Cybercrime Victimization: A Test of Routine Activities Explanations

Willis Danielson

05/18/2018
INTRODUCTION

Information and communication technologies (ICT) continue to be incorporated into more and more aspects of everyday life. Many people in developed nations live in state of “hyper-inter-connectivity” traveling with an ICT at all times (Bernat and Godlove 2012). Over the past thirty years this proliferation of ICTs has given rise to a new form of criminal behavior: cybercrime. In some cases, like that of the United Kingdom, various forms of cybercrime have become the most common form of crime, with online fraud and identity theft rates surpassing that of violent crimes (Williams 2016; Evans and Scott 2017). Although criminology has not been blind to this shift in criminal behavior, more research needs to be done into the theoretical frameworks that best fit explanations of cybercrime and cybercrime victimization.

Currently, two theories have been applied to investigations into cybercrime victimization. Some scholars have proposed that Gottfredson and Hirschi’s (1983) general theory of crime, whereby self-control is the key factor, can be useful in understanding digital criminality (Ngo and Paternoster 2011). Although Gottfredson and Hirschi’s (1983) theory was meant to explain offending, both the original authors and subsequent scholars have made the claim that it can also be used to explain victimization (Ngo and Paternoster 2011). Opposite the general theory of crime, routine activities theory (RAT) has also been presented as a possible explanation (Ngo and Paternoster 2011; Yar 2005; Ilievski 2016; Williams 2016). With the RAT framework, it is not self-control that creates the risk of cybercrime victimization, but individuals’ digital habits that place them at increased risk for becoming victims to cybercrime.

Despite a growing body of work on the subject of cybercrime victimization, neither of the frameworks presented previously has enough empirical evidence behind it to be claimed as the most appropriate theory. Using data from the Eurobarometer survey conducted in 2013, I aim to
add to the evidence supporting a RAT perspective. This is accomplished through the
collection of a set of logistic regressions that examine if cybercrime victimization and
individuals’ actions after victimization fit with the basic tenets of RAT.

**BACKGROUND AND THEORY**

**Routine Activities Theory and Cybercrime**

Cohen and Felson (1979) offer criminology the RAT perspective. Key to this theoretical
outlook are the behaviors and temporal characteristics that allow for a crime to occur, rather than
the factors that lead people to criminality which are the focus of many other theories used within
criminological research. According to RAT, three factors must converge for there to be an
extreme likelihood that a crime will be committed; (1) a motivated offender must be present, (2)
a suitable target must also be present, and finally (3) there must be a lack of capable guardianship
(Cohen and Felson 1979).

While numerous authors have used RAT to the study of cybercrime researchers have
pointed to certain difficulties. Yar (2005) highlights how the temporal and spatial convergence
important to RAT does not need to occur in the contexts of cybercrime, thus weakening the
theory’s applicability to cybercrime. To Yar the lack of this spatial-temporal dynamic makes
identifying suitable targets, in the terms that RAT originally defined them, difficult with
individuals not needing to be present for their own victimization. RAT’s proposition that the
lack of capable guardianship is also necessary for criminality is also problematic in reference to
cybercrime. Police officers can patrol beats and reduce the ability to criminals to engage in
deviance without observation, but there is no such social institution regulating online behavior in
real time.
Scholars testing the applicability of RAT to cybercrime victimization have found mixed results. Ngo and Paternoster (2011) examined the explanatory power of Gottfredson and Hirschi’s theory of self-control and RAT. Using a sample from a U.S. university, the authors found that lower levels of self-control were useful in explaining cybercrime where the individual is the victim, but that situational factors consistent with RAT were better predictors of cybercrime victimization where computer systems are the victim. Yet, in Ngo and Paternoster’s (2011) study, neither theoretical perspective was a stable predictor across all types of cybercrime victimization, and the authors concluded with a proposition that different theories may appropriate for different forms of cybercrime.

Williams (2016) offers some key insights into how the ideas of capable guardianship and the suitability of targets manifest in terms of cybercrime victimization. Williams found that passive guardianship in the form of anti-virus and secure web-browsers, and avoidance guardianship whereby individuals restrict their online activities were effective in significantly reducing identity theft victimization. These findings offer support to a RAT perspective in explaining cybercrime victimization, but Williams’ (2016) results also partially support a self-control explanation. Williams (2016) found that increased use of public computers was associated with an increased likelihood of being victimized, which could be tied to an individual’s lack of self-control and failure to log out of sensitive web portals after they are done using public computers.

Eck and Clarke (2003) help to resolve the issue of a lack of spatial convergence between offenders and victims of cybercrime by shifting the focus away from place to that of systems and networks. In other words, convergence still occurs, but this convergence happens when the networks and systems frequented by both victims and offenders overlap. Building on this work,
Reyns, Henson, and Fisher (2011) claim that the lack of temporal convergence is not an actual issue in the application of RAT to cybercrime. The interaction shared by victim and offender may be asynchronous, but it is an interaction nonetheless, and the only reason a temporal convergence is needed in traditional applications of RAT is because physical human interaction can happen in no other way.

**Cybercrime Victimization**

Despite cybercrime becoming the most common form of crime in some areas (Williams 2016; Evans 2017), like street crimes those who become victims of this type crime are not even distributed among populations. There are sociodemographic characteristics that appear to lead to an increased likelihood of cybercrime victimization.

In a cross-national analysis of cybercrime victimization in the United States, Finland, Germany, and the United Kingdom, Nasi et al (2015) found that several sociodemographic characteristics had significant effects on the likelihoods that an individual will be victimized online. Specifically, respondents that identify as males are more likely to be victimized than females; those that are below the age of 18 are more likely to feel they have been victimized online than those between the ages of 19 and 30; individuals living in large cities are more likely to have been victimized than those in suburban or rural areas; and individuals who are not employed are more likely to become victims of cybercrimes than individuals who are currently students. These authors also found that defamation of character and threats of violence were the most common forms of cybercrimes committed against males, while sexual harassment was the most common form of crime committed against females.

In a synthesis of findings present in nine different surveys, Van den Bergh and Junger (2018) were able to construct cybercrime victimization rates that could be generalized to all of
Europe. The authors found that between .6% and 3.5% of the population of Europe become victims of online purchase fraud each year. In a given year, between .4% and 2.2% of Europeans will have their bank account information compromised, and about .4% of Europeans will have their identities stolen online. Online harassment, such as cyber stalking, blackmail, slander, or threats of violence, happens to about 3% of Europeans each year.

Synthesis and Hypotheses

It is my position that, similar to the idea of “walking down dangerous streets”, an individual's internet usage will be significantly associated with likelihood of victimization, because higher usage rates puts them at a higher risk to experience system and network convergence with motivated offenders. RAT holds that behaviors and status predict victimization, while the general theory of crime focuses on self-control. In line with a RAT perspective I believe that certain attributes make an individual a more suitable target increasing the likelihood of victimization, and against a self-control explanation I believe that online security practices, as a proxy measure of self-control, will not have an effect on the likelihood of victimization. With cyberspace not being a physical space per se and its relatively recent prevalence in daily life conventional forms of guardianship may not be who individuals turn to after victimization. These positions are summarized in three hypotheses.

(1) Daily internet usage will be tied to increased likelihood of cybercrime victimization.

(2) Certain sociodemographic characteristics will make individuals more suitable targets, thus increasing these individuals’ likelihood of being victimized.

(3) Traditional forms of guardianship will not be perceived as capable of dealing with cybercrime, and will not be who individuals turn to after victimization.

DATA AND METHODS
Sample

The sample used for this study’s analyses comes from the 2013 Eurobarometer Surveys. The segment used focused on attitudes towards the current social climate, development related aid, cyber security, public transport, anti-microbial resistance, and space technology. The data was collected using multi-stage random probability sampling. Surveys were administered with both face-to-face interviews and computer assisted online techniques to individuals between the ages of 15 and 95. The full sample is representative across the Euro-zone, with data having been collected in Portugal, Malta, Greece, the Netherlands, Sweden, the United Kingdom, Latvia, Austria, Luxembourg, Ireland, Poland, Slovakia, Slovenia, France, Lithuania, Bulgaria, Croatia, Romania, Hungary, Spain, the Czech Republic, Belgium, Finland, Denmark, Italy, Germany, and Estonia. The full sample was comprised of 27,680 individuals, after placing analytic constraints on the data the final analytic sample was comprised of 17,254 individuals.

The use of this sample resolves some of the methodological problems faced by past work on cybercrime victimization. Many of the quoted studies used to inform my study’s analyses used data collected in university settings, and because of this the inferential power of their results suffers (see Ngo and Paternoster 2011; Reyns et al 2011). The use of Eurobarometer data allows for a wider scope of generalization for my results, as the sample is representative of the entire Euro-zone.
Measures

Outcome Measures

My measures of cybercrime victimization are constructed using four items. These items capture whether respondents had ever been victimized in regards to several forms of cybercrime. The first measured identity theft victimization, with the respondent being asked if someone had ever stolen their personal information and used it to impersonate them. The second measured if the respondent had ever received fraudulent emails asking for access to their computers, login credentials, or personal information. The third item measured if the respondent had ever purchased goods online only to not receive them or receive counterfeit goods. The last item measure if respondents had ever had their banking information stolen and used to purchase goods for other people. All of these measures were ordinal and used the same scale of possible responses. The responses for these questions were coded down into three categories with “0” = never, “1” = occasionally, and “2” = Often (don’t knows were coded as missing).

About 5% of included respondents reported having been victims of identity theft at some point. About 30% of respondents reported receiving fraudulent emails. About 9% of respondents had experienced fraudulent activities through e-commerce. About 5% of respondents reported having their banking information compromised and used to purchase good for others. The fact that receiving fraudulent emails is so common relative to other forms of cybercrime is not unexpected. It is likely that such emails facilitate these other forms of crime, and on those that fall prey to these false solicitations are likely to become victims of more serious cybercrime offenses. A more detailed breakdown of cybercrime victimization among my analytic sample can be seen in Figure 1.

Figure 1 about here
The second set of outcome measures used operationalize respondents’ perceptions of capable guardianship regarding cybercrime. The items used are in reference to who a respondent would contact if they were to become a victim of various forms of cybercrime. Respondents were asked to identify if they would contact the police, a website, vendor, consumer protection agency, another unoffered organization, no one, or if they didn’t know who they would contact. Respondents were allowed to mark more than one of these categories, and to create a set of unique observations only those that chose one category were included as valid cases in this measure. Results regarding these measures will be presented in a later section of this study.

*Independent Measures*

Two sets of independent measures make up the predictive variables in my analyses. The first are a set of sociodemographic characteristics that are meant to capture an individual’s suitability as a target of cybercrime. This first set are commonly included in statistical models as control variables, but in the case of my analyses they are an important part of aligning cybercrime victimization with an RAT explanation. The second set operationalizes victim-offender convergence. Victim-offender convergence is measured using ICT related behaviors. Descriptive statistics of these measures can be found in Table 1.

Table 1 about here

In terms of respondents’ sociodemographic characteristics, age, gender, student status, income, marital status, and locale of residence are modeled. Age is modeled as an interval ratio variable. Respondents’ student status is modeled as a dichotomous measure (“1” = currently a student, “0” = not currently a student). Income is operationalized using a measure of self-rated SES. Respondents were asked if their household was working class, middle class, or upper class. This measure was coded into three dichotomous measures, and working class is used the
reference category in analyses. Marital status is measured using an item that asked if respondents were single, cohabitating, or married. As with income/SES, this measure was also coded into three dichotomous variables, and respondents identifying as single are used as the reference group. A respondents locale of residence is modeled as a dichotomous measure (“1” = urban, “0” = rural).

The measures of an increased likelihood of victim-offender convergence are modeled using three items. The first captures if the respondent currently owns a desktop or laptop computer, and is included as a dichotomous measure (“1” = respondent owns a computer, “0” = respondent does not own a computer). The second captures if the respondent owns a mobile phone (“1” = owns a mobile phone, “0” = does not own a mobile phone). The last measure captures respondents’ frequency of internet use. Respondents were asked how often they used the internet with the possible responses being “1” = every day, “2” = frequently, and “3” = never. This variable was coded into a dichotomous measure with “1” = respondent uses the internet every day and “0” = respondent either does not use the internet every day or never uses the internet.

**Analytic Strategy**

To evaluate my hypotheses two analytic strategies are used. First, a set of nested order logistic regressions are constructed. The outcomes of interest in these models are the four types of cybercrime victimization outlined previously. Model one in these regressions predicts the likelihood of victimization based on respondents sociodemographic characteristics. Model 2 in these regressions adds in ICT related behaviors and ownership to see if who an individual is remains important to their likelihood of victimization despite their online behaviors. These regressions will be used to evaluate the validity of my first and second hypotheses. Next a graph
will be constructed based on who an individual thinks they will contact if they were to become victims of the four types of cybercrime mentioned previously. This will help to evaluate my third hypothesis.

RESULTS

Predicting Cybercrime Victimization

Table 2 present the results of ordered logistic regressions predicting the likelihood that an individual is in the highest category of victimization for various cybercrimes in the form of odds ratios, using sociodemographic characteristics and ICT related behaviors and ownership as predictors. Column 1 of the identity theft models shows that income, age, student status, and urban residence all have significant effects on the odds that individual has been a victim of identity theft. Specifically, a one year increase in age is associated with a decrease in the likelihood that an individual is in the highest category of identity theft victimization by a factor of .988, net of other sociodemographic characteristics. On average, the odds that a student is in the highest category of identity theft victimization are about 25% lower than they are for non-students, net of other factors. Compared to individuals identifying as working class, the odds that those identifying as upper class are in the highest category of identity theft victimization are about 96% higher, net of age, student status, gender, and marital status. Respondents living in urban contexts are significantly more likely to be in the highest category of identity theft victimization, compared to respondents living in in rural contexts. In column 2 of the identity theft models it can be seen that both owning a mobile phone or a computer has significant protective effects, while daily internet usage appears to increase the likelihood of victimization, net of sociodemographic characteristics.

Table 2 about here
In the case of receiving fraudulent emails soliciting personal information results are similar, but a few key differences. Respondents identifying as middle class were not significantly more likely to be victims of identity theft when compared to those living in working class household, but they are significantly more likely to be victims of phishing. On average, the odds that individuals in middle class households report receiving fraudulent emails often are about 52% higher than they are for individuals in working class households. This effect persists after controlling for ICT related behaviors and ownership, but is slightly attenuated after their inclusion. Individuals in upper class households are also significantly more likely to be in the highest category of phishing victimization compared to individuals in working class households. In fact, net of other sociodemographic characteristics, the odd that individuals identifying as upper class are in the highest category of phishing victimization are 116% higher than they are for those living in working class households. As with middle class individuals, this effect persist into the second model, but is attenuated after the inclusion of ICT related variables. Females are significantly less likely to report receiving phishing attempts often than males, net of ICT related factors and other sociodemographic characteristics. Also, individuals living in urban contexts are more likely to be in the highest category of phishing victimization, compared to those living in rural contexts, and net of all other factors. Marital status also has a significant effect, these results can be seen in Table 2. Unlike in the case of identity theft, ownership of a computer appears to exacerbate an individual’s risk for phishing.

In the case of being a victim of fraudulent e-commerce all predictors have significant effects, save for comparisons between cohabitating respondents and those that are single and mobile phone ownership. Age, has a protective effect with each additional year of age reducing the odds that an individual will be victimized by about 3%, net of other facts. Being a student
also has a significant protective effect, with student status being associated with odd that students have been victims being about 32% lower than the odds of non-students, controlling for other sociodemographic attributes and ICT related variables. The odds that both middle and upper class individuals have been victims of fraudulent e-commerce are significantly higher than they are for working class individuals, net of other factors. As with previous forms of cybercrime victimization, respondents living in urban contexts are significantly more likely to be in the highest category of victimization, with their odds of being victimized often being about 20% higher than they are for respondents living in rural areas. The odds that married individuals are in the highest category of victimization are about 16% higher than individuals who reported that they are single, controlling for other factors. Computer ownership significantly reduces the likelihood that an individual will be a victim of fraudulent e-commerce, while daily internet use significantly increases these odds.

In the case of credit fraud victimization results are dramatically different than those related to other forms of examined cybercrime. Only student status, socioeconomic status, locale of residence, and daily internet use have significant effects. On average, the odds that students are often victims of credit fraud are about 53% lower than they are for non-students, net of other factors. The odds that middle class individuals are in the highest category of victimization are about 16% higher than they are for those in the working class, and the odd that upper class individuals are in the highest category of victimization are about 94% higher than they are for working class individuals, after controlling for other sociodemographic attributes and ICT related variables. The odds that residents of urban spaces are often victims of credit fraud are about 21% higher than they are for residents of rural areas, controlling for sociodemographic predictors and ICT related items. On average, using the internet daily increases the odds than an individual
will be a victim of credit fraud often by about 54% compared to those that never use the internet or just frequently.

**Perceptions of Capable Guardianship**

One of the concerns expressed by other scholars in reference to the applicability of RAT to explanations of cybercrime prevalence is that of a lack of capable guardianship monitoring online activities. The data used in my analyses do not allow for a direct test of the effectiveness of current online guardianship, but they do allow for a test of individuals’ perceptions of the most capable guardians regarding cybercrime. Below is a graph displaying who individuals claim they would contact after being victimized. Results show, that far and away, traditional institutions of legal guardianship, such as the police, are still perceived as the most capable of dealing with cybercrime. The differences are so dramatic it hardly seems necessary to conduct tests to see if these differences are statistically significant. These results can be seen in Figure 2.

Figure 2 about here

**DISCUSSION AND CONCLUSION**

Past research has claimed that RAT may be a useful theoretical perspective in explaining what contributes to an individual’s likelihood of cybercrime victimization (Eck and Clarke 2003; Ngo and Paternoster 2011; Reynolds et al 2011; Williams 2016). Others have noted that the use of RAT in explanations of cybercrime victimization is problematic because of discontinuities between how cybercrimes are committed and street crimes are committed; namely, spatial-temporal convergence between victims and offenders (Yar 2005). To resolve these theoretical conflicts, Eck and Clarke (2016) reshaped the idea of victim-offender convergence into that of systems convergence. The work of Williams (2016) also helped to shift the
orientation RAT to fit with cybercrime by widening the definitions used to identify capable guardianship.

My results show support for a RAT perspective in the form that Williams (2016), Eck and Clarke (2003), and Reynolds et al. (2011) conceptualized it. The fact that people of higher socioeconomic status are consistently more likely to be victimized speaks to the idea that it is not self-control that determines victimization, but an individual’s suitability as a target. In other words, those with more to steal are more often victims. Similarly, individual’s living in more populated urban areas are more likely to be victimized than those living in sparsely populated rural areas. Although there does not need to be spatial-temporal convergence for cybercrimes to be committed, the more networks an individual comes in contact with and a higher number of other individuals coming in contact with these networks leads to a higher likelihood of systems convergence. The fact that daily internet use also supports a RAT perspective and the idea of system convergence. In all models daily internet use was significantly associated with increase odds of victimization, as an individual use the internet more often the more they leave traces of themselves increasing their digital footprint and increasing the chance that their information is encountered by a motivated offender. Oddly, owning a computer has a significant protective effect against cybercrime victimization in two of my models. It was expected that computer ownership would increase an individual’s digital footprint, and thus their likelihood of victimization. Yet, these result may actually reflect that with computer ownership comes higher levels of computer literacy which may lead to better online security habits.

Result largely confirmed my first and second hypotheses, but my third hypotheses proved to be incorrect. Traditional institutions of guardianship are still perceived as the most capable or appropriate guardians in regards to cybercrime. Far and away, police institutions were the most
commonly reported guardian respondents would turn to after cybercrime victimization. These results speak to perceptions of capable guardianship, but do not provide evidence that police institutions are in actuality effective guardians. Tangentially, the consistent result that people of higher socioeconomic status are more likely to be victimized casts further doubt on the already convoluted connection between SES and crime, especially the victim-offender overlap.

Despite encouraging results regarding the applicability of RAT to studies of cybercrime my study is not without limitation. Although nested models were presented there is little empirical value in this. Ordered logistic regression do not allow for true tests of moderation due to non-linearity. Any attenuation of effects must be treated carefully, and not viewed as definitive proof that any of the added measures moderate the effects of previously included items. Also, as mentioned previously my results regarding traditional forms of guardianship were only able to capture perceptions of capability.

Future research might use a set of true interval ratio outcomes to test if the effects of individual factors are moderated by ICT related behaviors and ownership. Also, there may be significant between country variation in cybercrime victimization, and more work should be done that is comparative in nature. Last, more work needs to be done to resolve the issue of capable guardianship online.

REFERENCES


Figure 2. Who would respondent contact after cybercrime victimization (N=10,897)

Table 1. Descriptive Statistics (N= 17,254)

<table>
<thead>
<tr>
<th>Category</th>
<th>Mean</th>
<th>Standard Error</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Ownership</td>
<td>0.954</td>
<td>0.210</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Mobile Phone Ownership</td>
<td>0.980</td>
<td>0.141</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Daily Internet Use</td>
<td>0.788</td>
<td>0.408</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Age</td>
<td>42.960</td>
<td>15.957</td>
<td>15</td>
<td>94</td>
</tr>
<tr>
<td>Student Status</td>
<td>0.098</td>
<td>0.297</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Working Class</td>
<td>0.360</td>
<td>0.480</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Middle Class</td>
<td>0.602</td>
<td>0.489</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Upper Class</td>
<td>0.038</td>
<td>0.190</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Female</td>
<td>0.525</td>
<td>0.499</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Single</td>
<td>0.331</td>
<td>0.471</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Cohabitating</td>
<td>0.140</td>
<td>0.348</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Married</td>
<td>0.529</td>
<td>0.499</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Urban</td>
<td>0.682</td>
<td>0.466</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Model</td>
<td>Subject Scores</td>
<td>Model</td>
<td>Subject Scores</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>-------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Table 2: Correlation Table (Revised) on Socio-demographic Characteristics and ICT Related Behaviors and Computer (N = 125) |