The British Journal of Criminology, 2022, **XX**, 1–23
https://doi.org/10.1093/bjc/azac021
Advance access publication 09 May 2022
Article

OXFORD

Fear of economic cybercrime across Europe: A multilevel application of Routine Activity Theory

Steven Cook, Luca Giommoni, Nicolas Trajtenberg Pareja, Michael Levi and Matthew L. Williams*

*Luca Giommoni, School of Social Sciences, Cardiff University, Cardiff, UK; giommonil@cardiff.ac.uk; Steven Cook, Department of Epidemiology, School of Public Health, University of Michigan, Ann Arbor, US; Michael Levi and Matthew L. Williams, School of Social Sciences, Cardiff University, Cardiff, UK; Nicholas Trajtenberg Pareja, School of Social Sciences, University of Manchester, Manchester, UK

Despite the increasing prevalence of cybercrime and its study by criminologists, very little research has examined the extent, nature, and impact of fear of cybercrime. In this study, we conducted a multilevel analysis of the 2018 Eurobarometer Cybersecurity Survey to test the applicability of routine activities theory on fear of economic cybercrime. We contribute to the literature by demonstrating that: (1) fear of economic cybercrime varies across EU member states; (2) country-level infrastructure development and income inequality are predictive of individual-level fear; (3) individual-level routine activities and sociodemographic variables are associated with fear; (4) country-level infrastructure development moderates the effects of individual-level guardianship. This paper concludes by emphasizing the importance of including country-level and individual-level determinants in fear of cybercrime research.

Key Words: fear of cybercrime, multilevel model, routine activity theory

INTRODUCTION

Online technology is fundamental to contemporary society, and its role increased exponentially during the Covid-19 pandemic. Crime data and criminological research show criminals are exploiting this increased dependency on digital technologies. European data show that rates of online crime have been increasing in recent years, far more so than offline crimes (Buil-Gil et al. 2021; Caneppele and Aebi 2019; Kemp et al. 2020; Levi 2017). Cyber-enabled frauds have been experienced by many EU and UK citizens, and are a frequent item in British tabloid and broadsheet newspapers. The UK Office of National Statistics (2022) estimated there were 6.98 million cases of fraud and computer misuse in England and Wales in the year ending September 2021, more than twice the number of thefts, burglaries and robberies combined. Between 2011 and 2020, e-commerce frauds on UK cards increased from £139.6 to £376.5 million, and in the first half of 2021, £753.9 million was lost to fraud, an increase of 30 per cent compared to 2020, with a similar amount being prevented by banking controls (UK Finance 2021). The landscape

of criminal victimization has shifted, and UK citizens are now substantially more likely to be victimized online than have their car stolen or home burgled.

Fear of crime is both a harm in itself and a trigger for other personal welfare-reducing activities, though it may *increase* welfare if it leads people to avoid 'reasonably likely' actual harms. Fears of cybercrimes can lead to reduced participation in economy and society, which becomes more consequential as citizens' advisory, offline banking and shopping services are reduced and made relatively more expensive, a trend accelerated by the pandemic. Alternatively, naivety about (frequently changing) real risks of online communications can lead to a range of scams. The high rate of victimization and the high emotional impacts suggest that it is reasonable to be fearful, even if 11 out of 12 people are not currently direct victims of fraud or cybercrime annually (ONS 2021, 2022). Despite the increasing prevalence of cybercrime and its study by criminologists, there is little evidence about the extent, nature and impact of fear of cybercrime. The limited evidence that does exist suggests that individuals may be more concerned about becoming victims of cybercrimes than of most types of terrestrial crimes. For example, preliminary data in England and Wales show that individuals are more worried about cybercrime victimization than they are about burglary or physical assault victimization (Brunton-Smith 2017). In Scotland, in line with previous years, in 2019/20 the crimes which the public were most likely to say they were very or fairly worried about (from those asked about) were fraud-related issues. More specifically, half (50%) of adults said they were worried about someone using their credit or bank details to obtain money, goods or services, whilst 39% were worried about their identity being stolen. By comparison, under a fifth (16%) of adults were worried about being physically assaulted or attacked in the street or other public place, whilst a tenth (10%) were concerned about being sexually assaulted. The crime type which Scottish adults thought they were most likely to experience in the next year was someone using their bank or card details to obtain money, goods or services, echoing the pattern seen in the results on worry about crime (Scottish Government 2021: 112–113).

Research has begun to identify that some of the sociodemographic risk factors associated with fear of crime are also associated with fear of cybercrime such as: gender, age, income or socio-economic status, education, and urban/rural context (Brands and van Wilsem 2021; Brunton-Smith 2017; Roberts et al. 2013; Virtanen 2017; Yu 2014). Yet, very little research has used population-based data to test the relevance of theory-driven factors. In addition, a lack of cross-national research makes it difficult to assess the generalizability of these factors across different contexts.

This paper addresses these gaps in the literature by presenting results from a EU-wide cross-national study that statistically tests the applicability of Routine Activity Theory (RAT) to fear of cybercrime (Cohen and Felson 1979). The analysis focuses specifically on fear of economic cybercrime, an umbrella term that covers criminal activity that involves a computer, networked device or a network to conduct online identity theft, online shopping fraud, phishing attacks, etc. The paper contributes to the literature by (i) developing a robust and consistent measure of fear of economic cybercrime across 28 EU states; and (ii) modelling both individual- and country-level predictors, drawn from RAT, to model fear of economic cybercrime. In the following sections, we explain the rationale of our theoretical framework, and develop and test a series of hypotheses examining the relative importance of individual- and country-level factors associated with the fear of economic cybercrime.

RAT AND CYBERCRIME

The basic premise of RAT is that crime is a function of three conditions: the presence of a motivated offender, the availability of a pool of targets that are made vulnerable by their risky routine

activities, and a lack of capable guardianship (Cohen and Felson 1979). There are reservations about the application of RAT to the cyber space, particularly given the nature of convergence of victims and offenders in such a '*spatiotemporally disorganized*' sphere (Leukfeldt and Yar 2016; Yar 2005). However, despite discontinuities between offline and online realm, some authors have argued that RAT can be adapted to explain cyber-victimization. Eck and Clarke (2003) argued that its explanatory power was dependent upon the 'shared physical space' requirement being expanded to include a 'shared network', where the perpetrator can reach a target through this network. Thus the victim-offender convergence can be achieved when cyberspace acts as proxy of physical space, and transactions are completed across time (Reyns 2011). Yar (2005) concluded that 'motivated offenders' and 'capable guardianship' concepts could be treated as largely similar between cyber and terrestrial settings.

Several studies have tested the applicability of RAT to cybercrime victimization. For example, Reyns (2011) found that elements of RAT were associated with identity theft (online and offline) victimization using the 2008/09 British Crime Survey. Likewise, Reyns and Henson (2015) found some routine activities such as online banking and purchasing affect the probability of suffering identity theft in nationally representative sample individuals from the Canadian General Social Survey. These results are broadly consistent with the findings from other studies conducted with smaller non-random student samples (Pratt et al. 2010; Wilsem 2013) . In the first multilevel cross-national study on cybercrime victimization, Williams (2016) found that the risky online routine activities of online auction selling and accessing in public places increased the likelihood of online identity theft victimization across Europe. Individual levels of guardianship (passive physical, active physical and personal avoidance) were all associated with online identity theft victimization. In addition, country-level proxies for guardianship (internet penetration and cyber security policy) moderated the effectiveness of individual-level guardianship on reducing the likelihood of cyber-victimization.

While RAT has been consistently linked to identity theft, the evidence base is less well established for other types of cybercrimes. For example, Bossler and Holt (2009) found that virus infection was not associated with guardianship measures, while Holt and Bossler (2008), Bossler et al. (2011) and van Wilsem (2011, 2013) found that physical guardianship (e.g. installing antivirus) did not have any effect cyber-harassment (see Reyns et al. (2011) for links between cyberstalking victimization, online guardianship, and online target attractiveness). Another study in the Netherlands showed that while some aspects of RAT, like visibility, are consistently associated with different types of cybercrime victimization (e.g. hacking, malware, stalking, etc.), others like technological or personal capable guardianship, have a less clear relationship (Leukfeldt and Yar 2016). One of the few studies that involved a representative panel confirms that not all RAT components are relevant, and while exposure predicted hacking and malware victimization, that was not the case for guardianship and target attractiveness (Guerra and Ingram 2020).

FEAR OF CYBERCRIME

To date, there are only a handful of studies exploring fear of cybercrime, and they present many of the problems associated with early research into fear of crime, such as inadequate sampling and the use of questions that do not measure appropriately fear of cybercrime. For instance, Higgins et al. (2008) examined the connection between perceived risk of online victimization and fear of cybercrime using a non-random sample of Facebook users, while Yu (2014) used a non-random sample of U.S. students. The use of convenience and non-random samples, however, precludes generalizability to the wider population and limits the ability to examine how fear of cybercrime may cluster together based on different social contexts.

Brunton-Smith (2017) and Virtanen (2017) identified several correlates of fear of cybercrime, yet both studies used generalized (how worried are you about being the victim of online crime?) instead of crime-specific measures (e.g., how worried are you about being the victim of online identity theft?). People can be worried about some types of cybercrime but not about others, and previous research shows that crime-specific measures provide substantively different results (Fisher and Sloan 2003; Lane and Fox 2013). For instance, one individual may be worried about becoming victim of cyber-harassment without being worried about a hacking attack, while the opposite may be true for another individual. It is therefore important to use crime-specific questions to ensure a consistent measurement of the same underlying construct across individuals. Moreover, empirical analysis of these individual demographic and socio-economic characteristics have not been integrated into a clear theoretical and analytical framework or analysed with more detail.

Mixed findings have emerged in relation to routine activities and fear of cybercrime. Although Roberts et al. (2013), using data from the Australian Survey of Social Attitudes, found online exposure was positively correlated with fear of online identity theft, Henson et al. (2013) found no relationship in a sample of US college students. More recently, Choi et al.'s study found limited support in the use of RAT to explain fear of identity theft. In a representative sample of the Korean population, they found that 'Of the nine different measures across three domains of routine activities assessed, only three were statistically significantly associated with fear of identity theft victimization' (Choi et al. 2021, p. 421). Specifically, they find that variables such as using the internet for banking and being previously exposed to online phishing attacks, increase people's fear of identity theft victimization. Similarly, Böhme and Moore (2012) found that EU residents who reported limited online exposure, in particular, banking and buying online, expressed higher levels of fear. Both Hille et al. (2015) and Brands and van Wilsem (2021) found fear of financial cybercrime increased as engagement with online banking and purchasing decreased. The latter study is one of the few to include a range of online guardianship measures, finding inconclusive negative correlations between fear and the use of spam filters and wireless network security. More population-based research examining in more details how guardianship measures operate alongside routine activities is needed to test the utility of RAT as an explanation for fear of cybercrime.

Perhaps more importantly research into fear of cybercrime has not yet considered the wider social environment in which cyber-criminal activity occurs. Brands and van Wilsem (2021) and Roberts et al. (2013), for instance, investigated fear of online financial crime and cyber-identity theft in, respectively, The Netherlands and Australia. While both studies looked at the influence of individual characteristics such as gender, income, previous victimization, they do not consider the direct and indirect effects of context-specific features. Individual characteristics, however, can interact with other socio-ecological determinants and influence the way we feel about cybercrime, in a similar way to our fear of crime (Reese 2009).

COUNTRY-LEVEL EFFECTS AND FEAR OF CYBERCRIME

Several studies have found significant cross-national differences in fear of offline crime across Europe (Buil-Gil et al. 2021; Kujala et al. 2019; Vauclair and Bratanova 2017; Vieno et al. 2013; Visser et al. 2013). These studies demonstrate the importance of examining country-level characteristics, which can be integrated within an individual-level theoretical framework to provide a more comprehensive picture of cybercrime-related fear.

Offline research has shown that several contextual factors including visible signs of disorder, poverty and income inequality are predictive of higher levels of fear (Brunton-Smith and Sturgis 2011; Moore and Shepherd 2006; Vauclair and Bratanova 2017; Wyant 2008). At the country

level, research using the International Crime Victimization Survey (ICVS) has consistently found that offline criminal victimization varies between countries and is related to urbanicity, economic inequality and age composition (Kesteren et al. 2013). In another study using data from the 2006 Eurobarometer, Vieno et al. (2013) found that individual-level economic insecurity and country-level income inequality were both predictive of fear. More recently, Kujali et al. (2019) analysed data from the European Social Survey and found that country-level inequality had a net effect on fear of crime after controlling for multiple indicators of poverty. While both of these studies were limited by using the 'fear of walking alone at night' standard item to measure fear of crime, meaningful cross-national differences have been found with different measurement strategies (Jackson and Kuha 2014), and increased levels of fear appear to be one of the consequences of economic insecurity, especially in countries with high levels of income inequality (Vieno et al. 2013).

No evidence currently exists that details the role that national context plays in predicting fear of cybercrime, although some research has examined contextual factors related to cybercrime perpetration and victimization. Kim et al. (2012) show how systems hacking *perpetration* patterns vary by country. When controlling for the country-level factor of economic performance they find significant differences in prevalence of hacking attempts by country and show the highest number of acts of perpetration emanate from Latvia, Slovenia and Estonia within the EU. The same study also found the countries that had not adopted the Council of Europe (CoE) Convention on Cybercrime and that had less developed Internet infrastructure (measured in terms of Internet penetration) harboured a disproportionate number of hacking perpetrators. In the first cross-national European study of cybercrime victimization, Williams (2016) found that high country Internet penetration, a proxy for infrastructure development, was associated with lower levels of online identity theft victimization and more effective online guardianship. In addition, country-level proxies for guardianship (internet penetration and cyber security policy) significantly moderated the effectiveness of individual-level guardianship on reducing the likelihood of cyber-victimization.

THE CURRENT STUDY

As with conventional fear of crime, we posit that with fear of cybercrime the individual does not exist in a vacuum; instead, the effects of their personal characteristics are, at least in part, a function of the national context in which individuals find themselves. The current study tests how individual-level variables linked to RAT interact with country-level factors to explain fear of economic cybercrime in Europe. In doing so, this is the first study to apply RAT to investigate the moderating effects of contextual factors on people's fear of cybercrime. Derived from previous research, we test the following four hypotheses:

Hypothesis 1 [H1]: Unobserved EU country characteristics will contribute to variations in economic cybercrimes.
Hypothesis 2 [H2]: Country-level regressors i) technology development and ii) income inequality will be associated with individual fear of economic cybercrimes.

The first two hypotheses quantify the degree to which fear of economic cybercrimes varies across the 28 countries in the EU and tests the application of RAT at the country level in assessing the association with *contextual* capable guardianship. Building on similar work conducted on online identity theft victimization (Williams 2016), we hypothesize that a high level of infrastructure development at the country level will provide a measure

of physical security against victimization that will be associated with lower levels of economic cybercrime fear at the individual level. We expect that infrastructure development, as a form of country guardianship, will operate independently from other national-level economic indicators.

Building on previous research that found a positive association between income inequality and fear of terrestrial crimes (e.g. Kujala et al. 2019; Vieno et al. 2013), we also hypothesize that fear of economic cybercrime will be higher in countries with higher levels of income inequality. We believe that economic and digital inequalities can lead to higher crime rates, which in turn, can lead to higher fear of economic cybercrime. Dodel and Mesch (2019), for instance, found that social disparities affect self-care behaviours such as antivirus use and setting robust passwords. Similarly, McGuire and Dowling (2013) found that minorities and those with lower socio-economic status are less likely to install security software on their devices. Hence, an association between inequality and cybercrime has been established, and we expect that individuals living in countries with higher levels of income inequality will be more likely to be fearful of economic cybercrime.

Hypothesis3 [H3]: Individual-level differences in guardianship and routine activities are associated with fear of economic cybercrime.

This hypothesis tests the application of RAT to fear of economic cybercrime at the individual level. It builds upon the work of van Wilsem (2013), Williams (2016) and Brands and van Wilsem (2021) by incorporating guardianship measures and tests the policy assumption that the adoption of guardianship measures reduces fear of cybercrime. The hypothesis also tests the association between individual-level routine activities and victimization experiences on fear of economic cybercrime while controlling for sociodemographic characteristics.

Hypothesis 4 [H4]: The association between individual-level guardianship measures will vary as a function of country-level technological development and country-level income inequality.

This final hypothesis tests the cross-level interaction between country- and individual-level guardianship measures to identify if moderating effects found in offline studies of fear of crime are also present for fear economic cybercrime (Brunton-Smith and Sturgis 2011; McGarrell et al. 1997; Taylor et al. 1985). We hypothesize that individual guardianship measures will be associated with lower levels of fear in countries with higher levels of technological development. We believe, in other words, that country-level technological development will moderate the effect of individual-level guardianship.

METHOD

Data

Statistical analyses were conducted on the 2018 Eurobarometer Cybersecurity Survey, a study commissioned by the European Commission. Country-level multi-stage random probability sampling was adopted, with sampling points drawn with probability proportional to population size (for a total coverage of the country) and to population density. Therefore, the Eurobarometer is the largest and most comprehensive cybercrime and security survey globally, that is statistically representative of the domestic population in Europe. The survey was designed to give a national comparative picture within the EU. Country geography was taken as the aggregate level

in this study, as fear of cybercrime is likely to have a limited lower-level geographic dependency above the individual household.[1]

Data for the survey were collected for all EU Member States between October 24, 2018 and November 7, 2018. Respondents were interviewed face-to-face in their homes and in their native language. A sample of 20,098 respondents was analysed for the study,[2] ranging from 268 respondents in Malta to 1171 respondents in Germany.[3] Item non-response was less than two percent for each of the independent variables, and missing values were listwise deleted and treated as missing at random.[4] The GESIS Leibniz Institut (2020) provides further details about the methodological features of the Eurobarometer survey.

INSTRUMENTS AND VARIABLES

Dependent variable

In accordance with the literature on fear of crime (Ferraro 1996; Fisher and Sloan 2003; Lane and Fox 2013), our analysis considers emotional reactions to fear of cybercrime (i.e. concern about cybercrime). While fearfulness may best be seen as a mental event that is not completely synonymous with worry or concern about crime (Hough 2004), fear of crime is largely understood by how it has been measured (Farrall et al. 1997), which is typical with questions about a negative emotional response, usually rooted in feelings of anxiety and dread (Ferraro 1996). These conceptual issues fed into measurement issues in the early literature. Several studies used interchangeably questions about perceived risks (How safe do you feel being out alone in your neighbourhood at night?) and emotions (how worried are you of crime?) to measure fear of crime. However, studies found that safety measures had two problems: 1) they tap into respondent's perception of likelihood of becoming victim of crime instead of the feelings/emotions connected to fear of crime; and 2) they inflate people's fear by eliciting 'fearful' responses (Ferraro and Grange 1987; Farrall et al. 2009). There is now general agreement among researchers that the best measurements of fear crime: (1) refer to emotions; (2) are crime- and location-specific; and (3) should measure emotional intensity (Ferraro 1996; Ferraro and Grange 1987; Lane and Fox 2013; Fisher and Sloan 2003).

Consistent with this approach, our dependent variable refers specifically to people's concern about fear of economic cybercrime, and is based on the following eight items, each measured on a Likert scale ranging from 1 to 4 with high values reflecting higher levels of concern. 'How concerned are you personally about experiencing or being a victim of: (#1) online identity theft; (#2) purchase theft fraud; (#3) cyberattacks; (#4) account being hacked; (#5) bank fraud; (#6) fraudulent emails; (#7) malicious software; (#8) ransomware.'[5]

The dimensionality of these items was first analysed with exploratory and confirmatory factor analysis. Principal component analysis revealed only one factor with eigenvalue greater than one which explained 62% of the variance. Confirmatory factor analysis using weighted least

1 This is an assumption, as victim and perpetrator co-location is not necessary and guardianship efforts are often national, not regional, meaning small geographies, such as towns and cities, are theoretically less likely to matter when it comes to fear of cybercrime (see Williams 2016).

2 The analytic sample of 20,098 used in the current analysis was based on a total population of 27,339 EU citizens who were interviewed. 5,662 cases were dropped because these individuals reported no internet use and they were not asked any cyber questions. A further 362 cases were dropped because the interviewer assessed their cooperation to be 'bad'. The remainder of cases were dropped because of item non-response.

3 The Eurobarometer provides different samples for East and West Germany. Because we are interested in identifying between-country effects, these two samples were combined.

4 Supplemental analyses revealed that missing data were not significantly associated with either the outcome or focal independent variables.

5 The survey also asked respondents about their concern over accidentally encountering material which promotes 'racial hatred or religious extremism' or 'child pornography' online. These two items were excluded because they measure content cybercrime, which is a theoretically distinct concept from the other measures of cybercrime included in this study (Williams 2016).

squares mean (WLS) estimation demonstrated good psychometric properties for the overall sample confirming the unidimensionality of the fear of economic cybercrime scale, but revealing that removing two items (fear of purchase theft fraud and bank fraud) significantly improved the goodness of fit (CFI = .98, RMSEA = .42, TLI = .96). Multilevel confirmatory factor analysis (MLCFA) using maximum likelihood (ML) estimation also showed good psychometric properties and better fit for the six-item scale in relation to the eight-item scales (CFI = .99, RMSEA = .043, TLI = .98, SRMR = .027). Therefore, we measured fear of economic cybercrime for each respondent who answered at least 5 of the 6 items (i.e. #1, #3, #4, #6, #7, #8).[6]

We also tested for cross-national factorial invariance and our results supported the configurational (i.e., same factor structure between countries) invariance (see Table 1). Principal component analysis conducted in each country of the sample confirmed unidimensionality across all samples showing in every case only one factor with eigenvalue greater than one (percentage of explained variance oscillated between 58% in the Netherlands and 84% in Malta). Confirmatory Factor Analysis using WLS in each country also confirmed that the unidimensional six-item scale in most of the cases of the sample revealed good fit (see Appendix Table A1, for model fit indices for each of the 28 countries).[7]

Individual-level covariates

This section reports the RAT and sociodemographic variables that we used to test our hypotheses (see Appendix Table A2 for coding details and descriptive statistics).

Online routine activities: exposure to risk

Several online routine activities were included to measure exposure to potential online risky situations: The *frequency of internet use* at home and on mobile devices was combined into a scale covariate (range 0–10), providing a direct estimate of time exposure time online. Five *online routine activities* (online banking, online purchasing, online selling, online social networking, accessing public services online) capture different types of online behaviours which potentially expose individuals to online risk. Both the frequency and variety of online behaviours increase the opportunity, if left unguarded, for cyber-victimization by motivated offenders. Variations in the exposure to risk, measured by individual online activities, have been linked with cybercrime fear (Brands and van Wilsem 2021; Hille et al. 2015; Roberts et al. 2013). From a RAT perspective, exposure to risk should be positively associated with cyber fear.

Proximity to victims is another type of exposure to risk, and research has demonstrated that both direct and indirect (i.e. vicarious) experiences with victimization increase individual fear of crime (Cook and Fox 2011; Lee and Hilinski-Rosick 2012). Because individual-level fear is expected to vary as a function of exposure to victimization, both measures were included in the current research. The respondents were asked whether they had personally been a victim or whether the respondents knew of any family, friends or acquaintances that had been a victim of the 8 types of cybercrimes that were used to develop the fear of cybercrime measure. Each of these items was coded as a dichotomous variable (0 = no, 1 = yes) and these items were summed to create two separate victimization measures: *1) number of experiences with different types of direct/personal victimization, 2) number of experiences with different types of indirect/vicarious victimization.*

6 The results from all multilevel models were estimated with both the 6-item and 8-item fear of economic cybercrime scales as a sensitivity analysis. The results were nearly identical and the substantive meaning of the findings did not change.

7 The countries which showed poor fit were Cyprus, Czech Republic, Finland and Spain with poor values of RMSEA (below critical value .05) and CFI (below the critical value .95) but with acceptable values of SRMR (below the threshold .05).

Table 1. *Measurement invariance fit indices for Fear of Cybercrime Scale, 2018 Eurobarometer cybersecurity survey*

Model	X²[a]	df[b]	CFI[c]	TLI[d]	SRMR[e]	RMSEA[f] [95% CI]
Configural	821.569***	261	0.954	0.924	.026	0.056 [0.051–0.060]
Metric	1250.037***	401	0.931	0.925	.041	0.055 [0.052–0.059]
Scalar	2827.447***	541	0.813	0.850	.062	0.078 [0.075–0.081]

[a]X2, Adjusted chi-squared test for model fit;
[b]df, degrees of freedom;
[c]*CFI*, Comparative Fit Index;
[d]*TLI*, Tucker-Lewis Index;
[e]*SRMR*, Standardized Root Mean Square Residual;
[f]*RMSEA*, Root Mean Square Error of Approximation

Online guardianship: security against risk

Consistent with research that adapted measures of capable guardianship for the online setting (Williams 2016), the current research identified eight measures of internet security. These items were combined, and three underlying components were identified through a PCA factor analysis: 1) *passive personal guardianship* (using only one computer, email spam filtering, installing antivirus and secure browsing); 2) *active personal guardianship* (changing security settings and passwords) and 3) *avoidance personal guardianship* (doing less online, such as banking and purchasing goods).

In addition, researchers have argued that engaging in self-protective behaviours can reduce the availability of suitable targets (Reynald 2010; Tewksbury and Mustaine 2003; Tseloni et al. 2004). This type of 'informal guardianship' assumes that arming oneself against potential victimization risk can be protective in and of itself (Tewksburgy and Mustaine 2003). This may be particularly true in the cyber-context where risks are usually inferred rather than directly observed, making online self-regulation a potentially important aspect of online capable guardianship. We, therefore, extend our conceptualization of guardianship to include a measure of informal guardianship, based on whether respondents feel like they can protect themselves against cybercrime (0 = totally disagree, tend to disagree, don't know; 1 = tend to agree, totally agree).

Individual-level control variables

Previous research has linked fear of cybercrime with sociodemographic variables (Brunton-Smith 2017; Virtanen 2017), and we, therefore, include the following control variables in our analysis: sex (binary); education (ordinal); rural (binary); deprivation (ordinal). Age was included as a continuous variable. Given that exposure to online risk is linked with higher levels of fear, and because younger people tend to be more embedded in the online setting, we also tested for a non-linear association between age and fear of economic cybercrime.

Country-level factors

To limit the chance of drawing spurious conclusions, we limit our analysis to two theory-driven important contextual factors. The Information and Communication Development (ICT) index, developed by the International Telecommunications Union (ITU) of the United Nations, was used as a country-level measure of technology development (ITU 2020). This index was empirically derived from three weighted sub-indices (infrastructure access, intensity, skills), allowing for cross-national comparisons. Previous research found that high country Internet penetration, a proxy for infrastructure development, was associated with lower levels of online identity theft victimization and more effective online guardianship (Williams 2016).

Income inequality is measured using the Gini coefficient for equivalized household income after taxes, the most widely used measure of inequality. The Gini coefficient ranges between 0, where everybody is equal, and 1, where all the country's income is earned by a single person. Appendix Table A3 provides more information about contextual variables.

Analytic strategy

Fear of cybercrime is predicted using multilevel models in the current analysis. Model 1 is a random intercept model including individual-level fixed effects and no country-level effects. This model shows the extent to which unobserved EU country characteristics contribute to variations in fear of economic cybercrime. Model 1 also examines the association between the individual RAT measures and fear, controlling for between-country variation. Model 2 adds the country-level effects and examines the extent to which technology development and income inequality are associated with individual fear of economic cybercrime. Model 3 extends the analysis to allow the slopes of the guardianship measures to vary between countries. In conceptual terms, this random coefficient model tests whether the effect of guardianship on fear varied by EU national context, an important prerequisite for establishing potential cross-level interactions. The final model includes cross-level interaction terms to determine whether the associations between our guardianship measures and fear of economic cybercrime is moderated by national-level income inequality and technology development. All descriptive and multilevel models were conducted using Stata v. 16.1. The confirmatory factor analyses were conducted in R, using the lavaan package (Rosseel 2012).

RESULTS

Figure 1 presents a caterpillar plot showing EU country rank ordering of fear of economic cybercrime with 95% confidence intervals. In EU states where confidence intervals sit above

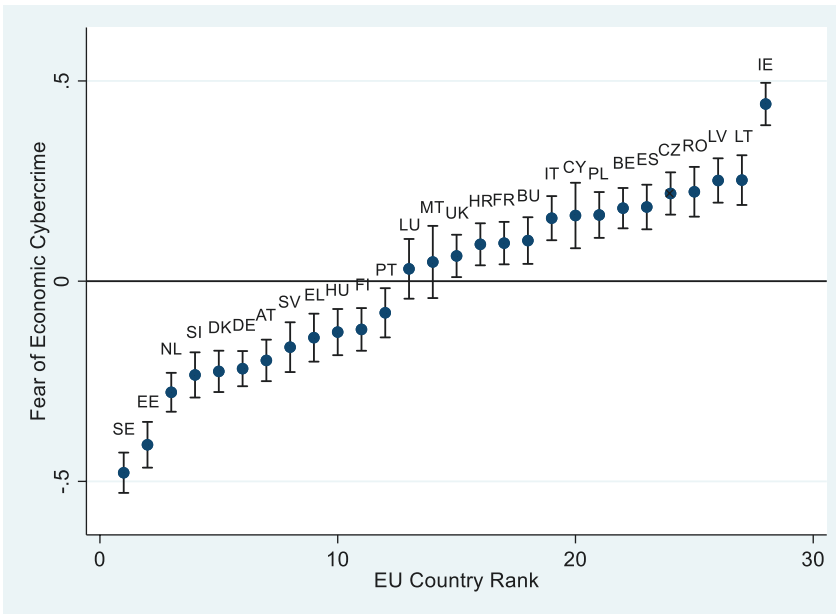

Figure 1. Ordered EU country effects for fear of economic cybercrime. Source: Authors' elaboration on 2018 Eurobarometer Cybersecurity Survey.

or below the mean line, survey respondents in these countries exhibit fear significantly above or below the average level in Europe. Following Ireland, a group of Eastern European countries (Lithuania, Latvia, Romania, Czech Republic) report the next highest average fear of economic cybercrime. The lower end of the plot is occupied by the three Nordic countries (Sweden, Denmark, Finland), along with the Netherlands, Germany, and Greece. Interestingly, several Eastern European countries also have lower than average fear, including Estonia, Slovenia, Slovakia, and Hungary.

Table 2 displays the coefficients for the multilevel models. Model 1 in Table 2 displays the individual factors associated with fear of economic cybercrime, controlling for the country-level differences. Significant demographic predictors associated with increased fear include being female, having trouble paying bills (deprivation), and living in a rural location. A non-linear relationship was identified between age and fear, evidenced by significant squared age terms in the model. This indicates a monotonic increasing function of fear by age until a turning point is reached, after which the function decreases. We estimated the value of x (age) where y (fear) was greatest finding the function turns at 41 years of age (see Figure 2). It also shows that there is a different turning point in fear of economic cybercrime between men and women, 45 and 35, respectively.

Many of the RAT measures are significantly associated with the dependent measure in the random intercept model. Fear of economic cybercrime increases with exposure to online risks, as the frequency of time spent online, and online banking are associated with higher levels. However, two exposure variables, i.e. purchasing goods online and social networking online, are significantly associated with lower levels of fear. Being a victim of economic cybercrime or knowing someone who has been victimized are also both significantly predictive of fear. All types of guardianship behaviours, including passive guardianship (only use own computer, do not open email from unknowns, only visit trusted websites and installed antivirus), avoidance guardianship (avoiding banking and shopping online), active guardianship (changing security settings and passwords), and informal guardianship (being able to protect yourself) are significantly associated with higher levels of fear. It is however possible that the relation is in the other direction and that people who are more afraid of cybercrime are also more likely to adopt security behaviours.

Model 2 builds on Model 1 by adding the two country-level effects to the random intercept model. Both country-level factors are significantly associated with fear of economic cybercrime. There is a negative and statistically significant association between the ICT technology development index and fear, revealing that individuals living in countries with a higher level of technology development tend to be less fearful relative to those living in countries with lower levels of technology development. Secondly, country-level income inequality emerges as significant and positive, as individuals living in countries with higher levels of income inequality report higher average levels of fear. These country-level variables significantly improved the fit of the multilevel model, and the country variance was reduced in Model 2.

Model 3 differs from the previous two models as the random components for the guardianship measures were all included in the random part of the multilevel equation. This model allowed the slope of each guardianship measure to vary between the EU countries. The results demonstrate that while each of the guardianship measures is significantly associated with higher levels of fear in the fixed part of the model, the random components are also significant, demonstrating that the strength of these associations varies significantly across EU countries. A likelihood ratio test showed an improved model fit ($\chi^2(16)$: 177.56, $p < 0.001$), suggesting there may be cross-level interactions between these variables and national-level factors.

Table 3 reports the results for the cross-level interactions between the individual-level guardianship measures and country-level income inequality and ICT development. These interactions

Table 2. *Individual and EU country correlates of fear of economic cybercrime, 2018 Eurobarometer cybersecurity survey*

	Model 1		Model 2		*Model 3*[a]	
Individual level Predictors	**Estimate**	**SE**	**Estimate**	**SE**	**Estimate**	**SE**
Intercept	2.24***	.074	2.23***	.103	2.21***	.101
Demographic Characteristics						
Descriptive Statistics on Independent Female	.131***	.011	.135***	.011	.128***	.011
Age	.008***	.002	.009***	.002	.009***	.002
Age2	–000**	.000	–.00***	.000	–.00***	.000
Education	.001	.008	.001	.008	–.002	.008
Employed	.000	.014	.000	.014	–.001	.014
Deprivation (diff. paying bills)	.077***	.013	.076***	.013	.076***	.013
Rural	0.54***	.013	.054***	.013	.051***	.013
Routine activities Variables						
Exposure to online Risk						
Internet frequency	.025***	.003	.025***	.003	.025***	.003
Internet use: Banking online	.044*	.014	.035*	.014	.030**	.014
Internet use: Purchase online	–.105***	.013	–.010***	.013	–.102***	.013
Internet use: Selling Online	–.015	.014	–.014	.015	–.13	.014
Internet use: Social Networking	–.027*	.013	–.027*	.013	–.024	.013
Internet use: Access Public Services	–.024	.014	–.023	.014	–.025	.014
Direct victimization	.131***	.013	.132***	.013	.136***	.013
Indirect Victimization	.063***	.013	.063***	.013	.063***	.013
Online personal Guardianship						
Passive guardianship	.102***	.006	.102***	.006	.098***	.010
Active guardianship	.058***	.006	.059***	.006	.064***	.011
Avoidance guardianship	.076***	.006	.076***	.006	.073***	.008
Informal guardianship	056***	.012	.056***	.012	.068*	.029
Country level variables[b]						
ICT development index			–1.12**	.059	–.178**	.055
Gini index			.019*	.009	.021*	.009
Random Components						
Passive guardianship random slope	--		--		.0018	
Active guardianship random slope	--		--		.0024	
Avoidance guardianship random slope					.0009	
Informal guardianship random slope					.020	
Level 1 variance	.588		.588		.588	
Level 2 variance	.053		.033		.038	
Number of Individuals/countries	20,098/28		20,098/28		20,098/28	
BIC	46,791.54		46,698.9.1		46,679.89	
Log-likelihood	–23,246.69		–23,240.1		–23,151.66	

*$p < .05$;
**$p < .01$;
***$p < .001$
[a] Model 3, the random coefficients model, was estimated with an unstructured covariance matrix.
[b] Both country-level variables were grand mean centred with a mean of 0 and a standard deviation of 1

allowed for an assessment of whether country-level income inequality and technological development are associated with variation in the slopes between countries. None of the interactions between the individual guardianship measures and income inequality are significant, suggesting

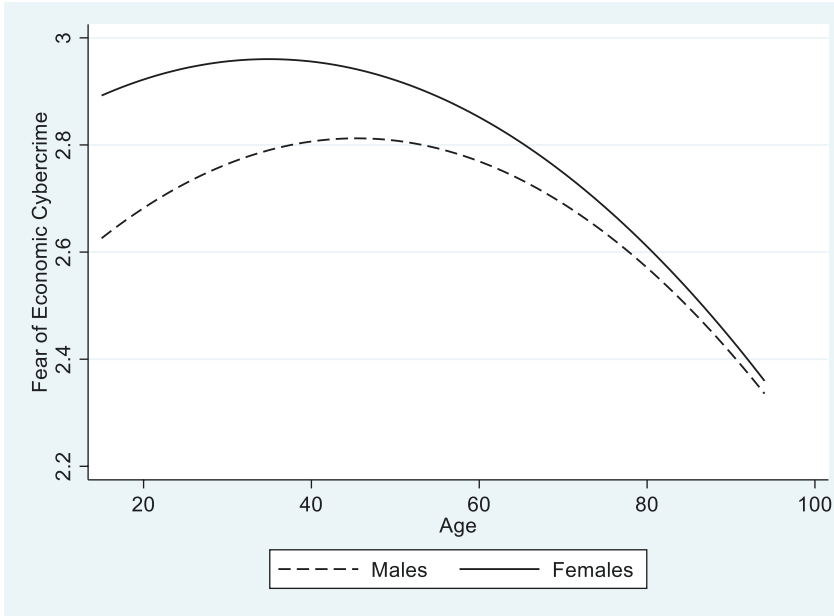

Figure 2. Fear of economic cybercrime by age and gender.

that while individuals living in countries with higher levels of income inequality tend to be more fearful of economic cybercrime, these levels of fear are independent of one's individual guardianship behaviour.

The guardianship measures, on the other hand, are significantly associated with the ICT development index, suggesting that the impact of guardianship varies depending on country-level economic development. The informal guardianship by ICT development interaction best fit the data and the negative association suggests that the effect of informal guardianship on fear is lower among countries with higher levels of country-level economic development. In order to better understand the effect of informal guardianship on fear of economic cybercrime by country-level economic development, the fitted values were plotted.[8] Figure 3 shows that in countries with less than an average amount of technological development, informal guardianship is associated with higher levels of fear. However, this positive association dissipated in countries with higher levels of technology development, and the direction of the association is inverted among individuals in countries with the highest level of technology development. The Netherlands, for instance, has one of the most highly developed technological infrastructures in the world, and its citizens who feel they can protect themselves online (self-protective/informal guardianship) are significantly less likely to be fearful of economic cybercrime.[9]

DISCUSSION

We examined how individual-level variables linked to RAT interact with country-level factors to predict fear of economic cybercrime among individuals living in Europe's 28

8 This interaction was calculated holding the effect of all other variables constant.

9 The country-specific effect for the Netherlands was estimated with a fixed effect regression model with country-level dummy variables. While this does not precisely reproduce the random coefficients model, this analytic approach does allow us to isolate different slopes for different countries Table 2. Individual and EU Country Correlates of Fear of Economic Cybercrime, 2018 Eurobarometer Cybersecurity Survey.

Table 3. *Multilevel models examining combinations of interaction effects between guardianship and national contextual variables, 2018 Eurobarometer cybersecurity survey*

Model	Interactions Included in the Model[a]	Estimate	SE	Log-likelihood
1	Informal guardianship x ICT Development Index	–.138***	.038	–23,189.86
2	Active guardianship x ICT Development Index	–.034*	.015	–23,223.15
3	Avoidance guardianship x ICT Development Index	.046***	.012	–23,224.25
4	Passive guardianship x ICT Development Index	.017	.016	–23,326.27
5	Informal guardianship x GINI Index	–.004	.007	–23,195.15
6	Active guardianship x GINI Index	.002	.003	–232,225.69
7	Avoidance guardianship x GINI Index	.000	.002	–23,190.47
8	Passive guardianship x Gini Index	.000	.003	–23,225.69

[a]All models include all individual-level predictors, the main effects of the contextual variables and random components for the intercept of the individual-level interaction term

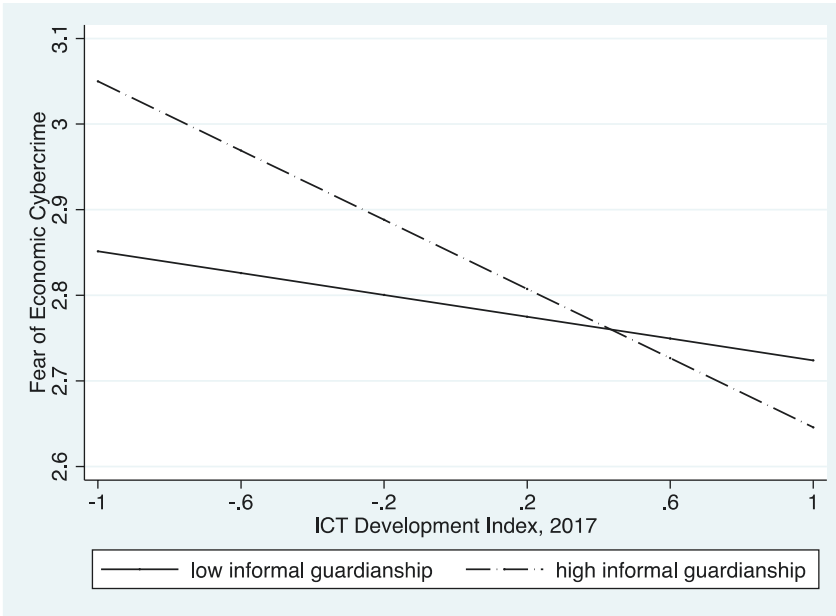

Figure 3. Fear of cybercrime among EU countries according to ICT development index and informal guardianship.

nation-states (including the now-departed UK). Our study contributes to the growing body of fear cybercrime research in four specific ways. First, we find that fear of economic cybercrime varies considerably across Europe's twenty-eight countries *[H1]*. The clustering of some Eastern European countries (e.g. Lithuania, Latvia, Romania, Czech Republic) at the top, and some Nordic countries (e.g. Sweden, Denmark, Finland) at the bottom of the distribution confirms our initial hypothesis that country-level factors play an important role in shaping individual's fear of economic cybercrime. This distribution closely

matches levels of fear of terrestrial crime observed in other studies across Europe (Visser et al. 2013; Van Dijk et al. 2007). For instance, Visser et al. (2013: 287) found that 'especially some countries in Eastern Europe show high levels of fear of crime and feelings of unsafety, whereas Nordic countries show relatively low levels of fear of crime and feelings of unsafety.' These cross-national differences, however, are not irreducible to regional differences, as Ireland and Spain had high average levels of fear of economic cybercrime, while Estonia, Slovenia and Slovakia had lower than average levels. These between-country differences suggest that fear of cybercrime cannot be understood by individual-level factors alone, necessitating a multilevel approach that adjusts for between-country clustering and can incorporate country-level factors.

Second, we find that country-level technology development and income inequality are both significantly associated with individual fear of economic cybercrime *[H2]*. The results demonstrate, for the first time, that a country's ICT technology development is significantly and negatively associated with fear of economic cybercrime at individual level *[H2]*. Previous research on online identity theft has already showed that developed ICT infrastructures are characterized by superior security which, in turn, harden offenders' targets and reduce individual risks of victimization (Williams 2016). The current study further suggests that developed infrastructures can reduce people's concern about economic cybercrimes. It is possible that developed ICT infrastructures increase people's trust, which makes them feel less vulnerable to cyberthreats.

We also find that individuals living in countries with higher levels of income inequality report higher fear of economic cybercrime; a finding consistent with research on fear of terrestrial crimes (Kujala et al. 2019; Vauclair and Bratanova 2017; Vieno et al. 2013). It is possible that income inequality reduces the acquisition of digital skills among the less affluent, which can lead to higher crime rates and fear of victimization (Dodel and Mesch 2019). It is also possible wider socio-economic distance may be associated with lower levels of trust between people, which could increase individual fearfulness (Kujala et al. 2019; Vieno et al. 2013). While we were not able to test which one of these two mechanisms is at play, both may contribute to explain why country-level income inequality is positively associated with fear of cybercrime.

Third, we identify several individual-level sociodemographic and RAT characteristics that are significantly associated with fear of economic cybercrime after controlling for between-country differences *[H3]*. Consistent with the literature on fear of terrestrial crimes (e.g. Brunton-Smith 2011; Carro et al. 2010; Pantazis 2000), we find that women were more likely to be fearful than men. This finding corroborates other fear of cybercrime research (Brunton-Smith 2017; Virtanen 2017). We also find that age has a significant curvilinear association with fear of economic cybercrime. Fear increases consistently after 18 years of age, though it peaks at 45 for men and 35 for women. After these ages, fear decreases, showing that young and middle-aged adults are more worried than older people about economic cybercrimes. The 35-55 age group is most likely to have dependent children, a privately-owned home and vehicle and are most likely to bank and shop online. Therefore, it appears that the cost and risk of economic cybercrime may be greatest for this age group relative to younger and older age groups. We also find that the most economically deprived, such as those struggling to pay their bills, report significantly higher levels of fear. For this group, the cost imposed by a possible cybercrime incident can further damage their precarious socio-economic conditions, making it more difficult for those individuals to recover from an economic loss.

This study adopted a RAT approach to explain fear of economic cybercrime, and we find that variables related to online daily activities, such as the frequency of internet use (both at home

and from mobile) and banking online are positively associated with fear. RAT postulates that daily routine activities can expose citizens to criminal opportunities and in turn affects trends in crime (Cohen and Felson 1979). This study provides evidence that online routine activities do not just influence terrestrial crime patterns but also individual's fear of economic cybercrime. People that make a frequent use of internet and online banking must be aware that this exposes them to higher risk of becoming victims of cybercrime, but are willing to accept these risks, presumably for the greater benefits they experience.

As other research has already identified, fear of offline and online crime was associated with direct victimization experiences, as victims of cybercrime report being more worried about cybercrime than non-victims (Brunton-Smith and Sturgis 2011; Virtanen 2017). Our findings extend this victimization-fear nexus by demonstrating that vicarious victimization is significantly associated with fear of economic cybercrime. It appears that fear of cybercrime may not solely associated by direct victimization experiences or by individual variation in risky online lifestyles, but also by the indirect victimization experiences of friendship and social networks (Lusthaus and Varese 2021).

Finally, the current research finds that country-level technological development moderates individual-level active guardianship and informal guardianship *[H4]*. Security behaviours such as routinely changing security settings and individuals' beliefs about their ability to successfully use computers are positively associated with fear of economic cybercrime in countries with low-level ICT development. However, this association changes direction and is negative in countries with high ICT technology development. People who believe they are able to navigate competently cyber-risks and implement appropriate security measures tend to be less fearful of economic cybercrime in countries such as the Netherlands, United Kingdom, Sweden, Denmark and Germany that have highly developed ICT infrastructures. These findings align with other research examining the contextual effects of RAT (Miethe and McDowall 1993; Williams 2016) and studies of terrestrial fear of crime. Both these branches of research show that individuals do not operate in a social vacuum, but, instead, the environment plays a key role in shaping individuals' worries and behaviours. Brunton-Smith and Sturgis (2011) found that contextual variables such as crime rates, ethnic diversity and visible signs of disorder in the neighbourhood moderate individual-level determinants of fear of crime. In this study, we found that, although online crime is often considered 'a crime without borders' (e.g. Moraski 2011), contextual factors can dissipate and even reverse the influence of individual-level correlates of fear of economic cybercrime. While cybercrime takes place in cyberspace, offline and proximal elements such as a person's country of residence are crucial in determining concerns about risks of becoming a victim (Lusthaus and Varese 2021).

CONCLUSIONS

Economic cybercrime has emerged as the most prevalent type of acquisitive crime in Great Britain (ONS 2022; Scottish Government 2021); the Irish Republic (CSO 2020) and Spain (Kemp et al. 2020), and elsewhere in the EU, yet very little academic research has examined individuals' economic cybercrime fears. The goal of this study was to develop a robust measure of economic cybercrime that is consistent across the member states of the EU (including the now-departed UK) and to examine the association between cyber fear and both individual-level and country-level factors. We adapted and extended the guardianship measures developed by Williams (2016) in the context of fear of economic cybercrime and found that each was significantly predictive in our models. Building on the work of Brunton-Smith and Sturgis (2011),

we investigated the influence of contextual factors, and our analyses confirm that country-level income inequality and infrastructure development both predicted individual fear of economic cybercrime.

A key innovation of this research was the inclusion of interactions between individual-level guardianship and country-level factors. We found that, in the European context, countries with higher levels of technology infrastructure moderated individual guardianship, a finding that is consistent with multilevel applications of RAT to the study of online identity theft (Williams 2016). This finding provides some evidence that fear of economic cybercrime may be reduced by enhancing technological development at the country level. It also points out that individual characteristics are insufficient to predict fear of cybercrime, and we also need to consider country-level factors to fully explain its variation.

The current study was limited by the cross-sectional design of the survey, and the results should be interpreted with the same level of caution required in all self-reported studies. Our non-randomized data means that our results could be affected by unmeasured confounding, and we could not account for the dynamic and complex interplay between our measures and the fear of economic cybercrime over time. This research was focused on examining individual- and country-level factors associated with cybercrime fear, and future research would benefit from better understanding these complex causal interrelationships. Additionally, while our multilevel approach allowed us to control for between-country differences, it is still possible that it did not completely account for *all* the between-country differences. Future work on fear of economic cybercrime could also be extended to include: (1) a larger selection of countries beyond EU member states, which would increase the level-2 sample size and would allow for the inclusion of a broader range of relevant country-level predictors; (2) adding more theory-driven predictors at the individual-level, such as low self-control and social capital, which may improve the prediction of fear of cybercrime; (3) exploring more sociodemographic, economic and cultural predictors at the country-level (e.g. age composition, economic insecurity, rates of online victimization, gender variables, etc.) which may improve prediction and allow for better incorporation of unmeasured cross-national singularities and (4) the continued development of mediation and moderation analyses in the multilevel context to help isolate the mechanisms responsible for cyber fear at different levels of analysis.

In conclusion, this study underscores the importance of both individual- and country-level mechanisms associated with fear of economic cybercrime, and the variations within and between countries suggest that it is inadequate to consider either alone. We believe that our new and more consistent measures, and our demonstration of the importance of context in accounting for the independent role of country-level variables on fear of cybercrime, provides a better baseline for future work on this important social phenomenon, which could affect economic and political engagement in the digital economy and society.

FUNDING

The authors received no financial support for the research, authorship, and/or publication of this article.

APPENDIX

Table A1. *Confirmatory factor analysis fit indices by country*

Country	*N*	CFI	TLI	SRMR	RMSEA
Austria	838	.968	.947	.026	.048
Belgium	913	.958	.930	.031	.045
Bulgaria	647	.945	.909	.023	.057
Croatia	840	.982	.969	.015	.036
Cyprus	337	.903	.839	.064	.096
Czech Republic	819	.937	.894	.032	.071
Denmark	857	.960	.933	.023	.058
Estonia	676	.983	.972	.018	.035
Finland	808	.888	.814	.042	.087
France	801	.943	.904	.030	.055
Germany	1163	.944	.906	.029	.065
Greece	641	.954	.923	.029	.063
Hungary	691	.963	.939	.015	.062
Ireland	823	.936	.996	.027	.052
Italy	761	.929	.882	.030	.058
Latvia	734	.973	.955	.023	.035
Lithuania	566	.926	.877	.033	.042
Luxembourg	397	.985	.975	.028	.031
Malta	271	.987	.979	.033	.031
Netherlands	973	.937	.895	.028	.059
Poland	709	.984	.973	.023	.031
Portugal	610	.957	.928	.037	.056
Romania	597	.946	.910	.028	.047
Slovakia	585	.983	.972	.024	.030
Slovenia	714	.963	.938	.035	.070
Spain	747	.917	.861	.042	.075
Sweden	896	.972	.953	.020	.040
United Kingdom	820	.998	.996	.012	.013

Note: CFI, Comparative Fit Index; TLI, Tucker-Lewis Index; SRMR, Standardized Root Mean Square Residual; RMSEA, Root Mean Squared Error of Approximation

Table A2. *Descriptive statistics on independent variables, 2018 Eurobarometer survey*

	Coding	*Weighted Sample**	
Individual Level Factors		**M (%)**	**95% CI**
Demographic characteristics			
Female	0 = male, 1 = female	50.1%	48.9%–51.1%
Age	scale (range 15–94)	43.94	43.5–44.3
Employed	0 = no, 1 = yes	61.3%	60.1%–62.5%
Education	scale (range 1–4)	3.35	3.3–3.4

Table A2. *Continued*

Individual Level Factors	*Coding*	*Weighted Sample**	
		M (%)	**95% CI**
Deprivation (difficulties paying bills)	1 = yes (some, most of time)	28.5%	27.4%–29.5%
Rural	0 = urban/suburban, 1 = rural	21.7%	20.7%–22.6%
Online Routine Activities			
Internet frequency: Home, Mobile	scale (range: 0–10)	9.06	9.0–9.1
Internet use: Banking	0 = no, 1 = yes	60.8%	59.6%–62.0%
Internet use: Purchasing	0 = no, 1 = yes	58.2%	57.0%–59.3%
Internet use: Selling	0 = no, 1 = yes	24.6%	23.6%–25.7%
Internet use: Social networking	0 = no, 1 = yes	62.4%	61.2%–63.6%
Internet use: Access public services	0 = no, 1 = yes	39.2%	38.1%–40.4%
Direct victimization	0 = no, 1 = yes	50.7%	49.4%–51.9%
Indirect victimization	0 = no, 1 = yes	45.7%	44.5%–46.9%
*Guardianship measures***			
Passive guardianship	Standardized scale from PCA (range: –1.25 to 1.76)	0	1
Active guardianship	Standardized scale from PCA (range: –.780 to 2.76)	0	1
Avoidance guardianship	Standardized scale from PCA (range: –.451 to 3.59)	0	1
Informal guardianship	0 = no, 1 = yes (agree, strongly agree)	70.7%	70.0%–71.7%

*All descriptive statistics were based on the analytic sample (n = 20,098), and following the guidance outlined in the Eurobarometer documentation, population-based weights were used for all descriptive statistics. For more detail on weighting, please see: https://www.gesis.org/eurobarometer-data-service/survey-series/standard-special-eb/weighting-overview
**Three of the guardianship measures (passive, active and avoidance) were constructed based on a principal components factor analysis and each was converted into a z-score with a mean of 0 and a standard deviation of 1

Table A3. *Descriptive information for country-level factors and individual fear of cybercrime*

Country	***N***	**ICT Development Index 2017**	**Gini Coefficient**	**Mean fear of Cybercrime (SD)**
Austria	815	8.02	27.9	2.64 (.771)
Belgium	889	7.81	26.0	3.0 (.696)
Bulgaria	615	6.86	40.2	2.96 (.798)
Croatia	826	7.24	29.9	2.93 (.834)
Cyprus	334	7.77	30.8	3.02 (.944)
Czech Republic	814	7.16	24.5	3.04 (.832)
Denmark	864	8.71	27.6	2.60 (.860)
Estonia	697	8.14	31.6	2.43 (.801)
Finland	804	7.88	25.3	2.72 (.753)
France	813	8.24	29.3	2.93 (.758)
Germany	1171	8.39	29.1	2.63 (.767)
Greece	643	7.23	33.4	2.69 (.841)
Hungary	692	6.93	28.1	2.71 (.885)

Table A3. *Continued*

Country	*N*	ICT Development Index 2017	Gini Coefficient	Mean fear of Cybercrime (SD)
Ireland	804	8.02	30.6	3.29 (.745)
Italy	716	7.04	32.7	3.0 (.701)
Latvia	747	7.26	34.5	3.09 (.813)
Lithuania	589	7.19	37.6	3.09 (.786)
Luxembourg	396	8.47	30.9	2.86 (.764)
Malta	268	7.86	28.2	2.90 (.941)
Netherlands	984	8.49	27.1	2.59 (.706)
Poland	690	6.89	29.2	3.00 (.758)
Portugal	602	7.13	33.5	2.77 (.789)
Romania	564	6.48	33.1	3.08 (.777)
Slovakia	572	7.06	23.2	2.67 (.725)
Slovenia	714	7.38	23.7	2.59 (.983)
Spain	735	7.79	34.1	3.03 (.826)
Sweden	920	8.41	28.0	2.37 (.750)
United Kingdom	820	8.65	33.1	2.89 (.822)

Source: Authors' elaboration on 2018 Eurobarometer Cybersecurity Survey

REFERENCES

Böhme, R. and Moore, T. (2012), 'How Do Consumers React to Cybercrime?', *2012 ECrime Researchers Summit*, 1: 1–12. doi: 10.1109/eCrime.2012.6489519.

Bossler, A. M. and Holt, T. J. (2009). *On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory*. Undefined./paper/On-line-Activities%2C-Guardianship%2C-and-Malware-An-of-Bossler-Holt/4fbfe4134d74a0c9629b4dcce4ff6f5a78739204 (accessed 28 August 2020).

Bossler, A. M., Holt, T. J. and May, D. C. (2011), 'Predicting Online Harassment Victimization Among a Juvenile Population', *Youth & Society*, 44: 500–23. doi: 10.1177/0044118X11407525

Brands, J. and van Wilsem, J. (2021), 'Connected and Fearful? Exploring Fear of Online Financial Crime, Internet Behaviour and Their Relationship', *European Journal of Criminology*, 18: 213–34. doi: 10.1177/1477370819839619

Brunton-Smith, I. (2011), 'Untangling the Relationship Between Fear of Crime and Perceptions of Disorder Evidence from a Longitudinal Study of Young People in England and Wales', *British Journal of Criminology*, 51(6): 885–99.

Brunton-Smith, I. (2017). 'Fear 2.0: Worry About Cybercrime in England and Wales', in M. Lee and G. Mythen (Eds.), *The Routledge International Handbook on Fear of Crime*, 93–105. Routledge.

Brunton-Smith, I. and Sturgis, P. (2011), 'Do Neighborhoods Generate Fear of Crime? An Empirical Test Using the British Crime Survey*', *Criminology*, 49: 331–69.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. and Díaz-Castaño, N. (2021), 'Cybercrime and Shifts in Opportunities During COVID-19: A Preliminary Analysis in the UK', *European Societies*, 23: S47–59.

Caneppele, S. and Aebi, M. F. (2019), 'Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes', *Policing: A Journal of Policy and Practice*, 13: 66–79.

Carro, D., Valera, S. and Vidal, T. (2010), 'Perceived insecurity in the public space: Personal, social and environmental variables', *Quality & Quantity*, 44: 303–14.

Choi, J., Kruis, N. E. and Choo, K. S. (2021), 'Explaining Fear of Identity Theft Victimization Using a Routine Activity Approach', *Journal of Contemporary Criminal Justice*, 37: 406–26.

Cohen, L. E. and Felson, M. (1979), 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review*, 44: 588.

Cook, C. L. and Fox, K. A. (2011), 'Fear of Property Crime: Examining the Effects of Victimization, Vicarious Victimization, and Perceived Risk', *Violence and Victims*, 26: 684–700.
CSO. (2020). *Crime and Victimisation 2019*. Central Statistics Office. https://www.cso.ie/en/releasesandpublications/ep/p-cv/crimeandvictimisation2019/
Dodel, M. and Mesch, G. (2019), 'An Integrated Model for Assessing Cyber-safety Behaviors: How Cognitive, Socioeconomic and Digital Determinants Affect Diverse Safety Practices', *Computers & Security*, 86: 75–91.
Eck, J. E. and Clarke, R. V. (2003), 'Classifying Common Police Problems: A Routine Activity Theory Approach', *Crime Prevention Studies*, 16: 7–40. https://www.academia.edu/17828081/Classifying_Common_Police_Problems_A_Routine_Activity_Theory_Approach.
Farrall, S., Bannister, J., Ditton, J. and Gilchrist, E. (1997). Questioning the measurement of the 'fear of crime': Findings from a major methodological study. *The British Journal of Criminology*, 37: 658–79.
Farrall, S. D., Jackson, J. and Gray, E. (2009). *Social Order and the Fear of Crime in Contemporary Times*. Oxford University Press.
Ferraro, K. F. (1996). 'Women's Fear of Victimization: Shadow of Sexual Assault?' *Social Forces*, 75: 667–90.
Ferraro, K. F. and Grange, R. L. (1987). The Measurement of Fear of Crime*. *Sociological Inquiry*, 57: 70–97. doi: 10.1111/j.1475-682X.1987.tb01181.x
Fisher, B. S. and Sloan, J. J. (2003), 'Unraveling the Fear of Victimization Among College Women: Is the "Shadow of Sexual Assault Hypothesis" Supported?', *Justice Quarterly*, 20: 633–59.
GESIS Leibniz Institut für Sozialwissenschaften. (2020). *GESIS - Leibniz Institute for the Social Sciences*. https://www.gesis.org/en/eurobarometer-data-service/survey-series/standard-special-eb/sampling-and-fieldwork (accessed 7 September 2020).
Guerra, C. and Ingram, J. R. (2020), 'Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data', *Deviant Behavior*, 0: 1–17.
Henson, B., Reyns, B. W. and Fisher, B. S. (2013), 'Does Gender Matter in the Virtual World? Examining the Effect of Gender on the Link Between Online Social Network Activity, Security and Interpersonal Victimization', *Security Journal*, 26: 315–30.
Higgins, G. E., Ricketts, M. L. and Vegh, D. T. (2008), 'The Role of Self-Control in College Student's Perceived Risk and Fear of Online Victimization', *American Journal of Criminal Justice*, 33: 223.
Hille, P., Walsh, G. and Cleveland, M. (2015), 'Consumer Fear of Online Identity Theft: Scale Development and Validation', *Journal of Interactive Marketing*, 30: 1–19.
Holt, T. J. and Bossler, A. M. (2008), 'Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization', *Deviant Behavior*, 30: 1–25.
Hough, M. (2004). Worry about crime: mental events or mental states?. *International Journal of Social Research Methodology*, 7: 173–76.
ITU. (2020). *The ICT Development Index (IDI): Conceptual framework and methodology*. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx (accessed 15 September 2020).
Jackson, J. and Kuha, J. (2014), 'Worry about Crime in a Cross-National Context: A Model-Supported Method of Measurement Using the European Social Survey', *Survey Research Methods*, 8: 109–25.
Kemp, S., Miró-Llinares, F. and Moneva, A. (2020), 'The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain', *European Journal on Criminal Policy and Research*, 26: 293–312.
Kim, S. H., Wang, Q. H. and Ullrich, J. B. (2012), 'A Comparative Study of Cyberattacks', *Communications of the ACM*, 55: 66–73.
Kujala, P., Kallio, J. and Niemelä, M. (2019), 'Income Inequality, Poverty, and Fear of Crime in Europe', *Cross-Cultural Research*, 53: 163–85.
Lane, J. and Fox, K. A. (2013), 'Fear of Property, Violent, and Gang Crime: Examining the Shadow of Sexual Assault Thesis Among Male and Female Offenders', *Criminal Justice and Behavior*, 40: 472–96.
Lee, D. R. and Hilinski-Rosick, C. M. (2012), 'The Role of Lifestyle and Personal Characteristics on Fear of Victimization among University Students', *American Journal of Criminal Justice*, 37: 647–68.
Leukfeldt, E. R. and Yar, M. (2016), 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis', *Deviant Behavior*, 37: 263–80.
Levi, M. (2017), 'Assessing the trends, scale and nature of economic cybercrimes: Overview and Issues', *Crime, Law and Social Change*, 67: 3–20.
Lusthaus, J. and Varese, F. (2021), 'Offline and Local: The Hidden Face of Cybercrime', *Policing: A Journal of Policy and Practice*, 15: 4–14. doi: 10.1093/police/pax042
McGarrell, E. F., Giacomazzi, A. L. and Thurman, Q. C. (1997), 'Neighborhood Disorder, Integration, and the Fear of Crime', *Justice Quarterly*, 14: 479–500.

McGuire, M. and Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

Miethe, T. D. and McDowall, D. (1993). 'Contextual Effects in Models of Criminal Victimization', *Social Forces*, 71, 741–59.

Moore, S. and Shepherd, J. P. (2006), 'The Cost of Fear: Shadow Pricing the Intangible Costs of Crime', *Applied Economics*, 38: 293–300.

Moraski, L. (2011), 'Cybercrime Knows No Borders', *Infosecurity*, 8: 20–3.

ONS. (2021). *Nature of crime: Fraud and computer misuse* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse (accessed 21 November 2021).

ONS. (2022). *Crime in England and Wales: Year ending September 2021*. Office for National Statistics. https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingseptember2021

Pantazis, C. (2000), ''Fear of Crime', Vulnerability and Poverty', *The British Journal of Criminology*, 40: 414–36.

Pratt, T. C., Holtfreter, K. and Reisig, M. D. (2010), 'Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory', *Journal of Research in Crime and Delinquency*, 47: 267–96. doi: 10.1177/0022427810365903

Reese, B. (2009), 'Determinants of the Fear of Crime: The Combined Effects of Country-Level Crime Intensity and Individual-Level Victimization Experience', *International Journal of Sociology*, 39: 62–75.

Reynald, D. M. (2010), 'Guardians on Guardianship: Factors Affecting the Willingness to Supervise, the Ability to Detect Potential Offenders, and the Willingness to Intervene', *Journal of Research in Crime and Delinquency*, 47: 358–90. doi: 10.1177/0022427810365904

Reyns, B. W. (2011), 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses', *Journal of Research in Crime and Delinquency*.

Reyns, B. W. and Henson, B. (2015), '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*.

Reyns, B. W., Henson, B. and Fisher, B. S. (2011), 'Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization', *Criminal Justice and Behavior*, 38: 1149–169. doi: 10.1177/0093854811421448

Roberts, L. D., Indermaur, D. and Spiranovic, C. (2013), 'Fear of Cyber-Identity Theft and Related Fraudulent Activity', *Psychiatry, Psychology and Law*, 20: 315–28.

Rosseel, Y. (2012), 'lavaan: An R Package for Structural Equation Modeling', *Journal of Statistical Software*, 48: 1–36.

Scottish Government. (2021). *Scottish Crime and Justice Survey 2019/20*. Scottish Government.

Taylor, R. B., Shumaker, S. A. and Gottfredson, S. D. (1985). 'Neighborhood-Level Links Between Physical Features And Local Sentiments: Deterioration, Fear Of Crime, And Confidence', *Journal of Architectural and Planning Research*, 2: 261–75.

Tewksbury, R. and Mustaine, E. E. (2003), 'College Students' Lifestyles and Self-Protective Behaviors: Further Considerations of the Guardianship Concept in Routine Activity Theory', *Criminal Justice and Behavior*, 30: 302–27. doi: 10.1177/0093854803030003003

Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. (2004), 'Burglary Victimization in England and Wales, the United States and the Netherlands A Cross-National Comparative Test of Routine Activities and Lifestyle Theories', *British Journal of Criminology*, 44: 66–91.

UK Finance (2021). *2021 Half year fraud update*. https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf (accessed 12 December 2021).

van Kesteren, J., van Dijk, J. and Mayhew, P. (2013), 'The International Crime Victims Surveys: A Retrospective', *International Review of Victimology*, 20: 49–69. doi: 10.1177/0269758013511742

van Wilsem, J. (2011), 'Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization', *European Journal of Criminology*, 8: 115–27. doi: 10.1177/1477370810393156

Vauclair, C. -M. and Bratanova, B. (2017), 'Income Inequality and Fear of Crime Across the European Rgion', *European Journal of Criminology*, 14: 221–41.

Vieno, A., Roccato, M. and Russo, S. (2013), 'Is Fear of Crime Mainly Social and Economic Insecurity in Disguise? A Multilevel Multinational Analysis', *Journal of Community & Applied Social Psychology*, 23: 519–35.

Virtanen, S. M. (2017), 'Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities', *Psychiatry, Psychology and Law*, 24: 323–38.

Visser, M., Scholte, M. and Scheepers, P. (2013), 'Fear of Crime and Feelings of Unsafety in European Countries: Macro and Micro Explanations in Cross-National Perspective', *The Sociological Quarterly*, 54: 278–301.

Williams, M. L. (2016), 'Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level', *The British Journal of Criminology*, 56: 21–48.

Wilsem, J. van. (2013). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, 29: 437–53. doi: 10.1177/1043986213507402

Wyant, B. R. (2008), 'Multilevel Impacts of Perceived Incivilities and Perceptions of Crime Risk on Fear of Crime: Isolating Endogenous Impacts', *Journal of Research in Crime and Delinquency*, 45: 39–64. doi: 10.1177/0022427807309440

Yar, M. (2005), 'The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory', *European Journal of Criminology*, 2: 407–27.

Yu, S. (2014), 'Fear of Cyber Crime Among College Students in the United States: An Exploratory Study,' *International Journal of Cyber Criminology'*, 8: 36–46.