VU Research Portal

Out of control online?

Berenblum, Tamar; Weulen Kranenbarg, Marleen; Maimon, David

published in

Journal of Crime and Justice
2019

DOI (link to publisher)

[10.1080/0735648X.2019.1692424](https://doi.org/10.1080/0735648X.2019.1692424)

document version

Publisher's PDF, also known as Version of record

document license

Article 25fa Dutch Copyright Act

[Link to publication in VU Research Portal](#)

citation for published version (APA)

Berenblum, T., Weulen Kranenbarg, M., & Maimon, D. (2019). Out of control online? A combined examination of peer offending and perceived formal and informal social control in relation to system-trespassing. *Journal of Crime and Justice*, 42(5), 616-631. [5]. <https://doi.org/10.1080/0735648X.2019.1692424>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

Out of control online? A combined examination of peer-offending and perceived formal and informal social control in relation to system-trespassing

Tamar Berenblum, Marleen Weulen Kranenbarg & David Maimon

To cite this article: Tamar Berenblum, Marleen Weulen Kranenbarg & David Maimon (2019) Out of control online? A combined examination of peer-offending and perceived formal and informal social control in relation to system-trespassing, Journal of Crime and Justice, 42:5, 616-631, DOI: [10.1080/0735648X.2019.1692424](https://doi.org/10.1080/0735648X.2019.1692424)

To link to this article: <https://doi.org/10.1080/0735648X.2019.1692424>

Published online: 02 Dec 2019.

Submit your article to this journal [↗](#)

Article views: 752

View related articles [↗](#)

View Crossmark data [↗](#)

Citing articles: 2 View citing articles [↗](#)

Out of control online? A combined examination of peer-offending and perceived formal and informal social control in relation to system-trespassing

Tamar Berenblum^{a*}, Marleen Weulen Kranenborg^{b*} and David Maimon^c

^aHebrew University of Jerusalem, Jerusalem, Israel; ^bVrije Universiteit (VU) Amsterdam; ^cGeorgia State University, Atlanta, GA, USA

ABSTRACT

Compared to the offline world, the online environment is more anonymous and therefore less easily controlled. Criminological theories generally show that people are more likely to commit crime when they experience or perceive less formal or informal social control. Consequently, one might assume that people are more likely to commit crime online than offline. As formal social control is lacking, informal social control and peer-offending may be important predictors of online offending. In this paper, we examine to what extent differences in perceived formal and informal online control are related to the likelihood that a person will commit a system-trespassing offense (i.e. malicious hacking). Additionally, we examine peer system-trespassing, and how this may interact with perceptions of formal and informal social control. In the logistic regression analyses we employ eight different measures for perceptions of formal and informal social control, in addition to peer-offending, and control variables. Both direct effects and interaction effects are examined. Our results show that peer-offending is an important predictor of system-trespassing and interaction effects show that perceived formal and informal online social control are related to this type of offending but only for specific groups. Implications will be discussed.

KEYWORDS

Social control;
system-trespassing; online
crime; cybercrime; hacking;
peer-offending

Introduction

System trespassing, more commonly referred to as hacking (Furnell 2002; Wall 2007/2010), occurs when an offender infiltrates a computer or a network without authorization with the goal of accessing, changing or even deleting data (McQuade 2006; Maimon et al. 2015). The motivations for such system trespassing are varied, and affect the offender actions on the system and consequently the harm experienced by the victims (Bachmann 2011; Bachmann and Corzine 2010; Chiesa, Ducci, and Ciappi 2008; Denning 2011; Fotinger and Ziegler 2004; Gordon and Ma 2003; Holt 2007, 2009; Holt and Kilger 2012; Jordan and Taylor 1998; National Crime Agency 2017; Nycyk 2010; Taylor 1999; Turgeman-Goldschmidt 2008; Voiskounsky and Smyslova 2003; Weulen Kranenborg 2018; Woo 2003; Woo, Kim, and Dominick 2004; Xu, Hu, and Zhang 2013).

Deviant online behavior and online crime (such as system trespassing) are increasing (Van Vuuren, Leenen, and Pieterse 2019; McAfee 2018; Grabosky 2017; National Crime Agency 2016) as a result of the increasing use of the internet, which in turn expands criminal opportunities (Brignall 2002), combined

CONTACT Tamar Berenblum tamar.berenblum@mail.huji.ac.il Hebrew University of Jerusalem.

*Co-first authors of this article.

Tamar Berenblum and Marleen Weulen Kranenborg are both to be regarded as co-first authors of this article.

© 2019 Midwestern Criminal Justice Association

with anonymity (Suler 2004) and the lack of (formal) online social control (Wall 2007/2010). However, the application of social control theory to the online environment should be further elaborated in order to contribute more meaningfully to the understanding of online crime. Therefore, this article sheds light on the context the internet provides with regard to social control and its enforcement – a challenge that should be addressed both theoretically and empirically.

Borrowing from the interactional theory of delinquency, which aims to expand the social control model by adding social learning aspects, this article contributes to a further theoretical development by applying formal and informal social control and social learning theories to the online context. In this paper we will combine the aforementioned elements of social control, peer-offending, Thoughtfully Reflective Decision Making (TRDM), and Information Technology (IT) knowledge in order to examine the extent to which these are related to system-trespassing offenses individually, but also how these may interact with each other. Using a sample of first-year undergraduate students ($N = 465$) comparable to the samples used in previous research, our approach provides a new perspective for this body of research and its relation to peer-offending by jointly examining peer-offending and several measures for both formal and informal online social control.

Theoretical background

The underlying premise of social control theories is that the motivation to commit a crime is embedded in human nature; accordingly, social control is an important mechanism through which society can enforce conformity. An argument common to the different theoretical approaches is that in the absence of such control, deviant behavior will occur (Vold and Bernard 1986). The minimization of social control on the internet may be one of the reasons why system-trespassing offenses are committed. In the online environment, the traditional concepts of formal control, governance, and enforcement are insufficient, since the global nature of the internet does not allow for effective regulation by one country on its own, and instead requires international cooperation and self-regulation of internet users and their communities (Barzilai-Nahon and Neumann 2005; Valverde 2000). This explains why, when discussing social control in the online environment, user communities have a vital role to play (Brenner 2007), and we may expect to see the growth of informal social control mechanisms such as collective responses, self-help practices, and peers (Cohen and Scull 1983; Cohen 1985). As formal online social control is limited, and informal social control is accordingly more important, peers' perceptions of and reactions to offending can be expected to affect deviant behavior online.

The importance of peers is an eminent theoretical concept in social learning theories (e.g. Akers 1998; Hirschi 1969; Pratt et al. 2009; Sampson and Laub 1993). From this perspective, criminal behavior has to be learned like any other human behavior. Sutherland (1939) discusses the components of social learning. His Differential Association Theory suggests that criminals become such by learning the relevant values, attitudes, techniques, and motives through a dynamic process of their interactions with others. Associating with peers who commit system-trespassing may, therefore, reinforce deviant behavior, increase deviant definitions, and provide ways to acquire the knowledge and skills that are needed to commit system-trespassing offenses as discussed above. These peers play an important role in teaching not only the techniques and tools (knowledge), but also affect the attitudes toward the behavior (Morris and Blackburn 2009).

McCuddy and Vogel (2015a) researched the effect of individual behavior and exposure to criminal behavior on online social networks. Their findings support the idea that online socialization may contribute to the understanding of online criminal behavior and that social networks and virtual peers have an effect, albeit in a very different way than the traditional offline networks (McCuddy and Vogel 2015b). Such strong positive effects have also been found in the context of online crimes. As for traditional crime (Pratt et al. 2009) online offending of peers has shown to be an important predictor of online offending of an individual, including system-trespassing offenses (Bossler and Burruss 2011; Donner et al. 2014; Holt 2007; Holt, Bossler, and May 2012; Holt, Burruss, and Bossler

2010; Holt and Kilger 2008; Hu, Xu, and Yayla 2013; Marcum et al. 2014; Morris 2011; National Crime Agency 2017; Rogers 2001; Weulen Kranenbarg, Ruiter, and Van Gelder 2019).

While much of the research examines elements of social learning theory in the context of digital piracy (see, for example: Higgins et al. 2012; Holt, Bossler, and May 2012; Hinduja 2003; Miller and Morris 2016), some studies examine the different components of the theory in the context of hacking. Holt, Burruss, and Bossler (2010), for example, examined several crimes, including hacking and found that differential associations explain much of the variation in online crime. Additionally, Morris and Blackburn (2009) found that the more serious the online crime is, the more prominent the role of the delinquent friends.

Borrowing from these two sets of theories – control theory (Hirschi 1969) and learning theory (Akers 1998) – Thornberry (1987) developed an interactional theory of delinquency, proposing an extended model of social control theory that includes elements from social learning theory. He argues that control, learning, and delinquency mutually affect one another. According to this model, delinquency is a dynamic process through which the delinquent behavior is learned and reinforced. This process that is strongly influenced by the offender's position in social structure and by their social bonds. A key component in examining such social bonds is the offender's association with delinquent peers, including the level of attachment to peers, the peers' delinquent behavior and values, and their reinforcing reactions to delinquent behavior.

The theoretical link between peer-offending, perceptions of informal social control, and the knowledge and skills needed to commit system-trespassing offenses demands integrated examination. Based on the literature review above, in this paper we seek to explore the interaction between social control perceptions and association with delinquent peers in the online environment. We hypothesize that: (1) *individual perceptions regarding the scope of formal and informal online social control will be correlated with engagement in system trespassing*. As explained above, social control is believed to be the main mechanism for preventing deviance, while its absence – or the subjective assumption that such control is missing (Weisburd 1989) – will lead to criminal behavior. Thus, we expect that the lower the perceptions of online social control, the more the respondent will be involved in system trespassing; (2) *peer system trespassing will be correlated with engagement in system trespassing*. Recent work in criminology has identified online peer-offending as an important predictor of the online offending of an individual. While our sample examines students from a different country, we anticipate a similar finding and assume that greater involvement of peers in system trespassing will also lead to higher levels of self-reporting; and (3) we hypothesize that *the two variables interact*, based on Thornberry's (1987) argument that control, social learning, and delinquency mutually affect one another. Such interaction is potentially affected by the characteristics of the online environment and the growing power of peers in this sphere, both as informal control agents and as members of the same deviant community.

Method

Sample and procedure

Our data collection effort was initiated in November 2014 and continued through January 2015.¹ It involved the participation of 465 first-year undergraduate students at the Hebrew University of Jerusalem.² Participants were asked to complete a questionnaire designed to address several subjects: (1) self-reporting of online behavior and online victimization; (2) knowledge of formal online social control practices; and (3) perceptions of social control and the level of control applied on the internet. The overall response rate was 33.3%;³ participants were mostly female (60.9%), with a mean age of 24.2.⁴

Measures

Dependent variable

The dependent variable system trespassing constituted a combination of two types of self-reported system-trespassing offenses. Respondents were asked if they engaged in one of the following two behaviors in the preceding 12 months: 'Tried to guess another's password to get into his/her computer account or files' (6.5%)⁵ and "accessed another person's computer account or files without his/her knowledge or permission to look at information or files" (7.0%). These two offending items were combined into one binary outcome variable ($\alpha = .54$). The binary outcome variable *system trespassing* was coded as 1 if a respondent answered 'yes' to at least one of these behaviors (10,1%; see Table 1 for descriptive statistics of all variables).

Independent variable: peer system-trespassing

For measuring *peer system trespassing*, respondents were asked if any of their close friends engaged in one of the following cyber-criminal behaviors in the preceding twelve months: 'Guessed another's password to get into his/her computer account or files' (17.8%), 'accessed another person's computer account or files without his/her knowledge or permission to look at information or files' (17.4%). Similar to the outcome variable, these items were combined in one binary variable *peer system-trespassing* ($\alpha = .60$), which was coded as 1 if a respondent answered 'yes' to at least one of these behaviors (26%).

Independent variables: online social control

First, two separate items were used to measure respondents' perceptions of formal and informal online social control. On a five-point scale (1 = no social control – 5 = excessive social control), respondents were asked to evaluate the level of social control enforced over the internet by the police (*formal social control*, $M = 2.1$) and other internet users (*informal social control*, $M = 2.2$).

In addition to these perceptions of social control, respondents were also asked to rate their agreement (1 = highly disagree – 5 = highly agree) with the following statements about social control of peers and by peers: 'As an internet user, I enforce social control over other users' (*control over peers*, $M = 2.4$); and 'peer social control is the most effective way to prevent online crime and deviant behavior' (*prevention by peers*, $M = 2.5$). Similarly, the following statements about formal control were rated on the same scale: 'It is not possible to monitor all of my online behavior' (*perception getting caught*, $M = 2.7$); and 'I am knowledgeable about the laws that regulate the cybersphere' (*laws online* $M = 1.7$). In addition, in order to measure neutralization or deviant definitions of offending behavior, respondents were asked to rate their agreement to the statement: 'If people do

Table 1. Variable descriptives.

Continuous variables	M	SD	Min	Max
Formal social control	2.12	.78	1	5
Informal social control	2.22	1.05	1	5
Control over peers	2.39	.96	1	5
Prevention by peers	2.47	.94	1	5
Perception getting caught	2.69	1.18	1	5
Laws online	1.71	.84	1	4
Neutralization	2.67	1.93	1	7
TRDM average	4.41	1.30	1	7
Computer/internet use	5.77	2.77	.63	17.5
IT knowledge	3.73	1.42	1	7
Age	24.15	2.62	16	51
Dummy variables	Yes (no) %			
System trespassing	10.11 (89.89)			
Increase social control	75.00 (25.00)			
Peer system-trespassing	26.01 (73.99)			
Female	60.69 (39.31)			

not want me to get access to their computer system, then they should have better computer security' (*neutralization*, $M = 2.7$). Lastly, respondents were asked (as a yes/no question) whether they want to 'increase online social control' (*increase social control*, 1 = 'yes', 74.8%). All these items were included as separate variables in the analyses.

Control variables

Thoughtfully Reflective Decision Making (TRDM) – 'TRDM' (Paternoster, Pogarsky, and Zimmerman 2011; Paternoster and Pogarsky 2009) is defined as the 'tendency of persons to collect information relevant to a problem or decision they must make, to think deliberately, carefully, and thoughtfully about possible solutions to the problem, apply reason to the examination of alternative solutions, and reflect back upon both the process and the outcome' (Paternoster and Pogarsky 2009, 104–5). Louderback and Antonaccio (2017) examined this concept in the context of the online environment and found that higher levels of TRDM predicted less computer-focused offending and victimization.

Adopting Paternoster and Pogarsky's (2009) scale, we created a TRDM measure from four survey items with response categories ranging from 1 = highly disagree – 7 = highly agree: 'When I have a problem to solve, one of the first things I do is get as many facts about the problem as possible;' 'When I am attempting to find a solution to a problem, I usually try to think of as many different approaches to the problem as possible;' 'When making decisions, I generally use a systematic method for judging and comparing alternatives;' and 'After carrying out a solution to a problem, I usually try to analyze what went right and what went wrong,' The average score for these four items (*TRDM average*, $M = 4.4$, $\alpha = 0.8$) will be used in the analyses.

In addition, in order to control for the extent to which respondents had the opportunity to commit online crime, we included a measure for their overall computer and internet use and a measure of their overall IT knowledge. Respondents' overall *computer/internet use* was constructed by taking the average of their answers to four questions about how many hours per weekday/ weekend day they typically spend using the internet or a computer ($M = 5.8$). In addition, their *IT knowledge* was measured by asking: 'How would you describe your level of familiarity with computer operating systems?', which they could answer on a seven-point scale (1 = beginner – almost no familiarity – 7 = expert – total familiarity, $M = 3.7$). While IT knowledge is a control variable, we also checked for interaction effects between IT knowledge and social control or peer offending, as the effect of peer offending or social control may differ between people with more or less IT knowledge. Lastly, we controlled for age and gender by including a binary variable *female* (1 = female, 60.9%) and a continuous variable for *age* ($M = 24.2$).

Non-response and analytical strategy

Missing values on the independent variables were imputed using the STATA 14 Multivariate Imputation by Chained Equations (MICE) procedure (based on Royston 2004). In line with Von Hippel (2007), the six respondents with missing values on the dependent variable were included in the imputation, but excluded from the analyses in this paper. After generating a total of 20 datasets, these were used to estimate the models, while adjusting the coefficients and standard errors for the variability between imputations by means of the Rubin (1987) combination rules.⁶ For the analyses of the binary dependent variable, logit models were used. As we are testing hypothesis, we used one-tailed significance tests.

Results

Models without interaction effects

Table 2 presents the results of three regression models. In Model 1, all online social control variables and the control variables have been included; the only variable not included is peer system-trespassing.

Table 2. Logit models system-trespassing without interactions (N = 465).

	Model 1		Model 2		Model 3	
	OR	SE	OR	SE	OR	SE
Formal social control	1.10	.23			.97	.23
Informal social control	.91	.15			.82	.16
Control over peers	1.11	.19			1.16	.23
Prevention by peers	.82	.15			.81	.17
Perception getting caught	1.21	.17			1.28	.20
Laws online	1.15	.23			1.18	.27
Neutralization	1.13	.09			1.13	.11
Increase social control	.50*	.18			.52	.21
Peer system-trespassing			22.03***	9.25	23.65***	10.28
TRDM average	.89	.12	.82	.13	.82	.13
Computer/internet use	.90	.06	.88*	.07	.87*	.07
IT knowledge	1.21	.16	1.27	.19	1.20	.19
Age	.94	.07	.99	.07	.99	.07
Female	1.55	.58	1.99*	.79	2.38*	1.03
R square ¹		.06		.28		.31

* $p < .05$; ** $p < .01$; *** $p < .001$ (one-tailed)

OR = Odds Ratio

SE = Standard Error

¹Average pseudo R square over imputed data

Model 2 includes peer system-trespassing and the control variables, but does not include the online social control variables. In Model 3, all variables are included, both peer system-trespassing and the social control variables, along with the control variables.

Model 1, which does not include peer system-trespassing, shows that the social control variables do not explain much of the variance in offending (just 6%). The only variable that is significantly related to online offending is the yes/no answer to the question whether respondents wanted to increase online social control ($p < .05$). This effect shows that if a person states that he/she wants to increase online social control, the odds that that person would commit an online crime are reduced by 50%. In other words, it seems to indicate that respondents who offend do not want more social control, while the respondents who do not offend want more online social control.

In line with previous research on similar samples (Bossler and Burruss 2011; Donner et al. 2014; Holt 2007; Holt, Bossler, and May 2012; Holt, Burruss, and Bossler 2010; Holt and Kilger 2008; Hu, Xu, and Yayla 2013; Marcum et al. 2014; Morris 2011; National Crime Agency 2017; Rogers 2001), Model 2 shows that peer system-trespassing is strongly related to the online offending of an individual ($p < .001$). When comparing the odds ratio of the peer-effect to the odds ratio's in Model 1, it is clear that the peer-effect is much stronger. If a person has delinquent peers, the odds that that person would commit an online crime 22.03 times more likely. In addition, the control variables computer/internet use and female are significantly related to offending. This model, which as noted includes only peer system-trespassing and control variables, already explains 28% of the variation in offending. However, as discussed in the introduction, since these offenses are committed online, it is important to consider to what extent a person's perceptions of social control in this space is also related to this person's online criminal behavior, and to what extent including those perceptions changes the effect of peer system-trespassing.

Lastly, a comparison of Model 2 and Model 3 shows that adding the social control variables to the model with peer system-trespassing actually strengthens makes the relationship between peer system-trespassing and the outcome variable: the odds ratio further increases from 22.03 to 23.65 (both $p < .001$). This model also explains about 3% more of the variance in the outcome variable than Model 2, which does not include the social control variables. Additionally, when comparing Model 2 with Model 3, some changes in the effects of the social control variables can be observed. The strength of the effect of almost all social control variables increases, but the most eye-catching change is in the odds ratio of the perception of formal social control. Adding peer system-trespassing

to the model changes that effect from a 10% increase in the odds to a 3% decrease in the odds. We should note, however, that the effect is not statistically significant in both models. Lastly, although the strength and the direction of the effect of *increase social control* changes little, the standard error increases when peer system-trespassing is added to the model, changing the effect from significant ($p < .05$) to insignificant ($p = .06$). The changes in the effects suggest that there may be some interaction effects between peer system-trespassing and some of the social control variables, especially perceived formal and informal social control, since these show the most notable changes.

Interaction effects

Based on Thornberry's (1987) interactional theory of delinquency, in this section we will first discuss interaction effects between the perceived formal and informal social control variables and peer system trespassing. In addition, we will examine the interactions between these social control variables and the only significant social control predictor in the models in Table 2, i.e. the yes/no answer to the question whether respondents wanted to increase online social control. Lastly, as discussed in the method section, we will report to what extent IT knowledge interacts with the social control variables.

Model 1 in Table 3 shows that there is a significant interaction effect of peer system-trespassing on the perception of formal social control by the police ($p < .01$). It shows that there is a positive significant effect of experiencing formal social control for people without delinquent friends ($p < .05$). At the same time, there is also a negative significant effect among respondents who do have delinquent friends ($p < .05$). In other words, a person who has delinquent friends is less likely to offend if that person has a higher perception of formal social control by the police. A person who does not have delinquent friends is actually more likely to offend if that person has a higher perception of formal social control by the police. This can also be concluded from the predicted probabilities graph in Figure 1. Model 2 in Table 3 shows that there is no significant interaction effect of peer system-trespassing and the perceived informal social control of other internet users.⁷

Table 4 shows the models with interactions of perceived formal and informal social control with the desire to increase online social control (yes/no). Model 1 shows that there is no significant

Table 3. Logit models including interactions of peer system-trespassing with perceived formal or informal social control (N = 465).

	Model 1		Model 2	
	β	SE	β	SE
Peer system-trespassing* Formal social control	-1.17**	.49		
Peer system-trespassing* Informal social control			.02	.45
Peer system-trespassing	5.82***	1.28	3.11**	1.02
Formal social control	.83*	.41	-.03	.24
Informal social control	-.18	.19	-.22	.40
Control over peers	.14	.20	.15	.20
Prevention by peers	-.25	.22	-.21	.21
Perception getting caught	.23	.16	.25	.15
Laws online	.20	.23	.16	.2
Neutralization	.14	.10	.12	.10
Increase social control	-.74*	.41	-.66	.40
TRDM average	-.17	.16	-.19	.16
Computer/internet use	-.15*	.08	-.14*	.08
IT knowledge	.18	.16	.18	.16
Age	-.00	.08	-.01	.07
Female	.82*	.43	.87*	.43
R square ¹		.33		.31

* $p < .05$; ** $p < .01$; *** $p < .001$ (one-tailed)

β = Coefficient

SE = Standard Error

¹Average pseudo R square over imputed data

Figure 1. Predicted probabilities of offending by peer system-trespassing and perceived formal social control.

Table 4. Logit models including interactions of increase social control with perceived formal or informal social control (N = 465).

	Model 1		Model 2	
	β	SE	β	SE
Increase social control * Formal social control	.11	.47		
Increase social control * Informal social control			-.64*	.38
Peer system-trespassing	3.17***	.44	3.22***	.44
Formal social control	-.08	.31	-.06	.2
Informal social control	-.20	.19	.20	.30
Control over peers	.14	.20	.20	.20
Prevention by peers	-.21	.21	-.21	.22
Perception getting caught	.24	.15	.27*	.16
Laws online	.16	.23	.18	.23
Neutralization	.12	.10	.11	.10
Increase social control	-.91	1.11	.77	.95
TRDM average	-.19	.16	-.21	.16
Computer/internet use	-.14*	.08	-.13*	.08
IT knowledge	.18	.16	.18	.16
Age	-.01	.07	-.01	.08
Female	.86*	.43	.96*	.44
R square ¹		.31		.32

* $p < .05$; ** $p < .01$; *** $p < .001$ (one-tailed)

β = Coefficient

SE = Standard Error

¹Average pseudo R square over imputed data

interaction with formal social control. However, with regard to the interaction with informal social control, Model 2 indicates a significant ($p < .05$) interaction effect, but only for respondents who desire to increase social control. Meaning that if a person wants to increase social control, the more that person perceives that there is informal social control, the less likely they are to offend; this may also be seen in the graph in Figure 2.

As a final check, we examined interaction effects between the social control variables and the respondents' IT knowledge. Only two interaction effects were found to be significant.⁸ These models

Figure 2. Predicted probabilities offending by increase social control and perceived informal social control.

are especially interesting with regard to the predicted probabilities of people who consider themselves to be IT experts (i.e. who score high on the IT knowledge variable). If their assessment of their own knowledge is correct, these people might be able to commit the more sophisticated types of system trespassing, which means that it is important to see how social control may affect their behavior.

Model 1 in Table 5 shows a significant ($p < .05$) interaction effect between IT knowledge and control over peers ('As an internet user, I enforce social control over other users.'). In addition, Model

Table 5. Logit model including interactions of IT knowledge with control over peers or prevention by peers ($N = 465$).

	Model 1		Model 2	
	β	SE	β	SE
IT knowledge * Control over peers	-.30*	.16		
IT knowledge * Prevention by peers			-.45**	.16
Peer system-trespassing	3.24***	.45	3.36***	.46
Formal social control	.00	.24	-.06	.24
Informal social control	-.24	.19	-.21	.20
Control over peers	1.33*	.66	.18	.20
Prevention by peers	-.18	.21	1.44**	.60
Perception getting caught	.26*	.15	.25	.16
Laws online	.19	.23	.28	.24
Neutralization	.13	.10	.10	.10
Increase social control	-.69*	.41	-.77*	.42
TRDM average	-.20	.16	-.19	.16
Computer/internet use	-.13*	.08	-.15*	.08
IT knowledge	.92*	.44	1.28**	.43
Age	.01	.08	-.02	.07
Female	.97*	.45	1.00*	.45
R square ¹		.32		.34

* $p < .05$; ** $p < .01$; *** $p < .001$ (one-tailed)

β = Coefficient

SE = Standard Error

¹Average pseudo R square over imputed data

2 in Table 5 shows a significant interaction effect between IT knowledge and prevention by peers ('Peer social control is the most effective way to prevent online crime and deviant behavior'; $p < .01$). Both interaction effects show that a one unit increase in IT knowledge reduces the positive estimates for control over peers and prevention by peers by .30 and .45, respectively. For people who score low on IT knowledge these two social control variables have a positive effect. For people who score high on IT knowledge this changes to a negative effect. While Model 3 in Table 2 shows that IT knowledge and these two social control variables do not have a significant effect on offending in general, these interactions show that for respondents who score high or low on IT knowledge, these measures of social control are important.

These interaction effects can be more easily interpreted by looking at the graphs in Figures 3 and 4. Figure 3 shows that if a person has a high score on IT knowledge and a low score on control over peers that person has the highest probability of offending. It also shows that if a person has extensive IT knowledge, they are not very likely to offend if they also score high on control over peers. The predicted probabilities are inverse for those who score low on IT knowledge. Similarly, Figure 4 shows that a person who has a high score on IT knowledge and a low score on prevention by peers has the highest probability of offending. It also shows that if a person has extensive IT knowledge, they are not very likely to offend if they also score high on prevention by peers. Again, the predicted probabilities are inverse for people who score low on IT knowledge.

Conclusion and discussion

Results and implications

In this study we examined the extent to which peer system-trespassing and different measures of formal and informal online social control are related to system-trespassing. Based on the theoretical

Figure 3. Predicted probabilities offending by IT knowledge and control over peers.

Figure 4. Predicted probabilities offending by IT knowledge and prevention by peers.

link between peer-offending, perceptions of social control, and knowledge and skills needed to commit system-trespassing offenses, we argued that social control and learning theory should be studied in conjunction. We hypothesized that (1) lower perceptions of online social control will lead to higher involvement in system trespassing; (2) higher involvement of peers in system trespassing will lead to higher levels of self reporting; and (3) there is an interaction effect of peer system-trespassing and the perception of formal social and informal control.

To examine these hypotheses, we used a sample of 465 first-year undergraduate students and examined both the direct effects of peer-offending and measures of formal and informal social control, as well as interaction effects between these variables.

The contribution of this paper is twofold. From a theoretical perspective, our study links two theoretical approaches – social control and learning – by examining Thornberry's (1987) theory in the context of the online environment. Furthermore, we juxtaposed a differential association with both types of social control, formal and informal, while focusing mainly on perceptions of informal social control. From a methodological perspective, we expanded the existing literature on online offending and online social control to Israel, thus examining whether the same trends that have been found in previous studies also emerge in additional cultural contexts.

In line with previous research (Bossler and Burruss 2011; Donner et al. 2014; Holt 2007; Holt, Bossler, and May 2012; Holt, Burruss, and Bossler 2010; Holt and Kilger 2008; Hu, Xu, and Yayla 2013; Marcum et al. 2014; Morris 2011; Morris and Blackburn 2009; Rogers 2001), the results showed that online peer-offending is strongly related to online offending. The different variables that measure different types of online social control, on the other hand, did not explain much of the variation in online offending in itself. The only significant result indicates that while most respondents feel that online social control should be increased, offenders are less likely to think so compared to non-offenders.

Nevertheless, combining the measures for social control with peer-offending yielded some interesting results. First, the results showed that, in general, perceived formal and informal online social control is not related to online offending. However, when specifically looking at a person who has delinquent friends, this person is less likely to offend if they have a higher perception of formal social control by the police. The opposite is true for people who do not have delinquent friends. In addition, if a person feels that online social control should be increased, the more that person perceives that there is informal social control, the less likely they are to offend. Both interaction results suggest that increasing the perception of social control may be effective for specific groups. With regard to formal social control, increasing perceptions of formal social control among people with friends who commit online crimes (26%, in our sample) may decrease their offending. Secondly, with regard to informal social control, increasing the perception of informal social control among people who feel that social control should be increased (75%, in our sample) may further decrease their offending. This group, however, is already less likely to offend than those who do not want to increase social control. Therefore, based on our results it seems reasonable to focus on increasing perceptions of formal social control among people who have friends who commit online crimes.

The final two results showed that people who consider themselves to have strong IT knowledge, and who also feel that forms of informal social control are not effective in preventing or controlling online criminal behavior, have the highest probability of offending. In contrast, people with strong IT knowledge who do feel that those forms of informal social control are effective are much less likely to offend. This suggests that some people who have the ability to commit more serious types of system-trespassing offenses may be influenced by informal social control. Future research with samples that include more highly-skilled respondents should examine this possibility in greater detail. These studies may identify whether and how perceptions of informal social control affect a person's decisions to use their IT knowledge in a legal or illegal way.

This study adds to the existing theoretical literature on social control and the relation between peer behavior and online offending, since it shows that prevention programs for people with online delinquent peers may benefit from increasing perceptions of formal social control. In an era when online communication clearly limits the prevention of such offending by controlling a person's online criminal social ties, it is interesting to see that it may also be effective to focus on that person's perceptions of formal social control, rather than informal social control. Results from take downs of drug markets, show how the offenders' perceptions of the level and scope of formal control increases as a result of these police interventions (Bradley and Stringhini 2019). It would be interesting to test the effect of such take downs and other police interventions in the context of system trespassing.

Limitations and future research

This cross-sectional survey study based on an Israeli student sample naturally has its limitations. In particular, perceptions of formal social control may be completely different in different countries. Therefore, these results are not generalizable to student populations from different countries. Accordingly, future research should examine peer-offending and social control for different samples, preferably including students and the general population in different countries and cultural contexts. In addition, this general student sample was not specifically aimed at students with high IT knowledge, and we only asked for their own estimation of their level of expertise. Since we found an interesting interaction effect between the perceived effectiveness of peer social control and IT knowledge, future studies may also specifically focus on this group of highly-skilled respondents and examine their actual knowledge and the effects of peer-offending and social control among them. Lastly, the perceptions were tested with regard to system-trespassing; different results might be obtained when other types of online crime are examined.

Since this study is cross-sectional, it is not possible to make any causal claims based on our results. Future longitudinal research should examine to what extent changes in perceptions of social control lead to changes in offending, and to what extent causal relationships differ between people with and

without delinquent friends. Another interesting avenue would be to conduct an experiment in which perceptions of formal and informal social are manipulated to gauge the impact that interventions intended to increase these perceptions may have on offending. When combined with survey data, such an experiment could also look at differences of the effect of the manipulation between people with and without delinquent peers.

Lastly, our measures of social control focused on perception, and not on actual formal or informal social control. It would be interesting to study to what extent differences in perceptions of formal and informal social control are actually based on the amount of social control that a person experiences. For example, it would be interesting to see whether a person who has a high perception of informal social control also has social contacts who actively try to control the person's online behavior. This will suggest whether it is more important to focus on perceptions or on actually increasing social control. Natural experiments, such as new ways in which universities are monitoring the behavior of their students on university networks, may provide opportunities to examine to what extent this increases student's perceptions of social control, and whether this influences their behavior.

In conclusion, this study indicates that increasing perceptions of formal and informal social control will benefit from specifically targeting the right audience. Thus policy makers and practitioners should develop unique interventions and communicate their actions and the control measure applied to distinct population groups. Future studies should further investigate the relations between peer-offending, map the peer-offending network and the way it allows for information transfer and the learning process, as well as examining actual and perceived formal and informal social control. This will further enhance our knowledge on both the relationships of peer-offending and on social control with types of online offending.

Notes

1. The survey was administered as part of a larger project on computer security and network usage entitled 'Deterrence, Prevention and Regulation of Computer Crimes: Human Focused Policy Study.' The project is directed by Dr. David Maimon and Prof. David Levi-Faur, and is supported by the Israeli Ministry of Science, Technology and Space.
2. The survey targeted all first-year students in introductory courses in the different faculties (Law, Education, Social Work, Humanities, and Social Science). Students in their early 20s were chosen, since the internet forms a very natural part of their everyday routine. In contrast to older populations who have had to adjust to and learn new norms and behaviors that are sometimes very different from the offline world, these students were born into this culture. Moreover, as adults, these students can be held accountable for their online behavior. Their accountability, and their vast use of the internet, expose them to more formal and informal online social control.
3. This response rate is in the common range which varies between 14% to 70% (Porter and Umbuch 2006). The relatively low rate is not surprising given the length of the survey (22 pages) and the fact that response rates to surveys in general have declined dramatically over recent years (Sax et al. 2003).
4. The age and gender profile of these students are similar to those of the population of students at the Hebrew University of Jerusalem (56.5% of the students are female and the mean age is 25.9), and to the general student population in Israel (54.5% of the students are female and the mean age is 24.7; CBS 2014).
5. Only 2.8% of the participants guessed another person's password without reporting any of the other system trespassing offences in the survey. However, it was included because it is the first step in system-trespassing and shows an inclination toward this behavior.
6. Running the analyses with non-imputed data resulted in models that were very similar to the ones presented here. Results can be requested from the first authors.
7. In addition to these interaction effects, we also tested interactions between the other social control variables and peer system-trespassing. None of these interaction effects were statistically significant. The results can be requested from the first authors.
8. The other results can be requested from the first authors.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This research was conducted with support from the Israeli Ministry of Science, Technology and Space [Grant No. 3-10888].

Notes on contributors

Tamar Berenblum is the research director of the The Federmann Cyber Security Center – Cyber Law Program, Faculty of Law, the Hebrew University of Jerusalem, Israel. Her research mostly focuses on cybercrime, online social control and digital rights. Tamar is also a research fellow of the NSCR (Netherlands Institute for the Study of Crime and Law Enforcement) and co-chair of the ESC Cybercrime Working Group.

Marleen Weulen Kranenborg is an assistant professor at VU Amsterdam, The Netherlands. Her research mostly focuses on cyber-dependent offenders. In her doctoral dissertation she empirically compared traditional offenders to cyber-offenders on four important domains in criminology: 1. offending over the life-course, 2. personal and situational risk factors for offending and victimization, 3. similarity in deviance in the social network, and 4. motivations related to different offense clusters. She recently started a large-scale longitudinal study into actual vs. perceived cybercriminal behaviour of offline vs. online social ties among youth. Marleen is also a research fellow of the NSCR (Netherlands Institute for the Study of Crime and Law Enforcement), board member of the ESC Cybercrime Working Group, and part of the steering committee of the IIRCC (International Interdisciplinary Research Consortium on Cybercrime).

David Maimon is an Associate Professor in the department of Criminology and Criminal Justice at the Georgia State University. David's research interests include cyber-enabled and cyber-dependent crimes and experimental research methods.

References

- Akers, R. L. 1998. *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston: Northeastern University Press.
- Bachmann, M., and J. Corzine. 2010. "Insights into the Hacking Underground." In *The Future Challenges of Cybercrime. Volume 5: Proceedings of the Futures Working Group 2010*, edited by T. Finnie, T. Petee, and J. Jarvis, 31–41. Quantico, VA: FBI.
- Bachmann, M. 2011. "Deciphering the Hacker Underground: First Quantitative Insights." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell, 105–126. New York: Information Science Reference.
- Barzilai-Nahon, K., and S. Neumann. 2005. "Bounded in Cyberspace: An Empirical Model of Self-regulation in Virtual Communities. Communities [Electronic Version]." In *Hawaii International Conference on System Sciences 38 (HICSS-38)*, 1–8. Accessed 23 July 2015. <http://ieeexplore.ieee.org/iel5/9518/30166/01385627.pdf>
- Bossler, A. M., and G. W. Burruss. 2011. "The General Theory of Crime and Computer Hacking: Low Self-control Hackers?" In *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell, 38–67. New York: Information Science Reference.
- Bradley, C., and G. Stringhini. 2019. "A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets." In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 453–463. Stockholm: IEEE, June.
- Brenner, S. 2007. "Cybercrime: Re-thinking Crime Control Strategies." In *Online Crime*, edited by Y. Jewkes, 12–28. UK: Willan Publishing.
- Brignat, T. 2002. "The New Panopticon: The Internet Viewed as a Structure of Social control." *Theory and Science* 3 (1): 1–13.
- Chiesa, R., S. Ducci, and S. Ciappi. 2008. "Appendix C: The Nine Hacker Categories." In *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, edited by R. Chiesa, S. Ducci, and S. Ciappi, 239–241. Boca Raton: CRC Press.
- Cohen, S., and A. Scull. 1983. "Introduction: Social Control in History and Sociology." In *Social Control and the State: Historical and Comparative Essays*, edited by S. Cohen and A. Scull, 1–16. Oxford: Martin Robertson.
- Cohen, S. 1985. *Visions of Social Control: Crime, Punishment and Classification*. Cambridge: Polity Press.
- Denning, D. E. 2011. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell, 170–186. New York: Information Science Reference.
- Donner, C. M., C. D. Marcum, W. G. Jennings, G. E. Higgins, and J. Banfield. 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. doi:10.1016/j.chb.2014.01.040.

- Fotinger, C., and W. Ziegler. 2004. *Understanding A Hacker's Mind: A Psychological Insight into the Hijacking of Identities*. <http://www.donau-uni.ac.at/de/departement/gpa/informatik/DanubeUniversityHackersStudy.pdf>
- Furnell, S. 2002. *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley.
- Gordon, S., and Q. Ma. 2003. "Convergence of Virus Writers and Hackers: Fact or Fantasy?" http://download.adamas.ai/dlbase/ebooks/VX_related/Convergence%20of%20Virus%20Writers%20and%20Hackers%20Fact%20or%20Fantasy.pdf
- Grabosky, P. N. 2017. "The Evolution of Cybercrime, 2006–2016." In *Cybercrime through an Interdisciplinary Lens*, edited by T. J. Holt, 15–36. New York: Routledge.
- Higgins, G. E., C. D. Marcum, T. L. Freiburger, and M. L. Ricketts. 2012. "Examining the Role of Peer Influence and Self-Control on Downloading Behavior." *Deviant Behavior* 33 (5): 412–423. doi:10.1080/01639625.2011.584275.
- Hinduja, S. 2003. "Trends and Patterns among Online Software Pirates." *Ethics and Information Technology* 5 (1): 49–61. doi:10.1023/A:1024910523384.
- Hirschi, T. 1969. *Causes of Delinquency*. Berkeley, CA: University of California press.
- Holt, T. J. 2007. "Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures." *Deviant Behavior* 28 (2): 171–198. doi:10.1080/01639620601131065.
- Holt, T. J. 2009. "The Attack Dynamics of Political and Religiously Motivated Hackers." Paper presented at the Cyber Infrastructure Protection Conference, New York.
- Holt, T. J., A. M. Bossler, and D. C. May. 2012. "Low Self-control, Deviant Peer Associations, and Juvenile Cyberdeviance." *American Journal of Criminal Justice* 37: 378–395. doi:10.1007/s12103-011-9117-3.
- Holt, T. J., G. W. Burruss, and A. M. Bossler. 2010. "Social Learning and Cyber-deviance: Examining the Importance of a Full Social Learning Model in the Virtual World." *Journal of Crime and Justice* 33: 31–61. doi:10.1080/0735648X.2010.9721287.
- Holt, T. J., and M. Kilger. 2008. "Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers." In *WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 2008. WISTDCS'08*, 67–78. Amsterdam: IEEE computer society.
- Holt, T. J., and M. Kilger. 2012. "Know Your Enemy: The Social Dynamics of Hacking." *The Honeynet Project*. <https://honeynet.org/papers/socialdynamics>
- Hu, Q., Z. Xu, and A. A. Yayla. 2013. "Why College Students Commit Computer Hacks: Insights from a Cross Culture Analysis." In *Pacific Asia Conference on Information Systems (PACIS)*, Jeju Island, Korea.
- Israel Central Bureau of Statistics. 2014. Students in Universities, Academic Colleges and Colleges of Education, by Degree, Sex, Age, Population Group and District of Residence. *Education Table 8.56: Statistical Abstract of Israel*, 440 [in Hebrew].
- Jordan, T., and P. A. Taylor. 1998. "A Sociology of Hackers." *The Sociological Review* 46 (4): 757–780. doi:10.1111/1467-954X.00139.
- Louderback, E. R., and O. Antonaccio. 2017. "Exploring Cognitive Decision-making Processes, Computer-focused Cyber Deviance Involvement and Victimization: The Role of Thoughtfully Reflective Decision-making." *Journal of Research in Crime and Delinquency* 54: 639–679. doi:10.1177/0022427817693036.
- Maimon, D., T. Wilson, W. Ren, and T. Berenblum. 2015. "On the Relevance of Spatial and Temporal Dimensions in Assessing Computer Susceptibility to System Trespassing Incidents." *British Journal of Criminology* 55 (3): 615–634. doi:10.1093/bjc/azu104.
- Marcum, C. D., G. E. Higgins, M. L. Ricketts, and S. E. Wolfe. 2014. "Hacking in High School: Cybercrime Perpetration by Juveniles." *Deviant Behavior* 35: 581–591. doi:10.1080/01639625.2013.867721.
- McAfee. 2018. "Economic Impact of Cybercrime— No Slowing Down." <https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf>
- McCuddy, T., and M. Vogel. 2015a. "More than Just Friends: Online Social Networks and Offending." *Criminal Justice Review* 40 (2): 169–189. doi:10.1177/0734016814557010.
- McCuddy, T., and M. Vogel. 2015b. "Beyond Traditional Interaction: Exploring the Functional Form of the Exposure-offending Association across Online Network Size." *Journal of Criminal Justice* 43 (2): 89–98. doi:10.1016/j.jcrimjus.2015.01.002.
- McQuade, S. C. 2006. *Understanding and Managing Cybercrime*. Boston: Pearson Education.
- Miller, B., and R. G. Morris. 2016. "Virtual Peer Effects in Social Learning Theory." *Crime & Delinquency* 62 (12): 1543–1569. doi:10.1177/0011128714526499.
- Morris, R. G. 2011. "Computer Hacking and the Techniques of Neutralization: An Empirical Assessment." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell, 1–17. New York: Information Science Reference.
- Morris, R. G., and A. G. Blackburn. 2009. "Cracking the Code: An Empirical Exploration of Social Learning Theory and Computer Crime." *Journal of Crime and Justice* 32: 1–34. doi:10.1080/0735648X.2009.9721260.
- National Crime Agency. 2016. *NCA Strategic Cyber Industry Group*. <https://www.uctf.gov.uk/OCTF/media/OCTF/documents/publications/Government%20Reports/Cyber-Crime-Assessment-2016-v1-2.pdf?ext=.pdf>
- National Crime Agency. 2017. *Pathways into Cyber Crime*. <http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file>

- Nycyk, M. 2010. "Computer Hackers in Virtual Community Forums: Identity Shaping and Dominating Other Hackers." Paper presented at the Online Conference on Networks and Communities: Debating Communities and Networks. Perth, WA, Australia: Department of Internet Studies, Curtin University of Technology, Online University Australia.
- Paternoster, R., and G. Pogarsky. 2009. "Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-term Consequences of Making Good Choices." *Journal of Quantitative Criminology* 25: 103–127. doi:10.1007/s10940-009-9065-y.
- Paternoster, R., G. Pogarsky, and G. Zimmerman. 2011. "Thoughtfully Reflective Decision Making and the Accumulation of Capital: Bringing Choice Back In." *Journal of Quantitative Criminology* 27: 1–26. doi:10.1007/s10940-010-9095-5.
- Pratt, T. C., F. T. Cullen, C. S. Sellers, L. Thomas Winfree, T. D. Madensen, L. E. Daigle, and N. E. Fearn. 2009. "The Empirical Status of Social Learning Theory: A Meta-analysis." *Justice Quarterly* 27: 765–802. doi:10.1080/07418820903379610.
- Rogers, M. K. 2001. "A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study." https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf
- Royston, P. 2004. "Multiple Imputation of Missing Values." *Stata Journal* 4 (3): 227–241. doi:10.1177/1536867X0400400301.
- Rubin, D. B. 1987. *Multiple Imputation for Nonresponse in Surveys*. New York: Wiley & Sons.
- Sampson, R. J., and J. H. Laub. 1993. *Crime in the Making: Pathways and Turning Points through Life*. Cambridge: Harvard University Press.
- Suler, J. 2004. "The Online Disinhibition Effect." *Cyberpsychology & Behavior* 7 (3): 321–326. doi:10.1089/1094931041291295.
- Sutherland, E. H. 1939. *Principles of Criminology*. Chicago: J.B. Lippincott Company.
- Taylor, P. A. 1999. *Hackers: Crime in the Digital Sublime*. London: Routledge.
- Thornberry, P. T. 1987. "Toward an Interactional Theory of Delinquency." *Criminology* 25 (4): 863–892. doi:10.1111/j.1745-9125.1987.tb00823.x.
- Turgeman-Goldschmidt, O. 2008. "Meanings that Hackers Assign to Their Being a Hacker." *International Journal of Cyber Criminology* 2 (2): 382–396.
- Valverde, F. 2000. "The International Internet Rating System: Global Protection for Children, Business and Industry." *New York School Journal of International and Comparative Law* 559: 559–586.
- Van Vuuren, J., L. Leenen, and P. Pieterse. 2019. "Framework for the Development and Implementation of a Cybercrime Strategy in Africa." In *Proceedings of the ICCWS 2019 14th International Conference on Cyber Warfare and Security*, edited by N. Van Der Waag-Cowling and L. Leenen, 156–167, Stellenbosch.
- Voiskounsky, A. E., and O. V. Smyslova. 2003. "Flow-Based Model of Computer Hackers' Motivation." *CyberPsychology & Behavior* 6 (2): 171–180. doi:10.1089/109493103321640365.
- Vold, G., and T. Bernard. 1986. *Theoretical Criminology*. Oxford: Oxford University Press.
- Von Hippel, P. T. 2007. "Regression With Missing Ys: An Improved Strategy For Analyzing Multiply Imputed Data." *Sociological Methodology* 37 (1): 83–117. doi:10.1111/j.1467-9531.2007.00180.x.
- Wall, S. D. 2007/2010. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." *Police Practice and Research: an International Journal* 8 (2): 183–205. doi:10.1080/15614260701377729.
- Weisburd, D. 1989. *Jewish Settler Violence: Deviance as Social Reaction*. Philadelphia: Penn State University Press.
- Weulen Kranenbarg, M. 2018. "Cyber-offenders versus Traditional Offenders: An Empirical Comparison." PhD diss., Vrije Universiteit Amsterdam. <http://dare.ubvu.vu.nl/handle/1871/55530>
- Weulen Kranenbarg, M., S. Ruiter, and J. L. Van Gelder. 2019. "Do Cyber-birds Flock Together? Comparing Deviance among Social Network Members of Cyber-dependent and Traditional Offenders." *European Journal of Criminology*: 1–21.
- Woo, H.-J. 2003. *The Hacker Mentality: Exploring the Relationship between Psychological Variables and Hacking Activities*. Athens, Georgia: University of Georgia. https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf
- Woo, H.-J., Y. Kim, and J. Dominick. 2004. "Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages." *Media Psychology* 6 (1): 63–82. doi:10.1207/s1532785xmep0601_3.
- Xu, Z., Q. Hu, and C. Zhang. 2013. "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56 (4): 64–74. doi:10.1145/2436256.