34	.40	-	.00	-.01	-.21	-.39
O1	.09	.11	-.14	-.18	.02	.03	.09	.20	.01	.04	-.06	-.01	.12	.06	.01	.12	-.04	.16	.18	.13	-	.31	.23	.23
O2	-.05	.08	-.25	-.13	.00	-.06	-.08	.07	.00	.19	.01	-.06	.11	.02	-.05	.13	-.03	.21	.19	.11	.47	-	.40	.27
O3	-.19	-.13	-.21	-.18	-.12	-.06	-.10	.10	.07	.20	.03	.09	-.03	-.11	-.10	-.12	-.04	.16	.11	-.13	.31	.39	-	.52
O4	-.16	-.05	-.10	-.22	-.12	-.05	-.14	-.07	-.19	.10	-.13	-.08	.03	-.19	-.14	-.13	-.23	.06	-.02	-.27	.22	.28	.45	-

Note. Table 3 includes all facet-level names and the corresponding codes used in this table.

Above diagonal: cyber sample ($N = 262$); below diagonal: offline sample ($N = 267$).

Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets.

Highlights

- Compared to offline offenders, cyber offenders' personality scores are more similar to those of a community sample.
- Cyber offenders score particularly high on Diligence, a facet of Conscientiousness.
- Cyber and offline offenders share low scores on Modesty, Fearfulness, Flexibility, and Aesthetic Appreciation.
- Cyber offenders are in between offline offenders and the community sample on Honesty-Humility.
- Cyber offenders and the community sample share higher scores on Conscientiousness and Openness to Experience.