Big Five Personality Traits of Cybercrime Victims

Article *in* Cyberpsychology, Behavior, and Social Networking · June 2017

DOI: 10.1089/cyber.2017.0028

2 authors, including:

Eric Rutger Leukfeldt
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)
32 PUBLICATIONS **111** CITATIONS

Cyberpsychology, Behavior, and Social Networking
Volume 00, Number 00, 2017

DOI: 10.1089/cyber.2017.0028

ORIGINAL ARTICLE

Big Five Personality Traits of Cybercrime Victims

Steve G.A. van de Weijer, PhD, and E. Rutger Leukfeldt, PhD

Abstract

The prevalence of cybercrime has increased rapidly over the last decades and has become part of the everyday life of citizens. It is, therefore, of great importance to gain more knowledge on the factors related to an increased or decreased likelihood of becoming a cybercrime victim. The current study adds to the existing body of knowledge using a large representative sample of Dutch individuals ($N = 3,648$) to study the relationship between cybercrime victimization and the key traits from the Big Five model of personality (i.e., extraversion, agreeableness, conscientiousness, emotional stability, and openness to experience). First, multinomial logistic regression analyses were used to examine the associations between the personality traits and three victim groups, that is, cybercrime victims versus nonvictims, traditional crime victims versus nonvictims, and cybercrime victims versus traditional crime victims. Next, logistic regression analyses were performed to predict victimization of cyber-dependent crimes (i.e., hacking and virus infection) and cyber-enabled crimes (i.e., online intimidation, online consumer fraud, and theft from bank account). The analyses show that personality traits are not specifically associated with cybercrime victimization, but rather with victimization in general. Only those with higher scores on emotional stability were less likely to become a victim of cybercrime than traditional crime. Furthermore, the results indicate that there are little differences between personality traits related to victimization of cyber-enabled and cyber-dependent crimes. Only individuals with higher scores on openness to experience have higher odds of becoming a victim of cyber-enabled crimes.

Keywords: Big Five; personality; cybercrime; victimization; hacking; online fraud

Introduction

Cybercrime is on the rise and poses a big threat to our digitized society. The prevalence of cybercrime has increased rapidly and has become part of the everyday life of citizens. For example, Statistics Netherlands reported that in 2015, 5.1 percent of Dutch citizens were victims of hacking, 3.5 percent of online consumer fraud, and 0.6 percent of identity theft.[1] Furthermore, a recent field trial of the Crime Survey for England and Wales shows almost 2.5 million hacking and malware incidents in 12 months.[2]

With the ongoing digitization of our society, it is expected that cybercrime victimization will only increase in the future. It is, therefore, of great importance to gain more knowledge on the factors related to an increased or decreased likelihood of becoming a cybercrime victim. This is recognized by cybercrime scholars, and various studies into cybercrime victimization have been done. However, the vast majority of these studies focus on the influence of self-control and the routine activities of victims (see, for example[3–12]).

The current study adds to the existing body of knowledge, by studying the relationship between the key traits from the Big Five model and cybercrime victimization. Little is known about the personality traits that are related to victimization of crime. The scarce studies that do study the personality of victims focus on victimization of traditional types of crime.[13,14] Up to now, no previous study has investigated the personality of victims of cybercrime.

This article's aim is to contribute to the knowledge about the personality characteristics of individuals who are the most at risk to become victims of cybercrime. With this knowledge, insights into opportunities for preventions are provided. The research question of the current study is twofold. First, it will be examined on which key traits from the Big Five model of personality (i.e., extraversion, agreeableness, conscientiousness, emotional stability, and openness to experience) victims of cybercrime differ from victims of traditional crime and nonvictims. Second, it will be examined whether victims of specific types of cybercrimes (i.e., hacking, online intimidation, virus infection, online consumer fraud, and theft from

Netherlands Institute for the Study of Crime and Law Enforcement, Amsterdam, The Netherlands.

bank account) differ on these personality traits compared to nonvictims.

Personality, Self-Control, and Victimization

Although no previous studies have investigated the link between the Big Five personality traits and cybercrime victimization, several studies have examined the level of self-control among victims of different types of cybercrime. According to Gottfredson and Hirschi's[15] general theory of crime, individuals with a lower self-control are more risk-taking, impulsive, shortsighted, insensitive to others, and seek more immediate and easy gratification. They are therefore more likely to be involved in criminal behavior. Schreck[16] argued that this theory could also be used to predict criminal victimization, since a lack of preventive behavior due to shortsightedness and risk-taking makes people more vulnerable to be victimized. According to Holtfreter, Reisig, and Pratt,[17] a low self-control is specifically a risk factor for noncontact crimes like fraud and cybercrime because at least some degree of victim cooperation is necessary for perpetration to be successful. In accordance with this line of reasoning, it has been shown that individuals with lower levels of self-control are at increased risk to become a victim of some types of cybercrime.[7,11,18]A meta-analysis of Pratt et al.[19] showed that self-control is a modest yet consistent predictor of victimization risk and that this association is even more robust when predicting noncontact forms of victimization, such as cybercrime victimization.

Jones, Miller, and Lynam[20] made the argument that the Big Five personality traits agreeableness, conscientiousness, and emotional stability capture many elements (e.g., impulsivity and insensitivity to others) of self-control as identified in Gottfredson and Hirschi's[15] theory. The overlap between self-control and agreeableness and conscientiousness has also been empirically shown by Van Gelder and De Vries[21] who found these traits to be important correlates with Grasmick's self-control scale.[22] Based on this overlap and the previous studies on the level of self-control of cybercrime victims, we expect that victims of cybercrime score different on the agreeableness and conscientiousness scales than nonvictims.

No previous studies have tested this hypothesis among victims of cybercrimes, but some studies did investigate the association between Big Five personality traits and victimization of traditional crime and victimization of cyberbullying. Wilcox et al.[14] used a 4-year panel study of 2,220 adolescents and showed a negative association between criminal victimization and agreeableness and conscientiousness. However, this was not a direct effect but an indirect effect mediated by having delinquent peers and exposure to illicit goods. A study of Ellrich and Baier[13] among 1,803 German police officers, on the other hand, only found that those with higher scores on openness to experience and neuroticism (i.e., lower scores on emotional stability) were more likely to be violently attacked. In a study among 572 young adult Facebook users, Peluchette et al.[23] found a lot of significant relationships between personality traits and online behavior, such as frequency of internet use, number of Facebook friends, posting indiscrete content, and having friends posting indiscrete content. However, only extraversion and openness to experience were significantly and positively related to victimization of both harsh and mild cyberbullying.

The associations between Big Five personality traits and cybercrime victimization might not be the same for all types of cybercrime. In general, two types of cybercrimes are distinguished.[24] The first category is called cyber-dependent crimes and includes new types of crimes which are aimed at Information Technology (IT) and committed through the use of IT (e.g., hacking). Cyber-dependent crimes form the second category and include traditional crimes which are not focused on IT, but for which IT is essential to commit the offence (e.g., fraud through the internet). In this study we will explore whether victims of cyber-enabled crimes (i.e., online intimidation, online consumer fraud, and theft from bank account) differ from nonvictims on other personality traits, than victims of cyber-dependent crimes (i.e., hacking and virus infection).

Methods

Data

In this article we make use of data of the LISS (Longitudinal Internet Studies for the Social sciences) panel administered by CentERdata. The LISS panel is a representative sample of Dutch individuals who participate in monthly internet surveys. The panel is based on a true probability sample of households drawn from the population register. Households that could not otherwise participate are provided with a computer and Internet connection, to ensure sufficient participation of elderly people, the unemployed, and low-income households (about 5 percent of the total sample). All household members of age 15 and older were asked to complete the surveys. A longitudinal survey is fielded in the panel every year, covering a large variety of domains, including work, education, income, housing, time use, political views, values, and personality. The total panel consists of 4,500 households, comprising about 7,000 individuals.

This study uses data from two surveys from the LISS panel, one that measures crime victimization and one that measures personality characteristics. The most recent survey on crime victimization was used, which was conducted in February 2012 and measures crime victimization in the past 2 years, spanning the period between February 2010 and February 2012. The key traits from the Big Five model of personality were measured annually. In this study we use the most recent measurement before February 2010. For most respondents this means that the personality traits were measured in May and June 2009. If respondents did not participate in the survey in 2009, data from May 2008 are used. Only respondents with valid answers on all personality traits and crime victimization were included in the analyses. The final sample consisted out of 3,648 respondents. The average age of these respondents was 51.29 years (standard deviation [*SD*]: 15.92) and 46.9 percent of them were male. Among these respondents, 89.9 percent was from Dutch origin, while the remaining respondents were either born abroad or had at least one parent who was born in another country. Most respondents (63.5%) were married, while 23.1 percent of the respondents were never married, 8.8 percent was divorced or separated, and 4.6 percent was a widow or widower.

Measurements

The dependent variable in this study is cybercrime victimization. This was measured by asking the respondents to indicate whether they fell victim to seven types of cybercrime in the last 2 years. Those seven types of cybercrime are summarized in Table 1. Two control groups were constructed, one with respondents who were only victimized by traditional crime and one with respondents who were not victimized at all. The seven items used to measure victimization of traditional crime are also summarized in Table 1. Respondents who fell victim to both a cybercrime and a traditional crime are included in the group of cybercrime victims. Only those who are only victimized by a traditional crime are included in the group of traditional crime victims. This resulted in a groups of 550 cybercrime victims (15.1 percent), 513 traditional crime victims (14.1 percent), and 2,585 nonvictims (70.9 percent).

The independent variables in this study are the key traits from the Big Five model of personality. These traits were measured using 50 items (i.e., 10 items per domain) from the International Personality Item Pool (IPIP).[25] Respondents were asked: ''*Please use the rating scale below to describe how accurately each statement describes you*''. They could use a scale ranging from 1 ''very inaccurate'' to 5 ''very accurate'' to answer these 50 items. These 50 statements can be found on the website of the IPIP (http://ipip.ori.org/newBigFive5broadKey.htm). Based on these scores a scale ranging from 0 to 40 was constructed for each of the Big Five traits. The respondents had an average score on the extraversion scale of 21.67 (*SD*: 7.34). This trait involves the following facets: friendliness, gregariousness, assertiveness, activity level, excitement seeking, and cheerfulness. The mean score on the agreeableness scale was 27.78 (*SD*: 7.05). The agreeableness scale involves the following domains: trust, morality, altruism, cooperation, modesty, and sympathy. The average score on the conscientiousness scale was 26.32 (*SD*: 7.12) and this scale comprises the following facets: self-efficacy, orderliness, dutifulness, achievement striving, self-discipline, and cautiousness. The respondents had a mean score of 23.36 (*SD*: 7.84) on the scale for emotional stability. This scale comprises the following domains: anxiety, anger, depression, self-consciousness, immoderation, and vulnerability. The scores on the openness to experience scale had an average of 23.90 (*SD*: 6.53). This scale involves the following facets: imagination, artistic interests, emotionality, adventurousness, intellect, and liberalism.

Table 1. Items Used to Measure Victimization

Cybercrime	*Traditional crime*
Could you please indicate for the following crimes whether you fell victim to it in the last 2 years, thus since February 2010?	
Intimidation by e-mail, SMS, MSN, or any other electronic channel	Intimidation by any other means (e.g., by letter, telephone, or face-to-face)
Others gained access to your computer without permission	Burglary or attempted burglary (of your home, shed, or garage)
Your computer was infected by a virus that caused damage, for instance, by deleting files on the hard disk	Theft from your car
Your credit card number was stolen and used to make a purchase, without your knowledge	Theft of your wallet or purse, handbag, or other personal possession (in the street, from a wardrobe, etc.)
You bought something through the Internet or e-mail, but did not receive the product	Wreckage of your car or other private property (garden, bicycle, etc.)
There was money taken from your bank account, without your permission	Maltreatment of such serious nature that it required medical attention
Someone has used your personal information for identity fraud (e.g., because someone pretended to be you after committing an offense, with the use of medical care, or with applying for a mortgage)	Maltreatment that did not require medical attention

Analyses

To examine the associations between the personality traits and the three victim groups, a multinominal logistic regression analysis was used since this is a categorical dependent variable. In these analyses, three comparisons were made between the three victim groups, that is, cybercrime victims versus nonvictims, traditional crime victims versus nonvictims, and cybercrime victims versus traditional crime victims. Next, five separate logistic regression analyses were performed to predict victimization of hacking, online intimidation, virus infection, online consumer fraud, and theft from bank account. Logistic regression analyses were used because the dependent variables in these analyses were binary (i.e., being a victim of a specific type of cybercrime or not). These analyses are not performed for victimization of stolen credit card numbers and identity fraud because the number of victims of these 2 crimes (32 and 11, respectively) was too low. Besides the 5 scales of the personality traits also gender and age (at February 2012) were included as control variables in all analyses.

Results

The results of the multinominal logistic regression analyses are displayed in Table 2. In Model 1 the personality traits of cybercrime victims are compared to those of nonvictims. Against our expectation, a significant association was found for conscientiousness, but not for agreeableness. Individuals who were more conscientious have a decreased risk to become a victim of cybercrime (Odds Ratio[OR]: 0.981). In addition, also people who showed more emotional stability were less likely to be victimized by cybercrime (OR: 0.959), while those who were more open to experience were more likely to be a victim of cybercrime (OR: 1.044). Moreover, the control variables show that men and young people were more likely to become victims of cybercrime than women and older people.

Table 2. Odds Ratios from Multinominal Logistic Regression Analyses Predicting Victimization

Victim group *Reference group*	*Model 1* *Cybercrime* *Nonvictim*	*Model 2* *Only traditional crime* *Nonvictim*	*Model 3* *Cybercrime* *Only traditional crime*
Extraversion	1.006	1.003	1.003
Agreeableness	1.014	1.014	1.000
Conscientiousness	0.981[a]	0.969[b]	1.012
Emotional stability	0.959[c]	0.983[a]	0.975[b]
Openness to experience	1.044[c]	1.026[a]	1.018
Gender (ref. = female)	1.394[b]	0.911	1.530[b]
Age	0.981[c]	0.993[a]	0.989[b]
N	3,135	3,098	1,063

[a]$p < 0.05$ (two sided); [b]$p < 0.01$; [c]$p < 0.001$.

In Model 2 the personality traits of traditional crime victims are compared to those of nonvictims. Similar to the result in Model 1, significant associations were found between victimization of traditional crime and conscientiousness (OR: 0.969), emotional stability (OR: 0.983), and openness to experience (OR: 1.026). Younger individuals were also more likely to become victims of traditional crime, while no significant difference in victimization risk was found between men and women.

In Model 3, the personality traits of cybercrime victims are compared to those who were only victimized by traditional crimes. Emotional stability was the only personality trait in this model that significantly predicts cybercrime victimization. Victims who were more emotionally stable were significantly less likely to have been a victim of cybercrime (OR: 0.975). Moreover, men and young people were significantly more likely to have been a victim of cybercrime than women and older people. The Nagelkerke R^2 of the multinominal logistic regression model is 0.046, which indicates that approximately 4.6 percent of the variance of the victim groups could be explained by the personality traits, gender, and age. The pseudo R^2 would even be lower if other measures of the explained variance were used, such as the McFadden R^2 (0.023) or the Cox-Snell R^2 (0.037). This further illustrates that this multinominal logistic regression model only explains a little bit of the variance.

Next, it was examined whether victimization of specific types of cybercrime could be predicted by the key traits from the Big Five model of personality. Table 3 shows the results of these logistic regression analyses. Individuals with higher scores on emotional stability were significantly more likely to become a victim of all types of cybercrime except hacking. Table 3 also shows that those who were more open to experiences were significantly more likely to become a victim of hacking (OR: 1.069) and a virus infection (OR: 1.029). Moreover, scores on conscientiousness were shown to have a significant and negative relationship with victimization of online intimidation (OR: 0.940). The results for the control variables show that young individuals were significantly less likely to become a victim of online intimidation, a virus infection, and online consumer fraud. Men were also significantly more likely to become a victim of online consumer fraud than women. The Nagelkerke R^2's in Table 3 range between 0.015 and 0.023 and would be even lower when other pseudo R^2 measures were used, which indicates that only a small proportion of the variance in victimization could be explained in each model.

Discussion

In this article, data from a large representative sample of Dutch individuals were used to examine the associations

Table 3. Odds Ratios from Logistic Regression Analyses Predicting Cybercrime Victimization

Type of crime	*Virus infection*	*Hacking*	*Online intimidation*	*Online consumer fraud*	*Money taken from bank account*
Extraversion	1.008	1.010	1.036	1.014	1.006
Agreeableness	1.002	0.976	1.010	1.018	1.030
Conscientiousness	0.991	0.978	0.940[a]	0.970	1.027
Emotional stability	0.967[c]	0.976	0.951[a]	0.932[c]	0.960[b]
Openness to experience	1.029[a]	1.069[b]	1.030	1.025	1.022
Gender (ref. = female)	1.306	0.902	1.095	1.782[b]	1.459
Age	0.989[a]	1.003	0.976[b]	0.981[b]	0.992
Nagelkerke R^2	0.020	0.015	0.061	0.061	0.023
N total	3,255	3,208	3,642	3,289	3,286
N victims	267	82	56	111	126

[a]$p < 0.05$ (one sided); [b]$p < 0.01$; [c]$p < 0.001$

between cybercrime victimization and key traits from the Big Five model of personality. Results showed that lower scores on conscientiousness and emotional stability and higher scores on openness to experience were significantly related to victimization risk of cybercrime. Previous studies showed that a low self-control is related to cybercrime victimization[7,11,18] and that the traits conscientiousness and agreeableness show both conceptual[20] and empirical[21] overlap with self-control. Against our expectation, however, only conscientiousness was shown to be related to cybercrime victimization in the current study, while no significant relationship was found with agreeableness. In addition, also lower scores on emotional stability and higher scores on openness to experience were shown to be associated with cybercrime victimization.

Remarkably, the same three personality traits (i.e., conscientiousness, emotional stability, and openness to experience) were also significantly related to victimization of traditional crime. This similarity in results for cybercrime and traditional crime indicates that these personality traits are not specifically associated with cybercrime victimization, but rather with victimization in general. A comparison between cybercrime victims and traditional crime victims showed that only those with higher scores on emotional stability were less likely to become a victim of cybercrime than traditional crime.

As cybercrimes differ in nature, differences were expected in personality traits related to victimization of cyber-dependent crimes and cyber-enabled crimes. However, our analyses show that this only applies to openness to experience. Individuals with higher scores on openness to experience have higher odds of becoming a victim of hacking or virus infection, but not of becoming a victim of the cyber-enabled crimes. Perhaps this is related with the modus operandi of hackers and malware attacks (see, for example, Leukfeldt, Kleemans, and Stol[26]). A common method, for example, is sending e-mails with an infected attachment. Users are persuaded to click on a link in the e-mail or open an attachment. Once this is done, the computer of the user is compromised. Perhaps the e-mail is drafted in such a way that users with a high degree of openness to experience are more inclined to perform the task. Future studies into the content of spam e-mails should include this psychological factor.

The current study has several strengths. A first strength is the topic of the study, since it is the first that examines the Big Five personality traits of cybercrime victims. Moreover, a large and representative sample of Dutch individuals is used which increases the generalizability of the results. Besides these strengths, there are also some limitations to the current study. First of all, due to the nonexperimental nature of the data, only associations between personality traits and cybercrime victimization could be investigated. The results, therefore, do not implicate direct causal effects. Second, we only measure victimization over a period of 2 years. It is therefore possible that those in the group of nonvictims have actually become a victim of cybercrime, but just not during the past 2 years. Moreover, only victimization of a limited number of types of crime was measured, which leaves open the possibility that nonvictims had become a victim of another type of crime. When some of those in the group of nonvictims are actually victims, this would likely underestimate the associations that were found. Third, the Nagelkerke R^2 of the regression models is relative low. This means that personality traits only explain a little part of the variance in cybercrime victimization and that other relevant variables were not included in the models. Fourth, although we used a representative sample of Dutch households, these results might not be generalizable to citizens from other countries. Since the Netherlands has a high Internet penetration rate, the chance to become a victim of cybercrime might be different compared to countries with a lower rate.

Future studies could further investigate whether the associations between personality traits and cybercrime victimization that were found in this study reflect direct effects or rather are mediated by other factors. The study by Wilcox et al,[14] for example, showed that the relationship between personality traits and traditional crime victimization was an indirect effect mediated by having delinquent peers and exposure to illicit goods. Moreover, Peluchette et al.[23] showed that the Big Five personality traits were also related to online behavior (e.g., frequency of Internet use, number of Facebook friends, and posting indiscrete content). It would be recommended if future studies examine whether the association between personality traits and cybercrime victimization is mediated by such factors as delinquent friends and online behavior. Moreover, in future research, new types of data should be used to measure risk on cybercrime victimization. Actual online behavior, for example, can be measured based on log files of computers of users theirselves, on systems of schools or employers or Internet service providers. Including such information might lead to a better prediction of cybercrime victimization, which would make it easier to take preventive measures.

Acknowledgments

The LISS panel data were collected by CentERdata (Tilburg University, The Netherlands) through its MESS project funded by the Netherlands Organization for Scientific Research.

Author Disclosure Statement

No competing financial interests exist.

References

1. Statistic Netherlands. (2016) *Veiligheidsmonitor 2015*. Den Haag: Centraal Bureau voor de Statistiek.
2. ONS. (2016) *Crime in England and Wales: Year Ending December 2015.* London: ONS.
3. Leukfeldt ER, Yar M. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. Deviant Behavior 2016; 37:263–280.
4. Jansen J, Leukfeldt ER. Phishing and malware attacks on online banking customers in the Netherlands: a qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology 2016; 10:79–91
5. Leukfeldt ER. Phishing for suitable targets in the Netherlands. Routine activity theory and phishing victimization. Cyberpsychology Behavior and Social Networking 2014; 17:551–555.
6. van Wilsem JA. Worlds Tied Together? Online and non-domestic routine activities and their impact on digital and

traditional threat victimization. European Journal of Criminology 2011; 8:115–127.
7. van Wilsem JA. ''Bought It, but Never Got It.'' Assessing risk factors for online consumer fraud victimization. European Sociologic Review 2011; 29:168–178.
8. Marcum CD, Higgins GE, Ricketts ML. Potential factors of online victimization of youth: an examination of adolescent online behaviors utilizing routine activity theory. Deviant Behavior 2010; 31:381–410.
9. Holt TJ, Bossler AM. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior 2009; 30:1–25.
10. Bossler AM, Holt TJ. On-line activities, guardianship, and malware infection: an examination of routine activities theory. International Journal of Cyber Criminology 2009; 3:400–420.
11. Ngo FT, Paternoster R. cybercrime victimization: an examination of individual and situational level factors. International Journal of Cyber Criminology 2011; 5:773–793.
12. Choi KS. Computer crime victimization and integrated theory: an empirical assessment. International Journal of Cyber Criminology 2008; 2:308–333.
13. Ellrich K, Baier D. The influence of personality on violent victimization–a study on police officers. Psychology, Crime & Law 2016; 22:538–560.
14. Wilcox P, Sullivan CJ, Jones S, et al. Personality and Opportunity An Integrated Approach to Offending and Victimization. Criminal Justice and Behavior 2014; 41:880–901.
15. Gottfredson MR, Hirschi T. (1990). *A general theory of crime*. Stanford University Press.
16. Schreck CJ. Criminal victimization and low self-control: An extension and test of a general theory of crime. Justice Quarterly 1999; 16:633–654.
17. Holtfreter K, Reisig MD, Pratt TC. Low self-control, routine activities, and fraud victimization. Criminology 2008; 46:189–220.
18. Bossler AM, Holt TJ. The effect of self-control on victimization in the cyberworld. Journal of Criminal Justice 2010; 38:227–236.
19. Pratt TC, Turanovic JJ, Fox KA, et al. Self-control and victimization: a meta-analysis. Criminology 2014; 52:87–116.
20. Jones SE, Miller JD, Lynam DR. Personality, antisocial behavior, and aggression: a meta-analytic review. Journal of Criminal Justice 2011; 39:329–337.
21. Van Gelder JL, De Vries RE. Traits and states: integrating personality and affect into a model of criminal decision making. Criminology 2012; 50:637–671.
22. Grasmick HG, Tittle CR, Bursik RJ, et al. Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. Journal of Research in Crime and Delinquency 1993; 30:5–29.
23. Peluchette JV, Karl K, Wood C, et al. Cyberbullying victimization: do victims' personality and risky social network behaviors contribute to the problem?. Computers in Human Behavior 2015; 52:424–435.
24. Holt TJ, Bossler AM. An assessment of the current state of cybercrime scholarship. Deviant Behavior 2014; 35:20–40.
25. Goldberg LR, Johnson JA, Eber HW, et al. The international personality item pool and the future of public-domain personality measures. Journal of Research in Personality 2006; 40:84–96.
26. Leukfeldt ER, Kleemans ER, Stol WP. A typology of cybercriminal networks: from low tech locals to high tech specialists. Crime, Law and Social Change 2017; 67:21–37.

Address correspondence to:
Dr. Steve G.A. van de Weijer
Netherlands Institute for the Study of Crime and Law Enforcement
PO Box 71304
Amsterdam 1008 BH
The Netherlands

E-mail: svandeweijer@nscr.nl