SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 235

UNDERSTANDING CYBERCRIME THROUGH A SOCIO-ECONOMIC LENS

Piotr WIŚNIEWSKI

Nicolaus Copernicus University, Faculty of Economics; psw@umk.pl, ORCID: 0000- 0002-2263-4851

Purpose: The purpose of this research is to examine the relationship between cybercrime and socioeconomic factors.
Design/methodology/approach: This objective was achieved by reviewing existing literature on socioeconomic factors impacting cybercrime and cybersecurity. Based on this, a set of quarterly secondary data was collected. A Vector Autoregression (VAR) model was employed to analyze how these variables influence both cybercrime and the economy. Finally, impulse response analysis was conducted to examine the dynamic interactions.
Findings: The research found that economic activity plays an important role in explaining cybersecurity vulnerabilities. Additionally, the growing penetration of technological solutions, both digital and physical, significantly influences these vulnerabilities. These findings demonstrate that cybercrime is both a social and technological phenomenon.
Research limitations/implications: The research was conducted using secondary data and proxies for certain factors (e.g., risky behavior, scale of cybercrime). Future studies should adopt an interdisciplinary approach integrating both technical and social dimensions.
Social implications: This research demonstrates that cybercrime is not solely a technological issue. While technology enables its existence, the root causes are fundamentally social. Therefore, investing solely in cybersecurity technologies may not adequately protect potential victims. Cybersecurity should be addressed as a public policy issue that goes beyond direct financial costs.
Originality/value: This article provides an economic analysis of cybercrime, offering a critical review of previous studies. It takes into account a broad range of factors, encompassing both society as a whole and specific groups directly affected by the issue.
Keywords: cybercrime, cybersecurity, vector autoregression.
Category of the paper: Research paper.

1. Introduction

In 2024 article titled “The Hidden Injustice of Cyberattacks“ (Tisdale, 2024) was published on Wired website. It outlined cybercrime effects on multiple facets of life: healthcare, economic opportunities, education and democracy. Mainstream media and non-academic communities

are beginning to perceive cybercrime as interdisciplinary problem that significantly influence their daily lives. This should motivate researchers from different disciplines to analyze cybercrime from their perspective. Despite significant scholarly interest, the field still lacks clarity about the risk factors associated with cybercrime offending and victimization.

Cybercrime is a complex phenomenon with technological and societal dimensions. The dynamic nature of cybercrime and the interdisciplinary nature of the field have resulted in the lack of a unified and commonly agreed-upon definition. Kosiński (2015) summarized previous attempts in definition that characterizes cybercrime in broader and narrower sense. In the narrow sense, cybercrime is synonymous with computer crime and includes any illegal activity that targets the security of computer systems and compromises the integrity of data. In the broad sense, cybercrime refers to all illegal activities conducted using computers.

Cybercrime is usually researched from the perspective of criminology or technology-related sciences. The social science perspective on cybercrime is a relatively new and growing research field. Economy is interested in cybercrime from a few perspectives. First are the costs of cybercrime for society, businesses, and individuals. Second is the market-like operations of cybercriminals and their motivations. Both focus only on property-related activities by cybercriminals. Third is the influence of socioeconomic environment on cybercrime existence. This relates to both sides of cybercrime- criminals and victims.

The goal of this article is to analyze the influence of socio-economic factors on cybercrime. The primary motivation behind this approach is the perception of cybercrime not merely as a technical problem but as a systemic issue.

2. Literature review

All crimes can be committed by force or deceit, whether traditional or cybercrime (Agustina, 2015). In cyberspace, force relates to hacking, and deceit to social engineering (Mitnick, Simon, 2016). People are particularly vulnerable to manipulation online due to the large number of potential victims, widespread personal information on social media, and the digital divide. The digital divide refers to disparities in access to digital resources or the ability to use them effectively (Aissaoui, 2022; Vassilakopoulou, Hustad, 2021). Both those highly proficient with digital technologies and those with limited access may be more vulnerable to victimization. This implies that cybercrime should be understood and analyzed not only as a technical issue, but primarily as a social problem.

There is a lack of standardized metrics to measure cybercrime (Songsrirote, 2025). Most existing research relies on proxy variables. This is due to the dynamic development of this phenomenon and the absence of a universally agreed-upon definition. There is no consensus

on which activities should be included in cybercrime metrics. Even when applying a cost-based approach, uncertainty remains about which costs should be considered.

This ambiguity in measurement frameworks highlights the need for robust theoretical models that can guide our understanding of cybercrime. Modern economic research on crime-related topics began with Becker's (1968) article. It was the first publication to apply a neoclassical economic approach to crime analysis. According to Becker, criminals are fully rational and seek to optimize their utility. In other words, the decision to commit a crime is based on a cost–benefit analysis and expected utility (Becker, 1968; Draca, Machin, 2015).

In the 1990s, economic analyses of crime became more refined, incorporating societal, cultural, institutional, and legal perspectives (Forst, 1994). These two approaches reflect duality in economic analysis and continue to evolve. Winter (2019) proposes a rational crime analysis by providing examples related to different types of crime and circumstances. The second edition of this work introduces behavioral analysis as well.

Among the behavioral approaches, General Strain Theory stands out as particularly relevant for explaining the social underpinnings of cybercrime. From a behavioral standpoint, commonly cited theories (besides full rationality) are Strain Theory, the Online Disinhibition Effect, Threat Avoidance Theory (TTAT) and Social Capital Theory.

General Strain Theory explains how social and cultural variables may lead to criminal behavior. For example, Lee and Sanchez (2018) showed that multiple social pressures could lead students to engage in cyberbullying. Academic frustration was linked to both internal and external responses. In this sense, illegal activities, whether online or offline, may share similar underlying variables. If the response to strain is external and involves illegal activity, it may or may not involve technology.

The Online Disinhibition Effect (Suler, 2004) explains why people do things in cyberspace that they would not do or say in other contexts. In the digital environment, they feel less restrained and more open due to six factors: Dissociative Anonymity, Invisibility, Asynchronicity, Solipsistic Introjection, Dissociative Imagination, and Minimization of Status and Authority.

Threat Avoidance Theory (Ilany-Tzur, Fink, 2025) aims to understand users' risk-avoidance behavior in technological contexts. This behavior is based on risk appraisal, which considers two factors: users' perception of threat and their belief in their ability to effectively avoid it by taking protective actions (efficacy). This process is influenced by individuals' risk tolerance. TTAT highlights two types of factors: individual traits and contextual variables. The first describes individual characteristics, and the second concerns the individual's environment.

These theories provide a theoretical context in which criminal behavior results from both individual and environmental characteristics.

To further illustrate the role of social and economic context in criminal behavior, research on immigration and crime provides additional insights. Research on the relationship between immigration and crime highlights the importance of cultural and socioeconomic factors (Coccia

et al., 2024). According to criminological theories, crime among immigrants can be explained by the importation model, cultural conflict, bias, or strain theory. The importation model suggests that some immigrants may come from high-crime areas and bring those behaviors with them. Cultural conflict theory posits that crime results from differences in norms and practices between immigrants' origin countries and their new countries due to traditions or norms. The bias model proposes that immigrants may be overrepresented in crime statistics due to discrimination and bias. Strain theory was discussed earlier. Except for bias, the others are directly related to social, economic, or cultural factors. However, such research serves only as a proxy since it includes crimes (e.g., violent crimes, homicide, sexual violence) that do not exist in cyberspace. The research confirms strain resulting from unemployment among immigrants who experience feelings of relative deprivation compared to employed native residents, which may lead to crime, including theft and expressive crimes.

Strain Theory forms the basis for analyzing the impact of socioeconomic factors on cybercrime. While rational crime theory is popular among mainstream economists, it does not fully incorporate institutional and social pressures on individuals and their behavior. Strain Theory explains how environmental elements can lead to individual actions or vulnerabilities.

Strain Theory is also a useful tool in exploring cyberbullying behaviors (Lee, Sanchez, 2018; Songsrirote, 2025). Academic shortcomings and the risk of losing scholarships were strongly correlated with cyberbullying. Students experiencing frustration tended to lash out, which created feedback loops affecting both perpetrators and victims. Interestingly, higher anonymity was associated with fewer incidents of cyberbullying.

Social Capital Theory, in the context of this article, focuses on "…how community networks and access to social resources influence individuals' vulnerability to cybercrime" (Songsrirote, 2025). Disadvantaged and lower socioeconomic groups often have limited access to social capital in the form of support networks, financial, emotional, and informational resources, making them more vulnerable.

While theories help explain behavioral mechanisms, economic approaches provide a complementary perspective—particularly through cost analysis frameworks. A simple economic approach to analyze the impact of cybercrime on society is through cost analysis. Wiśniewski and Boehlke (2016) distinguish between ex ante and ex post costs. Ex ante costs are additional expenditures due to the need to secure operations and property and exist regardless of whether cybercrime occurs. Ex post costs arise only if cybercrime happens and consist of damage resulting from an attack. Wright and Kumar (2023) further divide costs into prevention costs (ex ante), and first-order and second-order costs (ex post). First-order costs involve immediate financial, personal, or property losses, while second-order costs involve responses by victims or organizations (government, law enforcement). Threat avoidance behavior generates ex ante costs. Individuals fearing cybercrime are less likely to engage in online purchasing or banking, resulting in missed economic opportunities. This effect is more

pronounced in property crimes than interpersonal crimes and is strongly correlated with fear of offline crimes (Guedes et al., 2025).

Regional development plays a foundational role in cybercrime prevalence. Poverty, unemployment, and income inequality create societal strain that may lead to opportunistic behavior and cybercrime. Five main groups of factors influence cybercrime: social, economic, political, technological, and cybersecurity-specific (Chen et al., 2023). Research using generalized linear models shows that in low-income countries, cybercrime correlates strongly with higher education levels and internet access. In high-income countries, cybercrime relates more to income inequality (Gini Index) and wages in certain industries, particularly among highly skilled but undervalued individuals. These findings highlight research limitations; different factors influence cybercrime depending on a country's institutional framework and development level (Brosnan, 2018).

Building on the role of regional development, comparative research highlights notable differences in cybercrime dynamics between developed and developing countries. There are disparities in cybercrime incidence between developed and developing countries. High-income, technologically advanced countries experience more cybercrime. Tiutiunyk et al. (2024) identify factors such as population density, education, income level, and income inequality as drivers. Cybercrime causes not only economic losses but also emotional trauma. Individual vulnerabilities are the main weaknesses of social systems. Therefore, both monitoring and counteracting systems, along with public awareness programs to shape social and cultural attitudes, are necessary.

Previous research has investigated demographic, socioeconomic, and technological determinants of cybercrime (Padyab et al., 2024). These predictors tend to be context-specific and inconsistent. Sociodemographic variables are frequently used but show varying effects across groups. Women generally face a higher risk of harassment, although this is less significant in some professional settings such as academia. Regarding education, both lower and higher education levels have been associated with increased victimization, depending on the cybercrime type and other variables. Two consistent factors are prior offline victimization and interaction with digital platforms. Offline victimization is part of a broader vulnerability pattern, while online participation in communities and social media increases the risk of cybercrime victimization.

Taken together, these diverse predictors point to a broader pattern—one that shifts focus from attackers to the vulnerabilities embedded in target environments. To conclude, socioeconomic factors do not directly influence attackers, who often operate outside the target environment, but rather affect the resilience of environments against attacks.

Cybercrime poses less immediate physical risk than traditional crime. For example, in-person mugging or bullying can result in direct harm to perpetrators, which is generally absent in the digital sphere. Digital victimization is defined as "victimization (which are intentional, unwanted, nonessential, and harmful experiences) perpetrated with the assistance

of computerized technology, such as desktops, the Internet, or cell phones" (Hamby et al., 2018). Cyberbullying, harassment, and phishing are relatively well documented and researched. Research on financially motivated cybercrime is less developed but suggests it causes higher distress and greater impact on victims (Hamby et al., 2018), not only due to property loss but also because of direct contact with criminals. Most cybercrimes of this type involve deception or criminals boasting about their actions.

Providing cybersecurity is a complex task that requires considering technological, social, and individual factors. Cybersecurity programs must determine appropriate levels of user access and control based on resource needs and establish ROI for various expenditure scenarios. At the individual level, training must address staff fears and uncertainties both at work and in private life. Long-term success depends on creating feedback loops and preparing for emerging risks (Sabillon et al., 2016).

Property cybercrime, in a broader context, not only causes direct financial losses but also acts as a "tax on innovation" by disrupting innovation, market competition, and lowering returns for investors. This slows global technological progress (Songsrirote, 2025).

Cybercrime is more than just a technological problem. Since the Internet's inception, there has been a growing distinction between the "real" and "virtual" worlds. Cyberspace emphasizes both technical infrastructure and the deeply social, evolving community. Economically, cybercrime has become the black market of cyberspace. It is widespread, low-risk, and profitable, supported by a robust ecosystem of people with varying skill levels and specializations. Effective cybersecurity requires a better understanding of cybercrime (Malecki, 2017).

Yarovenko et al. (2023) identify factors influencing and influenced by cybercrime: corruption, crime levels, financial instability, and cryptocurrencies. Crime and the shadow economy often benefit from cybercrime. Existing illegal activities can be expanded or moved into the digital sphere.

3. Methods and results

Vector Autocorrelation model (VAR) was used in research. There were two reasons to use it. First is to check impulse response in data. Secon is based on the principles on the model (Akkaya, 2021):

- There are no internal and external presuppositions in the system.
- There is no zero-type restriction.
- There is no rigorous basic economic theory on which the model is based.

These principles are essential for research in cybercrime impact on economy and vice versa. Models need to be fully empirical, due to lack or conflicting theoretical assumptions. Another advantage of VAR in this type of research is that they reveal the connection between variables in terms of lags.

Data was analyzed using GRETL software.

Based on the literature and availability quarterly data about selected variables was gathered. All the data are for the 2004-2023 timespan. List of all variables, their description and sources are in table 1.

The are two variables related to the labor market. Unemployment takes into consideration whole population, where as "Wages Week Avg" focuses on wages in computer-related sectors. This allows us to capture both general population and specific, digital-related group situation. The same principia were used to gather data about GDP and e-commerce. One focuses on the whole economy and another on the sector that is the most vulnerable to cybercrime. Literature also focused on the devices used by population, so RSEAS were added to include this factor. Economics Uncertainty was included to provide perspective on expectation that may influence social capital. There was no direct data about cybercrime from this time frame and quarterly. Data about vulnerability (both technical and sociotechnical) were used as proxy. "Quick cash" variable represents changes in risky behavior in population. The more desperate the individuals are the more likely it is to search for quick ways to make money. This exposes them to the various types of scams. Logarithms were used on data and then they were normalized, due to large differences in values and units of measurement. Table 2 presents a correlation matrix for the data.

Due to its very high correlation with both GDP ($r = 0.98$) and Ecommerce ($r = 0.96$), the variable representing average weekly wages was excluded from the final specification to avoid multicollinearity and overlapping effects. This simplification improves interpretability without sacrificing model fit or statistical validity.

The first step in VAR estimation was to choose the lag (Osińska, 2007). The three criteria were used: Akaike (AIC), Schwarz-Bayesian (BIC) and Hannah-Quinn (HQC). On this basis lag 3 were chosen as it is the optimal solution according to AIC and HQC. BIC suggests that lag 1 should be used. Table 3 showcases result of these criteria.

Table 4 presents Equation 1 with Vulnerabilities as dependent variable.

First equation showcases statistically significant autoregressive behavior ($p < 0.001$). It is positively signed (0.62), which means that the increase in vulnerabilities in the previous quarter relates to a higher level of vulnerabilities in the current period.

The first and second lags of GDP are statistically significant which proves that economic activity plays an important role in explaining cybersecurity vulnerabilities. Due to first lag having a positive effect and second negative relationship over time may be nonlinear and dynamic. This may warrant further investigation with more advanced modeling techniques.

"Quick cash" which is proxy for risky behavior is significant in the model. This means that risky behaviors in the past result in less vulnerabilities in the present. One of the aspects of a good cybersecurity system is it ability to adapt to emerging threats which this variable proves.

Another significant variable is e-commerce. Increase in e-commerce results in decrease in vulnerabilities. This may be due to increased investment in cybersecurity and increase in awareness. RSEAS is also significant and the increase in sales of electronics decreases vulnerabilities. Unemployment is significant and the increase in it results in increased vulnerabilities, which are consistent with literature.

Table 5. include all the statistics for the first equation of VAR.

The regression model explains about 97% of the variance in the dependent variable, as indicated by a high R-squared value (0.969333) and an adjusted R-squared of 0.959816, suggesting a very good fit.

The F-test confirms that the included explanatory variables jointly have a strong effect on the dependent variable.

The Durbin-Watson statistics are approximately 2.00, indicating no significant autocorrelation problem in the residuals, which is also supported by the low autocorrelation coefficient (-0.040869)

Overall, the model appears robust, with well-fitting explanatory variables and no major econometric issues detected in terms of residual autocorrelation.

Table 6 presents Equation 2 with GDP as a dependent variable.

The second equation provides predictable results. Past (GDP_1) values of GDP have significant and positive effect on current GDP. Beyond that, the Economic Policy Uncertainty Index and Unemployment are significant and have negative impact on GDP. E-Commerce and RSEAS are significant and have positive impact on GDP as they are part of it.

Table 7. include all the statistics for the second equation of VAR.

The regression model explains about 99.96% of the variance in the dependent variable, as indicated by a very high R-squared value (0.999599) and an adjusted R-squared of 0.999474, suggesting an excellent fit.

The F-test confirms that the included explanatory variables jointly have a highly significant effect on the dependent variable ($p < 0.001$).

The Durbin-Watson statistics are approximately 2.29, indicating no significant autocorrelation problem in the residuals, which is also supported by the moderately low autocorrelation coefficient (−0.175306).

Overall, the model appears highly robust, with well-fitting explanatory variables and no major econometric issues detected regarding residual autocorrelation.

For the model series of tests were conducted. The Portmanteau test does not reject the null hypothesis of no residual autocorrelation up to lag 19 ($p = 0.1938$), indicating that the residuals behave as white noise globally. The ARCH test up to lag 4 returns high p-values across all lags

(e.g., 0.9471 at lag 1), suggesting no presence of autoregressive conditional heteroscedasticity — a desirable feature for consistent OLS estimators in the system.

The Doornik-Hansen multivariate normality test does not reject the null hypothesis ($p = 0.1321$), indicating that the joint distribution of residuals is not significantly different from multivariate normality. This supports the reliability of inference in the model, especially regarding hypothesis testing and impulse response functions.

Figure 1 presents impulse response in VAR model. The impulse response analysis reveals key dynamic interactions between the variables in the VAR system over a 20-quarter horizon:

- **Vulnerabilities → Vulnerabilities**:
  A one-standard-deviation shock to cybersecurity vulnerabilities results in an immediate positive effect on the same variable, which gradually dissipates over the first 5 quarters. This pattern suggests short-term persistence in cyber risk.
- **GDP → Vulnerabilities**:
  An exogenous increase in GDP leads to a rise in vulnerabilities in the first quarter. This effect diminishes rapidly by the 10th quarter and then tapers off more slowly until approximately quarter 20. This indicates that economic growth initially exacerbates cyber risk—potentially through increased digital exposure—before longer-term stabilizing mechanisms (e.g., investment in cybersecurity or policy adjustments) begin to take effect.
- **Vulnerabilities → GDP**:
  A shock to vulnerabilities initially exerts a small negative impact on GDP, which intensifies in the first quarter. In the second quarter, the economy partially recovers, but the negative effect deepens again, reaching its trough around the 7th quarter. From there, the adverse impact gradually diminishes over the remaining forecast horizon. This response suggests a delayed and non-monotonic economic cost of cyber risks, potentially reflecting the lagged adaptation of institutions and markets to security threats.
- **GDP → GDP**:
  A positive GDP shock leads to a sustained expansion, peaking around the 3rd quarter, followed by a gradual return to baseline over the following quarters. This pattern reflects the typical propagation of business cycle dynamics, where economic momentum persists for a short time before reverting due to stabilizing feedback.

4. Discussion

The results of VAR offered insights into the interrelationship between socioeconomic factors, cybercrime and economic activity. They confirm that cybercrime is multifaced and interdisciplinary problem.

The first key finding is that past levels of exposure to cybercrime significantly shape current risk levels. This means that vulnerabilities are not individual shocks but are persistent over time. Due to this a long-term strategy is necessary that involves constant learning and improving.

The second notable observation is the dual impact of GDP on vulnerabilities. Economic growth initially increases cybersecurity vulnerabilities. However, over time, this effect stabilizes, likely because of increased investment in protective infrastructure and institutional adaptation. This highlights the non-linear nature of the relationship between economic development and cyber risk—a point often overlooked in the literature.

The opposite—vulnerabilities affecting GDP—is equally important. The analysis reveals a delayed and fluctuating negative impact of cybercrime on GDP. This pattern indicates that the economy does not respond to shocks in a linear way. Instead, institutional order and adaptation delays may amplify economic costs over several quarters before recovery starts. Such lagged responses have important implications for both economic forecasting and cybersecurity policy, stressing the need for active rather than reactive approaches.

The effect of labor market conditions, particularly unemployment, on vulnerabilities confirms the relevance of social pressure mechanisms—consistent with General Strain Theory. Higher unemployment correlates with higher levels of vulnerability, possibly due to increased exposure to risky online behaviors or reduced access to protective technologies. The inclusion of the “quick cash” proxy further supports the behavioral foundation of cyber risk, indicating that desperation-driven behavior may initially increase risk but potentially lead to adaptation in subsequent periods.

From a methodological standpoint, the VAR model proved to be a robust tool, particularly given the absence of strong theoretical consensus in the field. The impulse response functions complement the static regression results by revealing the temporal structure and asymmetries in variable interactions.

5. Summary

In conclusion, this study highlights the necessity of treating cybercrime not merely as a technical phenomenon, but as a complex, systemic issue embedded in economic and social dynamics. Vulnerabilities are shaped not only by technological configurations but also by

economic conditions, labor markets, and behavioral incentives. Likewise, the consequences of cyber risk extend far beyond the digital sphere, exerting measurable macroeconomic effects over time.

References

1. Agustina, J.R. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology*, pp. 35-54. https://doi.org/10.5281/zenodo.22239
2. Aissaoui, N. (2022). The digital divide: a literature review and some directions for future research in light of COVID-19. *Global Knowledge, Memory and Communication*, pp. 686-708. https://doi.org/10.1108/GKMC-06-2020-0075
3. Akkaya, M. (2021). Vector Autoregressive Model and Analysis. In: B.A. Mercangöz (Eds.), *Handbook of Reseach on Emerging Theories, Models and Applications of Financial Econometrics* (pp. 197-214). Springer.
4. Alphabet (2025). *Google Trends*. Retrieved from: https://trends.google.com/trends/, 06.2025.
5. Becker, G.S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, pp. 169-217. https://doi.org/https://doi.org/10.1086/259394
6. Brosnan, S. (2018). The Socioeconomic Determinants of Crime in Ireland from 2003-2012. *The Economic and Social Review*, pp. 127-143
7. 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 and Social Sciences Communications volume*. https://doi.org/https://doi.org/10.1057/s41599-023-01560-x
8. Coccia, M., Cohn, E.G., Kakar, S. (2024). How immigration, level of unemployment, and income inequality affect crime in Europe. *Crime, Law and Social Change*, pp. 363-385. https://doi.org/https://doi.org/10.1007/s10611-024-10144-y
9. Draca, M., Machin, S. (2015). Crime and Economic Incentives. *The Annual Review of Economics*, pp. 389-408. https://doi.org/10.1146/annurev-economics-080614-115808
10. Federal Reserve Economic Data (2025). *Federal Reserve Economic Data*. Retrieved from: https://fred.stlouisfed.org/, 20.06.2025.
11. Forst, B. (1994). *The Socio-economics of Crime and Justice.* Routledge. https://doi.org/https://doi.org/10.4324/9781315486291
12. Guedes, I.S., Martins, J., Moreira, S. (2025). Explaining fear of cybercrime: A focus on interpersonal and property cybercrime differences. *European Journal of Criminology*. https://doi.org/https://doi.org/10.1177/14773708241312820

13. Hamby, S., Blount, Z., Smith, A., Jones, L., Mitchell, K., Taylor, E. (2018). Digital poly-victimization: The increasing importance of online crime and harassment to the burden of victimization. *Journal of Trauma & Dissociation*, pp. 382-398. https://doi.org/10.1080/15299732.2018.1441357
14. Ilany-Tzur, N., Fink, L. (2025). Device and risk-avoidance behavior in the context of cybersecurity phishing attacks. *International Journal of Information Management*. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2025.102919
15. Kosiński, J. (2015). *Paradygmaty cyberprzestępczości.* Warszawa: Difin.
16. Lee, G., Sanchez, M. (2018). Cyber Bullying Behaviors, Anonymity, and General Strain Theory: A Study of Undergraduate Students at a South Eastern University in the United States. *International Journal of Cyber Criminology*, pp. 84-96. https://doi.org/10.5281/zenodo.1467846
17. Lee, G., Sanchez, M. (2018). Cyber Bullying Behaviors, Anonymity, and General Strain Theory: A Study of Undergraduate Students at a South Eastern University in the United States. *International Journal of Cyber Criminology*. https://doi.org/10.5281/zenodo.1467846
18. Malecki, E.J. (2017). Real people, virtual places, and the spaces in between. *Socio-Economic Planning Sciences*, pp. 3-12. https://doi.org/https://doi.org/10.1016/j.seps.2016.10.008
19. Mitnick, K., Simon, W.L. (2016). *Sztuka podstępu. Łamałem ludzi, nie hasła.* Warszawa: Helion.
20. National Vulnerability Database (2025). *National Vulnerability Database*. Retrieved from: https://nvd.nist.gov/, 20.06.2025.
21. Osińska, M. (2007). *Ekonometria współczesna.* Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa "Dom Organizatora".
22. Padyab, M., Padyab, A., Rostami, A., Ghazinour, M. (2024). Cybercrime in Nordic countries: a scoping review on demographic, socioeconomic, and technological determinants. *SN Social Sciences*. https://doi.org/https://doi.org/10.1007/s43545-024-00990-x
23. Sabillon, R., Cano, J., Cavaller, V., Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*, pp. 165-176.
24. Songsrirote, N. (2025). Socioeconomic Determinants of Cybercrime Costs: A Panel Data Analysis of OECD Countries. *Asian Journal of Applied Economics*, pp. 30-57.
25. Suler, J. (2004). The Online Disinhibition Effect. *Cyber Psychology & Behavior*, pp. 321-326. https://doi.org/10.1089/1094931041291295
26. The Bureau of Labor Statistics (2025). *QCEW Data Files*. Retrieved from: https://www.bls.gov/cew/downloadable-data-files.htm, 20.06.2025.

27. The Census Bureau (2025). *The Census Bureau*. Retrieved from: https://www.census.gov/, 20.06.2025.
28. The U.S. Bureau of Economic Analysis (2025). *The U.S. Bureau of Economic Analysis*. Retrieved from: https://www.bea.gov/, 20.06.2025.
29. Tisdale, N. (2024). *The Hidden Injustice of Cyberattacks.* Retrieved from: https://www.wired.com/story/cybersecurity-marginalized-communities-problem/
30. Tiutiunyk, I., Pozovna, I., Zaskorski, W. (2024). Innovative Approaches to Ensuring Cybersecurity and Public Safety: The Socio-Economic Dimension. *Marketing i Menedžment Innovacij*, pp. 127-140. https://doi.org/https://doi.org/10.21272/mmi.2024.4-10
31. Vassilakopoulou, P., Hustad, E. (2021). Bridging Digital Divides: a Literature Review and Research Agenda for Information Systems Research. *Information Systems Frontiers*, pp. 955-969. https://doi.org/10.1007/s10796-020-10096-3
32. Winter, H. (2019). *The Economics of Crime: An Introduction to Rational Crime Analysis.* Routledge.
33. Wiśniewski, P., Boehlke, J. (2016). *Cyberprzestępczość w gospodarce.* Wydawnictwo Naukowe UMK.
34. Wright, D., Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*. https://doi.org/https://doi.org/10.1016/j.socimp.2023.100013
35. Yarovenko, H., Lopatka, A., Vasilyeva, T., Vida, I. (2023). Socio-Economic Profiles Of Countries – Cybercrime Victims. *Economics and Sociology*, pp. 167-194. https://doi.org/10.14254/2071-789X.2023/16-2/11

Appendix

Table 1.
Variables description

Variable name	Description	Source
Vulnerabilities	The variable represents the count of reported software vulnerabilities over time, sourced from the National Vulnerability Database (NVD), capturing trends in security risks for various products.	National Vulnerability Database
Wages Week Avg	Average weekly wages in the Computer Systems Design and Related Services sector	QCEW Data Files
GDP	Gross Domestic Product	The U.S. Bureau of Economic Analysis
Unemployment	Unemployment in USA	U.S. Bureau of Labor Statistics
Economic Policy Uncertainty Index	Measure of policy-related economic uncertainty	Federal Reserve Economic Data
E-commerce	U.S. retail e-commerce sales	Census Bureau
RSEAS	Advance Retail Sales: Electronics and Appliance Stores	Federal Reserve Economic Data
Quick cash	Popularity of the term "quick cash" in Google Searches	Google Trends

Source: Own research based on (National Vulnerability Database, 2025) (The Bureau of Labor Statistics, 2025) (The U.S. Bureau of Economic Analysis, 2025) (Federal Reserve Economic Data, 2025) (The Census Bureau, 2025) (Alphabet, 2025).

Table 2.
Correlation matrix

	Vulnerabilities	**GDP**	**Wages Week Avg**	**Unemployment**	**Economic Policy**	**Ecommerce**	**RSEAS**	**Quick cash**
Vulnerabilities	1.0000	0.9393	0.9006	-0.4619	0.2862	0.9383	-0.5954	0.3475
GDP	0.9393	1.0000	0.9836	-0.4269	0.2597	0.9694	-0.5961	0.5308
Wages Week Avg	0.9006	0.9836	1.0000	-0.3388	0.3359	0.9609	-0.6259	0.5517
Unemployment	-0.4619	-0.4269	-0.3388	1.0000	0.5283	-0.3708	-0.0864	-0.3079
EconomicPolicy	0.2862	0.2597	0.3359	0.5283	1.0000	0.3478	-0.6403	-0.0861
Ecommerce	0.9383	0.9694	0.9609	-0.3708	0.3478	1.0000	-0.6584	0.3928
RSEAS	-0.5954	-0.5961	-0.6259	-0.0864	-0.6403	-0.6584	1.0000	-0.2395
Quickcash	0.3475	0.5308	0.5517	-0.3079	-0.0861	0.3928	-0.2395	1.0000

Source: Own research.

Table 3.
AIC, BIC and HQC

Lag	AIC	BIC	HQC
1	-5,23673	-4,30265	-4,86411
2	-5,28885	-4,23023	-4,86655
3	-5,44138	-4,25821	-4,9694
4	-5,43238	-4,12467	-4,91072
5	-5,33067	-3,89841	-4,75932
6	-5,31701	-3,76021	-4,69598

Source: Own research.

Table 4.
Equation 1. Dependent variable: Vulnerabilities

Variable	Coefficient	Std. Error	t-Statistic	p-value
Vulnerabilities_1	0.616714	0.131999	4.672	1.82e-05
Vulnerabilities_2	-0.008839	0.145770	-0.06064	0.9519
Vulnerabilities_3	-0.030466	0.122545	-0.2486	0.8045
GDP_1	2.80810	0.875968	3.206	0.0022
GDP_2	-2.27788	0.919589	-2.477	0.0162
GDP_3	0.024083	0.360572	0.06679	0.9470
Unemployment	0.111220	0.078470	1.417	0.1617
Unemployment_1	0.016061	0.110197	0.1457	0.8846
Unemployment_2	-0.219804	0.100291	-2.192	0.0324
Ecommerce	-0.449997	0.170331	-2.642	0.0106
Ecommerce_2	0.202906	0.214988	0.9438	0.3492
RSEAS	0.108814	0.074854	1.454	0.1514
RSEAS_1	-0.179765	0.090084	-1.996	0.0507
RSEAS_2	0.011843	0.079096	0.1497	0.8815
Quickcash_2	-0.080630	0.045841	-1.759	0.0839
Economic Policy Uncertainty	0.030920	0.034588	0.8940	0.3750
S1	-0.041253	0.060789	-0.6786	0.5001
S2	-0.035535	0.069239	-0.5132	0.6097
S3	-0.085365	0.062684	-1.362	0.1785

Source: Own research.

Table 5.
Statistics of the first equation

Statistic	Value
Mean dependent variable	-0.105669
Std. dev. dependent variable	0.785175
Sum squared residuals	1.463244
Standard error of residuals	0.158834
R-squared	0.969333
Adjusted R-squared	0.959816
F-statistic (19, 58)	96.488
Prob(F-statistic)	8.06e-37
Autocorrelation residual rho1	-0.040869
Durbin-Watson statistic	2.002

Source: Own research.

Table 6.
Equation 2. Dependent variable: GDP

Variable	Coefficient	Standard Error	Student's t	p-value
Vulnerabilities_1	-0,00938022	0,0168323	-0,5573	0,5795
Vulnerabilities_2	0,0272498	0,0185883	1,466	0,1481
Vulnerabilities_3	-0,0216680	0,0156267	-1,387	0,1709
GDP_1	1,08921	0,111702	9,751	7,84e-14
GDP_2	0,00580047	0,117264	0,04946	0,9607
GDP_3	-0,170890	0,0459795	-3,717	0,0005
Unemployment	-0,0734403	0,0100063	-7,339	7,88e-10
Unemployment_1	0,0994994	0,0140522	7,081	2,15e-09
Unemployment_2	-0,0208484	0,0127889	-1,630	0,1085
Ecommerce	0,110543	0,0217204	5,089	4,06e-06
Ecommerce_2	-0,0154859	0,0274150	-0,5649	0,5743
RSEAS	0,0235436	0,00954529	2,467	0,0166
RSEAS_1	-0,0299520	0,0114874	-2,607	0,0116
RSEAS_2	0,00847335	0,0100862	0,8401	0,4043
Quickcash_2	0,00378002	0,00584554	0,6467	0,5204
Economic Policy Un~	-0,00968209	0,00441059	-2,195	0,0322
S1	0,0197387	0,00775176	2,546	0,0136
S2	0,0383029	0,00882924	4,338	5,81e-05
S3	0,0371427	0,00799337	4,647	1,99e-05

Source: Own research.

Table 7.
Statistics of the second equation

Statistic	Value
Mean of dependent variable	−0.062483
Standard deviation of dependent variable	0.880973
Sum of squared residuals	0.023794
Residual standard error	0.020254
R-squared	0.999599
Adjusted R-squared	0.999474
F-statistic (19, 58)	7602.990
p-value for F-test	2.54e-91
Residual autocorrelation - rho1	−0.175306
Durbin-Watson statistic	2.287933

Source: Own research.

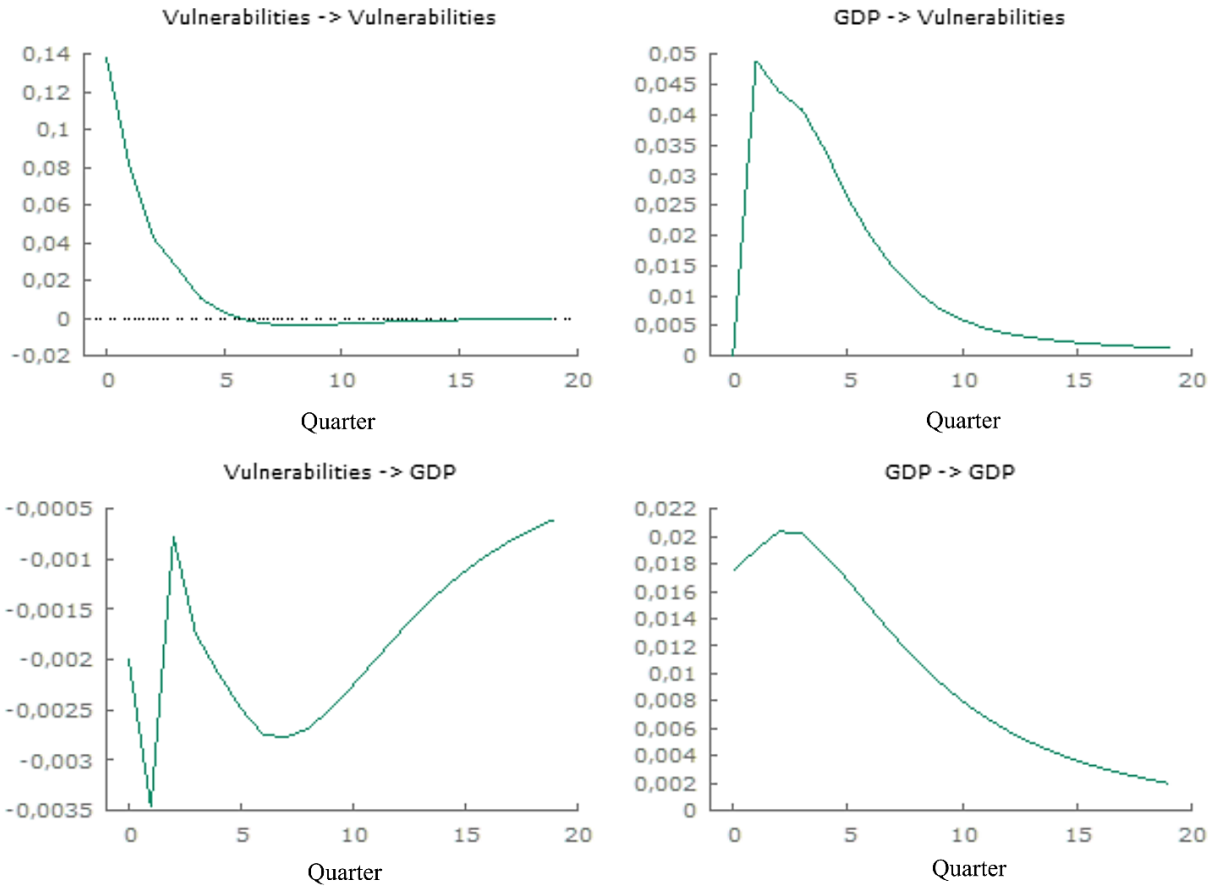

Figure 1. Impulse response in VAR model.

Source: Own research.