Asian Journal of Applied Economics Vol. 32 No. 1 (January-June 2025): 30-57

Copyright © 2025 Center for Applied Economics Research

ISSN: 2985-1610 (Online)

Received: 30 October 2024

Received in revised form: 25 December 2024

Accepted: 3 January 2025

Socioeconomic Determinants of Cybercrime Costs: A Panel Data Analysis of OECD Countries

Nitiphong Songsrirote*

Mahasarakham Business School, Mahasarakham University, Thailand

Abstract

Cybercrime imposes significant financial burdens on economies, yet its relationship with socioeconomic factors remains underexplored. This study examines how key socioeconomic determinants influence cybercrime costs across 33 OECD countries from 2012 to 2023. Using a Random Effects model with Generalized Least Squares (GLS) estimation, the analysis identifies key drivers of cybercrime-related expenditures. The findings reveal two counterintuitive relationships: higher household debt and greater internet penetration are associated with lower cybercrime costs, suggesting that economic constraints and digital connectivity may reduce exposure to cyber threats. Additionally, a higher Corruption Perception Index (CPI)—which indicates lower corruption—is linked to increased cybercrime costs, possibly due to governance complacency or increased digital activity in well-regulated economies. These results challenge conventional assumptions about economic vulnerability and cybersecurity risks. The study underscores the need for targeted cybersecurity education, stronger institutional frameworks, and proactive investment in cyber resilience to mitigate financial losses. Policymakers should address economic constraints, promote digital literacy, and ensure cybersecurity measures evolve alongside governance improvements.

Keywords: cybercrime; cost of cybercrime; socioeconomic factors; household debt; corruption

JEL Classification: K42; D73; O15

*Corresponding Author, Address: Mahasarakham Business School, Mahasarakham University, Khamriang Sub-District, Kantarawichai District, Maha Sarakham, 44150, Thailand, Email: nitiphong.s@msu.ac.th

1. Introduction

Cybercrime constitutes a considerable financial burden for both individuals and enterprises within OECD member states, with expenses increasing due to the escalating frequency and complexity of cyber threats. The estimated global financial impact of cybercrime is believed to range between $375 billion and $575 billion annually, thus surpassing the gross domestic product of many countries (Stewart, 2016). This economic burden is not solely borne by corporations, but also by individual victims who endure various forms of cybercrime, including online fraud and identity theft. Within European context, victimization surveys illustrate that the incidence of cybercrime, encompassing online shopping fraud and hacking, impacts a significant fraction of the population, with malware victimization rates ranging from 2% to 15% (Reep-van den Bergh & Junger, 2018). These criminal activities result in immediate financial losses alongside additional expenses related to recovery and mitigation efforts. For example, Italy documented $875 million in direct losses stemming from hacking, while incurring nearly $8.5 billion in recovery expenditures (Stewart, 2016). This underscores the extensive financial impact that cybercrime can impose on both individuals and national economies.

The economic impact of cybercrime extends beyond direct financial losses, influencing innovation and competitive dynamics within the marketplace. Cybercrime acts as a tax on innovation, reducing the return on investment for innovators and investors, consequently slowing global innovative progress (Stewart, 2016). This scenario is especially concerning OECD nations, where technological progress serves as a key driver of economic growth. The indirect costs associated with cybercrime, such as the need for enhanced cybersecurity protocols and the loss of consumer trust, further increase the financial pressures faced by businesses and individuals. In developed nations, the surge in online fraud has been pronounced, although it remains unclear whether this represents a shift from conventional crimes or indicates a new trend entirely (Levi, 2016). The lack of standardized metrics for measuring the comprehensive impact of cybercrime complicates efforts to quantify these costs; however, there is consensus that they are significant enough to require serious consideration and policy intervention (Levi, 2016).

A significant gap remains in understanding the complex relationship between specific socioeconomic variables and the financial effects of cybercrime, particularly within OECD member nations. While empirical studies have highlighted the rise of online fraud and its implications for national security, there is limited research on how variables such as the Household Debt-to-GDP ratio, GINI Coefficient, and Government Expenditure on Education relative to GDP influence the financial burden of cybercrime (Levi, 2016; Park et al., 2019). Moreover, the role of Internet Penetration Rate and National Cyber Security Index in moderating these costs remains understudied, despite evidence that technological capital and cybersecurity preparedness shape the frequency of cybercrime occurrences (Srivastava et al., 2020).

While the link between economic development and cybercrime has been established, the specific effects of unemployment rates and international tourist arrivals on cybercrime costs have not been thoroughly investigated.

Current econometric models have focused primarily on the fiscal impact of cybercrime through business disruption and information loss, without adequately addressing how these socioeconomic factors affect cost dynamics in developed economies (Kovalchuk et al., 2021). Additionally, the potential moderating influence of the Corruption Perception Index on the relationship between these socioeconomic parameters and cybercrime costs requires further study, as corruption can significantly affect the effectiveness of cybersecurity initiatives (Kshetri, 2006).

This study examines how various socioeconomic determinants—including household debt to GDP ratio, income disparity, unemployment levels, Internet accessibility, government investment in education, international tourist influx, levels of corruption, and cyber security Index—influence the financial costs of cybercrime in OECD member states. The aim is to analyze the impact of these determinants on cybercrime costs, using panel data and econometric methods to quantify relationships between the independent variables and cybercrime's financial implications. This research will identify which factors significantly influence cybercrime-related expenses and measure their impact. The key benefit of this study is providing policymakers and stakeholders with insights into the socioeconomic factors underlying cybercrime victimization. Understanding these relationships will help governmental bodies and organizations develop targeted interventions to reduce cybercrime's economic impact through improved cybersecurity initiatives, educational awareness campaigns, and addressing economic disparities that may increase cybercrime vulnerability. The findings will improve policymaking and help reduce the economic burden of cybercrime on society.

2. Literature Review

2.1 Background Theories

The social and economic factors affecting the cost of cybercrime, particularly regarding victimization, can be analyzed through various theoretical frameworks. These theories, primarily drawn from criminology, economics, and sociology, provide a comprehensive understanding of how socioeconomic variables influence both the experience and financial consequences of cybercrime victimization.

Routine Activities Theory (Cohen & Felson, 1979) provides a valuable framework for understanding the victimization phenomenon in cybercrimes. The theory identifies three essential components for criminal activities: a motivated offender, a suitable and unprotected target, and the absence of capable guardianship. These components interact to create conditions conducive to crime. Socioeconomic factors, including income level, education, and digital literacy, can significantly affect an individual's exposure to cybercrime risk. For example, individuals from lower-income groups may be unable to afford adequate cybersecurity protection, increasing their vulnerability to cyberattacks. Similarly, those with limited literacy or digital skills may fail to recognize potential cyber threats, making them likely targets. Victimization in these cases can severely impact victims' financial ability to recover from such crimes, potentially widening existing economic disparities.

The Theory of Social Structure and Anomie, developed by Merton (1938), provides crucial insights into the relationship between socioeconomic factors and cybercrime victimization. Merton argues that individuals from disadvantaged socioeconomic backgrounds are more likely to experience strain due to the disconnect between society's goals and their means of achievement. When applied to cybercrime, this strain theory suggests a higher incidence of both offenders and victims among disadvantaged groups. Those who are financially vulnerable, often from lower socioeconomic classes, may face greater victimization risks, while more affluent individuals typically have both better protection against victimization and greater resources for recovering from losses

Rational Choice Theory (Becker, 1968) provides an alternative framework for understanding victimization dynamics by examining both offender and victim decision-making processes. Through this theoretical lens, cybercrime victimization emerges as a calculated risk assessment, where socioeconomic factors influence the perceived costs and benefits for both perpetrators and targets. For example, individuals with fewer resources may underestimate cybercrime risks due to limited awareness or inability to secure their personal information. Conversely, higher-income individuals may face lower victimization rates as they invest more extensively in cybersecurity measures. However, when high-income individuals are victimized, the impact often extends beyond immediate financial losses to include reputational damage with potentially long-term economic consequences.

Social Capital Theory (Bourdieu, 1986) and related digital social capital theories illuminate how community networks and access to social resources influence individuals' vulnerability to cybercrime. Those with limited social capital, often from lower socioeconomic groups, typically have restricted access to support networks and resources crucial for recovery after cybercrime incidents. In contrast, individuals with substantial social capital benefit from stronger networks that can provide financial, emotional, and informational support following victimization. Consequently, cybercrime victims with limited social capital often face more severe impacts, lacking the resources to mitigate losses or prevent future incidents.

The combined frameworks of Strain Theory and Victimology further elucidate the relationship between socioeconomic factors and cybercrime victimization patterns. Research demonstrates that individuals experiencing financial stress, social inequality, or economic hardship face higher risks of cybercrime victimization (Ferguson, 2017). Their vulnerability in online spaces stems from insufficient resources for adequate cybersecurity protection. Beyond direct monetary losses, cybercrime victimization entails significant non-monetary costs, including emotional distress, time loss, and reputational damage—impacts that disproportionately affect individuals from lower socioeconomic backgrounds.

These theoretical frameworks collectively offer a comprehensive understanding of how socioeconomic factors influence both the likelihood of cybercrime victimization and its associated costs. This understanding is essential for developing targeted policies and interventions aimed at reducing cybercrime's impact on vulnerable populations.

2.2 Linking Variables to Theories

The key variables in this study—Cost of Cybercrime, Household Debt, Income Inequality, Unemployment, Corruption, Internet Penetration, Government Expenditure on Education, International Tourist Arrivals, and Cybersecurity—can be analyzed through various criminological and economic frameworks. Each variable's relationship to specific theories depends on how it illuminates aspects of cybercrime victimization. The following analysis examines how each variable correlates with relevant theoretical constructions.

2.2.1 The Cost of Cybercrime

The cost of cybercrime is fundamentally linked to Rational Choice Theory (Becker, 1968), which suggests that individuals engage in criminal behavior based on a systematic cost-benefit analysis. For potential cybercriminals, reduced perceived costs—due to anonymity, low detection risk, or limited legal consequences—may increase their likelihood of engaging in cyber attacks. For potential victims, the economic implications of cybercrime influence their vulnerability, especially when the cost of protective measures appears to outweigh the perceived benefits of prevention.

2.2.2 Household Debt

Household debt aligns with Merton's Strain Theory (Merton, 1938), which suggests that individuals or households under financial stress may become more vulnerable to cybercriminal activities. People with high debt levels often have fewer resources to invest in protective measures or cybersecurity systems, making them attractive targets for digital fraud. Additionally, the psychological pressure of economic hardship may increase the likelihood of individuals turning to online fraud as a means of financial relief or out of desperation.

2.2.3 Income Inequality

Income inequality creates a social divide where individuals from lower-income groups have limited access to cybercrime protection resources. According to Merton's Social Strain Theory (Merton, 1938), wealth disparities increase social tension, which in cybercrime manifests either increased victimization (due to insufficient resources for prevention and recovery) or as motivation for individuals from lower socioeconomic groups to engage in cybercriminal activities. Similarly, Routine Activities Theory (Cohen & Felson, 1979) suggests that economically disadvantaged individuals, having fewer protective resources, become more attractive targets for cybercriminals, thus increasing their vulnerability.

2.2.4 Unemployment

Unemployment is a key variable in Social Structure and Anomie Theory (Merton, 1938). When individuals face economic hardship due to unemployment, they become more vulnerable to cybercrime victimization because they lack the financial resources to protect themselves in the digital environment. Additionally, limited job opportunities may increase the likelihood of individuals turning to cybercrime as a means of economic survival, creating a cycle of victimization and criminal activity.

2.2.5 Corruption

Corruption weakens institutional effectiveness, including law enforcement and cybersecurity frameworks, making it harder to protect individuals against cybercrime and pursue justice. Social Capital Theory (Bourdieu, 1986) suggests that corruption erodes social trust and weakens social networks, making individuals more vulnerable to cybercriminal activities. Furthermore, Routine Activities Theory (Cohen & Felson, 1979) indicates that corruption reduces the availability of capable guardians (such as law enforcement and regulatory bodies), making it easier for cybercriminals to exploit potential victims.

2.2.6 Internet Penetration

The growth of internet access fundamentally increases the availability of potential targets, as described in Routine Activities Theory (Cohen & Felson, 1979). As internet connectivity expands, the pool of possible targets for cybercriminal activities grows. While increased internet usage creates opportunities for individuals and businesses, those lacking adequate digital literacy or cybersecurity measures become particularly vulnerable to victimization.

2.2.7 Government Expenditure on Education

Government investment in education directly relates to the development of digital literacy, which can be viewed as a form of social capital (Bourdieu, 1986), enhancing people's ability to recognize and resist cybercriminal activities. Well-funded educational programs, particularly those focusing on digital literacy, can reduce cybercrime victimization by addressing threat awareness for both potential victims and offenders. Through the lens of Rational Choice Theory (Becker, 1968), education increases potential offenders' awareness of consequences while reducing potential victims' vulnerability by providing essential cybersecurity knowledge.

2.2.8 International Tourist Arrivals

International tourist arrivals influence cybercrime vulnerability, especially in areas where tourists are perceived as wealthy or unaware of local cyber threats. Routine Activities Theory (Cohen & Felson, 1979) suggests that tourists often make ideal targets because they are unfamiliar with local cybersecurity risks, lack appropriate protective measures, and may not know local cybercrime patterns or available safeguards. Social Structure and Anomie Theory (Merton, 1938) also applies when tourists have economic advantages over residents, making them specific targets for cybercriminal activities.

2.2.9 Cybersecurity

Cybersecurity serves as a primary defense against cybercrime and is crucial in reducing victimization risk. Within Routine Activities Theory (Cohen & Felson, 1979), cybersecurity acts as a capable guardian, preventing criminals from successfully targeting individuals or organizations. Rational Choice Theory (Becker, 1968) suggests that individuals and organizations evaluate cybersecurity investment costs against potential benefits, particularly reduced victimization risk. Greater investment in cybersecurity decreases opportunities for criminals, thus reducing the likelihood of victimization.

2.3 Related Research

2.3.1 Cost of Cybercrime

The financial impact of cybercrime, especially regarding victimization, encompasses both measurable and intangible consequences for individuals and organizations. Cybercrime victimization represents harm suffered through illegal activities involving computer systems or networks, including identity theft, unauthorized access, and fraudulent schemes (Arifi & Arifi, 2024; Tonellotto, 2019). Beyond direct financial losses, victims experience significant psychological impacts, such as reduced feelings of safety and diminished trust in digital environments (Borwell et al., 2021).

Several factors influence victimization patterns, including demographic characteristics (age, gender, and digital literacy), technology types, and protective measures such as antivirus software (Ntsama et al., 2023). Theoretical frameworks, particularly the general theory of crime and the lifestyles/routine activities paradigm, emphasize how personal and contextual factors affect victimization. These theories indicate that low self-control and high-risk online behaviors increase cybercrime vulnerability (Ngo & Paternoster, 2011).

In this study, the cost of cybercrime is defined as the total impact—both tangible and intangible—on individuals and organizations from illegal activities involving computer systems or networks. This definition includes direct financial losses, psychological harm, and broader societal effects. Addressing these costs requires strengthening cybersecurity awareness and resilience (Arifi & Arifi, 2024; Tonellotto, 2019).

2.3.2 Household Debt and Cost of Cybercrime

The relationship between household debt and cybercrime victimization costs is shaped by interrelated financial and psychological factors. Victims of cybercrime experience financial losses that compound their existing household debt, creating additional financial strain when compensation is unavailable. These combined losses significantly impact victims' well-being (Borwell et al., 2021).

People with high household debt levels face heightened risk of substantial losses from specific forms of cybercrime, particularly online shopping fraud and banking/payment fraud (Reep-van den Bergh & Junger, 2018). The psychological impact is substantial, as victims struggle with the emotional distress of being unable to recover financial losses. This distress becomes more severe when victims are already managing significant household debt (Borwell et al., 2021).

Cases involving known perpetrators create particularly complex psychological challenges. The betrayal of trust compounds the financial impact, making recovery from economic hardship even more difficult. This interconnection between household debt and cybercrime consequences highlights the importance of developing both preventive measures and comprehensive victim support systems.

2.3.3 Income Inequality and Cost of Cybercrime

Income inequality plays a crucial role in determining both the costs and prevalence of cybercrime victimization, especially as financial technology (FinTech) and internet access expand. Growing income gaps increase cyber vulnerability for both individuals and organizations. This vulnerability is most apparent in the FinTech sector, where those with limited financial resources often cannot afford adequate cybersecurity protection, making them frequent targets of fraud, hacking, and other cybercrimes (Bakari et al., 2023).

Income inequality typically coincides with other socioeconomic challenges, including low educational attainment and high poverty rates, creating conditions conducive to cybercriminal activity. Regions with significant income disparities often show higher concentrations of cybercrime perpetrators, as economic inequality generates social tension and increases the likelihood of illegal activities (Park et al., 2019).

Lower-income victims experience particularly severe emotional and financial consequences from cybercrime. These individuals often suffer substantial financial losses without compensation, coupled with significant emotional distress. This pattern demonstrates how income inequality amplifies cybercrime's negative effects, especially for those with the fewest resources to recover from such incidents (Borwell et al., 2021).

2.3.4 Unemployment and Cost of Cybercrime

Unemployment significantly influences cybercrime's financial impact, particularly regarding victimization, through its connection to socioeconomic vulnerabilities that increase cyber threat exposure. Song et al. (2016) demonstrate that structural factors like unemployment correlate with higher cyber-theft victimization rates. Unemployed individuals often have limited access to secure online environments and typically rely on home internet usage, which is associated with increased victimization risk.

Despite government efforts to combat cybercrime, high unemployment rates contribute to increased cybercriminal activity, suggesting a strong link between economic distress and cybercrime prevalence (Manbe, 2014). Unemployment also increases vulnerability to identity theft, a costly form of cybercrime, as individuals experiencing economic hardship become more susceptible to fraudulent schemes (Nkosi & Olofinbiyi, 2023).

Research identifies unemployment, along with other socioeconomic and demographic factors, as a key determinant of cybercrime victimization, highlighting how economic instability increases cyber threat vulnerability (Ntsama et al., 2023). Borwell et al. (2024) emphasize that cybercrime victims, especially those unemployed, often face severe stress and financial difficulties, further compromising their socioeconomic stability.

Unemployment thus creates a dual impact: increasing both the likelihood of cybercrime victimization and the severity of its economic and psychological consequences. Addressing these challenges requires comprehensive strategies that combine victim support with measures to reduce economic instability.

2.3.5 Corruption and Cost of Cybercrime

Corruption amplifies cybercrime's financial impact by fostering environments conducive to criminal activities, thus increasing victims' economic burden. In highly corrupt environments, weak governance and regulatory frameworks typically lead to increased cybercrime victimization. This pattern is evident in nations that consistently rank high in cybercrime perpetration despite various reform efforts (Manbe, 2014).

Corrupt officials may directly engage in cyber extortion, using their positions to target individuals and organizations for financial gain, which magnifies economic impacts and undermines both governance and economic development (Raimberdiyev, 2023). These crimes extend beyond financial losses to create significant psychological impacts, including traumatic stress and damaged self-image. Such effects are particularly severe in corrupt systems where legal recourse and victim support are limited (Borwell et al., 2024).

Socio-demographic factors, especially digital literacy and ICT proficiency, significantly influence victimization patterns. When corruption undermines educational systems and infrastructure development, it can further increase cybercrime victimization costs (Ntsama et al., 2023).

Corruption thus serves as both an enabler of cybercrime and an amplifier of its consequences. Effective solutions must address both corruption and cybersecurity through integrated policy approaches.

2.3.6 Internet Penetration and Cost of Cybercrime

Internet penetration significantly influences cybercrime's financial impact through increased exposure and vulnerability to cyber threats. Higher internet penetration correlates with increased cyber victimization, including identity theft, cyber harassment, and cyberattacks, which often result in psychological and emotional damage to victims (Al-Ali & Al-Nemrat, 2017).

The internet's ubiquitous nature provides cybercriminals with anonymity, allowing them to exploit personal data stored online and increasing victimization risk for all users, including occasional ones (Jaishankar, 2011). Digital footprints and privacy vulnerabilities compound this risk, as evidenced by targeted hacking incidents based on gender and other demographic characteristics (Odunze, 2018). Research shows that contextual factors, such as internet access location, affect victimization rates, with home internet access associated with higher victimization frequencies (Song et al., 2016).

The financial impact of cybercrime is substantial: phishing activities alone cause approximately $120 million in quarterly losses, while global cybercrime costs range between $100 billion and $200 billion, representing a significant portion of global GDP (Lesk, 2011).

These findings emphasize the need for robust cybersecurity measures and comprehensive incident response strategies to address the risks and financial impacts associated with increased internet penetration.

2.3.7 Government Expenditure on Education and Cost of Cybercrime

Government investment in education significantly impacts the economic ramifications of cybercrime, particularly victimization, by enhancing human capital and raising awareness of cybersecurity threats. Educational expenditures have a long-term effect on reducing criminal activities, including cybercrime, through the development of human capital (Atems & Blankenau, 2021). As cybercrime victimization increases alongside the proliferation of internet usage, the critical role of education in mitigating these vulnerabilities becomes increasingly evident (Arifi & Arifi, 2024).

Cybersecurity education is particularly vital, given that 95% of security breaches are attributed to human error, often exploited through social engineering tactics that leverage human vulnerabilities (Bulai et al., 2022). Investments in cybersecurity education empower individuals and organizations with the knowledge and skills necessary to mitigate cyber threats, thereby reducing their susceptibility to victimization.

As cybercrime continues to evolve, increasing awareness and understanding of its impact is essential for preventing future victimization (Arifi & Arifi, 2024). Governmental commitment to educational funding, especially in cybersecurity, plays a pivotal role in reducing the financial burdens of cybercrime. By equipping individuals and organizations with the tools to protect themselves, education funding fosters resilience and mitigates the broader economic consequences of cybercrime (Bulai et al., 2022).

2.3.8 International Tourist Arrivals and Cost of Cybercrime

International tourist arrivals significantly influence the financial implications of cybercrime, particularly through the lens of victimization. Tourists, especially those from foreign countries, are more vulnerable to various offenses, including cybercrime, due to their unfamiliarity with local environments and digital landscapes. This vulnerability is especially evident in the hospitality sector, where international visitors are often targeted for crimes such as theft, emphasizing the need for enhanced preventive measures to protect this group (Zhao & Ho, 2006).

The relationship between tourism and criminal activity is complex, with travelers frequently perceived as affluent and unfamiliar with local customs, making them easy targets. This susceptibility extends to cybercrime, as tourists engage in online interactions and digital transactions while traveling (Moore & Berno, 1995). Cybercrimes such as phishing and malware exploitation impose significant financial costs on both individuals and businesses, with global losses estimated at $375 billion to $575 billion annually (Stewart, 2016). For example, phishing alone accounted for losses of $560 million in 2010 (Lesk, 2011).

As tourists increasingly rely on digital platforms for transactions and activities, their heightened exposure to cyber threats exacerbates the global financial burden of cybercrime. Understanding tourists' online behaviors and implementing targeted cybersecurity measures can help mitigate the economic impact of cybercrime associated with international tourism (Miró-Llinares et al., 2020).

2.3.9 Cyber Security and Cost of Cybercrime

Cybersecurity significantly impacts the economic ramifications of cybercrime, particularly in terms of victimization, as it influences both explicit and implicit financial liabilities for individuals and organizations. Explicit costs of cybercrime include immediate economic losses from data breaches, fraud, and intellectual property theft, which range from hundreds of millions to billions of dollars annually (Lewis & Baker, 2013). Implicit costs, however, often surpass these direct losses, encompassing recovery expenses, increased insurance premiums, and investments in enhanced cybersecurity measures to prevent future incidents (Stewart, 2016).

For instance, recovery costs following cyberattacks can far exceed the initial financial losses. In Italy, hacking losses of €875 million led to recovery expenditures totaling €8.5 billion—nearly ten times the direct financial damage (Stewart, 2016). Cybercrime, affecting approximately 67% of computer users, necessitates widespread and costly cybersecurity measures across various sectors (James & Murray, 2003).

Beyond financial losses, the economic consequences of cybercrime include business disruptions, diminished consumer trust in online transactions, and opportunity costs such as service interruptions and reduced employment opportunities (Lewis & Baker, 2013). Additionally, the reputational harm suffered by companies targeted by cybercrime can have long-lasting financial repercussions, potentially undermining their competitive advantage in the marketplace (Lewis & Baker, 2013).

Cybersecurity plays a critical role in mitigating these costs by reducing both the likelihood and severity of cybercrime incidents. Effective cybersecurity measures protect individual and organizational assets, alleviating substantial financial and reputational damage (Woods & Walter, 2022).

3. Methodology

3.1 Data Collection

The study uses panel data from 33 OECD (Organization for Economic Co-operation and Development) countries spanning 2012 to 2023. Data is sourced from established international organizations to ensure accuracy and relevance:

- Cost of cybercrime (CCBC): Statista database, based on annual monetary damage estimates
- Household Debt-to-GDP (HDGDP): International Monetary Fund (IMF)
- Corruption Perception Index (CPI): Transparency International
- National Cyber Security Index (NCSI): e-Governance Academy Foundation
- World Bank indicators:
  - GINI Coefficient (GINI)
  - Unemployment Rate (UNEMP)
  - Internet Penetration Rate (IPEN)
  - Government Expenditure on Education to GDP (EDGDP)
  - International Tourist Arrivals (INTA)

3.2 Model Specification

This study analyzes panel data using the Generalized Least Squares (GLS) estimation method within a Random Effects (RE) model framework. The RE model was selected because the unobserved individual effects are assumed to be unrelated to the independent variables, reducing bias and improving efficiency. GLS-based methods provide efficient estimation by adjusting for potential heteroskedasticity and autocorrelation in error terms. The RE model estimates the error-associated covariance matrix, improving standard error accuracy and model parameter estimation. The model specification is as follows:

$$CCBC_{it}=\beta_0+\beta_1 HDGDP_{it}+\beta_2 GINI_{it}+\beta_3 UNEMP_{it}+\beta_4 CPI_{it}+\beta_5 IPEN_{it}+\beta_6 EDGDP_{it}+\beta_7 INTA_{it}+\beta_8 NCSI_{it}+u_i+\varepsilon_{it}$$

where $CCBC_{it}$ is the cost of cybercrime for country i at time t (billion U.S. dollars), which is defined as the cost of cybercrime encompasses tangible impacts on individuals and organizations. Cybercrime victimization denotes the damage sustained by individuals because of illicit actions involving computer systems or networks, which may encompass identity theft, unauthorized access, and fraudulent online schemes. $HDGDP_{it}$ is Household Debt-to-GDP ratio for country i at time t (percentage). $GINI_t$ is Gini Coefficient Index for country i at time t (percentage). $UNEMP_{it}$ is Unemployment rate for country i at time t (percentage). CPI_{it} is corruption perception index for country i at time t (percentage), which is scored on a scale of 0 (highly corrupt) to 100 (very clean). $IPEN_{it}$ is internet penetration rate for country i at time t (percentage). $EDGDP_{it}$ is government expenditure on education as a percentage of GDP (percentage). $NCSI_{it}$ is national cyber security index (percentage). $INTA_{it}$ is international tourist arrivals (percentage). ECM_{t-1} denotes lagged value of residuals (represents the error correction term capturing the speed of adjustment to long-run equilibrium). ε_{it} is error term for unobserved factors for country i at time t. β_0 is intercept (constant term). $\beta_1, \beta_2, \ldots, \beta_7$ are coefficients representing the effect of each independent variable on the cost of cybercrime. i indexes countries, t indexes time (years), and Δ denotes the first difference operator.

The examination of the Error Correction Model (ECM) necessitates an investigation into unit roots and cointegration, which represent vital components in guaranteeing the precision of the model. To rectify these concerns, the author performs tests to ascertain the presence of unit roots and cointegration. Should any anomalies be identified, remedies are implemented through the differencing of the data and the application of logarithmic transformations. These methodologies facilitate the stabilization of the data and rectify deviations, thereby enabling a more seamless transition from the Level Model to the Error Correction Model, which is imperative for effectively capturing short-term dynamics while preserving long-term equilibrium relationships.

After applying the natural logarithm transformation and differencing, and employing an Error Correction Model (ECM) specified by ϕECM_{t-1}, which captures the long-term equilibrium relationships, the model would become:

$$\Delta lnCCBC_{it} = \beta_0 + \beta_1 \Delta lnHDGDP_{it} + \beta_2 \Delta lnGINI_{it} + \beta_3 \Delta lnUNEMP_{it} + \beta_4 \Delta lnCPI_{it} + \beta_5 \Delta lnIPEN_{it} + \beta_6 \Delta lnEDGDP_{it} + \beta_7 \Delta lnINTA_{it} + \beta_8 \Delta lnNCSI_{it} + \phi ECM_{t-1} + u_i + \varepsilon_{it}$$

3.3 Diagnostic Test

Various crucial diagnostic tests in panel data regression analysis must be executed to trace accurate and unprejudiced results. They consisted of stationarity test, cointegration test, multicollinearity test, fixed and random effects test, cross-sectional dependence test, model specification test, heteroscedasticity test, and autocorrelation test.

4. Results

4.1 Results of Diagnostic Test

4.1.1 Stationarity Test

The modified inverse chi-squared (Pm) test statistics yield mixed results regarding the stationarity of the time series variables under consideration. The variables $\Delta lnCCBC_{it}$, (Pm=15.3586, p-value= 0.0000), $\Delta lnHDGDP_{it}$ (Pm=11.2535, p-value= 0.0000), $\Delta lnGINI_{it}$ (Pm=31.1500, p-value= 0.0000), $\Delta lnUNEMP_{it}$ (Pm=8.7509, p-value= 0.0000), $\Delta lnCPI_{it}$ (Pm=21.4071, p-value= 0.0000), $\Delta lnIPEN_{it}$ (Pm=16.3062, p-value= 0.0000), $\Delta lnEDGDP_{it}$ (Pm=24.9689, p-value= 0.0000), $\Delta lnNCSI_{it}$ (Pm=172.7849, p-value= 0.0000), and $\Delta lnINTA_{it}$ (Pm=30.3891, p-value= 0.0000) all exhibit statistically significant test statistics at the 5% threshold. As a result, the null hypothesis—which posits the presence of a unit root—is rejected for these variables, thereby confirming their stationarity.

4.1.2 Cointegration Test

The Augmented Dickey-Fuller (ADF) test statistic is -2.7762, with a p-value of 0.0028. Since the p-value is smaller than 0.05, we reject the null hypothesis of no cointegration at the 5% significance level. This result suggests that the variables are likely to be cointegrated, indicating the presence of a long-run equilibrium relationship among them.

4.1.3 Multicollinearity Test

The Variance Inflation Factor (VIF) analysis indicates that multicollinearity is not a severe issue in the model. The largest VIF value of 1.12, observed for the ΔlnCPI$_{it}$ variable, is well below the commonly suggested threshold of 10, indicating that while some multicollinearity is present, it is not strong enough to compromise the model's reliability. The VIF values for other variables, such as ΔlnUNEMP (1.12) and ΔlnEDGDP (1.09), suggest moderate multicollinearity with the remaining variables. However, the VIF values for ΔlnCCBC$_{it}$, ΔlnHDGDP$_{it}$, ΔlnGINI$_{it}$, ΔlnCPI$_{it}$, ΔlnIPEN$_{it}$, ΔlnNCSI$_{it}$, and ΔlnINTA$_{it}$) range from 1.02 to 1.04, indicating very low multicollinearity. Furthermore, the mean VIF of 1.06 confirms that, overall, multicollinearity is low across the model, ensuring that the regression coefficients remain reliable for interpretation and inference.

4.1.4 Fixed and Random Effects Test

The Hausman test yields a Chi-square statistic of 9.97 with 8 degrees of freedom and a p-value of 0.2674. Since the p-value is significantly higher than the commonly used significance levels (e.g., 0.05), we fail to reject the null hypothesis. This indicates that the differences in coefficients between the fixed effects and random effects models are not systematic. Consequently, the random effects model is the appropriate specification for this dataset.

4.1.5 Cross-Sectional Dependence Test

The Pesaran cross-sectional independence test yields a test statistic of 0.599 with a p-value of 0.5491. Since the p-value exceeds the common significance threshold (0.05), we fail to reject the null hypothesis, indicating that there is no evidence of cross-sectional dependence in the dataset.

4.1.6 Model Specification Test

The link test does not indicate any misspecification of the model. The insignificance of the squared predicted values (_hatsq) variable (t = -0.10, p-value = 0.922) suggests that the current model specification is appropriate. This result implies that there is no strong evidence of nonlinearity or omitted-variable bias, reinforcing the validity of the model. Furthermore, the model is statistically significant, and the predicted values (_hat) account for a substantial portion of the variance in the dependent variable, supporting the robustness of the regression results.

4.1.7 Heteroscedasticity Test

The Chi-square statistic with one degrees of freedom is 0.15 and the p-value is 0.6960, far higher than the usual threshold of significance (p-value < 0.05). That is, we are unable to reject the null hypothesis of non-constant variance. Thus, there is not much evidence of heteroskedasticity in your model which implies that the error terms are constant across all values of independent variables and homoscedasticity assumption holds.

4.1.8 Autocorrelation Test

The Wooldridge test for autocorrelation in the panel data had returned an F-statistic (1,29) = 0.000, p-value = 1.0000. We do not reject the null hypothesis of no first-order autocorrelation since the p-value is large (much greater than 0.05).

4.2 Findings and Discussion

The model fit statistics obtained from the ECM analysis give crucial information on the adequacy of the model employed to describe cybercrime costs. The Wald Chi-Square statistics of the model is 133.15 and these variables are significant at confidence level 99%, respectively, demonstrating very high potential explanatory power in explaining variance of the dependent variable. This importance indicates that the independent variables in total make a significant contribution to predicting the changes of cybercrime cost. Using a robust sample size of 32 groups and 328 observations in total, this analysis can produce reliable results. These model fit indicators combined support the statistical fitness of the ECM used in this analysis to explain differences in the relative level of cybercrime costs over time across nations. The Error Correction Model (ECM) based on the data provided can be expressed as follows:

$$\Delta \ln CCBC_{it}=0.0298^{***}-0.8834^{***}\Delta \ln HDGDP_{it} - 0.1174\Delta \ln GINI_{it} -0.1550\Delta \ln UNEMP_{it} + 1.5697^{**}\Delta \ln CPI_{it}$$

$$- 3.3701^{***}\Delta \ln IPEN_{it} - 0.2267\Delta \ln EDGDP_{it} - 1.0736\Delta \ln NCSI_{it} -0.0423\Delta \ln INTA_{it} - 0.2435^{***}ECMt_{-1}$$

*** denotes significance at the 0.01 level. ** denotes significance at the 0.05 level. * denotes significance at the 0.1 level.

The results of the empirical analysis reveal that several independent variables have significant association with cybercrime cost (ΔlnCCBC) over time at country level. The coefficients capture the short-run dynamics as well as long-run adjustment in the model.

4.2.1 Household Debt-to-GDP Ratio

The coefficient of -0.8834 (p-value = 0.000) indicates a significant inverse relationship between household debt and cybercrime costs. This finding suggests that higher household debt levels constrain disposable income, affecting cybercrime patterns through macroeconomic dynamics and victimization patterns. High household debt levels can create economic instability, as shown by the negative long-term relationship between household debt and GDP output. Excessive debt burdens restrict economic growth and reduce disposable income (Kim, 2016). This economic stress may increase cybercrime vulnerability as individuals seek risky financial alternatives online. The broader macroeconomic environment, including economic development and income inequality, also influences household property crime victimization rates (Uludag et al., 2009). Rising household debt creates increased financial pressure that reduces resources available for cybersecurity measures. This financial constraint leads to greater vulnerability to cyber threats due to limited access to protective resources. The interaction between household debt and other macroeconomic factors, particularly income inequality and financial sector dynamics, can amplify these vulnerabilities. Heavily indebted households often lack access to essential cybersecurity resources (Samad, 2023). Thus, the Household Debt-to-GDP ratio indirectly influences cybercrime victimization costs by affecting both economic stability and individual financial resilience, two crucial factors in determining household vulnerability to cybercrime.

4.2.2 Gini Coefficient

Income inequality is not statistically significant to the future cybercrime costs (coefficient for Gini Coefficient is -0.1174 and p-value = 0.7030), in which this implies that short-run also are wonderful economically without effect on cybercrime costs by it. The correlation between income inequality, operationalized through the GINI coefficient, and the economic burden of cybercrime victimization lacks statistical significance, as delineated by various factors elucidated in academic discourse. Firstly, the empirical literature regarding the nexus between income inequality and criminality remains ambiguous, with investigations revealing negligible or economically trivial impacts of inequality on crime statistics (Pazzona, 2024). This implies that income inequality may not serve as a principal catalyst for criminal conduct, including instances of cybercrime. Additionally, the association between income inequality and criminal activity may be spurious, given that income disparity frequently correlates with nation-specific variables such as cultural distinctions, which can obfuscate the analytic outcomes (Neumayer, 2005). Furthermore, when poverty is accounted for in the analysis, income inequality seems to show no relation to various categories of crime, including those that could be considered analogous to cybercrime, such as larceny and robbery (Pare & Felson, 2014). This observation suggests that poverty, rather than inequality, may serve as a more direct influencing factor of criminality. Moreover, while certain studies identify a considerable association between inequality and financial crimes, such findings are not universally generalizable and are contingent upon other socioeconomic determinants such as employment opportunities and the efficacy of the legal framework (Scorzafave & Soares, 2009). Finally, the influence of inequality on crime exhibits inconsistency across disparate contexts, with some research indicating significance solely in relation to violent crime, while not extending to property crime, which might be more intricately linked to cybercrime (Balthazar, 2012). These complexities and inconsistencies inherent in the data and theoretical paradigms contribute to the absence of a statistically significant correlation between income inequality and the economic implications of cybercrime victimization.

4.2.3 Unemployment Rate

Unemployment has a coefficient of -0.1550, and p-value= 0.2760 which means it did not have a significant impact on the cost of cybercrime. The correlation between unemployment and the financial implications of cybercrime victimization is not statistically significant, as evidenced by various factors elucidated in the referenced studies. Initially, macro-level examinations, such as the one executed by Song et al., imply that structural elements like unemployment affect the locations from which users engage with the internet, yet do not directly correlate with the incidence of cybercrime victimization itself (Song et al., 2016). In addition, the study examining the link between unemployment and criminal behavior found no meaningful correlation between unemployment rates and crime data, suggesting that unemployment does not fundamentally trigger criminal acts, such as cybercrime. (Frederick et al., 2016). In addition, Manbe's examination of cybercrime in Nigeria accentuates the significance of technological vulnerabilities and global interconnectivity in enabling cybercrime, as opposed to socio-economic determinants such as unemployment (Manbe et al., 2014). Lastly, van de Weijer's investigation highlights the relevance of individual characteristics, such as diminished self-control and particular online behaviors, in the context of cybercrime victimization, rather than overarching socio-economic circumstances (Weijer, 2019). Collectively, these scholarly works indicate that while unemployment may exert influence over certain behaviors or situational factors, it does not possess a direct, statistically significant effect on the economic repercussions associated with cybercrime victimization.

4.2.4 Corruption Perception Index

The findings indicate that higher corruption perception index (lower corruption) being associated with an increase in the cost of cybercrime, indicated by the positive and significant coefficient of 1.5697 (p-value = 0.0180). An augmentation in the Corruption Perceptions Index (CPI), which signifies a perception of diminished corruption, may precipitate an escalation in the costs associated with victimization in the realm of cybercrime due to a multitude of interrelated factors. Firstly, as the CPI advances, it frequently exemplifies improved governance and enhanced transparency, which can foster greater trust in digital platforms and e-government services (Paul & Adams, 2023). This heightened trust may inadvertently compel individuals and organizations to adopt a more complacent stance towards cyber threats, as they perceive an environment that is ostensibly safer, thus rendering them more susceptible to cybercrime (Al-Nemrat et al., 2010). Moreover, the perception of diminished corruption is typically correlated with economic advancement and the enhancement of institutional frameworks (Donchev & Ujhelyi, 2014). Such advancements can yield more sophisticated digital infrastructures and augment levels of online engagement, which, while advantageous, also create additional opportunities for cybercriminals to exploit. As individuals and enterprises increasingly interact with digital services, the potential ramifications and costs associated with cybercrime victimization escalate, given that more valuable data and assets are rendered vulnerable (Al-Nemrat et al., 2010). Additionally, perception indices, such as the CPI, are subject to the influence of various factors, encompassing economic and institutional progressions, which may not necessarily align with actual reductions in corruption or crime but can significantly affect the way risks are perceived and managed (Donchev & Ujhelyi, 2014). Consequently, although a heightened CPI implies a less corrupt milieu, it may paradoxically result in increased costs of cybercrime victimization due to an amplified exposure and dependency on digital systems, all in the absence of corresponding enhancements in cybersecurity awareness and protective measures.

4.2.5 Internet Penetration Rate

A negative and significant coefficient of -3.3701 with p-value = 0.0000 highlights that higher internet penetration results in lower cost of cybercrime. The correlation between Internet penetration rates and the reduction in the financial burden of cybercrime victimization can be elucidated through a multitude of interrelated elements. Although there exists no direct empirical substantiation that associates increased Internet penetration with a rise in the number of cybercrime offenders, the underlying infrastructure and socioeconomic conditions significantly influence the dynamics of cybercriminal behavior. The rise in income levels, superior educational outcomes, and greater broadband access are positively linked to cybercrime, implying that these conditions create settings that are supportive of cybercriminal acts (Park et al., 2019). As an increasing number of individuals and organizations become cognizant of these risks, they are likely to implement superior cybersecurity protocols, thereby lessening the overall effects and expenses associated with cybercrime (Arifi & Arifi, 2024). Furthermore, the transition from traditional to online criminal activities, as evidenced by the reduction of offline crimes, implies that the Internet has transformed societal behaviors and crime deterrence methodologies, resulting in a more resilient private security sector capable of alleviating cybercrime-related costs (Caneppele & Aebi, 2019). This intricate interplay of variables suggests that while Internet penetration may engender specific conditions conducive to cybercrime, it equally equips society with the necessary tools and awareness to confront and diminish the financial implications tied to cybercrime victimization.

4.2.6 Government Expenditure on Education

The coefficient for government expenditure on education is -0.2267 and p-value = 0.2400, so their value will not have a significant short-term effect over the cost of cybercrime. Government investment in educational initiatives does not exert a significant influence on the financial implications associated with cybercrime victimization, chiefly due to the inherent distinctions between cybercrime and conventional criminal activities, which are more directly affected by educational funding. The rates of traditional criminal offenses, encompassing violent and property crimes, have demonstrated a delayed yet considerable reaction to increases in educational expenditures, as educational enhancement contributes to the development of human capital and a gradual decline in criminal behavior over time (Atems & Blankenau, 2021). Conversely, cybercrime functions within a digital landscape wherein the primary vulnerabilities are not necessarily correlated with overall educational attainment but are instead tied to specific levels of cybersecurity awareness and practices. The phenomenon of cybercrime victimization is predominantly propelled by human errors and social engineering techniques that capitalize on deficiencies in specialized cybersecurity knowledge rather than on general educational qualifications (Bulai et al., 2022). Despite the augmentation of government allocations for educational purposes, the swift advancement and intricate nature of cyber threats necessitate a concentrated focus on cybersecurity education and awareness initiatives to effectively diminish associated risks (Joshi & Deshpand, 2022). Moreover, the ubiquitous presence of the internet and the burgeoning global user base exacerbate the challenge, as the ramifications of cybercrime can extend to any individual, irrespective of their educational level (Arifi & Arifi, 2024). Consequently, although general educational expenditures yield broader socio-economic advantages, their efficacy in mitigating cybercrime victimization remains constrained without a dedicated emphasis on cybersecurity education and awareness (Bulai et al., 2022; Arifi & Arifi, 2024).

4.2.7 International Tourist Arrivals

The coefficient for international tourist arrivals is -0.0423 and p-value = 0.1100, indicating no significant effect on the cost of cybercrime in the short run. The correlation between international tourist arrivals and the financial implications of cybercrime victimization appears to be negligible, attributable to the specific types of offenses that are commonly linked with tourism. The scholarly investigations conducted primarily emphasize tangible offenses, including property theft and personal assaults, as opposed to cybercriminal activities. In addition, tourist arrivals exert a substantial influence on crimes targeting property and individuals; however, it fails to address the phenomenon of cybercrime (Montolio & Planells, 2016). In a similar vein, the predominant offenses affecting tourists are of a physical nature, such as pickpocketing, with no reference made to cybercrime (Omisore et al., 2013). Moreover, tourist arrivals are shown to affect crime rates in the short term; once again, the focus remains on physical offenses rather than cybercrime (Mehmood et al., 2016). Furthermore, tourists are inclined to consider the risk of physical victimization when selecting destinations, thereby indicating that cybercrime does not constitute a primary concern for these travelers (Altindag, 2014). This apparent disregard for cybercrime within the tourism context implies that, while international tourist arrivals may exert an influence on certain categories of crime, they do not significantly affect the economic burden of cybercrime victimization, which is frequently characterized by a greater complexity and a less direct association with physical presence or tourist-related activities. Consequently, the existing body of literature fails to furnish compelling evidence of a substantial relationship between international tourist arrivals and the financial ramifications of cybercrime victimization, given that the offenses associated with tourism predominantly manifest as physical character.

4.2.8 National Cyber Security Index

The National Cyber Security Index provides a -1.0736, p = 0.730 coefficient, also not significant. This analysis indicates that the cyber security index has no significant impact on the cost of cybercrime. The limited efficacy of cybersecurity measures in diminishing the financial repercussions of cybercrime victimization can be ascribed to multiple factors. Despite substantial financial allocations towards cybersecurity initiatives, the global financial impact of cybercrime persistently surpasses $1 trillion each year, signifying that these endeavors have not appreciably alleviated economic detriments or victimization frequencies (Allahrakha, 2024). One contributing factor is the swift advancement and heightened complexity of cyber threats, which frequently outstrip the progression of defensive technologies and methodologies. Cybercriminals take advantage of inadequacies within digital infrastructures, which are inherently imperfect, resulting in continuous victimization (Manbe, 2014). Furthermore, the surging population of internet users and the proliferation of digital services furnish cybercriminals with increased avenues for illicit activities, thereby exacerbating the challenges associated with mitigating cybercrime (Arifi & Arifi, 2024). Additionally, the psychological and economic repercussions for victims are substantial, yet frequently undervalued, contributing to the aggregate costs associated with cybercrime (Borwell et al., 2021). Despite interventions from both governmental and non-governmental entities, the nation continues to serve as a notable epicenter for cybercrime, underscoring the challenges inherent in reducing victimization solely through cybersecurity measures (Manbe, 2014). Consequently, while the role of cybersecurity is paramount, its current execution has not substantially alleviated the economic strain imposed by cybercrime victimization.

4.2.9 ECM (Error Correction Term)

The principal conclusion of the study, characterized by a substantial and negative error correction term of -0.2435 with a p-value of 0.0000, indicates that the model displays a pronounced propensity for rapid adjustment towards long-term equilibrium after transient disturbances. This finding suggests that approximately 24.4% of any observed disequilibrium is rectified in each period, thereby illustrating a relatively swift reallocation of the variables involved. This result accentuates the sensitivity of the determinants influencing cybercrime victimization to transient shocks. It signifies that the dynamics of cybercrime costs within OECD nations are not immutable, but rather susceptible to prompt alterations in response to variations in essential socioeconomic indicators, including unemployment rates, household indebtedness, or levels of internet penetration. Hence, this swift adjustment underscores the potential efficacy of policy interventions designed to alleviate the financial repercussions associated with cybercrime. Furthermore, the expeditious adjustment process emphasizes the critical need for timely policy initiatives aimed at tackling the underlying factors that contribute to cybercrime victimization. Given that the variables related to cybercrime can rectify themselves in a relatively rapid manner, governmental entities and organizations can adopt a proactive stance in response to economic or social upheavals. This implies that by fortifying cybersecurity frameworks, enhancing digital literacy, and addressing economic disparities such as income inequality and unemployment, nations can more effectively mitigate the financial burdens imposed by cybercrime. The study presents a persuasive rationale for targeted interventions that can expedite recovery from cybercrime-related shocks, thereby diminishing both the immediate and enduring costs associated with online victimization.

5. Theoretical and Policy Implications

5.1 Theoretical Implications

5.1.1 Economic Constraints and Cybercrime

The theoretical ramifications of this notion reside in comprehending the way financial stressors, particularly the prevalence of excessive household indebtedness, affect an individual's susceptibility to victimization by cybercrime. Historically, financial stress has been examined primarily concerning its detrimental impacts on both mental and physical health; however, this theoretical construct presents a novel viewpoint by evaluating its potential influence in curtailing online engagements and, by extension, minimizing exposure to cyber threats. In instances where households are burdened by significant debt, their financial resources are generally constrained, which may lead to a diminished capacity for discretionary expenditures, inclusive of online transactions or investments. Therefore, individuals may elect to confine their digital visibility or moderate the amount of personal information they reveal, subsequently reducing their likelihood of falling prey to cybercriminal acts. This mechanism elucidates an indirect yet essential correlation between financial distress and a decrease in susceptibility to cyber threats.

Moreover, by contextualizing this relationship within the framework of state economic behavior, it becomes feasible to broaden this theoretical paradigm to encompass extensive macroeconomic conditions and their influence on individual cyber vulnerability. The fiscal policies enacted by the state, alongside economic regulations and initiatives aimed at alleviating financial burdens on households (for example, debt relief schemes or economic stimulus measures), could markedly alter the landscape of cyber risk. For instance, when governmental authorities introduce strategies to mitigate household debt or bolster economic recovery, individuals may experience an enhanced sense of financial security, which could catalyze greater participation in online activities. This, in turn, may lead to elevated exposure to cybercrime risks. Hence, an understanding of the economic milieu and its intersection with cyber vulnerability unveils new research trajectories in both the fields of economics and cybersecurity. This theoretical proposition urges policymakers to contemplate not solely direct financial assistance but also the broader ramifications of financial well-being on cyber risk behaviors, positing that economic interventions may yield dual advantages: alleviating financial stress while simultaneously influencing the digital safety of individuals.

5.1.2 Corruption and Cyber Vulnerability

The outcomes of this investigation yield considerable theoretical implications that enhance our comprehension of the interplay between the Corruption Perceptions Index (CPI) and the financial repercussions of cybercrime victimization. The positive and statistically significant correlation between an elevated CPI and heightened costs associated with cybercrime contests the traditional notion that diminished corruption invariably results in a decline in criminal activities, including those of a cyber nature. This paradox indicates that enhancements in governance and transparency, which are generally associated with diminished corruption, may unintentionally heighten susceptibility to cybercrime by fostering a spurious sense of security among both individuals and organizations. This occurrence elucidates the intricate dynamics between perceived safety and actual risk, necessitating a reassessment of the prevailing assumptions surrounding governance and its repercussions on cybercrime.

A salient theoretical implication emerging from the findings is the imperative to reevaluate the influence of governance and institutional trust on the shaping of individuals' risk perceptions, especially concerning cyber threats. As the CPI ascends and the perception of corruption diminishes, individuals and organizations may exhibit increased complacency in their cybersecurity practices. The augmented confidence in digital platforms and e-government initiatives, which typically accompanies advancements in governance, may culminate in a decrease in risk-averse behaviors, such as the allocation of resources toward robust cybersecurity protocols or the implementation of proactive threat management strategies. This observation is congruent with existing literature on risk perception, which posits that individuals may perceive a diminished necessity for protective measures in environments they deem safer, notwithstanding the persistence of objective risks at elevated levels.

Another pivotal theoretical implication arises from the heightened exposure to cybercrime engendered by technological and institutional advancements. As digital infrastructures proliferate and online services expand, both individuals and enterprises encounter augmented cyber risks. This phenomenon is particularly pronounced in contexts characterized by enhanced governance and transparency, which frequently correspond with increased levels of online engagement and more valuable digital assets. Although these advancements may facilitate economic and institutional development, they concurrently furnish additional avenues for cybercriminals to exploit inherent vulnerabilities. The findings suggest that, despite the advantages associated with technological progression, the augmented interconnectedness and digital exposure may paradoxically exacerbate the costs linked with cybercrime victimization, as a greater volume of sensitive data and assets becomes susceptible to compromise.

Ultimately, the study accentuates the intricacies inherent in the relationship between perceived and actual levels of corruption. CPI is influenced by variables such as economic development and institutional reforms, which may not accurately reflect the efficacy of anti-corruption initiatives or the genuine mitigation of crime, including cybercrime. The results indicate that a heightened CPI, while indicative of reduced corruption, does not necessarily align with a diminishment in the financial costs associated with cybercrime victimization. This underscores the necessity for future research endeavors to investigate more nuanced indicators of both governance quality and cybersecurity preparedness. A more profound understanding of how perceptions of governance affect tangible security outcomes could inform more precise policy recommendations aimed at enhancing both institutional transparency and digital protection strategies.

5.1.3 Internet Penetration and Cyber Awareness

The theoretical ramifications of enhanced internet penetration resulting in diminished costs associated with cybercrime victimization may be scrutinized through the lenses of criminology, economics, and technology. From a criminological standpoint, as an increasing number of individuals and organizations attain internet access, their vulnerability to potential cybercrime threats correspondingly escalates. Nevertheless, this heightened vulnerability is frequently counterbalanced by augmented awareness and availability of security resources. As the user base of the internet expands, individuals are also more inclined to participate in digital literacy initiatives and implement preventative strategies such as cybersecurity tools, which have the capacity to alleviate the severity of victimization-related costs. This indicates that although the incidence of cybercrime may rise, the aggregate cost, particularly in terms of financial and emotional repercussions, may diminish owing to the provision of mitigation strategies.

From an economic viewpoint, the expanded accessibility of the internet has the capability to lower the marginal expenditures linked to the commission of cybercrimes. Cybercriminals can engage a broader array of victims with minimal financial investment, employing automated instruments such as malware, phishing, and ransomware to scale their nefarious activities. This reduction in operational costs implies that cybercriminals can exploit a greater number of victims without incurring significant resource outlays. However, the associated costs of victimization may persist at elevated levels, especially for individuals and organizations that are deficient in requisite security infrastructure. As a result, while the economic burden of cybercrime may be perceived as lower for the perpetrators, the financial and operational costs for victims could still be substantial, even amidst increased internet accessibility.

From a technological perspective, heightened internet penetration also facilitates the implementation of more advanced security measures, thereby potentially decreasing the costs of cybercrime victimization for both individuals and organizations. As internet users become increasingly acquainted with security technologies such as encryption, firewalls, and multi-factor authentication, the efficacy of cyberattacks is correspondingly diminished. This technological progression serves as a counterbalance to the reduced costs of executing cybercrime, as defenders are armed with superior tools to thwart and mitigate attacks. Consequently, this may culminate in a reduction of the overall impact of cybercrime on victims, as they are better equipped to manage and recuperate from assaults. In summation, the interplay between heightened internet penetration and reduced costs of cybercrime victimization is intricate. While enhanced internet access may facilitate easier and more cost-effective targeting of victims by cybercriminals, the concomitant escalation in cybersecurity awareness and technological advancements can substantially mitigate the financial and psychological burdens of victimization. This dual dynamic emphasizes the necessity for ongoing innovation in both cybercriminal methodologies and defensive mechanisms, ensuring that the costs associated with victimization remain manageable despite the escalating prevalence of cyber threats.

5.1.4 Cybersecurity and Education

The theoretical ramifications derived from this analysis suggest that the association between governmental expenditures on education and victimization due to cybercrime is considerably more intricate than the simplistic correlation observed in conventional criminal activities. Although investments in education are frequently correlated with a decline in traditional crime rates, their influence on cybercrime appears to be considerably constrained. This limitation arises predominantly from the distinctive attributes of cybercrime, which transpires within a digital context where elements such as technological susceptibilities and human fallibilities assume a more significant role than does general educational attainment. The results elucidate that governmental financing for education, which customarily prioritizes extensive human capital development, fails to adequately address the specific knowledge deficiencies pertinent to cybersecurity. This underscores the necessity for a more focused strategy aimed at alleviating cybercrime, extending beyond the traditional educational paradigms.

The findings indicate that the efficacy of educational expenditures in mitigating cybercrime victimization is contingent upon the specific nature of criminal activity. Conventional offenses, including violent and property crimes, are subject to the influence of enduring societal transformations engendered by education, as individuals with augmented human capital are more inclined to engage in lawful conduct. Conversely, the victimization associated with cybercrime is predominantly shaped by individual susceptibilities, such as vulnerability to phishing schemes or social engineering tactics, which are not directly affected by general educational initiatives. This observation highlights a theoretical divergence in the way education exerts influence across various categories of crime, suggesting that the ramifications of education on criminality are contextually dependent and necessitate a more customized framework to comprehend its disparate effects across diverse realms.

From a theoretical perspective, the results bolster the emerging acknowledgment that cybercrime constitutes a distinct phenomenon necessitating specialized knowledge and methodologies. The function of education in the prevention of cybercrime is not interchangeable with general educational policies directed at crime reduction. Rather, the theoretical framework for comprehending cybercrime victimization must integrate a specialized emphasis on cybersecurity awareness and digital literacy. The dynamics of cybercrime are propelled by factors that transcend general educational achievement, including the accessibility of cyber tools, the rapidity of technological progress, and the proliferation of online social manipulation strategies. Consequently, crime prevention theories must adapt to address the specific challenges presented by digital environments, accentuating cybersecurity education and digital skills training as essential components.

Ultimately, these findings suggest that prospective theoretical models of crime prevention ought to encompass a multidimensional approach that addresses both traditional and digital crime landscapes. The disparate effects of educational expenditure on conventional crime versus cybercrime necessitate a revised comprehension of the intersection between education and criminality. This endeavor would entail the formulation of theories that consider the distinct mechanisms through which education influences criminal behavior across varying contexts, considering both the broad, longitudinal societal impacts of general education and the immediate, specialized requirements pertaining to cybersecurity awareness. This theoretical advancement will be imperative for the formulation of more effective public policies and interventions tailored to the unique challenges presented by the digital era.

5.2 Policy Implications

5.2.1 Addressing Cybersecurity Complacency in Low Corruption Environments

The correlation between the Corruption Perception Index (CPI) and the financial repercussions of cybercrime victimization presents significant policy considerations for governments and cybersecurity stakeholders. An elevated CPI may imply enhanced governance yet can create a deceptive security perception, inciting complacency towards cybersecurity vulnerabilities. This misapprehension could lead to diminished vigilance and lesser cybersecurity investments, rendering entities more vulnerable to cybercrime. Consequently, policymakers need to advocate for simultaneous governance reforms and comprehensive cybersecurity education, highlighting the necessity of digital literacy and consistent cybersecurity investment. Implementation can occur through public awareness efforts, educational programs, and incentives for SMEs to enhance security protocols. Regulatory frameworks must adapt to the evolving cyber threat landscape, necessitating regular cybersecurity audits, real-time reporting, and stringent penalties for noncompliance. Furthermore, global collaboration is essential for effectively addressing cybercrime, as threats transcend national jurisdictions. By adopting an integrated strategy towards governance and cybersecurity, governments can alleviate the contradictory consequences of a heightened CPI and protect against escalating cybercrime expenditures.

5.2.2 Increasing Cybersecurity Awareness through Education

To augment cybersecurity awareness through educational initiatives, policy considerations ought to concentrate on the incorporation of cybersecurity training into educational frameworks at every level, encompassing primary education through tertiary institutions. Governments and educational entities should give precedence to the formulation of thorough and accessible training programs that encompass fundamental cybersecurity principles, appropriate online conduct, and the criticality of data privacy. Furthermore, policies should advocate for continuous professional development for individuals within the labor force, thereby ensuring they remain informed about the latest cyber threats. Cooperative efforts between the public and private sectors are essential to guarantee the extensive availability of resources, and policies should provide incentives for organizations to deliver cybersecurity awareness training for their personnel. By establishing a culture of cybersecurity consciousness, these policies will diminish the dangers posed by cyberattacks and equip individuals to defend their personal and organizational data with enhanced effectiveness.

5.2.3 Addressing Economic Constraints

Policy implications indicate that the amalgamation of financial stability protocols with consumer protection regulations may serve a vital function in mitigating susceptibility to cybercrime. By instituting policies that tackle economic strains—such as alleviating household indebtedness and advancing financial literacy—governments can assist individuals in circumventing financially precarious online conduct that frequently renders them vulnerable to cyber threats. Moreover, strategies aimed at bolstering financial security, including the assurance of access to affordable financial services, could diminish the motivation for individuals to partake in fraudulent or hazardous online transactions. Consequently, such initiatives not only promote economic prosperity but also establish a safeguard against the escalating threats of cybercrime, ultimately aiding in the creation of a more secure digital landscape for consumers.

5.2.4 Long-term Investment in Cybersecurity Infrastructure

Continuous investment in cybersecurity infrastructure is imperative for the enhancement of national security, economic fortitude, and the safeguarding of critical industries. Policymakers ought to prioritize the allocation of funding and the establishment of incentives for enterprises, particularly those classified as small and medium-sized, to implement robust cybersecurity protocols. Furthermore, regulatory frameworks should advocate for the ongoing advancement of resilient infrastructure, facilitate public-private partnerships, and mandate the regular revision of security protocols to effectively counter emerging threats. Long-term strategies must also encompass the cultivation of skilled professionals in cybersecurity domains, alongside the establishment of a legal and ethical framework to oversee data privacy and cyber resilience. The government is required to adopt a proactive stance in promoting innovation while ensuring that cybersecurity is seamlessly integrated into every tier of technological advancement, thereby protecting both private and public sector systems from increasingly sophisticated cyber threats.

6. Conclusion

This study examines how socioeconomic factors affect cybercrime costs in OECD countries from 2012 to 2023. Using a Random Effects model with Generalized Least Squares estimation, we identified household debt, internet penetration, and corruption as key determinants influencing cybercrime's financial impact.

The findings reveal two counterintuitive relationships: higher household debt and greater internet penetration are associated with lower cybercrime costs, suggesting that economic constraints and digital connectivity may reduce cyber risk exposure. Additionally, a higher Corruption Perception Index (CPI) can paradoxically increase cybercrime costs. This occurs when perceived improved governance leads to organizational complacency about cybersecurity risks. The combination of increased digital engagement and insufficient cybersecurity awareness creates opportunities for cybercriminals, resulting in higher victimization costs despite lower corruption levels.

While income inequality, unemployment, and government education expenditure showed no significant short-term effects on cybercrime costs, our research highlights the importance of long-term investment in cybersecurity education and awareness. These investments are essential for building a resilient digital society that can adapt to evolving cyber threats.

The study's theoretical implications emphasize how economic behavior intersects with cyber vulnerability, demonstrating that financial stability and digital literacy are crucial in fighting cybercrime. Our policy recommendations focus on four key areas: strengthening institutional integrity, enhancing cybersecurity education, addressing economic constraints, and maintaining sustained investment in cybersecurity infrastructure.

References

Al-Ali, A. A. H., & Al-Nemrat, A. (2017). Cyber victimization: UAE as a case study. In *Proceedings of the 2017 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 19–24). London, UK: IEEE.

AllahRakha, N. (2024). Impacts of cybercrimes on the digital economy. *Uzbek Journal of Law and Digital Policy*, *2*(3), 29–36.

Al-Nemrat, A., Jahankhani, H., & Preston, D. S. (2010). Cybercrime victimisations/criminalisation and punishment. In S. Tenreiro de Magalhães, H. Jahankhani, & A. G. Hessami (Eds.), *Global security, safety, and sustainability. ICGS3 2010. Communications in computer and information science* (Vol. 92, pp. 106–119). Berlin, Heidelberg: Springer.

Altindag, D. T. (2014). Crime and international tourism. *Journal of Labor Research, 35*(4), 443-461.

Arifi, D., & Arifi, B. (2024). Cybercrime victimization. In T. Pajuste, H. Bellani (Miço), & S. Maslo Cerkic (Eds.), *Legal perspectives in the modern era of technological transformations* (pp. 193–204). Bucharest, Paris, Calgary: ADJURIS.

Atems, B., & Blankenau, W. (2021). The 'time-release', crime-reducing effects of education spending. *Economics Letters, 209*, 110143.

Bakari, N., Mohamed, I., & Nazuri, S. (2023). Understanding cyber threats vulnerability of future victimization in fintech. *Business and Management Horizons, 11*(1), e21543.

Balthazar, K. R. (2012). *The socioeconomic determinants of crime: The case of Texas* (Master's thesis). Universidade Católica Portuguesa, Portugal.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169-217.

Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review, 40*(6), 933-954.

Borwell, J., Jansen, J., & Stol, W. (2024). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology, 31*(1), 156–181.

Bourdieu, P. (1986). The forms of capital. In J. G. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241-258). Westport, CT: Greenwood Press.

Bulai, R., Turcanu, D. S., & Ciorba, D. (2022). Education in cybersecurity. In *Central and Eastern European eDem and eGov Days* (Vol. 335, pp. 2–14). *335*, 2-14.

Caneppele, S., & 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*(1), 66–79.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Donchev, D., & Ujhelyi, G. (2014). What do corruption indices measure? *Economics and Politics, 26*(3), 346–370.

Ferguson, C. J. (2017). The effect of socioeconomic status on victimization in the digital world: A study of vulnerability factors. *Journal of Criminal Justice, 48*, 27-36.

Frederick, S. A., Jozefowicz, J. J., & Nelson, Z. T. (2016). A dynamic panel data study of the unemployment-crime relationship: The case of Pennsylvania. *Economics Bulletin, 36*(1), 471-477.

Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring internet crimes and criminal behavior*. London & New York: Routledge.

James, M. L., & Murray, B. E. (2003). *Computer crime and compromised commerce* (Research Note 2003-04 No. 6). Department of the Parliamentary Library, Australia.

Joshi, S. V., & Deshpand, P. K. K. (2022). Cyber crime education. *Sanshodhan, 11*(1), 169805.

Kim, Y. K. (2016). Macroeconomic effects of household debt: An empirical analysis. *Review of Keynesian Economics*, *4*(2), 127-150.

Kovalchuk, O., Shynkaryk, M., & Masonkova, M. (2021). Econometric models for estimating the financial effect of cybercrimes. In *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 381–384). IEEE.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy, 4*(1), 33–39.

Lesk, M. (2011). Cybersecurity and economics. *IEEE Security & Privacy, 9*(6), 76–79.

Levi, M. (2016). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change, 67*(1), 3–20.

Lewis, J. A., & Baker, S. (2013). *The economic impact of cybercrime and cyber espionage*. Washington, DC: Center for Strategic and International Studies.

Manbe, D. A., Magaji, S., & Damagun, Y. M. (2014). Cybercrimes and victimization: An analysis of economic-cost implications to Nigeria. In *Proceedings Book of ICETSR, 2014, Malaysia: Handbook on the emerging trends in scientific research* (pp. 777–785). PAK Publishing Group.

Mehmood, S., Ahmad, Z., & Khan, A. A. (2016). Dynamic relationships between tourist arrivals, immigrants, and crimes in the United States. *Tourism Management, 54*, 383-392.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672-682.

Miró-Llinares, F., Drew, J. M., & Townsley, M. (2020). Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. *International Journal of Cyber Criminology, 14*(2), 374-387.

Montolio, D., & Planells, S. (2016). Does tourism boost criminal activity? Evidence from a top touristic country. *Crime & Delinquency, 62*(6), 741-764.

Moore, K., & Berno, T. (1995). Relationships between crime and tourism. *Visions of Leisure and Business, 11*(2), 45-60.

Neumayer, E. (2005). Is inequality really a major cause of violent crime? Evidence from a cross-national panel of robbery and violent theft rates. *Journal of Peace Research, 42*(1), 101–110.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(2), 725-740.

Nkosi, S. L., & Olofinbiyi, S. A. (2023). The evaluation of cybercrime in South Africa: A review of the impact of identity theft menace on the economy. In S. O. Ehiane, S. A. Olofinbiyi, & S. M. Mkhize (Eds.), *Cybercrime and challenges in South Africa* (pp. 29–49). Singapore: Palgrave Macmillan.

Ntsama, J. E., Tchakounte, F., Tchakounte Tchuimi, D., Faissal, A., Fotso Kuate, F. A., Effa, J. Y., Udagepola, K. P., & Atemkeng, M. (2023). Determinants of cybercrime victimization: Experiences and multi-stage recommendations from a survey in Cameroon. In R. A. Saeed, A. D. Bakari, & Y. H. Sheikh (Eds.), *Towards new e-Infrastructure and e-Services for Developing Countries* (pp. 317–337). Springer Nature Switzerland.

Odunze, D. (2018). Cyber victimization by hackers: A criminological analysis. *Public Policy and Administration Research, 8*(1), 8–15.

Omisore, E. O., Badiora, A. I., & Fadoyin, O. P. (2013). Victim travel–to-crime areas: The experience from Nigerian international tourist attraction site. *International Journal of Criminology and Sociological Theory, 6*(4), 204–216.

Pare, P.-P., & Felson, R. B. (2014). Income inequality, poverty, and crime across nations. *British Journal of Sociology, 65*(3), 346-376.

Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The economics of cybercrime: The role of broadband and socioeconomic status. *ACM Transactions on Management Information Systems, 10*(4), 1–23.

Paul, C., & Adams, S. O. (2023). The effect of e-government development indices (EGDI) on corruption perception index in sub-Saharan Africa: A panel data analysis. *African Journal of Science, Technology, Innovation and Development, 16*(1), 17–25.

Pazzona, M. (2024). Revisiting the income inequality-crime puzzle. *World Development, 145*, 106520.

Raimberdiyev, S. (2023). Combating cyber extortion by corrupt officials. *Uzbek Journal of Law and Digital Policy, 1*(4), 1–18.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(5), 1–14.

Samad, K. A. (2023). Systematic literature review on the macroeconomic factors of household debt. *Economics and Finance Education*, 18, 102-118.

Scorzafave, L. G. D. S., & Soares, M. (2009). Income inequality and pecuniary crimes. *Economics Letters, 104*(1), 40–42.

Song, H., Lynch, M., & Cochran, J. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice, 41*, 583-601.

Srivastava, S., Das, S., Udo, G., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: A cross-country study. *Journal of Global Information Technology Management, 23*(3), 112–137.

Stewart, P. (2016). Trading cybercrime for jobs and commerce or paying up: Using the WTO to combat cybercrime. *The George Washington International Law Review, 48*, 475–511.

Tonellotto, M. (2019). Crime and victimization in cyberspace: A socio-criminological approach to cybercrime. In S. K. S. (Ed.), *Handbook of research on digital crime, cyberspace security, and privacy* (pp. 145–160). IGI Global.

Uludag, S., Colvin, M., Hussey, D. L., & Eng, A. L. (2009). Modernization, inequality, routine activities, and international variations in household property crimes. *International Journal of Criminal Justice Sciences*, 4(2), 1–17.

Weijer, S. van de. (2019). Predictors of cybercrime victimization: Causal effects or biased associations? In *Cybercrime and its victims: Critical issues in international perspective* (pp. 41–59). Routledge.

Woods, D. W., & Walter, L. (2022). Reviewing estimates of cybercrime victimization and cyber risk likelihood. In *Proceedings of the 7th IEEE European Symposium on Security and Privacy Workshops 2022* (pp. 150–162). IEEE.

Zhao, J., & Ho, T. (2006). Are foreign visitors more likely victimized in hotels? Policy implications. *Security Journal, 19*(2), 123-134.