

August 2025

Does cybercrime indicate serious offending behavior? A cross-national comparative analysis of cybercrime severity

Janne Joonas Vepsäläinen
Tampere University, janne.vepsalainen@tuni.fi

Markus Kaakinen
University of Helsinki, markus.kaakinen@helsinki.fi

Atte Oksanen
Tampere University, atte.oksanen@tuni.fi

Iina Savolainen
Tampere University, iina.savolainen@tuni.fi

Anna Markina
University of Tartu, anna.markina@ut.ee

See next page for additional authors

Follow this and additional works at: <https://aisel.aisnet.org/amcis2025>

Recommended Citation

Vepsäläinen, Janne Joonas; Kaakinen, Markus; Oksanen, Atte; Savolainen, Iina; Markina, Anna; Løvschall Langeland, Camilla; Meško, Gorazd; Povh, Iza Kokoravec; and Valdimarsdóttir, Margrét, "Does cybercrime indicate serious offending behavior? A cross-national comparative analysis of cybercrime severity" (2025). *AMCIS 2025 Proceedings*. 37.
https://aisel.aisnet.org/amcis2025/sig_sec/sig_sec/37

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2025 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Presenter Information

Janne Joonas Vepsäläinen, Markus Kaakinen, Atte Oksanen, Iina Savolainen, Anna Markina, Camilla Løvschall Langeland, Gorazd Meško, Iza Kokoravec Povh, and Margrét Valdimarsdóttir

Does cybercrime indicate serious offending behavior? A cross-national comparative analysis of cybercrime severity

Completed Research Full Paper

Janne Vepsäläinen
Tampere University
janne.vepsalainen@tuni.fi

Markus Kaakinen
University of Helsinki
markus.kaakinen@helsinki.fi

Atte Oksanen
Tampere University
atte.oksanen@tuni.fi

Iina Savolainen
Tampere University
iina.savolainen@tuni.fi

Anna Markina
University of Tartu
anna.markina@ut.ee

Camilla Løvschall Langeland
University of Oslo
c.l.langeland@jus.uio.no

Gorazd Meško
University of Maribor
gorazd.mesko@um.si

Iza Kokoravec Povh
University of Maribor
iza.kokoravec@um.si

Margrét Valdimarsdóttir
University of Iceland
margretva@hi.is

Marina Rezende Bazon
University of São Paulo
mbazon@ffclrp.usp.br

Neal Hazel
University of Salford
n.hazel@salford.ac.uk

Noora Ellonen
Tampere University
noora.ellonen@tuni.fi

Abstract

Despite the growing importance of cybercrime, its severity compared to offline crime is unclear. This study used data from the representative International Self-Report Delinquency Study (N = 28,325) to compare four cybercrimes—hacking, cyberfraud, cyberhate, and online sexual abuse—with offline crimes among 13–17-year-olds in Europe and South America. Item Response Theory was used to analyze the criminal behavior indicated by cybercrimes compared to offline crimes and their effectiveness in distinguishing between young individuals with high and low levels of delinquency. The results show that although cybercrime offending indicate relatively serious criminal behavior, traditional crimes more accurately differentiate between young people with different levels of criminal behavior. These patterns are observed in both continents, with some differences. This study has implications for anti-cybercrime policies.

Keywords

Item Response Theory, cybercrime, adolescents.

Introduction

The significant decline in crime in the Global North that began in the early 1990s has been partly attributed to shift in technology-mediated lifestyles (Farrell & Birks, 2018; Miró-Llinares & Moneva, 2019; Bossler & Berenblum, 2019). While advances in security technologies (Farrell, 2022) and changes in time use (Vilhelmson et al., 2018) have reduced vulnerability to traditional crime, the risks of virtual abuse have risen as more interactions rely on information and communication technologies (ICT). This is reflected in a simultaneous drop in conventional offline crime and an increase in cybercrime (Bossler & Berenblum, 2019; Smith & Stamatakis, 2020; Tcherni et al., 2016). The shift is particularly pronounced among young people, making adolescents a key demographic for cybercrime research (Maras et al., 2024; Peterson & Densley, 2017).

Cybercrime is an umbrella term that covers various acts often categorized as either cyber-enabled or cyber-dependent crimes (Choi et al., 2020). Cyber-enabled crimes are traditional crimes that have been adopted in online environments, such as online harassment. In contrast, cyber-dependent crimes, such as hacking, exist only in digital environments. While all these acts involve ICT, they differ in nature, targets, and technological skills required. Some cybercrimes are widely accessible and easy to commit (e.g., hate speech) as some are more sophisticated “high-tech” cybercrimes (e.g., ransomware) (van der Wagen & Pieters, 2020).

While the focus of crime has shifted from offline to online, the relationship between cybercrime and traditional crime remains unclear in many respects. The debate over whether cybercrime is a distinct form of crime makes it difficult to understand its nature as opposed to offline crime (Smith & Stamatakis, 2020; Payne, 2020). According to the well-known “old wine in a new bottle” statement, cybercrime is a conventional criminality carried out in a technological context and can therefore be explained as offline crime (Grabosky, 2001). On the other hand, cybercrime is qualitatively different from offline crime in many respects. For example, spatial distance (Tcherni et al., 2016), a heightened level of anonymity (Chetry & Sharma, 2023), and the ability to simultaneously target multiple human victims and technical/virtual elements (van der Wagen & Pieters, 2020) are unique for cybercrime.

Research has identified both unique and shared characteristics between cybercrime and traditional crime (Maras et al., 2024; Weulen Kranenbarg et al., 2019; Kaakinen et al., 2024), but how cybercrime offending reflects the seriousness of individual criminal behavior remains unclear (Fissel & Lee, 2023; Breen et al., 2022). Criminal behavior is often defined as an individual trait reflected in varying levels of criminal acts (Moffitt, 1993). However, the empirical challenges of comparing cybercriminals with offline offenders (Weulen Kranenbarg, 2021) and the limitations of common measures of criminal behavior (Osgood et al., 2002) make it unclear whether cybercrime indicates higher or lower levels of criminal behavior than offline crime.

This study uses Item Response Theory (IRT) and large cross-national survey data from 12 countries from Europe and South America to examine the relative seriousness of cybercrime compared to offline crimes among adolescents. Focusing on hacking (Holt et al., 2020), cyberfraud (Reep-van den Bergh & Junger, 2018), online hate speech (Kaakinen et al., 2020), and image-based sexual abuse (Henry et al., 2018), we assess how these offenses relate to individual level of criminal behavior and their effectiveness in distinguishing between individuals with high and low levels of criminal behavior compared to offline crimes.

Our study focuses on adolescents, a key group for cybercrime research, as both general and cybercrime offending peak during this age period (Maras et al., 2024; Moffitt, 1993). Studying its relative seriousness with survey data can aid prevention, especially since self-reports address underreporting in administrative data (van de Weijer et al., 2019). As crime severity varies by demographics (Conrad et al., 2010) and culture (Henshel et al., 2016), we compare cybercrime in Europe and South America, where inequality and ICT access may shape offending patterns. Growing attention to human factors in cybersecurity has also increased interest in cybercrime victimization within HCI research to design safer digital environments (Al-Khater et al., 2020; Baror et al., 2021).

Measuring cybercrime seriousness

Crimes vary in seriousness, but empirically modeling this hierarchy is complex. Studies show that both law enforcement (Holt & Bossler, 2012) and the public (Fissel & Lee, 2023) view cybercrime as less serious than offline crime. This is likely due to its spatial remoteness and lack of direct physical violence, contributing to the notion that cybercrime is often perceived as victimless (Tcherni et al., 2016; Fissel & Lee, 2023). Perceptions of cybercrime are also shown to be influenced by misconceptions and technological familiarity and further clouded by its rapidly evolving nature (Fissel & Lee, 2023).

Crimes can also be evaluated based on their cost, but the financial impact of cybercrime, while significant, is difficult to quantify due to a large variation between data sources (Smith & Stamatakis, 2020; Dodge & Burruss, 2020). Moreover, monetary loss does not capture the human experience. Cybercrime victims experience psychological distress, insecurity, and uncompensated financial loss, but these human impacts are not reflected in official estimates of cybercrime cost (Borwell et al., 2022; Dreißigacker et al., 2024; Kaakinen et al., 2018). On the other hand, while victims' perspectives are crucial, the seriousness of different crimes can't be compared solely based on subjective experiences.

Measuring cybercrime seriousness is further complicated by country-level differences. Culture, ICT availability, and socioeconomic factors all influence cybercrime (Henshel et al., 2016; Chen et al., 2023). These factors may contribute to culture-specific cybercriminal behavior, where cybercrime is associated with more serious criminal behavior in some countries but is a low-threshold crime in others, highlighting the need for cross-national studies of cybercrime.

Multi-item measures of self-reported offending are most widely used methods for assessing individual level of criminal behavior (Osgood et al., 2002), but by simply summing different offences they don't capture the differences in seriousness between different crime types (Conrad et al., 2010). They also tend to over-represent minor offences, which are more common and therefore more likely to be reported (Conrad et al., 2010). Researchers have turned to linear hierarchical measures like IRT to address these challenges in measuring criminal behavior (Piquero et al., 2002; Conrad et al., 2010; Osgood et al., 2002). IRT models the relationship between individuals' underlying latent traits and their probability of responding in a certain way to specific survey items reflecting that trait. Criminologists have adapted this method to rank self-reported offenses on a common scale, overcoming limitations of traditional crime measures (e.g. Piquero et al., 2002). However, it has not yet been used to compare the seriousness of cybercrime and offline crime.

Research questions

While cybercrime is increasingly relevant form of crime, its relationship to traditional crime remains unclear. To address current methodological limitations of crime measurements, we use IRT and representative city samples of adolescents from Europe and South America to compare the relative severity of cybercrimes and traditional crimes through the following research questions:

RQ1: What is the level of criminal behavior indicated by cybercrimes compared to offline crimes?

RQ2: How effectively do cybercrimes discriminate between young individuals with high and low levels of criminal behavior?

RQ3: Are there differences in the level of criminal behavior indicated by cybercrimes and their ability to discriminate between young individuals with different levels of criminal behavior between Europe and South America?

Data and Methods

Data

This study uses cross-national survey data from the fourth International Self-Report Delinquency Study (ISRD4), which began data collection in 2022. The respondents were school children aged 13–17 (N=28,325, 51% male, Mage = 15.01, SD = .007) from 12 countries: Argentina, Brazil, Venezuela, Finland,

Denmark, Sweden, Norway, Iceland, Lithuania, Estonia, the United Kingdom, and Slovenia. Standardized questionnaires were administered to school classes sampled from two cities per country, resulting in representative city samples of adolescents. Further details on data collection and sampling can be found in the ISRD4 study protocol (Marshall et al., 2022).

Measures

Fourteen items were used to measure respondents' crime experiences. These were sharing an intimate image/video of a person online without the person's consent (hereafter referred to as image-based sexual abuse), online hate speech (hereafter referred to as cyberhate), duping or deceiving someone online (hereafter referred to as cyberfraud), hacking, robbery, carrying a weapon, participating in a group fight, assault, shoplifting, burglary, car/motorcycle theft, graffiti painting, damaging property, and selling drugs. All questions had binary response options (0 = *no*, 1 = *yes*), with positive responses followed by a frequency question for the past 12 months ("*How many times in the last 12 months? If never, write '0.'*"). Based on these responses, a binary 12-month prevalence variable was created for each offense, indicating whether the respondents had committed each offense at least once in the past year.

Statistical analyses

We applied two-parameter logistic model (2PLM) of IRT to compare cybercrime severity to offline crime (Ackerman et al., 2023). In social sciences, unobservable phenomena like criminal behavior are called latent traits, often inferred from survey responses using instruments designed to measure these traits (Ackerman et al., 2023). IRT models the relationship between a latent trait (denoted by θ) and the likelihood of endorsing specific items. Since θ don't have any intrinsic scale of measurement, it is interpreted through standardized normal distribution, where most respondents are clustered around 0 and only 1.3% is more than 2.5 units away from 0 (Osgood et al., 2002; Samejima, 1969). This artificial scale allows respondents to be assigned a location on the scale corresponding their individual level of θ (in this case, level of criminal behavior). Respondents at different locations on the θ scale have different probabilities of endorsing the items from which θ is derived, as the likelihood of endorsement increases with the level of the latent trait.

The key parameters of IRT are difficulty (b) and discrimination (a). The b parameter refers to the location on the θ scale where the probability of endorsing the item exceeds .5. Higher b values indicate more "difficult" items, as higher θ levels are required for them to be endorsed. The a parameter reflects how well an item discriminates between individuals at different levels of θ (Osgood et al., 2002). Higher values indicate a greater increase in response probability as θ increases. These parameters can be plotted to Item Characteristic Curves (ICCs), which visually depict the probability of endorsing an item at different levels of the latent trait.

The b parameter was interpreted as relative seriousness of an offense, as higher b values indicated that a higher level of criminal behavior was required for endorsement. The a parameter provided insight into which offenses best distinguished serious criminal behavior among youth. To compare items, we assessed the overlap of 83.4% confidence intervals (CIs; reported only in text). No overlap indicated that the items differed at a significance level of $p < .05$ (Knol et al., 2011). Multiple-group IRT models were used to examine differential item functioning (DIF) between European and South American adolescents. Here, we first constrained all item parameters to be equal across regions, then estimated an alternative model allowing cybercrime parameters to vary and compared model fit using a likelihood ratio test. DIF in the b parameter would suggest that committing a cybercrime requires different levels of criminal behavior in each region, while DIF in the a parameter would indicate differences in how well cybercrimes discriminate between low and high delinquent youth across regions. The IRT analyses assumed that a single latent trait accounted for response behavior across the selected items (Ackerman et al., 2023). For all statistical analyses, we used Stata 17.0 statistical software.

Results

To test the suitability of the variable set for IRT, we conducted a confirmatory factor analysis, where all items loaded onto a single factor with acceptable fit ($\chi^2(77) < 0.001$, RMSEA = .055, SRMR = .042), allowing

us to proceed with the analysis. Table 1 reports the difficulty parameters (*b*) and the discrimination parameters (*a*) for cybercrimes and offline crimes. The results are presented in three models: results for the full sample (Model 1) and the European (Model 2) and South American (Model 3) subsamples. For Models 2 and 3, only results for cybercrimes are shown, as other variables are held constant across regions to highlight differences in cybercrime.

Analyses with full data (Table 1) showed that cyberhate ($b = 2.50$, 83.4% CI [2.42, 2.60], $p < .001$) had the lowest *b* value among cybercrimes and differed statistically significantly from all other cybercrimes in severity (no overlapping CIs). However, its confidence intervals overlapped with offline crimes like drug selling and assault, making it comparable to crimes often considered serious. Hacking ($b = 2.71$, 83.4% CI [2.62, 2.80], $p < .001$), cyberfraud ($b = 2.71$, 83.4% CI [2.62, 2.81], $p < .001$), and image-based sexual abuse ($b = 2.85$, 83.4% CI [2.76, 2.95], $p < .001$) had overlapping confidence intervals with each other and ranked similarly to robbery and burglary, leaving them only behind car/motorcycle theft in terms of severity. Notably, the threshold for committing even minor crimes is high for youth, as even shoplifting, the least serious crime studied, had a relatively high item difficulty.

Table 1: The results of Item Response Theory analysis for the entire sample and the European and South American subsamples.

	Model 1: Total		Model 2: Europe		Model 3: South America	
	(<i>b</i>)	(<i>a</i>)	(<i>b</i>)	(<i>a</i>)	(<i>b</i>)	(<i>a</i>)
<i>Cybercrime</i>						
Cyberhate	2.50	1.65	2.44	1.71	2.50	1.88
Hacking	2.71	1.95	2.75	2.16	2.19	2.23
Cyberfraud	2.71	2.24	2.67	2.31	2.55	2.65
Image-based sexual abuse	2.85	1.86	2.81	1.87	2.62	2.51
<i>Offline crime</i>						
Shoplifting	1.92	1.94	–	–	–	–
Carrying a weapon	2.07	2.09	–	–	–	–
Vandalism	2.13	2.63	–	–	–	–
Graffiti	2.14	2.10	–	–	–	–
Group fight	2.34	2.03	–	–	–	–
Selling drugs	2.44	2.52	–	–	–	–
Assault	2.55	3.09	–	–	–	–
Extortion/robbery	2.74	3.96	–	–	–	–
Burglary	2.76	3.63	–	–	–	–
Car/motorcycle theft	3.13	2.68	–	–	–	–
θ mean			0		0.35	
θ variance			1		0.58	

Note 1: All parameters were statistically significant at a significance level of $p < .001$.

Note 2: Offline crime parameters are omitted in models 2 and 3 as they are constrained to be equal across country groups.

Analyses of cybercrime discrimination based on the full sample showed that cyberhate ($a = 1.65$, 83.4% CI [1.57, 1.74], $p < .001$) had the lowest discrimination of all the items, with no overlapping confidence intervals. Image-based sexual abuse ($a = 1.86$, 83.4% CI [1.76, 1.97], $p < .001$) and hacking ($a = 1.95$, 83.4% CI [1.85, 2.06], $p < .001$) also had low discrimination, comparable to shoplifting and group fighting. Cyberfraud ($a = 2.24$, 83.4% CI [2.11, 2.38], $p < .001$) had the highest *a* value among cybercrimes and was comparable, for example, group fighting, carrying a weapon and graffiti painting. However, offline crimes such as robbery, burglary, assault, and car/motorcycle theft discriminated between respondents at different levels of criminal behavior far more accurately than any cybercrime studied.

The results of the country group differences are visualized in Figure 1 as ICCs, illustrating the probability of endorsing each cybercrime at different levels of criminal behavior. Cyberhate and cyberfraud followed similar patterns across regions. However, hacking was associated with higher levels of criminal behavior in Europe ($b = 2.75$, 83.4% CI [2.66, 2.84], $p < .001$) than in South America ($b = 2.19$, 83.4% CI [2.078, 2.32],

$p < .001$), with no overlapping confidence intervals, indicating a regional difference in hacking severity. Additionally, image-based sexual abuse was less effective in discriminating individuals with different levels of criminal behavior in Europe ($a = 1.87$, 83.4% CI [1.75, 1.98], $p < .001$) than in South America ($a = 2.51$, 83.4% CI [2.13, 2.89], $p < .001$), as shown by a steeper ICC in South America. To formally assess differential item functioning, we conducted a likelihood ratio test, comparing an unconstrained model to one where all item parameters, except for cybercrimes, were constrained to be equal across country groups. The test result ($p < .001$) indicated statistically significant difference in cybercrime items between Europe and South America, further confirming differences in the severity of hacking and the discrimination of image-based sexual abuse.

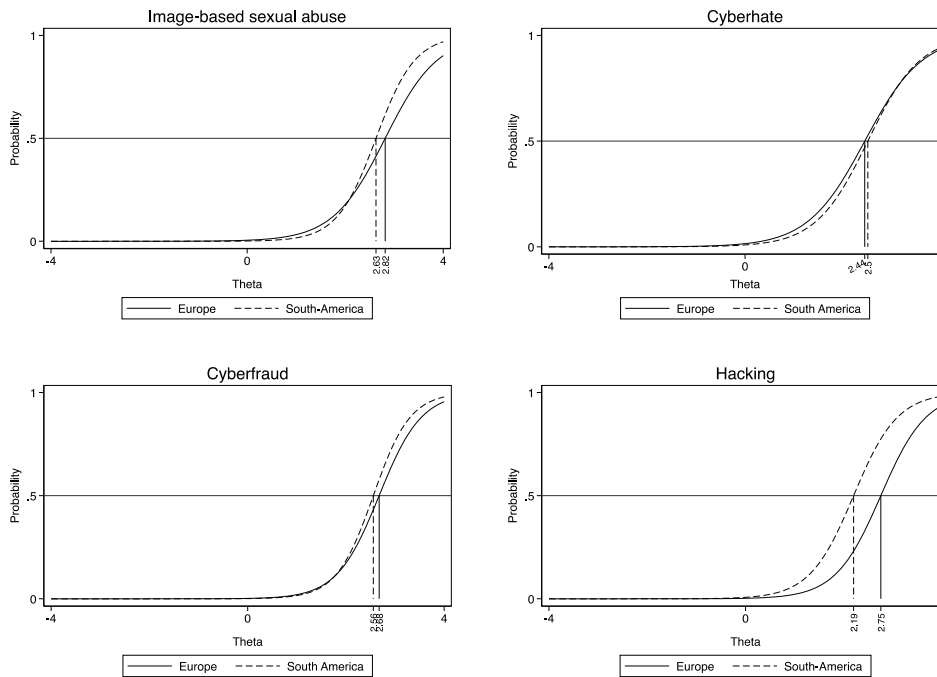


Figure 1: Item Characteristic Curves of the European and South American cybercrime survey items

Discussion

This study examined the relative seriousness of cybercrimes (hacking, cyberfraud, cyberhate, and image-based sexual abuse) compared to traditional offline crimes among 13–17-year-old adolescents in Europe and South America using IRT. The first research question concerned the level of criminal behavior indicated by cybercrimes compared to offline crimes. Our results suggest that cybercrimes are among the offenses that require the highest levels of criminal behavior. Cybercrimes, particularly hacking, cyberfraud, and online image-based sexual abuse, were comparable in seriousness to offline crimes like robbery and burglary. Cyberhate was less serious but still aligned with offenses like assault.

Our second research question looked at the ability of cybercrime to discriminate respondents at different levels of criminal behavior. Our findings show that cybercrimes were less effective at differentiating individuals with varying levels of criminal behavior than offline crimes. This suggests that while cybercrime generally indicates serious criminal behavior, its likelihood does not increase as sharply with higher levels of criminal behavior as it does for many offline crimes. Thus, crimes like assault, robbery, and burglary are more effective at identifying youth with serious criminal behavior.

Our final research question examined differences in cybercrime severity between Europe and South America. Hacking was associated with higher levels of criminal behavior among European adolescents, while image-based sexual abuse more accurately distinguished adolescents with different levels of criminal behavior in South America. Cyberhate and cyberfraud showed consistent patterns across both regions.

Cybersecurity professionals often possess strong technical skills but lack criminological insight needed to effectively prevent cybercrime (Ho et al., 2022). HCI research has similarly emphasized human factors in cybersecurity, aiding in anticipating attacker behavior, identifying vulnerabilities, and enhancing defence strategies (Henshel et al., 2016). Our findings suggest cybercrimes are not widespread, low-threshold offenses but are primarily committed by adolescents indicating serious criminal behavior. Despite its anonymity (Chetry & Sharma, 2023) and low risk (Tcherni et al., 2016), cybercrime does not seem more attractive than offline crime to youth with lower levels of criminal behavior. We also observed differences among cybercrimes: hacking and cyberfraud tend to involve small group of highly delinquent individuals while hate speech is a relatively lower-threshold offense. This supports prior findings that hacking is often organized and severe (Dodge & Burruss, 2020; Borwell et al., 2022), whereas cyberhate is socially driven (Kaakinen et al., 2020). Although cybercrimes can have serious impacts, they are often viewed as less severe than offline crimes (Payne, 2020; Fissel & Lee, 2023). Since resource allocation for crime prevention aligns more with perceived seriousness than crime frequency (Leukfeldt & Holt, 2022), our findings can guide policy, prevention, and safer ICT system design.

While cybercrime generally signals serious criminal behavior, its ability to discriminate between youth with different levels of criminal behavior is limited, making traditional offline crimes more effective indicators for identifying high-risk youth. This aligns with prior research showing that many cybercriminals specialize in cybercrime, unlike offline offenders who engage in diverse criminal behavior, suggesting cybercrime is not reliable indicator of broad and serious crime offline (Leukfeldt & Holt, 2022). However, some cybercrimes, such as cyberfraud, were more predictive of serious delinquency. Previous research has highlighted the limitation of cybersecurity controls targeting cybercrime broadly rather than specific cybercrimes and our findings could inform targeted prevention strategies and risk assessment tools (Ho et al., 2022; Henshel et al., 2016). Additionally, the rise of cybercrime necessitates further research to refine detection methods, including machine learning and algorithm-based investigations (Singh et al., 2024; Al-Khater et al., 2020; Rasmi & Jantan, 2013).

Regional differences were also found supporting previous findings on the potential cultural and technological influences on cybercriminal behavior (Kaakinen et al., 2024; Dodge & Burruss, 2020). However, youth with lower-level criminal behavior engaged in hacking less in Europe than in South America, suggesting IRT access alone does not explain seriousness of cybercrime, pointing instead to qualitative regional differences in hacking-related crimes (van der Wagen & Pieters, 2020). This highlights the need for culturally adaptive prevention and security measures (Chen et al., 2023). Understanding these patterns can help HCI professionals and developers create region-specific security solutions and crime prevention strategies.

While this study was based on representative data and robust methods, it also has limitations. First, it is important to note that the country samples are not nationally representative, as in most of the participating countries data were collected from two major cities. Therefore, the comparisons reflect differences between the urban areas of the participating countries, not between entire countries. Moreover, some variability in sampling designs across countries further affects comparability (see more in Marshall et al., 2022). The sample was also limited to adolescents in Europe and South America, making it uncertain whether the findings generalize to adults or other regions. Also, IRT provides a statistical approach to ranking crime severity but does not account for other relevant factors, such as legal frameworks, victim perspective, or financial harm. Despite these limitations, the study provides a valuable framework for assessing cybercrime severity and highlights the need for further research on cybercrime trends.

Conclusion

This IRT-based study of 12 countries in Europe and South America shows that cybercrime is an indicator of serious criminal behavior among young people. However, many offline crimes, such as assault, burglary, and robbery, are more accurate in discriminating between young people with different levels of criminal behavior. Moreover, the relative seriousness of different cybercrimes exhibits regional differences, with hacking being associated with higher levels of criminal behavior among European adolescents, while image-based sexual abuse more effectively discriminated between adolescents at different levels of criminal behavior in South America. This study offers new insights into the seriousness of cybercrime relative to

offline crime, highlighting differences in cybercrime severity across cultural contexts. Overall, the higher prevalence of certain cybercrimes, such as hacking, does not seem to suggest that young people engage in them due to their ease but rather indicates the organized nature of most cybercrimes. These findings underscore the need for early intervention and prevention strategies to deter youth from prolonged cybercriminal careers, complemented by culturally and crime-specific cybersecurity solutions.

REFERENCES

- Ackerman, T., Ma, Y., Ma, M., Pacico, J. C., Wang, Y., & Xu, G. (2023). Item response theory. In R. J. Tierney, F. Rizvi, & K. Ercikan (Eds.), *International Encyclopedia of Education (Fourth Edition)* (pp. 72–85). Elsevier. <https://doi.org/10.1016/B978-0-12-818630-5.10010-7>
- Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, 8, 137293–137311. <https://doi.org/10.1109/ACCESS.2020.3011259>
- Baror, S. O., Venter, H. S., & Adeyemi, R. (2021). A natural human language framework for digital forensic readiness in the public cloud. *Australian Journal of Forensic Sciences*, 53(5), 566–591. <https://doi.org/10.1080/00450618.2020.1789742>
- Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review*, 40(4), 933–954. <https://doi.org/10.1177/0894439320983828>
- Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime & Justice*, 42(5), 495–499. <https://doi.org/10.1080/0735648X.2019.1692426>
- Breen, C., Herley, C., & Redmiles, E. M. (2022). A large-scale measurement of cybercrime against individuals. In *Proceedings of the ACM Conference* (pp. 1–41). ACM. <https://doi.org/10.1145/3491102.3517613>
- Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities & Social Sciences Communications*, 10(1), 71–10. <https://doi.org/10.1057/s41599-023-01560-x>
- Chetry, A., & Sharma, U. (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *International Journal of Experimental Research and Review*, 32, 195–205. <https://doi.org/10.52756/ijerr.2023.v32.017>
- Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 27–43). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_2
- Conrad, K. J., Riley, B. B., Conrad, K. M., Chan, Y. F., & Dennis, M. L. (2010). Validation of the Crime and Violence Scale (CVS) against the Rasch Measurement Model including differences by gender, race, and age. *Evaluation Review*, 34(2), 83–115. <https://doi.org/10.1177/0193841X10362162>
- Dodge, C., & Burruss, G. (2020). Policing cybercrime: Responding to the growing problem and considering future solutions. In *The Human Factor of Cybercrime* (pp. 339–358). Routledge.
- Dreißigacker, A., Müller, P., Isenhardt, A., & Schemmel, J. (2024). Online hate speech victimization: Consequences for victims' feelings of insecurity. *Crime Science*, 13(1), 4–13. <https://doi.org/10.1186/s40163-024-00204-y>
- Farrell, G. (2022). Forty years of declining burglary in the United States: Explanation and evidence relating to the security hypothesis. *Security Journal*, 35(2), 444–462. <https://doi.org/10.1057/s41284-021-00284-4>
- Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop? *Crime Science*, 7(1), 8–14. <https://doi.org/>

- Fissel, E. R., & Lee, J. R. (2023). The cybercrime illusion: Examining the impact of cybercrime misbeliefs on perceptions of cybercrime seriousness. *Journal of Criminology*, 56(2/3), 150–169. <https://doi.org/10.1177/26338076231174639>
- Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243–249. <https://doi.org/10.1177/a017405>
- Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice & Research*, 19(6), 565–581. <https://doi.org/10.1080/15614263.2018.1507892>
- Henshel, D., Sample, C., Cains, M., & Hoffman, B. (2016). Integrating cultural factors into human factors framework and ontology for cyber attackers. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (pp. 123–137). Springer International Publishing. https://doi.org/10.1007/978-3-319-41932-9_11
- Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, 115, 102611. <https://doi.org/10.1016/j.cose.2022.102611>
- Holt, T. J., & Bossler, A. M. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking*, 15(9), 464–472. <https://doi.org/10.1089/cyber.2011.0625>
- Holt, T. J., Navarro, J. N., & Clevenger, S. (2020). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime and Delinquency*, 66(11), 1533–1555. <https://doi.org/10.1177/001128719875697>
- Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 129–137. <https://doi.org/10.1089/cyber.2016.0728>
- Kaakinen, M., Sirola, A., Savolainen, I., & Oksanen, A. (2020). Impulsivity, internalizing symptoms, and online group behavior as determinants of online hate. *PloS one*, 15(4). <https://doi.org/10.1371/journal.pone.0231052>
- Kaakinen, M., Vauhkonen, T., Vepsäläinen, J., & Räsänen, P. (2024). From online hate speech to offline hate crime? Testing individual-level associations with a nationally representative sample of adolescents aged 15-17. In J. Hawdon, & M. Costello (Eds.), *Research Handbook on Hate and Hate Crimes in Society* (pp. 250-262). Edward Elgar. <https://doi.org/10.4337/9781803925738.00021>
- Knol, M. J., Pestman, W. R., & Grobbee, D. E. (2011). The (mis)use of overlap of confidence intervals to assess effect modification. *European Journal of Epidemiology*, 26(4), 253–254. <https://doi.org/10.1007/s10654-011-9563-8>
- Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, 126, 106979. <https://doi.org/10.1016/j.chb.2021.106979>
- Maras, K., Sweiry, A., Villadsen, A., & Fitzsimons, E. (2024). *Computers in Human Behavior*, 151, 108011. <https://doi.org/10.1016/j.chb.2023.108011>
- Marshall, I., Birkbeck, C., Enzmann, D., Kivivuori, J., Markina, A., & Steketee, M. (2022). International Self-Report Delinquency (ISR4) study protocol: Background, methodology, and mandatory items for the 2021/2022 survey. Northeastern University. https://www.ssoar.info/ssoar/bitstream/handle/document/78879/ssoar-2022-marshall_et_al-International_Self-Report_Delinquency_ISR4_Study.pdf
- Miró-Llinares, F., & Moneva, A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “Did cybercrime cause the crime drop?” *Crime Science*, 8(1), 1–5. <https://doi.org/10.1186/s40163-019-0107-y>

- Moffitt, T. E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review*, 100(4), 674–701. <https://doi.org/10.1037/0033-295X.100.4.674>
- Osgood, D. W., McMorris, B. J., & Potenza, M. T. (2002). Analyzing multiple-item measures of crime and deviance I: Item response theory scaling. *Journal of Quantitative Criminology*, 18(3), 267–296. <https://doi.org/10.1023/A:1016008004010>
- Payne, B. K. (2020). Defining cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 3–25). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_1
- Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? *Aggression and Violent Behavior*, 34, 193–200. <https://doi.org/10.1016/j.avb.2017.01.012>
- Piquero, A. R., MacIntosh, R., & Hickman, M. (2002). The validity of a self-reported delinquency scale: Comparison across gender, age, race, and place of residence. *Sociological Methods & Research*, 30(4), 492–524. <https://doi.org/10.1177/0049124102030004002>
- Rasmi, M., & Jantan, A. (2013). A new algorithm to estimate the similarity between the intentions of cyber crimes for network forensics. *Procedia Technology*, 11, 540–547. <https://doi.org/10.1016/j.protcy.2013.12.226>
- Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, 7(1), 1–15. <https://doi.org/10.1186/s40163-018-0079-3>
- Samejima, F. (1969). Estimation of latent ability using a response pattern of graded scores. *Psychometrika*, 34(4P2), 1–97. <https://doi.org/10.1007/BF02290599>
- Singh, R., Sellitto, D., & Smith, S. D. (2024). An investigation of the role of cybersecurity professionals in shaping AI integration and strategy. *AMCIS 2024 Proceedings*, 29. <https://aisel.aisnet.org/amcis2024/security/security/29>
- Smith, T., & Stamatakis, N. (2020). Defining cybercrime in terms of routine activity and spatial distribution: Issues and concerns. *International Journal of Cyber Criminology*, 14(2), 433–459. <https://doi.org/10.5281/zenodo.4769989>
- Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, 33(5), 890–911. <https://doi.org/10.1080/07418825.2014.994658>
- van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, 17(4), 480–497. <https://doi.org/10.1177/1477370818812016>
- van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 16(4), 486–508. <https://doi.org/10.1177/1477370818773610>
- Vilhelmson, B., Ellmér, E., & Thulin, E. (2018). What did we do when the Internet wasn't around? Variation in free-time activities among three young-adult cohorts from 1990/1991, 2000/2001, and 2010/2011. *New Media & Society*, 20(8), 2898–2916. <https://doi.org/10.1177/1461444817737296>
- Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only, and the victimization-offending overlap. *Deviant Behavior*, 40(1), 40–55. <https://doi.org/10.1080/01639625.2017.1411030>
- Weulen Kranenbarg, M. (2021). The challenges of empirically comparing cybercriminals and traditional offenders. In *Researching Cybercrimes* (pp. 107–126). Springer International Publishing. https://doi.org/10.1007/978-3-030-74837-1_6