Towards the normalization of cybercrime victimization

A routine activities analysis of cybercrime in Europe

Junger, Marianne; Montoya, Lorena; Hartel, Pieter; Heydari, Maliheh

DOI
10.1109/CyberSA.2017.8073391

Publication date
2017

Document Version
Final published version

Published in
International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2017

Citation (APA)
Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. In *International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2017* (pp. 1-8). IEEE. https://doi.org/10.1109/CyberSA.2017.8073391

Towards the normalization of cybercrime victimization

A routine activities analysis of cybercrime in Europe

Marianne Junger
Dept. of Industrial Engineering and Business Information Systems
University of Twente
Enschede, The Netherlands
m.junger@utwente.nl

Lorena Montoya, Pieter Hartel
Dept. of Services, Cyber-security and Safety
University of Twente
Enschede, The Netherlands

Maliheh Heydari
Allameh Tabataba'i University
Teheran, Iran

***Abstract*—This study investigates the relationships between users' routine activities and socio-economic characteristics and three forms of cybercrime victimization of 1) online shopping fraud, 2) online banking fraud and 3) cyber-attacks (i.e. DDoS attacks). Data from the Eurobarometer, containing a sample of 17,811 online European citizens was analyzed. The results generally support the Routine Activities Theory. There were few differences by sex. Younger respondents were more at risk of online purchase fraud, but older respondents more of online banking fraud. Few economic characteristics were related to victimization. The three forms of victimization were interrelated relatively strongly. The characteristic of victims of online crime differ from those of traditional crime. We propose that digitalization leads to a 'normalization of victims' of cybercrime.**

Keywords—cybercrime, victimization, online shopping fraud, online banking fraud, cyber-attacks, Routine Activities Theory

I. INTRODUCTION

With the increase of internet use, crime has moved from the physical to the digital world and citizens worldwide have become vulnerable to digital crime [1]. It is unclear whether 'old' explanations apply to online crime and therefore, several authors argue about the need to investigate whether theories and the known risk factors of traditional crime hold in cyber space [2]. The aim of the present research was to study the risk factors of three forms of online fraud: i.e. online purchase fraud, denial of access to online services and online banking fraud. Our aim was to assess whether users' routine activities, socio-economic characteristics are related to online fraud victimization in the same way as they are associated with traditional crime. We also investigate whether one type of online victimization can be used to predict (statistically) another form of online victimization. The analysis was based on data from the Eurobarometer, a sample of 17,811 online Europeans citizens from 27 countries.

Computer-related fraud entails acts 'committed intentionally and without right, causing loss of property to another person by any a) input, alteration, deletion or suppression of computer data, b) interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person' [3].

The inability to access online services usually results from Distributed Denial-Of-Service attacks (DDoS). Often websites of governments or financial institutions are targeted [4]. For electronic extortion purposes, online gaming companies are also targets of DDoS attacks [5]. Just as a crime consists of a script involving a chain of steps, so does it involve a chain of victims. The major 'victims of DDoS attacks' are the owners of the attacked websites. However, internet users who can't access services face a problem as well, which may be serious or less serious depending on the service and the urgency of the task they want to perform. For ease of presentation we will use the word 'victim'.

Online banking fraud refers to the 'fraudulent act of surreptitiously accessing and/or transferring funds from an individual's online bank account for the purposes of financial gain. In some cases, individuals may even be duped by a criminal into making fraudulent money transfer themselves [6].

Online banking fraud can start with a phishing email that directs users to a tampered website where login information has to be filled-in or which installs malware on a computer which then steals login information [7, 8].

While there is considerable research literature on traditional crime victimization, the research on cybercrime victimization is more recent and less comprehensive [9, 10]. The following overview of previous work investigates similarities and

differences between traditional crime and cybercrime.

II. Related work

A. Routine Activities Theory

Research on victimization has focused on the opportunities and routine activities of users (RAT). RAT stresses the importance of exposure of targets and victims to potential attackers and decreased guardianship for explaining crime. RAT states that victims are given choices on whether to be victims, mainly by not placing themselves in situations in which crime can be committed against them [11]. Research on traditional crime has supported RAT e.g. the amount of time individuals spent outdoors as well as the activities performed at night and during weekends are strong correlates of their likelihood of victimization for a broad variation of crime types (for a review see [12]).

It is not yet clear whether the new online opportunities created by Internet and Information Communication Technology (ICT) influence the type of victims and attackers involved in crime. Opportunities for crime are created by the immediate environment, including the available technology. Accordingly, new technologies thus shape new opportunities, and these developments can affect the type of attackers and victims that get involved in crime [11].

Several studies reported that some online behaviors increase the risk of cybercrime victimization e.g. a) risk taking, such as the tendency to easily click on links, being related to general online victimization [13], b) time spent purchasing goods and time spent on online forums being related to consumer fraud [14], c) time spent online and on social media being related online harassment victimization [15, 16], d) making purchases online being related to consumer fraud targeting and fraud [17], e) performing online banking, online shopping and placing personal information online being related to online identity theft [18]. In each of these studies increased exposure was associated with increased chances of victimization.

Besides supportive findings, some studies found that many RAT measures aren't related to victimization [19, 20]. However, overall, a recent review concluded that traditional criminological theories, including RAT, are supported by cyberspace research [21], reinforcing the idea that cybercrime resembles traditional crime 'old wine in new bottles'[22].

Few studies have investigated systematically the relationships between socio-economic factors and cybercrime victimization [23]. In contrast, such characteristics have been studied extensively for victims of traditional crime.

The present study investigates the associations between routine activities and opportunity factors for online victimization. We also hypothesize that language is an opportunity factor; since the most used language online is English [24]; countries with many English speakers should be more at risk because users can read spam and phishing mails written in this language.

B. Socio-economic factors

For traditional crime, victims tend to be male, young (in their twenties or younger), non-white (with some exceptions, such as personal larceny), poor, and single (i.e. never married, divorced). Later research has supported these findings [25-27]. Few studies have been conducted for cybercrime and the results are inconsistent for age, sex and economic indicators.

C. Multiple victimization

In the physical world, crime victims are at higher risk of being repeat victims or of being victims of two or more different types of crimes [28], hence supporting the 'flag' (i.e. risk heterogeneity) and the 'boost' (i.e. event dependence) explanations (for a review, see [29]). There is some evidence that multiple victimization applies to cybercrime. Research suggests that there is often a crime chain: e.g. the phishing or hacking is a step to steal someone's identity in order to withdraw money from a bank account [30]. In addition, other studies suggest repeat victimization; for example, some websites being repeatedly attacked [31, 32].

This overview shows contrasting findings with respect to the impact of online routine activities and socio-economic factors on cybercrime. The contribution of our paper is the study of the associations between online fraud, i.e. shopping and banking, and DDoS attacks with user's routine activities, socio-economic characteristics and other cybercrime victimization. It analyzed a large randomized sample from European citizens.

III. METHOD

A. Sample

The Eurobarometer regularly surveys public opinion in the European Union (EU) using a representative sample in each of the member states. [33] was used in the present study (N=27,680). It covers age 15 and older residents of the (at that time) 27 Member States of the EU and Croatia (the latter joined the EU in 2013). The design consists of a multi-stage, random probability sample. The Eurobarometer interviews were conducted face-to-face in people's homes and in the national language. CAPI (Computer Assisted Personal Interview) was used in the countries where this technique was available. The Eurobarometer does not currently publish response rates. In the past, its response rates varied. For the 2002 sweep in which it surveyed 16 countries, the response rates varied from 23% (Great Britain) to 84% (France). In 8 of the countries/regions, it was lower than 50% [34].

B. Measures

Dependent variables.

Three dependent variables were used to measure online fraud. The questions were: 'Cybercrimes can include many different types of criminal activity. How often have you experienced or been a victim of the following situations?': a) online purchase fraud, b) inability to access to online services and, c) online banking fraud. These three variables were dichotomized with 0= not victimized, and 1= victimized.

Independent variables.

Opportunity factors. Information was available on the type of computer device used by respondents, i.e. desktop, laptop, tablet, smartphone, TV or other means. Multiple answers were possible. Answer categories were dichotomized: 0=absent, 1=present. The percentage of English speaking population was provided by [35]. A country variable was included to control for the correlation of values within countries.

Routine activities. First, questions were asked about the frequency of internet access 'at work', 'at home', or 'elsewhere' (categories: 1= once a day or more, 2= several times a week, 3= once a week, 4=less often). Second, respondents reported which activities they performed: banking, purchasing, selling, social networking, e-mail, reading news, playing games, watching TV, or other activities (categories: 0=absent, 1=present). Multiple answers were also possible.

Socio-economic variables. Age was categorized as: 1= 15 to 24, 2= 25 to 34, 3= 35 to 44, 4= 45 to 54, 5= 55 to 64, 6= 65 to 74, 7= 75 and older. Sex was categorized as 0=female, 1=male.

Economic characteristics were measured through several variables. Education was measured as number of years of education: 'How old were you when you stopped full-time education?' Categories were: 1= under 15 or no education, 2=16-19, 3= 20 or higher, and 4=Still studying. Current occupation was categorized as: 1=self-employed, 2=managers, 3=other white collars, 4=manual workers, 5=house persons, 6=unemployed, 7=retired, 8=students. Social class self-assessment was measured by the following question: 'Do you see yourself and your household belonging to…?, categorized as: 1= working class, 2=the middle class of society, 3=the upper class of society. Measures used to assess users' financial situation included:

- Personal job situation measured as: How would you judge your current situation?; categorized as: 1=very bad & rather bad, 2=rather good, 3=very good. Wealth was measured with 3 items:
- A wealth index measured the ownership of expensive goods e.g. internet connection at home, a car, music cd player, computer, television, DVD player, categories ranging from 3 (less than three items) to 6 (6 items).
- House/apartment ownership as 0=no and 1=yes.
- Financial difficulty was measured with the question 'During the last twelve months, how often have you had difficulties with the payment of your bills at the end of the month…?', categorized as: 1=most of the time, 2=from time to time, 3=almost never/never.

IV. ANALYSIS

As mentioned above, the sample size was N=27,680. However, analyses were done on three selections of respondents exposed to possible attacks. For online purchase fraud, the sample included only those doing online purchases (N=7,458); for DDoS attacks, only those online at least some of the time (N=15,383); for online banking fraud, only those performing online banking transactions (N=8,713).

Several variables were dichotomized as 0=no/absent, and 1=yes/present. Many variables were used as categorical variables to identify non-linear relationships, e.g. age was recoded into eight categories.

Marital status and household composition were unrelated to the independent variables and were hence dropped thereafter.

The data was analyzed using multi-level logistic regression using the country variable to control for the correlation of values within individual countries. The primary outcome measure is an Odds Ratio (OR), which is a measure of association between an exposure and an outcome. The OR represents the odds of an outcome occurring given a particular exposure, compared to the odds of the outcome occurring in the absence of that exposure. A value of 1 constitutes the baseline, OR values below 1 are said to be 'lower odds' whilst those above 1 to be 'higher odds'. P-values below 0.05 were considered to be 'statistically significant'.

The cases with 'missing' or 'don't know' values were filtered out, leaving effective samples of 15,383 for the DDoS attacks; 8,713 for online banking fraud and 7,449 for online shopping fraud respectively for the multivariate analysis.

V. RESULTS

Among respondents who shop online, 12.3% were victims of online purchase fraud. Among those who bank online, 6.4% reported online banking fraud and among those who are online, 13% could not access a website because of a DDoS attack. Below the main findings are discussed, focusing on the major statistically significant findings (see figure 1).[1]

A. Purchase fraud

Victims of online purchase fraud use their laptop to access the internet relatively often (OR=1.22). They are online to sell goods (OR=1.37), or watch TV (OR=1.23) but less often to e-mail (OR=0.66) or read the news (OR=0.76). They are relatively young, age 15 to 24. They don't differ from non-victims with respect to sex, and most economic factors, such as educational level and occupation. They have reported less often than non-victims to have financial difficulties (OR=0.79). Time spend online is hardly associated with victimization of online purchase fraud, with one exception: victim of online purchase fraud are online once a week 'elsewhere' (meaning not 'at home' or 'at work') (OR=1.70). Victims of online purchase fraud report relatively often that they encounter a website under attack and have been a victim of online banking fraud (OR= 1.52 and OR=2.66, respectively).

B. DDoS attacks

Respondents unable to access internet websites were characterized by several factors. First, they accessed the internet relatively often using a tablet (OR=1.17) or a TV (OR=1.26). They used the internet for online banking (OR=1.46), or for selling goods (OR=1.17), but not for e-mail

[1] A table with the prevalence of the dependent variables (descriptive statistics) and a table with the regression models are available from the corresponding author upon request.

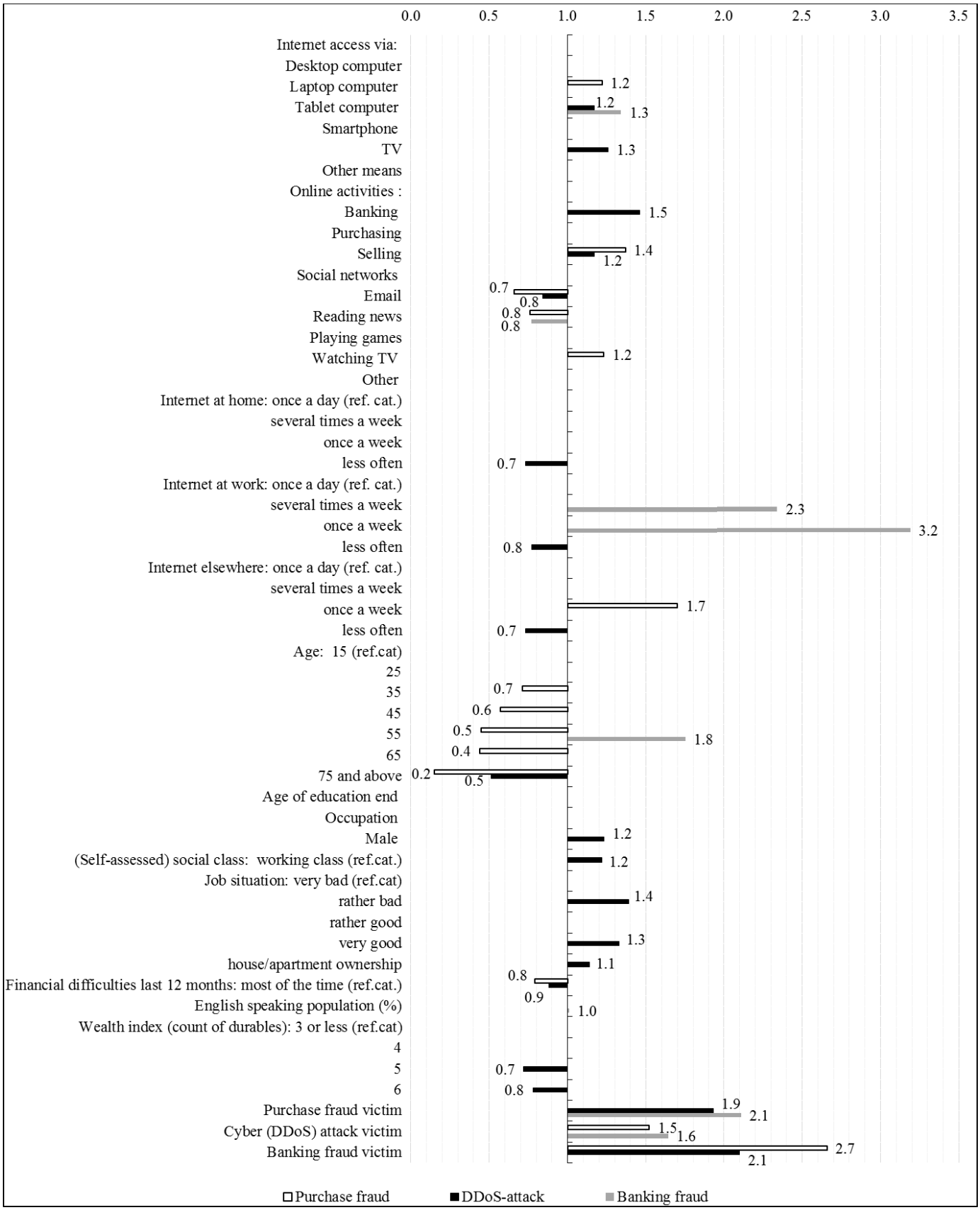

Figure 1: Odds Ratios (ORs) for banking fraud, DDoS attacks and purchase fraud.

(OR=0.84). DDoS victims aren't different from other online users in terms of frequency of access or where they access the internet from, but those who are online infrequently at home, at work or elsewhere have a low risk (OR ranging between 0.73-0.77). Similarly, the likelihood is constant for respondents from all age groups, with the exception of the very old (75 and older) who have a lower likelihood than others (OR=0.51). Males are relatively often victims (OR=1.23). DDoS victims are relatively well off, they consider themselves as being 'high social class' (OR=1.22), have a very good job situation (OR=1.33), are house/apartment owners (OR=1.14) and have no financial difficulties (OR=0.88) in contrast with respondents who were not victims of the DDoS attacks. Two findings don't fit the general trend of wealthy users being more at risk of a DDoS attack. First, those with a 'very good job situation are as likely to be victims as those with a 'rather bad' situation (OR=1.39). Second, users who own 4, 5, or 6 expensive items have relatively low odds of being victims (OR=0.88, 0.72 and 0.78 respectively). DDoS victims are more likely than non-victims to be also a victim of online purchase and banking fraud (OR= 1.93 and OR=2.10, respectively).

C. *Online banking fraud*

Victims of online banking fraud use a tablet computer (OR=1.34) and access the internet at work relatively often ('several times a week': OR=2.34, 'once a week': OR=3.19). They read news online relatively infrequently (OR=0.77). Respondents age 55-64 are victimized almost twice as often (OR=1.75). Living in a country with a high percentage of English speaking persons increases victimization risk (OR=1.01). None of the socio-economic variables was related to victimization. Victims of online banking fraud are also relatively often victims of online purchase fraud or of a DDoS attack (OR= 2.11 and OR=1.64, respectively).

Country. The (intra-class) correlation of responses among respondents from the same country is 0.30, which is considered a large effect size, meaning that relationships within each country tend to be very similar. Little variation was found across European Union countries.

VI. Discussion

The present research investigated whether online purchase fraud, DDoS attacks, and online banking fraud are related to routine activities, socio-economic characteristics and other types of victimization. The findings show that, among those who were at risk, 12.3% of the respondents were victims of online purchases fraud, 6.4% reported online banking fraud, and 13% could not access a website because of a cyberattack.

To the best of our knowledge, no previous research looked into the inability to access websites due to a DDoS attack. Accordingly, we cannot compare our findings with previous research. The main findings can be summarized as follows.

A. *Routine Activities Theory*

Our study found global support for the RAT. Users who were online using a tablet, a laptop or a TV were more at risk. It seems unlikely that these specific devices are less well protected or updated but rather that these users are less knowledgeable of ICT in general and of their specific device in particular. It is also possible that they use their device for relatively risky activities. We found no studies that investigated the type of device in relation to cybercrime and therefore no comparisons can be made with previous research.

Certain activities are related to higher victimization. Selling is related to higher online purchase fraud. This is in line with other studies reporting that online shopping is associated with consumer fraud [14, 17].

Performing online banking is related to higher risk of a DDoS attack, which a plausible since such attacks are often directed at banks [5]. Doing online banking was unrelated to online purchase fraud and online banking fraud, in contrast with previous findings [18, 36]. This is possibly because we selected respondents who do online banking, and who purchase online. It is plausible that the way people pay does not matter but what matters instead is the way goods or services are provided. We are among the few who have controlled for other forms of digital' victimization as we included the other two dependent variables in the regression model.

Watching TV online is related to online purchase fraud. A possible explanation is that victims of online purchase fraud are relatively young and that younger people use their TV more often to go online, for instance for gaming.

Frequency of going online was also related to victimization. Respondents who go online only seldom, have a low risk of a DDoS attack, possibly due to decreased exposure. Those who are relatively often online at work have a higher likelihood of online banking fraud. This is unexpected, as most research suggests that work PCs are less vulnerable than home PC's [37]. No previous study reported similar results. However, we found no study that investigated differences between being online at home or at work. This finding emphasizes the importance of what users do at work. A possible explanation, assuming that phishing is an important modus operandi of online banking fraud, could be that it is easier for attackers to collect large amounts of professional e-mail addresses, as these are often available on corporate websites, whereas private e-mail addresses are usually not on online lists. This explanation is in line with [38]'s study who reported that websites and user groups are used by attackers to harvest emails.

It was also found that those accessing the internet once a week 'elsewhere' have a high online purchase fraud risk. 'Elsewhere' may be outdoors, in transit or indoors, for instance, in an educational facility [39]. 34-year olds and younger, who are most at risk of online shopping fraud, might also access the internet 'elsewhere'.

Being active on social media is not related to higher victimization risk in our study, in line with [19] and [36], but in contrast to [13, 14, 19, 30].

Our findings show a higher percentage of English-speaking population in a country being related to higher odds of online banking fraud. This suggests that language is an opportunity factor at the country level in the digital world. The existing literature is limited although our result is consistent with a survey by Paypal [40] which shows that victimization is higher in Canada, United States and United Kingdom compared to

France, Germany and Spain. Similarly, Taylor [41] found that after controlling for other factors, cheque and credit card fraud was also more prevalent in English speaking businesses.

Overall the present findings support the view that opportunities and Routine Activities are associated to victimization, in line with studies on consumer fraud [14, 17], online identity theft [18] and a recent literature review [21]. However, research literature shows that many variables have been used to operationalize RAT and only a few of them are associated with victimization in the expected manner. Future research therefore needs to dig deeper into the opportunity structures of specific crimes (see also [19]).

B. Socio-economic factors

The present findings show that 34-year olds and younger have higher online purchase fraud risk, in line with findings on online consumer fraud [14, 17]. 55-64 year olds have higher risk of online banking fraud, in line with [36]'s findings on identity theft. All age categories are at risk of a DDoS attack except for the 75 year olds and older. These findings are probably all related to a combination of the frequency of being online and performing specific activities, such as online shopping, performing online banking, or visiting specific websites in the case of a DDoS attack.

Sex was unrelated to online purchase fraud and online banking fraud, in line with previous research [16-19, 42-44]. DDoS attacks were reported more often by males. It is not possible to compare this finding with previous research. The most plausible explanation is that males, more often than females, are online for activities such as banking or gaming which are relatively often a target of such attacks [45].

Economic factors were unrelated to online purchase fraud or online banking fraud, in line with research on consumer fraud, phishing and online banking [17, 30, 43]. A DDoS attack was usually reported by those better off (those who owned their house or apartment and had no financial difficulties). It is possible that these respondents more often perform activities online such as banking, filling in government forms or gaming that may be the target of an attack [45]. [36] also reported the better off being at higher risk although his study focused on identity theft.

C. Multiple victimization

This study strongly supports multiple online victimization, in line with previous studies [16, 18, 30]. Being a victim of one type of crime was related relatively strongly and consistently with the other two types of victimization. This phenomenon might result from a crime chain e.g. online banking fraud origins in online selling or purchase payments which provided a criminal with the victim's bank account number.

The present data supports risk heterogeneity. Online selling and financial difficulties predict more than one type of victimization, in line with research showing that similar characteristics make individuals vulnerable to more than one type of crime [16, 30, 46]. The present study doesn't allow to draw any conclusions regarding event dependence. [47] reported that some fraudulent schemes, such as deceptive sale of bogus shares, targets specific individuals repeatedly. Similarly, in the US fraudsters specifically target elderly people repeatedly [48]. A third explanation relates to 'crime chains'. For example, by clicking on the wrong link and downloading malware criminals can access a computer system and e.g. get online banking account information or make fraudulent offers to a victim. Via online purchases, users can also get into contact with fraudulent traders [49].

D. Comparison of traditional with online crime

The present study as well as previous work shows significant differences with respect to the socio-economic correlates of cybercrime in comparison with the findings on traditional crime. For traditional crimes, victims are young, male, have a low educational level and are less wealthy [25, 27, 50], which might be due to these categories being more often outdoors [51-53]. The digitalization of society, however, causes offending and victimization of cybercrime to be less related to being outdoors. Findings of previous research, reviewed above, and from the present study suggest that online victims may be more similar to average citizens than victims of traditional crime. Victims of online crime are both male and female, and for some crimes (online banking fraud, identity theft), of all ages or relatively old. [54] found that victims of online fraud were more often female (40%) and older than 35 (35.2%) compared to victims of traditional fraud (31.5% and 20%, respectively), resembling more the Dutch average. Accordingly, it is the view of the present authors that digitalization leads to a 'normalization' of victims of cybercrime, meaning that digital victims, in the statistical sense, are more similar to the average citizen than the victims of traditional crime. The study of [55] suggests that the same might apply to attackers. The reason behind this normalization might be that computers are present everywhere and every European is online a considerable amount of time [56], thus the modus operandi to commit an offence is available at home to (almost) everyone. Therefore, this study does not find support for the idea of 'old wine in new bottles' [22].

In sum, the principles of RAT and Rational choice [57] hold in cyberspace but lead to different outcomes. Future research should focus more explicitly on this issue. The interrelationships between these three forms of victimization (i.e. online shopping fraud, online banking fraud and DDoS attacks) were relatively strong. There were limited differences by sex. Age effects differed by victimization type, younger ages groups were more at risk for online purchase fraud but older age groups more for online banking fraud. Generally, economic characteristics were unrelated to victimization, but DDoS attacks were reported more often by relatively wealthy respondents.

E. Study limitations

The formulation of the questions on cybercrime was not very precise e.g. some users may not realize, when they cannot access a website, that this is the result of a DDoS attack. In addition, it is not possible to derive frequencies since respondents were asked whether they had ever been victims of a particular crime, hence there was no time frame.

The present research can only show whether relationships exists, hence it shows correlation rather than causality.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

REFERENCES

[1] D. S. Wall, *Cybercrime: The transformation of crime in the information age*. Cambridge, UK: Polity press, 2007.

[2] B. W. Reyns, B. Henson, and B. S. Fisher, "Cybercrime," in *The Encyclopedia of Theoretical Criminology*, ed: John Wiley & Sons, Ltd, 2014.

[3] Council of Europe, "Convention on cybercrime," Budapest CETS No.185, 23/11/2001 2001.

[4] T. J. Holt, A. M. Bossler, and K. C. Seigfried-Spellar, *Cybercrime and digital forensics: An introduction*. Abingdon, Oxon: Routledge, 2015.

[5] R. A. Paulson and J. E. Weber, "Cyberextortion: an overview of distributed denial of service attacks against online gaming companies," *Issues in Information Systems,* vol. 7, pp. 52-56, 2006.

[6] FFA, "Fraud, the facts 2015," ed. London, UK: Financial Fraud Action UK, 2013.

[7] J. Milletary and C. C. Center, "Technical trends in phishing attacks," *Retrieved December,* vol. 1, p. 3.3, 2005.

[8] R. G. Brody, E. Mulig, and V. Kimball, "Phishing, pharming and identity theft," *Academy of Accounting and Financial Studies Journal,* vol. 11, pp. 43-56, 2007.

[9] J. P. Lynch, "Problems and promise of victimization surveys for cross-national research," *Crime and Justice,* vol. 34, pp. 229-287, 2006.

[10] G. Cliff and C. Desilets, "White collar crime: What it is and where it's going," *Notre Dame Journal of Law, Ethics & Public Policy,* vol. 28, pp. 481-523, 2014.

[11] M. Felson and R. V. Clarke, "Opportunity makes the thief practical theory for crime prevention," Home Office, London, UK 98, 1998.

[12] N. Tilley and A. Sidebottom, "Routine activities and opportunity theory," in *The handbook of juvenile delinquency and juvenile justice*, M. D. Krohn and J. Lane, Eds., ed Oxford, UK: Wiley, 2015, pp. 331-348.

[13] K.-S. Choi. (2008, Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology 2,* 308–333. Available: http://www.cybercrimejournal.com/Choiijccjan2008.htm

[14] J. van Wilsem, "'Bought it, but never got it'. Assessing risk factors for online consumer fraud victimization," *European Sociological Review,* vol. 29, pp. 168-178, 2013.

[15] T. J. Holt and A. M. Bossler, "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization," *Deviant Behavior,* vol. 30, pp. 1-25, 2008.

[16] J. van Wilsem, "Hacking and harassment—do they have something in common? Comparing risk factors for online victimization," *Journal of Contemporary Criminal Justice,* October 31, 2013 2013.

[17] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory," *Journal of research in crime and delinquency,* vol. 47, pp. 267-296, August 1, 2010 2010.

[18] B. W. Reyns and B. Henson, "The thief with a thousand faces and the victim with none identifying determinants for online identity theft victimization with routine activity theory," *International Journal of Offender Therapy and Comparative Criminology,* p. 0306624X15572861, 2015.

[19] F. T. Ngo and R. Paternoster. (2011, Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology 5*. Available: http://www.cybercrimejournal.com/ngo2011ijcc.pdf

[20] T. J. Holt and A. M. Bossler, "Examining the Relationship Between Routine Activities and Malware Infection Indicators," *Journal of Contemporary Criminal Justice,* vol. 29, pp. 420-436, 2013.

[21] T. J. Holt and A. M. Bossler, "An assessment of the current state of cybercrime scholarship," *Deviant Behavior,* vol. 35, pp. 20-40, 2014/01/01 2014.

[22] P. N. Grabosky, "Virtual criminality: old wine in new bottles?," *Social & Legal Studies,* vol. 10, pp. 243-249, 2001.

[23] T. J. Holt and E. Lampke, "Exploring stolen data markets online: Products and market forces," *Criminal Justice Studies,* vol. 23, pp. 33-50, 2010.

[24] Internet World Stats. (2014). *Top ten languages used in the web - June 30, 2015*. Available: http://www.internetworldstats.com/stats7.htm

[25] J. Bunch, J. Clay-Warner, and M.-K. Lei, "Demographic characteristics and victimization risk: Testing the mediating effects of routine activities," *Crime & Delinquency,* December 6, 2012 2012.

[26] T. Hope, J. Bryan, A. Trickett, and D. R. Osborn, "The Phenomena of Multiple Victimization. The Relationship between Personal and Property Crime Risk," *British Journal of Criminology,* vol. 41, pp. 595-617, September 1, 2001 2001.

[27] J. L. Lauritsen, R. J. Sampson, and J. Laub, H., "The link between offending and victimization among adolescents," *Criminology,* vol. 29, pp. 264-292, 1991.

[28] L. E. Grove and G. Farrell, "Repeat Victimization," *Oxford Bibliographies Online: Criminology,* 2011.

[29] L. E. Grove, G. Farrell, D. P. Farrington, and S. D. Johnson, "Preventing repeat victimization: A systematic review. ," National Council for Crime Prevention, Stockholm, Sweden2012.

[30] T. J. Holt and M. G. Turner, "Examining risks and protective factors of on-line identity theft," *Deviant Behavior,* vol. 33, pp. 308-323, 2012.

[31] T. Moore and R. Clayton, "Evil Searching: Compromise and recompromise of internet hosts for phishing," in *Financial Cryptography and Data Security*. vol. 5628, R. Dingledine and P. Golle, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 256-272.

[32] E. Bursztein, B. Benko, D. Margolis, T. Pietraszek, A. Archer, A. Aquino*, et al.*, "Handcrafted fraud and extortion: Manual account hijacking in the wild," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 2014, pp. 347-358.

[33] European Commission, "Eurobarometer 79.4. TNS Opinion, Brussels [producer]. GESIS Data Archive, Cologne. ZA5852 Data file Version 3.0.1. DOI: 10.4232/1.11871," ed. Brussels, Belgium, 2014.

[34] The European Opinion Research Group (EORG), "Eurobarometer 58.2. The mental health status of the European population," European Opinion Research Group (EORG), Brussels2003.

[35] European Commission, "Special Eurobarometer 243. Europeans and their languages," ed. Brussels, Belgium: European Commission, Directorate-General for Communication, 2006.

[36] B. W. Reyns, "Online routines and identity theft victimization further expanding routine activity theory beyond direct-contact offenses," *Journal of research in crime and delinquency,* vol. 50, pp. 216-238, 2013.

[37] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The psychology of security for the home computer user," in *Proceedings - IEEE Symposium on Security and Privacy*, 2012, pp. 209-223.

[38] G. Schryen, "The impact that placing email addresses on the Internet has on the receipt of spam: An empirical analysis," *Computers & Security,* vol. 26, pp. 361-372, 8// 2007.

[39] S. Nylander, T. Lundquist, and A. Brännström, "At home and with computer access: why and where people use cell phones to access the internet," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2009, pp. 1639-1642.

[40] Payment News. (2008, PayPal studies differences in identity theft by country. Retreived from: http://www.paymentsnews.com/2008/10/paypal-studies.html.

Available: Retrieved 21 January, 2014, from http://www.paymentsnews.com/2008/10/paypal-studies.html
[41] N. Taylor, *Crime against businesses in two ethnically diverse communities*: Australian Institute of Criminology, 2006.
[42] J. v. Wilsem, "Gekocht, maar niet gekregen: Slachtofferschap van online oplichting nader onderzocht," *Tijdschrift voor Veiligheid,* vol. 9, pp. 16-29, 2010.
[43] E. R. Leukfeldt, "Phishing for suitable targets in The Netherlands: routine activity theory and phishing victimization," *Cyberpsychology, Behavior, and Social Networking,* vol. 17, pp. 551-555, 2014.
[44] J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," in *2012 International Conference on Innovations in Information Technology, IIT 2012*, 2012, pp. 249-254.
[45] M. D. Griffiths, M. N. Davies, and D. Chappell, "Demographic factors and playing variables in online computer gaming," *CyberPsychology & Behavior,* vol. 7, pp. 479-487, 2004.
[46] M. Button, C. Lewis, and J. Tapley, "Fraud typologies and the victims of fraud. Literature review," ed. London, UK: University of Portsmouth. Centre for Counter Fraud Studies, Institute of Criminal Justice Studies. National Fraud Authority, 2009.
[47] National Fraud Authority, "The National Fraud Strategy. A new approach to combating fraud 2009-2011," ed. London, UK: National Fraud Authority, 2009.
[48] M. Button, C. Lewis, and J. Tapley, "Support for the victims of fraud: an assessment of the current infrastructure in England and Wales," ed. London, UK: University of Portsmouth. Centre for Counter Fraud Studies, Institute of Criminal Justice Studies. National Fraud Authority, 2009.
[49] A. Aleem and A. Antwi-Boasiako, "Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat," *International Journal of Law, Crime and Justice,* vol. 39, pp. 140-160, 2011.
[50] M. R. Gottfredson, "Substantive contributions of victimization surveys," in *Crime and Justice. An annual review*. vol. 7, M. Tonry and N. Morris, Eds., ed Chicago, Ill.: The University of Chicago Press, 1986, pp. 251-288.
[51] E. E. Mustaine and R. Tewksbury, "Predicting risks of larceny theft victimization: a routine activity analysis using refined lifestyle measures," *Criminology,* vol. 36, pp. 829-858, 1998.
[52] J. L. Lauritsen, J. Laub, H., and R. J. Sampson, "Conventional and delinquent activities: implications for the prevention of violent victimization among adolescents," *Violence and Victims,* vol. 7, pp. 91-108, 1992.
[53] A. Tseloni, K. Wittebrood, G. Farrell, and K. Pease, "Burglary victimization in England and Wales, the United States and the Netherlands: A Cross-national comparative test of routine activities and lifestyle theories," *The British Journal of Criminology,* vol. 44, pp. 66-91, 2004.
[54] M. Junger, L. Montoya, P. Hartel, and M. Karemaker, "Modus Operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) gefaciliteerde criminaliteit. (Modus Operandi study of Information and Communication Technology (ICT) facilitated crime.," Universiteit Twente. Available at: http://eprints.eemcs.utwente.nl/23227/01/0_MOIT_DEF_Rapport_def_2013.pdf, Enschede, Nl2013.
[55] J. Jansen, M. Junger, L. Montoya, and P. Hartel, "Offenders in a digitized society," in *Cybercrime and the Police*, W. P. Stol and J. Jansen, Eds., ed The Hague, Nl.: Eleven International Publishing, 2013, pp. 45-59.
[56] H. Seybert and P. Reinecke. (2013, Internet use statistics - individuals. *Statistics in Focus. Industry, Trade and Services*. Available: http://epp.eurostat.ec.europa.eu/statistics_explained/extensions/EurostatPDFGenerator/getfile.php?file=130.89.102.94_1404221556_79.pdf
[57] D. B. Cornish and R. V. Clarke, "Rational choice perspective," in *Environmental Criminology and Crime Analysis*, R. Wortley and L. Mazerolle, Eds., ed Abingdon, UK: Willan, 2008.