Deviant Behavior

ISSN: 0163-9625 (Print) 1521-0456 (Online) Journal homepage: http://www.tandfonline.com/loi/udbh20

Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis

Eric Rutger Leukfeldt & Majid Yar

To cite this article: Eric Rutger Leukfeldt & Majid Yar (2016): Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, DOI: 10.1080/01639625.2015.1012409

To link to this article: http://dx.doi.org/10.1080/01639625.2015.1012409

DEVIANT BEHAVIOR
http://dx.doi.org/10.1080/01639625.2015.1012409

Routledge
Taylor & Francis Group

Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis

Eric Rutger Leukfeldt[a] and Majid Yar[b]

[a]Open University of the Netherlands, Heerlen, the Netherlands, NHL University of Applied Sciences, Leeuwarden, the Netherlands, Dutch Police Academy, Apeldoorn, the Netherlands; [b]University of Hull, Hull, Yorkshire, UK

ABSTRACT

The central question of this article is whether routine activity theory (RAT) can be used as an analytical framework to study cybercrimes. Both a theoretical analysis and an analysis of empirical studies have thus far failed to provide a clear answer. The multivariate analysis presented in this article tries to avoid some of the limitations of other RAT-based studies. Based on a large sample (N = 9,161), the effects of value, visibility, accessibility, and guardianship on victimization of six cybercrimes have been studied. Analysis shows some RAT elements are more applicable than others. Visibility clearly plays a role within cybercrime victimization. Accessibility and personal capable guardianship show varying results. Value and technical capable guardianship show almost no effects on cybercrime victimization.

ARTICLE HISTORY
Received 10 September 2014
Accepted 9 December 2014

Introduction

The study of cybercrimes (offenses that involve and depend on the use of new communication technologies for their commission) is now an established area of criminological research. Over the past two decades, there has emerged a substantial body of scholarship that addresses a wide range of on-line offenses, including computer “hacking,” the distribution of malicious software, software and media “piracy,” fraud, stalking, bullying, the distribution of obscene and hateful representations, and sexual victimization of both adults and children. One of the more intriguing issues facing cybercrime scholarship relates to the efficacy or otherwise of established criminological theories in understanding or explaining patterns of on-line offending and victimization. This question turns on whether, if, or to what extent theoretical concepts developed in relation to the “terrestrial” world can be legitimately applied to a supposedly novel “virtual” environment. The greater part of such discussion has focused on situational theories of crime, in particular the Routine Activities Theory (henceforth RAT) developed by Cohen and Felson (1979). The choice of RAT as a “test case” for criminological theory’s purchase on cybercrime arises, perhaps, from a number of factors. First, it is an established and widely mobilized theory that has been used to analyze various forms of criminal behavior, including burglary (Cohen and Felson 1979), homicide (Messner and Tardiff 1985), automobile theft (Rice and Csmith 2002), and domestic violence (Mannon 1997). Second, its clear analytical schema permits relatively straightforward application across a range of scenarios. Third, it offers clear cues for policy and crime-prevention, as seen in “situational crime prevention” strategies that draw on RAT. Early discussions of the efficacy of RAT with respect to cybercrimes centered on theoretical reflections concerning the similarities and differences between virtual and terrestrial environments, and between patterns of on-line and off-line behavior. However, the explanatory efficacy of a theory cannot be decisively established without its empirical application. Consequently, theoretical discussions have been more recently supplemented by studies of cybercrime that seek to

CONTACT Eric Rutger Leukfeldt ✉ e.r.leukfeldt@nhl.nl Open University of the Netherlands, P.O. Box 2960, 6401 DL Heerlen, The Netherlands.

apply RAT to a variety of on-line offenses, and in doing so assess its ability to explain the patterns evident in crime and victimization data. While such studies offer important insights into RAT's purchase on cybercrimes, they are nevertheless subject to a number of limitations; these include the reliance on a limited sampling set (such as college students—Marcum 2008), limited sample size (Choi 2008), and the focus on a single form of crime (such as malware infection—Bossler and Holt 2009). In this article, we seek to further assess the usefulness of RAT with respect to cybercrimes through multivariate analysis of a large data set (N = 9,161) that spans a range of cybercrimes. We examine three forms of cyber-victimization—hacking and malware infection (computer-focused crimes), identity fraud and consumer fraud (financial crimes), and stalking and threatening communications (interpersonal crimes) so as to enable comparison of RAT's relative applicability to different types of cybercrime.

The article is structured into four substantive sections. In the first section, we review the theoretical discussion of RAT and its suitability for analysing and explaining cybercrimes. In the second, we review the findings of studies that empirically apply RAT to various cybercrimes, and note some of the methodological and analytical issues they entail. In the third section, we offer an analysis of the three aforementioned types of cybercrime based on our own data set. In the fourth and final section we discuss the applicability of RAT to cybercrimes in light of our findings.

RAT and cyberspace: Theoretical discussions

In 2001, the journal *Social and Legal Studies* published a paper by Wanda Capeller, entitled "Not Such a Neat Net: Some Comments on Virtual Criminality" (Capeller 2001). In this paper, she argues that cyberspace comprises a new, de-territorialized, dematerialized, and disembodied environment that is in crucial ways discontinuous with the terrestrial world. Consequently, she suggests, the emergence of this virtual reality "requires the scientific community to revise its philosophical, historical and sociological assumptions," including those associated with the analysis of crime (2001:229). In a response to Capeller's contribution, and published alongside it, Peter Grabosy takes issue with the "overgeneralization and hyperbole, which characterize a great deal of discourse on the digital age" (Grabosky 2001:243). In contrast to Capeller, he suggests that "'virtual criminality' is basically the same as the terrestrial crime with which we are familiar." He supports his argument by turning to RAT, seeking to establish the congruence between virtual and terrestrial crime by demonstrating the theory's ability to make sense of crimes occurring in the virtual environment:

> One of the basic tenets of criminology holds that crime can be explained by three factors: motivation, opportunity, and the absence of a capable guardian. This explanation can apply to an individual incident as well as to long-term trends. Derived initially to explain conventional "street" crime, it is equally applicable to crime in cyberspace. (Grabosky 2001:248)

In this exchange, we see the delineation of a dispute about "conventional" criminology's ability to grasp cybercrime by making recourse to its established theoretical, conceptual, and analytical resources. For "transformationists" like Capeller, cybercrime is a novel phenomenon by virtue of the new space within which it is configured. For "continuists" like Grabosky, it is simply a case (to borrow his phrase) of "new wine in old bottles." In a similar vein, McGuire (2007:5) critiques what he calls the "pseudo-distinction" between virtual and real space, a distinction he feels supports a dangerously distorted view of the nature and extent of cyberthreats. In this debate, RAT (alongside perspectives derived from it, such as situational crime prevention) is often mobilized to demonstrate that cybercrime can be understood and explained by recourse to criminology's received resources (see, e.g., Newman and Clarke 2003; Pease 2001; Choo 2011).

A systematic theoretical reflection on RAT's capacity to explain patterns of cybercrime is offered by Yar (2005). He proceeds by, first, considering each of the core elements of RAT's schema of the criminogenic situation (motivated offenders, suitable targets, and absence of capable guardians) testing them in terms of their applicability to the on-line environment. With respect to motivated offenders, these would appear to be in no short supply in the on-line environment—variously fraudsters, hackers, pirates, stalkers, and so on. Similarly, there are numerous targets suitable for predation—proprietary data, personal information, on-line payment and purchasing services, as well as computer systems themselves that may be compromised and disrupted by unauthorized intrusion and interference. Likewise, capable guardians may take a variety of forms, including network administrators, forum moderators, users, and peers (what Williams 2010, dubs "netizens"), as well as a range of automated protections such as firewalls, virtual private networks, anti-virus and anti-intrusion software, and ID authentication and access management systems. Thus far, we may conclude that the virtual and terrestrial organization of the criminal event are homologous, and can hence be adequately analysed using RAT or similar situational theories. However, Yar suggests, looking a little deeper we find some significant differences between terrestrial and virtual crime scenarios. For example, the conceptualization of a suitable target in RAT is itself a composite made up of a number of elements, captured in the acronym VIVA (value, inertia, visibility, and accessibility). The properties of potential targets across these dimensions, and in combination, determine their suitability for predation. Considering the property of inertia ("physical properties of objects or persons that might offer varying degrees of resistance to effective predation"; Yar 2005:420), this would appear difficult to transpose in a straightforward way to the virtual environment, given that cybertargets do not possess physical properties such as weight, but are rather "weightless" aggregations of data. However, Yar does concede that the size of a digital object (the amount of data comprising a file for example) may offer resistance to predation in terms of the speed at which it can be downloaded.

In addition to considering the transposability of RAT's various elements to the virtual context, Yar further reflects on what he calls the "ecology and topology of cyberspace" (2005: 414). He notes that RAT is an ecological approach to crime causation, and as such is dependent on the ability to localize offenders and targets in space and time—the criminogenic event occurs when the motivated offender and target come together in space and time, in the absence of a capable guardian. The ontology of the terrestrial world is one that affords relations of proximity and distance between offenders and their prospective targets, and we can assess the likelihood of a criminal event according to whether convergence between them is possible or likely. The virtual environment appears to be configured very differently from the terrestrial, insofar as it is "anti-spatial" (Mitchell 1995:8)—there is "zero distance" between any two points in the virtual world, and this collapse of spatial distance renders it problematic to speak of convergence or divergence between offenders and targets. Irrespective of any physical distance between persons or objects (such as computers), in cyberspace everything appears to be immediately co-present. Consequently, without the ability to identify relations of proximity or distance between offenders and targets, the grasp of RAT on virtual offending appears problematic.

Theoretically driven reflections, such as those noted above, offer a valuable starting point for considering the applicability of RAT (and other "conventional" theories of crime) to cyberspace. However, such explorations cannot in and of themselves definitively confirm or refute the theory's explanatory efficacy in relation to cybercrime—this further requires that the theory be empirically tested. In the next section we consider a number of such applications of RAT, and consider the limitations apparent in those studies as well as their indeterminate conclusions.

RAT and cybercrime: A review of empirical studies

Our literature review identified eleven studies that have used (parts of) RAT to explain victimization in cybercrimes (see Table 1 for an overview).[1] All eleven are self-report studies, six among college students (n between 204–578), two on-line panels (n = 4,353 and n = 6,201), two telephone surveys (n = 104 and 992), and one among Dutch citizens (n = 8,379).

[1] Two other studies used RAT to explain cyberbullying. These studies are not part of our review (Hinduja and Patchin 2008; Navarro and Jasinski 2012).

Table 1. Empirical studies applying RAT to cybercrime.

Study	Population	Cybercrimes	RAT*	+/– **
Choi, 2008	*N* = 204, college students	Computer viruses	Va: No	+
			In: No	+
			Vi: Yes (3 items)	
			Ac: No	
			CG: Yes (2 items)	
Bossler and Holt, 2009	*N* = 570, college students	Malware infection	Va: No	–
			In: No	–
			Vi: Yes (11 items)	
			Ac: No	
			CG: Yes (13 items)	
Hutchings and Hayes, 2009	*N* = 104, residents of Brisbane Metropolitan area	Phishing	Va: No	–
			In: No	–
			Vi: Yes (3 items)	
			Ac: No	
			CG: Yes (6 items)	
Holt and Bossler, 2009	*N* = 578, college students	Online harassment	Va: No	–
			In: No	-
			Vi: Yes (9 items)	
			Ac: No	
			CG: Yes (8 items)	
Marcum et al., 2010	*N* = 744, college students	Sexually explicit material	Va: No	+
		Non-sexual harassment	In: No	+
		Sexual solicitation	Vi: Yes (6 items)	–
			Ac: Yes (4 items)	
			CG: Yes (5 items)	
Pratt et al., 2010	*N* = 992, adults in Florida	Consumer fraud	Va: No	+
			In: No	
			Vi: Yes (2 items)	
			Ac: No	
			CG: No	
Ngo and Paternoster, 2011	*N* = 295, college students	Computer virus	Va: No	–
		Harassment (non) stranger	In: No	–
		Unwanted pornography	Vi: Yes (4 items)	–
		Sexual solicitation	Ac: Yes (3 items)	
		Phishing	CG: Yes (3 items)	
		Defamation		
Reyns et al., 2011	*N* = 974, college students	Cyberstalking	Va: No	–
			In: No	–
			Vi: Yes (5 items)	–
			Ac: Yes (3 items)	
			CG: Yes (3 items)	
Van Wilsem, 2011a	*N* = 4,353, on-line panel, repr. for Dutch households	Threat	Va: No	+
			In: No	
			Vi: Yes (7 items)	
			Ac: No	
			CG: No	
Van Wilsem, 2011b	*N* = 6,201, on-l ine panel, repr. for Dutch households	Consumer fraud	Va: No	+
			In: No	
			Vi: Yes (6 items)	
			Ac: No	
			CG: No	
Leukfeldt, 2014	Repr. for Dutch population (15+) (*N* = 8,379).	Phishing	In: No	–
			Vi: Yes (12 items)	–
			Ac: Yes (6 items)	–
			CG: Yes (3 items)	–

*Parts of RAT that have been measured. V = Value, In = Inertia, Vi = Visibility, Ac = Accessibility, CG = Capable guardian. The number of items correspond with the variables shown in the final analysis. If, for example, authors present a construct of three variables, this is seen as one variable.

**+ means this part of RAT (largely) explains victimization, – means this part of RAT (largely) does not explain victimization.

The studies show different outcomes regarding the usability of RAT for cybercrimes. This might be because the studies focus on different cybercrimes and use different aspects of RAT (see Table 1). Most studies focus on one cybercrime. Only Ngo and Paternoster (2011) and Marcum, Higgins, and Ricketts (2010) include more cybercrimes in their analysis, respectively seven and three. A total of nine crimes are analyzed across the ten studies: malware (3), consumer fraud (2), phishing (3), harassment (2), threat, defamation, stalking, sexual solicitation and receiving unwanted pornography. Furthermore, the element of visibility is measured in all studies (based on RAT), guardianship in most and some studies include accessibility (also measured according to RAT). Five are (mostly) positive about the applicability of the theory and six others are (mostly) negative. Hereafter, these studies will be briefly described. Table 1 provides an overview of the studies and furnishes information about the population, types of cybercrimes measured and independent variables.

First, we will consider the studies that show positive results. Choi (2008) conducted a self-report survey among college students (N = 204) into victimization by computer viruses. Choi looked at both on-line activities—such as using e-mail and downloading—and technical guardianship (such as use of anti-virus software). According to the study, college students with a technical capable guardian have a decreased risk of virus victimization. Furthermore, risky on-line behaviors and risky on-line leisure activities increases the odds of virus victimization.

Marcum et al. (2010) studied victimization by three types of offenses among 744 freshmen students: unwanted sexually explicit material, unwanted non-sexual harassment and unwanted sexual solicitation. Parts of RAT included are visibility (on-line activities such as instant messaging [IM] and social network sites), accessibility (twelve types of information shared on social network sites), and guardianship (persons in the room while using a computer, use of filtering or monitoring software by parents). Marcum et al. (2010:382) conclude that “participating in behaviors that increased exposure to motivated offenders and target suitability in turn increased the likelihood of the three types of victimization measured.” Protective measures such as a capable guardian, however, do not decrease the likelihood of victimization.

Pratt, Holtfreter, and Reisig (2010) conducted a telephone survey among adults in Florida (N = 992) in 2004 about targeting by 13 types of consumer fraud (for example, “an investment deal that turned out to be phony” and “agreed to buy a product or a service for a certain price but was later charged a lot more”). Respondents were asked how the scammer contacted them. Three “options” were “Internet-related”: through an Internet auction site, from a website, and by e-mail. Pratt et al. only looked at hours spent on-line and website purchases. Both activities increased the odds for Internet fraud targeting.

Van Wilsem (2011a, 2011b) used data from the LISS panel (Longitudinal Internet Studies for the Social Sciences), which is representative for Dutch households, to investigate on-line threats and consumer fraud victimization. In both studies Van Wilsem looked at the effects of on-line activities such as e-mailing, surfing, shopping, and chatting. Findings of the 2011a study show that non-domestic and Internet routine activities are related to both on-line and off-line threat victimization. On-line shopping and visiting forums and social network sites increase the odds for on-line threat victimization. The 2011b study into consumer fraud shows that on-line shopping and forum participation increase the odds of fraud victimization.

Six other studies show (mostly) negative results regarding the applicability of the RAT. Bossler and Holt (2009) investigate victimization by malware among college students (N = 570). The authors included both on-line activities such as shopping, chatting, and banking and guardianship (computer skills, anti-virus, and deviant peers). They conclude that most routine activities on the computer, as well as personal and physical guardianship, are not correlated with data loss from malware victimization.

Hutchings and Hayes (2009) interviewed 104 participants, 40 of whom reported receiving a phishing mail, and 1 reported being a victim. Due to a lack of victims, the study shows no statistically significant outcome relating to phishing victimization. The authors present a case study of the victim and present some analysis of phishing attempts.

Holt and Bossler (2009) used a self-report survey ($N = 578$) among college students to investigate on-line harassment. They looked at the effects of routine computer use (time spent on-line, shopping, and e-mailing), social guardianship (peer involvement in computer crime) and physical guardianship (use of protective software). The main conclusions are that "[m]ost measures of routine activity theory do not affect the odds of being harassed on-line" (Holt and Bossler 2009:13). Only "time spent in chat rooms" and "involvement in computer deviance" increases the risk. According to the authors, general exposure to others on-line does not increase victimization, but spending time on-line with others in a specific context does.

Ngo and Paternoster (2011) looked into seven forms of cybercrime victimization (computer viruses, harassment by a stranger, harassment by a non-stranger, unwanted pornography, sexual solicitation, phishing, and defamation) among college students ($N = 295$). Three parts of RAT were included: visibility (on-line activities such as IM and chatting), accessibility (chatting with strangers, providing information), and guardianship (level of computer skills and use of security software). "The results indicate that neither individual nor situational characteristics consistently impacted the likelihood of being victimized in cyberspace. … although five of the coefficients in the routine activity models were significant, all but one of these significant effects were in the opposite direction to that expected from the theory" (Ngo and Paternoster 2011:773). Only instant messaging increases the odds for on-line harassment by a non-stranger.

Reyns, Henson, and Fisher (2011) applied RAT to cyberstalking victimization (college students, $N = 974$). These authors also looked at the effects of on-line visibility, accessibility, and guardianship. The authors note that "[t]he online exposure variables did not produce consistent effects across the types of pursuit behaviors" (Reyns et al. 2011:1160). Among the on-line proximity variables, only "adding strangers" appears to be significantly related to victimization. Furthermore, having a profile tracker is not a protective variable, but increases the odds of victimization (perhaps this is because victims install one *after* they have been harassed).

Leukfeldt (2014) looked at phishing victimization of Dutch citizens ($N = 8{,}379$). Different elements of RAT were measured: personal and financial characteristics, on-line activities and on-line accessibility. The author concludes that these elements do not appear to increase risk of victimization.

Conclusions

Based on the studies shown in Table 1, it is difficult to assess the value of RAT in explaining cybercrime. First, because, the studies focus on different types of crime: ranging from computer viruses to stalking and fraud. Needless to say, these crimes are different in nature and the usability of RAT will therefore be variable also. However, studies focusing on the same type of crime (e.g., malware or fraud) also show different outcomes. Some show (mostly) positive effects, while others show (mostly) no effects.

Secondly, as Table 1 shows, the studies have a number of limitations which makes it difficult to generalize results. Most studies are based on a student population, focus on only one cybercrime, use a limited part of RAT, or use a very limited number of variables. It therefore remains unclear whether RAT can be used to explain (certain types of) cybercrimes.

Current study: Added value and expectations

Added value

The purpose of this article is to determine the usefulness of RAT in explaining different types of cybercrimes. As demonstrated in the preceding discussion, a number of studies use RAT in addressing cybercrimes. However, it becomes clear that these studies have various limitations that make it difficult to determine whether or not RAT is suitable for analyzing cybercrimes. Of course, every study has its limitations. Researchers do not have infinite budgets or time available. This also plays a role in the present analysis, but we try to avoid some of the limitations of the existing studies into RAT and cybercrime.

The analysis in this article adds to the existing empirical studies in three respects. First, we use a relatively large representative data set (N = 9,161). This is in contrast to a number of empirical studies in the third section, which use relatively small student populations. Our results are therefore representative for all citizens and not just for students.

Second, the operationalization of RAT can be more extensive than in most previous studies. Although RAT comprises several elements that interact, some studies only pay attention to (sometimes a limited number or clustered) on-line routine activities. The influence of capable guardians is usually included in the analysis, but none of the studies test, for example, all aspects of the VIVA acronym. In the present study, the following parts of RAT are covered: value, visibility, accessibility, and capable guardianship.[2]

Third, we examine the applicability of RAT to different types of cybercrime. Cybercrime is a catch-all term that covers many types of offenses. By examining a limited number of cybercrimes, results cannot be generalized. To do so would be akin to undertaking an analysis of theft and then purporting its validity with respect to all types of crime. We found only one study applying RAT to multiple types of cybercrime (Ngo and Paternoster 2011).[3] Unfortunately this survey was held among a select population (295 college students, with a response rate of 19%). In this article we look at the applicability of RAT regarding six cybercrimes. These crimes can be divided into three different offense types. This is interesting because it is possible that (parts of) RAT is suitable for certain types of cybercrime, and not for others. The following cybercrimes are included in the analysis: malware, hacking, identity theft, consumer fraud, stalking, and threats. There are two so-called high-tech crimes: malware and hacking. Furthermore, two types of fraud and two forms of interpersonal offenses are included. This creates a broad view of the applicability of RAT to a variety of cybercrimes.

Current study: Measuring the effects of VIVA and guardianship

According to RAT, the degree to which someone is a suitable target for a motivated offender largely explains victimization. In order to see if this is true for cybercrimes, the four elements that make a victim attractive to a motivated offender are measured. In addition, the impact of capable guardianship is of interest. This is, according to RAT, the most important factor for reducing victimization.

The analysis in this article is exploratory in nature. We tested whether and to what extent RAT is useful in explaining various cybercrimes. Therefore, we do not formulate hypotheses per offense. The earlier studies treated in the third section demonstrate that this is difficult. Instead, we operationalize the concepts of RAT: value, inertia, visibility, accessibility, and guardianship. Across all the variables, we then look at the impact on various offenses. In this way, the effect of different variables on all the offenses can be compared and variables that give unexpected results are not removed beforehand. Below, the digital variant of VIVA and guardianship are presented. In the “Data and Methods” section, the variables that will be used to test the different elements of RAT are described in detail.

Value

Offenders are particularly interested in goals to which they, for whatever reason, assign value. Value can be operationalized in different ways. For example, the commercial value of a smartphone or the quantity of 50 dollar notes in one’s purse. A translation into a digital version of the term “value” is

[2] See the “Data and Methods” section. Inertia could not be translated to the on-line world.

[3] Marcum et al. (2010) looked at three cybercrimes, but these were all closely related to each other.

difficult to make. We restrict ourselves to a well-measurable "value": his or hers financial characteristics. These variables are especially likely to play a role in fraud offenses, but it is also conceivable that they play a role in hacking and malware victimization.

Inertia

Cohen and Felson (1979) describe inertia simply as the physical properties of the item and the ease with which the object can be carried. While digital files have no weight, Yar (2005), points out that files and technological specifications can be seen as a form of inertia, because they determine the levels of resistance that a target may offer, thereby affecting its suitability.

Visibility

Visibility refers to the visibility of the objects an offender wishes to steal. On-line visibility of a victim may contribute to the degree to which someone is a suitable target. Because of his or her on-line activities, a person becomes visible for the motivated offender. The question is which behavior on the Internet actually makes users suitable targets for cybercrimes.

Accessibility

Accessibility in the off-line world relates to the layout of neighborhoods, the placement of goods in easily accessible locations and other features of everyday life, making it easier for perpetrators to come into contact with a target. In the on-line world, users need software such as operating systems and Web browsers to access it. Motivated offenders abuse holes in the software to attack users (e.g., to infect them with malware). Users with widely used "popular" systems with well-known weaknesses are more accessible than users who use special operating systems. The type of software, therefore, relates to the degree of target accessibility.

Capable guardian

Bystanders can play an important role as capable guardians. The social environment occupied by an individual can thereby be a protective element. The data sets that we have, however, contain no information about this. Some studies operationalize the social capable guardian in terms of whether or not an individual has deviant peers. Information about this is also absent from our datasets. However, guardianship can also come in other forms, namely technical and personal.

Users can make themselves less accessible to offenders. They can, for example, take protective measures by installing anti-virus software and keeping it up to date (the technical capable guardian). Holes in software that can be abused by criminals thereby vanish.

Finally, technical knowledge and awareness of on-line risks from potential victims may also determine their accessibility. Internet users with a high degree of technical knowledge and/or who are aware of the risks that they face on-line, are more able to anticipate attacks and therefore have a lower risk of becoming a victim. We call this personal capable guardianship.

Data and methods

This article offers secondary analysis performed on the dataset of Domenie et al. (2013), supplemented with data sets from Statistics Netherlands. First a brief description of these data sets will be provided. Thereafter, the specific variables and analysis used in this article are described.

The questionnaire of Domenie et al. (2013) was administered in April 2011 among a random sample comprising 21,800 citizens aged 15 years and older. Participants received an invitation letter in April 2011 and a reminder letter in May 2011. To increase the response rate, in the months of

May to July 2011, the people who had not cooperated were called (up to a maximum of six times). Respondents could complete the questionnaire either on-line, by phone, or on paper.

In total, 10,314 people responded (47.3%). The analysis for this article is conducted on 9,161 respondents who reported using the Internet (88.8% of respondents). Statistic Netherlands tested the representativeness of the response (see Domenie et al. 2013). The response was not representative in terms of a number of demographic characteristics. Young people (15–34 year olds), single households, people in highly urban areas, non-Western immigrants, and people from the west of the Netherlands were underrepresented.

To gain insight into the financial situation of respondents, files from the Social Statistical Database (SSB) of Statistics Netherlands were linked to the dataset of Domenie et al. (2013). The SSB is a non-public database of linkable records and surveys that are mutually matched. More than forty records are available, ranging from, for example, data from tax to unemployment agencies. A detailed explanation of the composition of the SSB files is given by Arts and Hoogteijling (2002).

Dependent variables

The dependent variables—victimization by hacking, malware infection, identity theft, consumer fraud, cyberstalking, and cyberthreats—are dichotomously coded (1 = victim, 0 = no victim). Respondents were asked about victimization in the last twelve months. To reduce telescoping effects, it was asked how often the respondent had been victimized in the last five years. This question is not included in the analysis.

Based on three questions, it was attempted to ascertain if respondents were hacked: "someone changed your website or social network site (e.g., Facebook) without your consent," "someone has broken into your computer and destroyed, altered or stolen data," and "someone has broken into your email or logged onto your email account without your permission." These questions could be answered with a yes or a no.

Malware is short for malicious software. Examples of malware include viruses, worms, trojan horses, and spyware. Malware infection is difficult to measure. It is not always clear to users whether or not their computer has been infected. For that reason, respondents were asked whether the user has noted during the past twelve months that malware was present on his or her computer. Response options were: "yes," "no," and "I do not know."

Identity fraud entails committing fraud with a created/adopted identity (De Vries et al. 2007). Such an offense may be undertaken, for example, by creating a false identity or by stealing an identity of a real person (identity theft). The latter may be performed by stealing digital personal data, for example by phishing or spyware. In the questionnaire, the following definition was given: "Identity fraud means someone is using your personal or financial information without your consent to earn money. For example, someone withdraws money from your bank account, purchases products on your behalf or requests official documents on your behalf. Usually, identity fraud is due to identity theft, but it is also possible you (unwillingly) have provided the information yourself."

Respondents could answer "yes," "no," and "I do not know." Thereafter, respondents were asked to indicate how the offender had obtained the identity. Both off-line and on-line methods could be chosen. Only the on-line methods are used in our analysis as the cyber-version of identity theft. Options were: "data entered on a (phishing) website or a hacked website" or "data provided through email." There was also an option "other." Here respondents could fill in others methods. These answers were analyzed by the researchers. Only if an on-line method was used is the respondent seen as a victim of cyber identity theft.

Consumer fraud is operationalized as follows: "Have you purchased a product or service over the internet and at least paid a portion thereof, and the product or service is never delivered, because the seller scammed you?" Response options were "yes," "no," and "I do not know."

Stalking is operationalized as "deliberate and repeated harassment of a person with the intent to make that person do something or to make him/her afraid." This definition is based on Dutch legislation. The following was also added: "stalking can occur by always carrying out the same act or by several acts, including following/tailing, spying, unwanted calls or emails or by damaging (digital) properties." Options were: "yes," "no," and "I do not know." Thereafter, respondents were asked how they were stalked. Both on-line and off-line methods were inquired about. Only respondents who selected one or more of the seven on-line methods (such as receipt of unwanted e-mails and instant messages) are seen as victims.

Finally, threat is defined as: "threat with—in most cases—physical violence or death against a person or his/her property." This definition is also based on Dutch legislation. The respondent could again answer "yes," "no," and "do not know." To find out if someone was victim of a cyberthreat, the respondent was asked to indicate which means had been used. Examples are (multimedia) messages via mobile phones and social network sites. Only respondents who selected one or more on-line means are seen as victims.

Independent variables

Different parts of RAT are measured in this study. First, the concept of value is studied. This required us to determine the financial characteristics of each respondent. The financial characteristics measured are: personal income, household income, value of financial assets and property and amount of savings. The data was obtained from Statistics Netherlands.

On-line visibility is measured by looking at various on-line activities. First the level of Internet usage is assessed. A five-point scale is used, ranging from never to (almost) daily. In addition, the following activities are measured: targeted browsing (search for news or targeted information search), untargeted surfing, e-mailing, using MSN and Skype, using on-line chat rooms, on-line gaming, activity on Internet forums, profile sites, tweeting, downloading, and on-line shopping.

To measure digital accessibility, respondents were asked which operating system and Web browser they had installed on their most commonly used computer. With regard to operating systems, respondents could choose from: Windows, Mac, Linux, or mobile systems (Android, iOS, etc.). Regarding Web browsers: Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Other.

In order to measure technical capable guardianship, respondents were asked if they had an up-to-date virus scanner. In order to measure personal capable guardianship, respondents were asked about their technical knowledge and on-line risk awareness. Technical knowledge is based on knowledge about their own operating system, Internet browser, virus scanner and Internet connection. Risk awareness (using a four-point scale, ranging between "never" and "often") comprises the variables:

- I open e-mails from unknown senders.
- I open attachments or files from unknown senders.
- I download via Torrent applications (e.g., BitTorrent or Vuze) and/or peer-to-peer systems (e.g., Gnutella, Kazaa, or Limewire).
- I watch for the "lock" if I pay on-line.
- I note the "s" after "http" when I pay over the Internet or when I use Internet banking.
- If I buy something over the Internet, I'm trying to figure out if the seller is trustworthy.
- I'm aware what kind of information I leave about myself on the Internet.
- I use strong, hard to guess passwords of at least eight characters with numbers and letters.
- I use different passwords for different accounts.
- I change my passwords for security reasons.

Results

The results of the multivariate analysis are presented for each type of cybercrime separately. First the high-tech crimes of hacking and malware are discussed. Thereafter, the fraud offenses—identity theft and consumer fraud—are covered. Finally, results regarding the interpersonal offenses of stalking and threats are described.

High-tech crimes

Table 2 shows the results of the multivariate analysis of hacking and malware victimization. First, an analysis of the background characteristics is presented. Age has a significant effect on hacking victimization; the younger a user, the higher the risk. Other background characteristics, such as gender and educational level do not have any effect. These characteristics do play a role in malware victimization. Gender, education level, and having a paid job have an effect on victimization. Women, people with a higher education level and a paid job have a higher chance of becoming a victim of malware.

None of the value variables have a significant effect on hacking victimization. Becoming a hacking victim has nothing to do with someone's personal income or financial assets. Personal income does have an effect on victimization via malware. That sounds logical at first. A lot of malware is in fact designed to steal user credentials in order to commit fraud. People with significant amounts of money in their bank account would seem to be more interesting (i.e., suitable as targets) than people with limited financial resources. It was also found that people with higher levels of education and paid employment have an increased risk of victimization. These are two indicators of the level of

Table 2. Multivariate analysis of hacking and malware.

	Hacking		Malware	
	B	S.E.	B	S.E.
Constant	−4.647**	1.332	−6.296***	.591
Background characteristics				
Gender (Man = ref)	−.126	.132	−.321***	.067
Age	−.028***	.005	.002	.002
Education level	.031	.041	.095**	.021
Work (12h per week or more)	.055	.147	.180**	.074
Value				
Personal income	−.003	.003	−.005**	.001
Household income	.003	.003	.002	.001
Financial assets	.000	.000	.000	.000
Financial possessions	.000	.000	.000	.000
Savings	−.002	.001	.000	.000
Visibility (Online activities)				
Frequency of internet use	.486	.249	.233**	.091
Targeted browsing	.178	.098	.156**	.048
Direct communication: e–mail	.027	.080	−.049	.041
Direct communication: MSN, Skype	.129*	.061	−.020	.034
Chatting in chat boxes	.031	.081	−.015	.053
Online gaming	−.041	.063	.084*	.034
Active on online forums	.229**	.084	.142	.051
Active on social network sites	.181**	.065	−.015	.034
Twitter	.003	.072	.014	.050
Downloading	−.029	.062	.078*	.033
Untargeted browsing	.044	.067	.139***	.033
Buying online	−.177	.154	.387***	.084
Accessibility				
OS: Windows	−.170	.244	.912***	.184
Browser: Internet Explorer	−.291	.158	.125	.085
Browser: Google Chrome	.028	.150	.089	.076
Browser: Firefox	−.194	.166	.173*	.082
Browser: Opera	−.301	.612	.289	.265
Browser: Safari	−.348	.278	−.362	.188
Technical guardian				
No virus scanner	.384	.218	−.111	.154
Personal guardian				
Computer knowledge	.061	.138	.167	.090
Online risk awareness	−.336**	.114	−.007	.059
Nagelkerke R^2	10.7		8.4	
N	8,077		8,378	

**p* < .05; ***p* < .01; ****p* < .001.

one's income. However, analysis shows that people who have less money are at increased risk of victimization. The reason for this is unclear.

Besides chatting in chat rooms, all variables of on-line visibility affect at least one of the two high-tech crimes. However, there are no variables that influence victimization by both offenses. Direct communication via MSN and Skype and being active in on-line forums and social networking sites leads to an increased risk of hacking victimization. The latter two activities in particular provide literally an increased on-line visibility. Other variables play a role in malware victimization. These can be divided into "being on-line" and specific on-line activities. The first category includes the variables of Internet use and targeted browsing. The activities within the second category include playing on-line games and on-line shopping.

Despite the fact that a relatively large number of variables have an effect on hacking or malware victimization, the variables do differ per offense. Hacking involves conduct in which victims literally have a greater on-line visibility, for example, by frequently visiting on-line forums and social networking sites. Motivated offenders may be able to meet potential victims here or select them by means of the information left by victims in those on-line locations (see also Van Wilsem 2011b). On-line visibility as such is not a factor in malware victimization; with this type of crime, the visibility variables related to the amount of time someone is on-line (surfing), increasing the risk of victimization. Thus, being on-line more frequently increases the chance of a malware infection. Also specific on-line activities like on-line gaming and shopping do increase the risk.

The result that on-line shopping increases the risk of malware victimization can be explained by the goal of malware: the interception of user credentials to commit fraud. People who pay on-line need to enter their credit or debit card details or have to log on to their Internet banking account. These actions are of interest to offenders who wish to acquire financial information. Another explanation could be that people who do not pay on-line do become a victim of malware infection, but never notice it because malware could not capture their credentials and consequently no fraud was committed. Indeed, this is a form a victimization that cannot be measured with a self-report study.

Variables relating to on-line accessibility do not have any effect on hacking victimization. In the case of malware, however, they do play a role. Users with a Windows operating system have an increased risk of malware victimization. As already outlined, this may be because this is a widely used operating system. It is simply more profitable for offenders to write malware for this system because there are more potential victims. It also appears that users have an increased risk of victimization with the Firefox browser. At the time of data collection for this study this was the most popular browser after Internet Explorer.[4]

As a protective factor, the personal guardian "on-line risk awareness" plays a role in hacking victimization. People with lower on-line risk awareness have a higher risk of victimization of this cybercrime. Apparently, people with a higher risk-awareness are better equipped to guard themselves against attacks from a hacker. None of the protective factors play a role in malware victimization. Why having a virus scanner does not protect against malware infection is not entirely clear. The fact that a scanner only detects known malware plays a role. A user who has a virus scanner remains receptive to infections of new or unknown malware types. Furthermore, if offenders exploit so-called zero-day exploits (a flaw in software for which no "patch" is available) a virus scanner has no effect.

Cyberfrauds

Table 3 shows that none of the background variables have a significant effect on victimization by identity theft. Men and women of all ages and education levels have an equal chance of becoming a victim of this cybercrime. In the case of consumer fraud, age and having a paid job affect victimization. People who are less educated and those without paid work have a greater risk of victimization. Perhaps this has to do with the nature of this crime: fraud through on-line sale and auction sites where the buyer paid for a product, but never got it. Most frauds appear to happen on a commonly used Dutch selling site where citizens can buy and sell new and used objects. Perhaps

[4] http://gs.statcounter.com/#browser-NL-monthly-201101-201106

Table 3. Multivariate analysis of identity theft and consumer fraud.

	Identity theft		Consumer fraud	
	B	S.E.	B	S.E.
Constant	−7.630***	2.418	−14.825***	2.488
Background characteristics				
Gender (Man = ref)	−.413	.294	.027	.159
Age	.013	.011	−.010	.006*
Education level	.106	.093	−.124	.048**
Work (12 h per week or more)	.645	.350	.165	.177
Value				
Personal income	−.005	.006	.000	.003
Household income	.003	.007	−.002	.003
Financial assets	−.001	.001	−.001	.000
Financial possessions	.000	.001	.000	.000
Savings	−.001	.002	.001	.001
Visibility (Online activities)				
Frequency of internet use	−.432	.328	.761	.382*
Targeted browsing	.632*	.247	.212	.126
Direct communication: e-mail	.141	.184	.250	.104*
Direct communication: MSN, Skype	.006	.145	−.207	.082*
Chatting in chat boxes	.198	.196	.115	.112
Online gaming	.001	.157	.028	.078
Active on online forums	−.245	.261	.126	.111
Active on social network sites	.121	.143	.049	.078
Twitter	−.100	.228	−.030	.108
Downloading	−.169	.152	−.058	.078
Untargeted browsing	.114	.139	.108	.080
Buying online	−.180	.346	3.313	.715***
Accessibility				
OS: Windows	−.259	.592	.105	.359
Browser: Internet Explorer	−.074	.357	−.192	.189
Browser: Google Chrome	.090	.327	.365	.172*
Browser: Firefox	.257	.339	.070	.191
Browser: Opera	.241	1.044	−.272	.736
Browser: Safari	−.129	.609	−.290	.384
Technical guardian				
No virus scanner	.350	.521	−.126	.331
Personal guardian				
Computer knowledge	.536	.449	.345	.231
Online risk awareness	−.144	.247	−.326	.143*
Nagelkerke R^2	5.2		10.4	
N	8,378		8,378	

*p < .05; **p < .01; ***p < .001.

people with a lower level of education and those without paid work have less money to spend and. therefore. are forced to look for bargains on the Internet.

In both fraud offenses financial characteristics of respondents do not play a role. Both those with high and low personal income and financial assets have an equal chance of becoming a victim.

Regarding variables related to on-line visibility, only “targeted browsing” increases the odds for victimization of identity theft. None of the other variables increase or decrease the risk. In the case of consumer fraud, frequency of Internet use and direct communication via e-mail, MSN, and Skype play a role. The latter activities reduce the risk of victimization, while the other variables increase the risk. Making purchases on-line is also a risk-increasing activity for this form of Internet fraud.

On-line accessibility plays a role in on-line consumer fraud. People who use the Google Chrome browser are at higher risk of becoming a victim of on-line consumer fraud. What the relationship is between victimization and browser usage is unclear. Perhaps there is a third variable that is not measured that is responsible for this effect.

Finally, Table 3 shows that a higher degree of on-line risk perception does reduce risk in the case of consumer fraud. People with better knowledge of on-line risks are more able to guard themselves against this type of fraud and are less often victims. The other variables related to guardianship have no effect on the risk of victimization of the two fraud offenses.

Interpersonal cybercrimes

Of the demographic characteristics, only age has a significant effect on victimization by on-line threats (Table 4). The younger a person is, the greater the likelihood of victimization. The other background characteristics show no effect on risk of victimization for both crimes.

None of the variables relating to "value" increase or decrease the odds of victimization by these interpersonal offenses.

For both on-line stalking and threats it holds that direct forms of communication, e-mail, MSN, and Skype increases the risk of victimization. In addition, Tweeting is a risk-increasing activity when it comes to threat victimization. Apparently, these variables generate a high level of on-line visibility or ensure that the offender and victim come together in time and space. Table 4 also indicates that untargeted browsing reduces the risk of threats. The reason for this is unclear.

Table 4. Multivariate analysis of stalking and threat.

	Stalking		Threat	
	B	S.E.	B	S.E.
Constant	−6.422**	2.113	−8.604**	3.238
Background characteristics				
Gender (Man=ref)	−.003	.009	−.041	.013
Age	−.009	.075	−.006***	.095
Education level	−.268	.270	−.680	.363
Work (12h per week or more)	−.003	.009	−.041	.013
Value				
Personal income	−.008	.007	.003	.010
Household income	−.009	.006	−.012	.008
Financial assets	.000	.001	−.001	.001
Financial possessions	.001	.001	.002	.001
Savings	.001	.002	.000	.002
Visibility (Online activities)				
Frequency of internet use	.026	.369	.135	.549
Targeted browsing	−.096	.182	.062	.228
Direct communication: e–mail	.425**	.166	.459*	.209
Direct communication: MSN, Skype	.286*	.115	.431*	.157
Chatting in chat boxes	−.160	.168	.173	.164
Online gaming	−.015	.118	.130	.140
Active on online forums	.111	.159	.291	.176
Active on social network sites	.049	.127	−.162	.163
Twitter	.228	.130	.458**	.145
Downloading	.056	.119	.068	.151
Untargeted browsing	.053	.131	−.396**	.159
Buying online	.575	.330	−.098	.358
Accessibility				
OS: Windows	.206	.556	.839	.869
Browser: Internet Explorer	.652*	.321	−.083	.381
Browser: Google Chrome	.220	.270	−.396	.371
Browser: Firefox	.397	.287	.154	.378
Browser: Opera	−17.022	4285.134	−16.131	4016.549
Browser: Safari	.359	.554	−.189	.829
Technical guardian				
No virus scanner	−.578	.640	−.468	.799
Personal guardian				
Computer knowledge	−.456	.252	.404	.389
Online risk awareness	.176	.230	.058	.289
Nagelkerke R^2	10.9		18.5	
N	8,387		8,387	

*p < .05; **p < .01; ***p < .001.

With respect to on-line accessibility, victims of stalking are more likely to use the Internet Explorer browser. As with fraud, it is unclear what the relationship is between browser use and victimization. Perhaps there is a third non-measured variable that is responsible for this effect.

Finally, none of the variables that are measured with respect to capable guardianship have an effect on victimization by these interpersonal offenses. Perhaps this relates to the fact that guardianship is measured based on specific on-line variables (use of a virus scanner, computer literacy, and on-line risk perception) and old-fashioned forms of off-line guardianship play a more important role.

Conclusion and discussion

Conclusion

The theoretical reflection presented in the second section illustrates the debate surrounding the applicability of RAT in explaining cybercrimes. There seems to be no consensus about this. For "transformationists" cybercrime is a novel phenomenon by virtue of the new space within that it is configured, while for "continuists" it is simply a case of "new wine in old bottles." The first group pleads for the development of new criminological theories, while the latter group argues existing theories, like RAT, can be used. A systematic theoretical reflection on RAT's capacity to explain patterns of cybercrime, by Yar (2005), shows that not all parts of RAT are translatable into an on-line variant. Inertia, for example, it difficult to transpose in a straightforward way to the virtual environment. The same goes for the convergence in time and space of offenders and suitable targets, as the virtual environment is "anti-spatial."

These theoretical explorations, however, cannot definitively confirm or refute the theory's explanatory efficacy in relation to cybercrime. Empirical studies are required. Therefore, empirical studies into cybercrime which use RAT as a theoretical perspective have been analyzed in the third section of this article. The analyses show it is not possible to determine the applicability of RAT for explaining cybercrimes based on these studies. This is caused by a number of factors. Most studies have major methodological restrictions, caused, for example, by small non representative samples or a poor operationalization of RAT. Furthermore, most studies focus on only one cybercrime, while the total range of cybercrimes examined is very broad (ranging from malware to sexual solicitation). Based on this, unsurprisingly, the studies show different results. Some are (mostly) positive about the applicability of RAT, while others are (mostly) negative about it. Additionally, the value of these results is difficult to assess. Indeed, the research limitations render comparison of results inherently problematic. On-line routine activities in study "x" into malware might be completely different to the on-line activities measured by study "z" into fraud. If there are similarities or differences, what causes them: the activities, the method, or the specific population?

The multivariate analysis presented in this article tries to avoid some of the limitations of other RAT-oriented studies. Based on a large sample of Dutch citizens, the effects of value, visibility, accessibility, and guardianship on victimization by six cybercrimes have been studied. Analysis clearly shows not all parts of RAT are usable in explaining cybercrimes (see Table 5). Visibility plays a role in all six cybercrimes. Accessibility and personal capable guardianship show varying results. The value of the target and technical capable guardianship show almost no effects on victimization.

First, there are RAT elements that do not have any or little effect on victimization: financial value and technical capable guardianship. Although personal income does have an effect on malware victimization, this is not in the expected direction: the less money one earns, the higher the chance of being a victim. It is not clear how this can be explained, especially because victims do have a higher educational level and more often have a job (which makes one think they should have a higher income).

Table 5. Effects of VIVA and capable guardian variables.

Cybercrime	Value	Visibility	Accessibility	Tech. cap. guardian	Pers. cap. Guardian
Hacking		+			+
Malware	+	++	++		
Identity theft		+			
Consumer Fraud		++	+		
Stalking		+	+		+
Threat		++			

+ means less than half of variables measured show significant influence on victimization.
++ means more than half of variables measured show significant influence on victimization.

Two other elements of RAT, accessibility and personal capable guardianship, show varying results concerning applicability. Regarding accessibility, both the operating system and browser used by respondents show effects on malware victimization. As pointed out earlier, this might be because malware is a typical high-tech crime and, therefore, technical elements like operating systems and Web browsers form an important opportunity structure for offenders to attack potential victims. Why the Web browser also has effects on victimization by fraud and stalking is not clear. Perhaps the effect is actually cause by a third, non-measured variable, which also affects browser choice.

Personal capable guardianship is a protective factor in the case of hacking and stalking. In both crimes, the better one can estimate on-line risks, the better he or she is protected against these two crimes.

Visibility—the extent of on-line routine activities—plays a role in all six cybercrimes. Except for chatting, all variables have a significant impact on one or more cybercrimes. In the case of malware, consumer fraud, and threats, most variables of this element have a significant impact on victimization. Different types of variables play a role within these crimes. Just being on-line, for example, plays a major factor in malware victimization. The amount of time spent on-line and the amount of time surfing the Web (both targeted and untargeted browsing) increases the odds for victimization. Additionally, specific activities like on-line gaming and buying on-line increases the risk for this cybercrime. Other types of routine on-line activities influence threat victimization. Direct forms of on-line communication and using Twitter increase the risk on victimization. Untargeted browsing works as a protective factor for this crime, although why remains unclear.

Hacking, identity theft and stalking have a limited number of significant on-line routine activity variables. For both hacking and consumer fraud, frequency of Internet use and direct communication increase risk of victimization. Furthermore, shopping on-line is a risk factor for fraud victimization and being active on fora and social network sites increases the risk of hacking victimization. Targeted browsing is the only routine on-line activity that has any effect on identity theft victimization.

Discussion

The central question of this article is whether RAT can be used as an analytical framework to study cybercrimes. Both a theoretical analysis and an analysis of empirical studies using RAT as a theoretical framework do not provide a clear answer. Although this article tries to tackle a number of problems in other RAT studies, the analysis presented here also has a number of limitations. Hopefully, however, both analyses presented in this article provide a fundament for a deeper exploration of usability of (elements) of RAT.

The significant impact of RAT elements differ greatly between the six cybercrime measured. The high-tech crime malware scores the most significant variables (12), while identity fraud has the least number (1). Is RAT more suitable to measure a high-tech crime such as malware infection than it is to identity fraud? Or is RAT suitable for both, and is the selection of suitable targets simply different?

Some elements of RAT seem to be more applicable than others. Visibility variables, for example, show significant effects for all six cybercrimes. On-line routine activities clearly play a role within cybercrime victimization. Value and guardianship seem to have a low number of significant variables. Future research should consider why this is the case and which other (including potentially off-line) variables could be of importance for these RAT elements.

What is striking is that within all three categories of cybercrimes victims often simply spent more time on-line. This is particularly reflected in the variables "frequency of Internet use" and everyday activities such as targeted browsing and direct communication. Being more extensively on-line thus provides a greater chance of becoming a victim of on-line crimes.

Overall, the usability of RAT seems to have a number of restrictions, at least in the way RAT has been operationalized in this article. The on-line translations used for the traditional RAT elements seem to be best equipped to measure malware victimization. Future research should include routine activities and protective factors in the off-line world. These may perhaps offer a better explanation for cybercrimes than their on-line variants.

An important question in case of cybercrimes where RAT elements seem to have little effect on victimization is whether these crimes have changed traditional RAT elements to the extent that they are no longer able to explain victimization. Why do financial characteristics of victims not increase the odds of victimization by identity theft and malware? These are two crime types where the offender only seeks to acquire the money of victims. Does the Internet provide offenders the opportunity structure to gain profits by simply (automatically) attacking as many individuals as possible, instead of only focusing an attack on those from whom potentially large sums may be illegally acquired? In that case, the importance of "value" and perhaps "visibility" is shifting to "on-line accessibility" in the case of financial crimes. Further research is needed to address these questions if our understanding of RAT's usefulness, as well as its limitations, are to be established in respect of cybercrimes.

Notes on contributors

ERIC RUTGER LEUKFELDT is researcher of cybercrime at the Cyber Safety Research Group of NHL University of Applied Sciences and the Dutch Police Academy. He is also a Ph.D. candidate in organized cybercrime at the Open University of the Netherlands. His current research (2012-2-16) aims to provide insight into criminal organizations specialized in financial cybercrimes such as credit card fraud and phishing. In the period 2007–2013 Rutger carried out several studies on the nature and extent of cybercrime and on the organization of law enforcement in relation to cybercrime. He has published in various (international) peer-reviewed journals on this topic.

MAJID YAR is an independent researcher and writer, and formerly a Professor of Sociology at the University of Hull, UK. His recent publications include *Cybercrime and Society*, 2nd edition (2013), *Crime, Devaince and Doping: Fallen Sports Stars, Autobiography and the Managment of Stigma* (2014), and *The Cultural Imaginary of the Internet: Virtual Utopias and Dystopias* (2014).

References

Arts, C. H. and E. M. J. Hoogteijling. 2002. "*Het Sociaal Statistisch Bestand 1998 en 1999*." [The Social Statistics Database 1998 and 1999]. Den Haag/Heerlen: CBS.

Bossler, A. M. and T. J. Holt. 2009. "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3(1):400–420.

Capeller, W. 2001. "Not Such a Neat Net: Some Comments on Virtual Criminality." *Social and Legal Studies* 10(2):229–242.

Choi, K.S. 2008. "Computer Crime Victimization and Integrated Theory: An Empirical Assessment." *International Journal of Cyber Criminology* 2(1):308–333.

Choo, K. 2011. "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers and Security* 30(8):719–731.

Cohen, L. and M. Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44:588–608.

De Vries, U. R. M. Th., H. Tigchelaar, M. van der Linden, and A. M. Hol. 2007. *Identiteitsfraude: een afbakening: Een internationale begripsvergelijking en analyse van nationale strafbepalingen*. Utrecht: Universiteit Utrecht.

Domenie, M. M. L., E. R. Leukfeldt, J. A. van Wilsem, J. Jansen, and W. P. Stol. 2013. *Victims of Offenses with a Digital Component among Dutch Citizens: Hacking, Malware, Personal and Financial Crimes Mapped*. The Hague: Eleven International Publishers.

Grabosky, P. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies* 10(2):243–249.

Hutchings, A. and H. Hayes. 2009. "Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?" *Current Issues in Criminal Justice 20*(3):433–451.

Holt, T. J. and A. M. Bossler. 2009. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization." *Deviant Behavior* 30(1):1–25.

Leukfeldt, E.R. 2014. "Phishing for Suitable Targets in the Netherlands. Routine Activity Theory and Phishing Victimization." *Cyberpsychology, Behavior and Social Networking* 17(8):551–555.

Mannon, J. 1997. "Domestic and Intimate Violence: An Application of Routine Activities Theory." *Aggression and Violent Behavior* 2(1):9–24.

Marcum, C. 2008. "Identifying Potential Factors of Adolescent Online Victimization for High School Seniors." *International Journal of Cyber Criminology* 2(2):346–367.

Marcum, C. D., G. E. Higgins, and M. L. Ricketts. 2010. "Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory." *Deviant Behavior* 31(5):381–410.

McGuire, M. 2007. *Hypercrime: A Geometry of Virtual Harms*. London: Routledge.

Messner, S. and K. Tardiff. 1985. "The Social Ecology of Urban Homicide: An Application of the 'Routine Activities' Approach." *Criminology* 23(2):241–267.

Mitchell, W. J. 1995. *City of Bits: Space, Place and the Infobahn*. Cambridge, MA: MIT Press.

Newman, G. and R. Clarke. 2003. *Superhighway Robbery: Preventing Ecommerce Crime*. Cullompton: Willan Press.

Ngo, F. T. and R. Paternoster. 2011. "Cybercrime Victimization: An Examination of Individual and Situational Level Factors." *International Journal of Cyber Criminology* 5(1):773–793.

Pease, K. 2001. "Crime Futures and Foresight: Challenging Criminal Behaviour in the Information Age." Pp. 18–28 in *Crime and the Internet*, edited by D. Wall. London: Routledge.

Pratt, T. C., K. Holtfreter, and M. D. Reisig. 2010. "Routine Online Activities and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory." *Journal of Research in Crime and Delinquency* 47(3):267–297.

Reyns, B., B. Henson, and B. S. Fisher. 2011. "Being Pursued Online. Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization." *Criminal Justice and Behavior* 38(11):1149–1169.

Rice, K. J. and W. R. Csmith. 2002. "Socioecological Models of Automotive Theft: Integrating Routine Activity and Social Disorganization Approaches." *Journal of Research in Crime and Delinquency* 39(3):304–336.

Williams, M. 2010. "The Virtual Neighbourhood Watch: Netizens in Action." Pp. 562–581 in *Handbook of Internet Crime*, edited by Y. Jewkes and M. Yar. Cullompton: Willan.

Wilsem van, J. A. 2011a. "Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization." *European Journal of Criminology* 8(2):115–127.

Wilsem van, J. A. 2011b. "'Bought It, but Never Got It.' Assessing Risk Factors for Online Consumer Fraud Victimization." *European Sociologic Review* 29(2):168–178.

Yar, M. 2005. "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2(4):407–427.