Economic and Social Drivers of Cybercrime

Teodore Giorgobiani *

* LCC International University, Klaipėda, Lithuania,
ORCID: https://orcid.org/0009-0009-8054-0974,
e-mail: Teodore.giorgobiani.work@gmail.com

DOI: 10.32353/khrife.4.2024.10 UDC 004.49:343.9
Received: 14.10.2024 / Reviewed: 18.10.2024 / Accepted for printing: 25.12.2024 /
Available online: 31.12.2024

The present paper aims to promote an understanding of relatively recent social phenomena such as cybercrime. Modern global realities of technological advancements and heavy dependence on digital tools emphasize threats cybercrime presents. Therefore, it is important to examine factors driving cybercrime rates to create effective preventive mechanisms. The paper uses regression analysis built on the recently published, first-ever World Cybercrime Index. Cybercrime scores of 94 countries were analyzed based on the effect of 6 predictor variables. Analysis displayed that the degree of economic freedom has an inverse effect on cybercrime scores, and innovation level directly increases cybercrime rates with less probability. It is recommended for researchers interested in the topic to be attentive to future releases of WCI to be able to conduct more massive, time-series analysis.

Keywords: *economic factors; cybercrime; regression analysis; economic freedom index.*

Introduction

Modern global social and development environments can be described as an era of technological advancements. The daily lives of billions of people are strongly influenced by technology. Most industries and sectors' operations heavily depend on

This article is translation of the original Ukrainian content, which source is available at the link: *https://khrife-journal.org/index.php/journal* (translated by Andriy Bublikov). The author acknowledges translation as corresponding to the original.

computing systems and technological advancements. Such environment promoted the creation of a relatively recent form of delinquency called cybercrime. Cybercrime encompasses a wide range of illegal activities carried out using digital devices or networks. Such activities include various forms of fraud, identity theft, data breaches, computer viruses, scams, and expanded upon in other malicious acts. Similarly to other social occurrences, there are specific reasons and factors driving rates of cybercrime and pushing cybercriminals towards committing illegal activities. It is important to examine the factors influencing the rates of cybercrime across the globe in order to be able to identify conditions encouraging an expansion of digital crimes and prevent them from occurring. Moreover, the economic conditions of people are often one of the main reasons pushing them to commit malicious acts. Additionally, the fields of cyber forensics and criminalistics have become essential in addressing cybercrime. These disciplines focus on the identification, collection, and analysis of digital evidence, which is crucial for tracking cybercriminal activities and developing effective preventive measures. The present research aims to find the relationship between various economic and social factors and the rates of cybercrime across the globe.

Literature Review

One of the most prominent sociological theories that tries to explain social behavior is Rational Choice Theory. Rational choice theory tries to predict human behavior stating that people are rational actors evaluating the cost-benefit of their actions (Abell, 2000; Hechter, 1992; Hodgson, 2012). The theory distinguishes between two main approaches: people maximize manifest payoffs and people maximize profitability. While the first approach that people maximize manifest payoffs was falsified by empirical analyses, the second claim that society maximizes utility is supported. The utility is unfalsifiable as it is an inherited behavior that can be observed even in non-human organisms. Such wide applicability is perceived as a weakness as it does not account for specificities of history, socio-economic systems, and other distinguishable human factors.

Rational Choice Theory is a great tool for explaining the actions of cybercriminals. Based on the theory, economic benefits are the main driver for people to commit cybercrime (Laszka & Schwartz, 2016; Li & Whinston, 2020; Milgrom & Roberts, 1988). Cybercriminals are accessing the risks of being caught against the financial opportunities they might gain. Li and Whinston (2020) point out that with the development of cyber-currency, the risks of being caught went down as monetary transactions in cryptocurrencies are harder to track. Another factor influencing the actions of cybercriminals is interdependent cybersecurity (Laszka & Schwartz, 2016). If the network security is perceived as weak due to inadequate investments by other users, the perceived costs of engaging in cybercrime are reduced, making it more attractive. Moreover, the rational actions of cybercriminals can also be seen in their reputation management techniques (Holt & Bossler, 2014; Kshetri, 2006). They often honestly return the stolen data after the victims pay a ransom so that future victims will confidently be willing to pay them. Moreover, the lack of law enforcement and international law mechanisms reduces the risks of facing harsh punishments, making such an activity attractive for people seeking economic gains.

Another theory that is applicable to explain cybercrimes is Routine Activity Theory (RAT). RAT is a theory focused

on explaining the patterns in criminal activities (Cohen & Felson, 1979; Felson, 1987; Felson & Clarke, 1998). It shifts its focus from the nature of criminals and concentrates on the environment suitable for crime to occur. RAT emphasizes three key elements for crime to exist: the existence of a motivated criminal, the presence of a suitable target, and the absence of a guardian preventing the crime. Based on the theory, the lack of any of these elements, results in the prevention of crime. The theory explains how daily, routine, actions of people help to bring these three elements together and tries to explore the crime trends. For instance, the Routine Activity Theory explains that the dispersion of activities away from households and families increases opportunities for crime. Also, crime has been rising with the popularization of more durable, light goods, which increased the number of potential targets, and the increase of female labor which raised the absence of unguarded households.

The concept of Routine Activity Theory can be applied to cybercrimes by incorporating its three core pillars of motivated criminals, suitable targets, and absence of guardianship and analyzing their applicability to the scale of cybercrimes (Ahmad & Thurasamy, 2022; Kigerl, 2012; Leukfeldt & Yar, 2016). Existing literature highlights that the most important factor influencing increasing trends of cyberattacks is target visibility. Online routine activities like shopping and banking expose potential targets to criminals. On the other hand, financial gains from a single crime are less significant in predicting the trends as the offenders might exploit the vast accessibility of targets online rather than focusing on high-value individuals. The applicability of RAT to cybercrimes has also been accessed on the international level (Kigerl, 2012). The results displayed that countries with higher numbers of internet users and loose legal mechanisms against cybercrime are more often encountering cyberattacks. Offenders are more likely to come from places with high unemployment levels and a significant percentage of the population having IT skills.

Unlike Routine Activity Theory, Strain Theory tries to explain the reason for a person to commit delinquencies. Strain Theory is a sociological concept focused on explaining the actions of crimes through the perspective of social influence (Agnew, 1992; Agnew & Brezina, 2019). Unlike other sociological theories focusing on social and individual relations in one's crimes like Social Control Theory and Social Learning Theory, the Strain Theory highlights the negative relations that lead individuals to feel strain due to being treated in undesired ways. Negative relations cause increased negative emotions like anger, which encourages individuals to pursue delinquency as a coping mechanism. The theory emphasizes three main sources of strain: failure to achieve positively valued goals, removal of positively valued stimuli, and presentation of negative stimuli. The theory recognizes that individuals might react to the same environment and conditions differently and suggests possible reasons for a person to copy strain with delinquency: availability of coping resources, individual temperament and personality, social environment, and perceived legitimacy of coping strategies.

General Strain Theory can be useful for explaining the behavior of cybercriminals. Cyberspace can become an effective environment for people to copy their strain (Chism & Steinmetz, 2017; Hay & Ray, 2020). For example, academic failure can lead individuals to pursue cyberbullying as an attempt to feel control and power. Similarly, financial strain can influence one to engage in cybercrimes. A strain for cyber-

crime might also occur for the victims of such cybercrime, who might find committing new cybercrimes a way to copy their negative emotions. Moreover, the empirical evidence supports the application of the Strain Theory to crimes (Hay & Ray, 2020). Research has shown that individuals feeling strain are more likely to engage in some form of cyber offending.

Development theories like the Theory of Economic Development by Joseph A. Schumpeter and the Modernization Theory can suggest a comprehensive basis for understanding the threads between cybercrime patterns and states' economic indicators. Unlike traditional approaches to economic development, Schumpeter (2021) highlights the importance of innovation, entrepreneurship, and banking systems. The first concept explained in his theory is a circular economic flow, which is akin to traditional, steady economic development. This is a system that is regularly kept in equilibrium. For economic development, the author points out that such a circular flow has to be disrupted by innovation, which often damages the steady equilibrium. Talented entrepreneurs who are agents for change and development often need investment which must be done through well-organized credit and banking systems. On the other hand, the Modernization Theory tries to explain the basis of societal changes and the transformation of traditional states to modern ones (Inglehart & Baker, 2000). The Theory puts core emphasis on industrialization which leads to economic development, increased education levels, and changes in gender roles, and social norms.

Entrepreneurship has a significant correlation with the prevalence of cybercrime (Kshetri, 2010; Srivastava et al., 2020). Entrepreneurs create various forms of tech and e-commerce companies that become desired targets for cyberattacks. With the increase of innovation and development that is based on entrepreneurial activities and innovation, cybercriminals are lured to actively seek financial gains. In this sense, a clear connection can be seen between Schumpeter's Economic Development Theory and Routine Activity Theories. The positive correlation between economic development and increased cybercrime levels can also be explained by Modernization. Arthur (1991) states that "The modernization theory of crime... has assumed that increased criminality is an unavoidable consequence of socioeconomic and industrial development" (p. 1). Such an approach indicates that with the development and modernization of informational technologies, cybercrime levels also increase.

Another theory that enables us to discuss and speculate reasons and patterns of cybercrimes, is Relative Deprivation Theory. The theory is a sociological concept that emphasizes the importance of self-comparison in one's life (Smith et al., 2019; Webber, 2007). The core principles of the theory are rooted in the concept of comparison. Relative Deprivation Theory states that an individual perceives itself in contrast to others, of normative standards imposed by a commune. Despite the objective conditions of a person, he or she might still feel deprived due to not matching expectations or being around people who are perceived as better. The theory has found its usage in various fields including politics, sociology, health, and criminology. Empirical evidence proves that feelings of relative deprivation might lead to psychological and emotional issues. Relative deprivation can lead to a person feeling anger, frustration, and resentment which can manifest in various forms including through passive dissatisfaction or engagement in various forms of social protests, movements, and fights against the perceived injustice.

As relative deprivation leads to various forms of negative emotions, criminal acts might become a coping mechanism for deprived individuals (Kawachi et al., 1999; Mishra & Novakowski, 2016). Intense feelings of anger and frustration are driving factors for individuals to engage in criminal behavior. Under the influence of such emotions, people are more prone to risky, damaging acts. Moreover, a perceived unequal environment leads to the destruction of social communities, which leads to increased levels of crime. Also, relative deprivation happens in terms of perceived socioeconomic inequality; this leads individuals to engage in criminal acts to raise their self-value. A clear line can be drawn between Relative Deprivation and Strain Theories. The negative feelings caused by relative deprivation are similar to those explored in the Strain theory. Relative deprivation can be one of the causes of social strain.

An important theory in explaining the high crime rates that unify cultural, social, and institutional context is the Institutional Anomie Theory (IAT) (Bernburg, 2002; Chamlin & Cochran, 1995; Bjerregaard & Cochran, 2008). IAT is based on the classical Anomie Theory developed by Émile Durkheim and further elaborated by Robert K. Merton. The theory, in its foundations, is focused on instrumental crime in the industrial society of America. Some of the core concepts that Institutional Anomie Theory incorporates are the social position of non-economic institutions, anomie, monetary culture, and economic institutions. The Anomie is an idea borrowed from classical Anomie theory and it refers to the state of normlessness. The theory explains that cultural emphasis on monetary success in combination with weekend non-economic institutions leads to higher rates of instrumental crimes. For anomie not to emerge, along with strong economic institutions in the state, non-economic institutions such as the family, education, and church must have a strong influence on society to regulate social norms. In a situation where economic institutions overshadow non-economic ones, an individual feels justified in pursuing any means to achieve financial goals. Moreover, the study on the applicability of Institutional Anomie Theory in the cases of cybercrime revealed important insights (Dearden et al., 2021). The research conducted on the 215 self-admitted cybercriminals exposed a curvilinear relationship between Institutional Anomie and cybercrimes which means that both high and low levels of anomie are associated with high cybercrime rates. However, findings showed that a high level of anomie is associated with crimes focused on financial gains such as fraud and scams, while a low anomie level relates to other forms of cyber offenses such as illegal downloads or online drug purchases.

Interactions between political rule and the economic system have been of interest to various economists and social philosophers throughout many centuries. The theories of political economy have been formulated and explored by economists like Adam Smith, Karl Marx, John Maynard Keynes, and others. The essence of the Marxian theory of political economy is the theory of historical materialism (Sweezy, 1943). The theory explains that social superstructures are created fundamentally based on the material conditions of society. Such an idea leads to the assumption that the development of social structures like government, legal and political systems, and ideological systems such as culture, religion, and philosophy is driven by factors like modes of production and the conflicts that arise within them (Albritton, 1993; Heilbroner, 1984; Sweezy, 1943; Rowlinson & Hassard, 2000).

The theory proceeds that the created superstructures can also influence material systems and stabilize the economic base. The theory of political economy addresses complex dynamics of production, distribution, and consumption of goods and services within a society, and how these dynamics are influenced by and influence political decisions, institutions, and structures. In its essence, Marx's work focuses on the inherent issues within the capitalist system. Some of the core ideas of Marxian political economy theory are the labor value and the accumulation of capital. Marx explains that commodity value is determined by the socially necessary time of labor for its creation. However, in the capitalist mode of production, profit is made through the extraction of surplus value from workers which is the difference between the value produced by labor and the wages paid to the laborers. Marx explains that capital accumulation is a process when capitalists reinvest surplus value to create more capital. These two tenets of the capitalist mode of production make the system unstable and prone to issues like underconsumption, overproduction, profit loss, imperialism, and class clash. The government serves primarily as an instrument of the ruling capitalist class, ensuring the conditions necessary for capital accumulation and suppressing challenges to the capitalist order. In his view, the class conflict between the bourgeoisie (capitalist) and proletariat (working class) would inevitably lead to the overthrow of the capitalist mode of production through the revolutionary movements.

The economic issues inherent to the capitalist mode of production also lead to social problems like systemic inequalities, and deprivation of accessible goods for the working class (Chambliss, 1975; Lynch et al., 1994). Lynch et al. (1994) explain that such an environment creates the basis for the increased crime rates. In Marxian views, people are not inherently prone to committing crimes, but it happens due to the socio-economic environment created in the capitalist system. One of the contradictions that exist in such a system is related to the system's dependence on the mass consumption of goods by the proletariat despite capitalism's nature of keeping the working class's purchasing power low. These conditions encourage the proletariat to access desirable goods by illegal means. Moreover, in Marxist theories, the legal system is constructed to serve the capitalist elite to help them maintain dominance and disparity (Chambliss, 1975). This means that criminal law defines such acts as illegal not because they violate moral norms but because they threaten to destabilize a capitalist system. For instance, laws against theft or vagrancy disproportionately target the poor, while white-collar crimes committed by the bourgeoisie often go unpunished. Also, criminal acts have a functional purpose in capitalism by reducing unemployment; such acts not only create jobs for criminals but also for legal workers like policemen, judges, lawyers, and so on.

The constructed theoretical propositions are based on the Rational Choice, Routine Activity, and Marxian Theory of political economy. These theories explain cybercrime and crime rates from multiple levels of analyses including individual, environmental, and institutional. Based on the Marxian theory of political economy, high levels of socio-economic equality, and a more capitalistic economic structure should lead to increased cybercrime rates (TP1). On the other hand, Rational Choice and Routing Activity theories highlight the importance of other factors like levels of low level of cybersecurity, high rates of technological advancement, and high unemployment rates in determining the high degree of cybercrime (TP2).

Methodology

In the context of understanding economic factors that influence cybercrime rates in various countries, it is important to implement a well-suited research methodology that will comprehensively answer the imposed research question, preventing the nuanced nature of data from hindering the success of the work. The section will provide a blueprint of chosen research methodologies and the reasoning behind them. The research implements a quantitative method of data analysis due to its concrete nature and suitability with RQ and theoretical propositions. The primary method used for this research is cross-sectional regression analyses utilizing data from 94 countries.

Regression analysis is a statistical method used primarily in various fields of social sciences, but primarily in econometrics. The regression tries to find statistically significant effects of independent variables on dependent ones. Linear regression was used to analyze the effects of various economic factors on the cybercrime rate in sample 94 countries. One of the main advantages of using regression analyses is that it is one of the rare research methods that can lead to the assumption of causality and help predict influential variables. However, regression has its disadvantages one of which is the possibility to have violated assumptions. The main assumptions that must be tested before proceeding to the regression itself are heteroskedasticity, autocorrelation, multicollinearity, endogeneity, and normality of distribution.

The main tenant for the analyses is the first-ever World Cybercrime Index (WCI) by Bruce et al. (2024). Although, the WCI included all 197 UN countries, only 96 of them received the overall WCI score. The dependent variable for the regression analyses is based on the overall WCI score which ranks and evaluates countries based on their contribution to global cybercrime. Countries with 3 or more missing factor variable values were removed, leaving only 94 states for analysis. Since WCI was first ever published in 2024 and there are no other year evaluations available, it is impossible to execute sophisticated panel data or time-series analyses. As stated by Bruce et al. (2024), the data for constructing WCI was collected in 2021. Therefore, independent variables will be based on the data from 2021. 6 independent variables are implemented to test their relationship with the cybercrime index. 5 variables including Unemployment Rate (UR), Global Innovation Index (GII), Cybersecurity Index (GCI), Economic Freedom Index (EFI), and Economic Inequality Index (EII) are primary factor variables focusing on testing theoretical propositions. In addition, one control variable, Gross Domestic Product per capita (GDPc), was implemented to account for other potential influencers. EFI and EII are implemented to test the claims of Marxian political economy theory on the importance of socio-economic factors and economic structure (capitalism) in determining a country's contribution to a global level of cybercrime. The other 3 variables, including UR, GII, and GCI, are focused on testing the Rational Choice and Routine Activity theories.

Empirical Findings

Before proceeding to the regression, it is crucial to test whether the data holds the assumptions necessary for analyses to go smoothly. Some of the most important assumptions for cross-sectional regression are the normality of distribution, no multicollinearity, and homoscedasticity. The Shapiro-Wilk test displays that all of the variables except for the Economic Inequal-

ity Index are not normally distributed (see Appendix, Figure 2). However, it is expected that abnormal distribution is present in the data for the social sciences. Another important assumption testing of no multicollinearity displayed that the Variance Inflation Factor is less than 4 for each variable. This means that the data is not multicollinear (see Appendix, table 5). Finally, the Brausch-Pagan test with a P-value higher than 0.05 (P-value = 0.6452, see Appendix, table 4) fails to reject the null hypothesis of homoscedasticity and adheres to the assumption.

Descriptive statistics

Descriptive statistics summarize key characteristics of the dataset, highlighting insights into data distribution, central tendency, and variance.

Table 1

Descriptive statistics

	UR	GII	GCI	EII	GDPc	EFI	WCI Score
Valid	94	84	94	94	93	93	94
Missing	0	10	0	0	1	1	0
Median	5.371	34.35	80.56	0.57	10.359	62.5	0.465
Mean	7.024	35.601	67.954	0.563	91.775	62.583	3.01
Std. Deviation	4.816	12.776	31.193	0.088	225.015	11.415	8.288
Minimum	0.396	15	1.35	0.39	1.135	5.2	0.08
Maximum	28.77	65.5	100	0.75	977	82.4	58.39

As Table 1 displays, the variable Global Innovation Index has the most missing values. All other variables combined except for GII have 2 missing values combined. The median of the Global Cybersecurity Index highest of all; however, its mean value is lower than the median. GDP per capita displays the greatest disparity between mean and median values with 91,775 and 10,359 respectively. The variable Economic Freedom Index displays the smallest difference between mean and media.

Before proceeding to the regression analysis, it is important to extract the maximum possible details from the given dataset. One of the methods of analysis for understanding the relation between various variables is a correlation test. The correlation test allows us to find variables that correspond to each other either positively or negatively.

Figure 1

Correlation plot

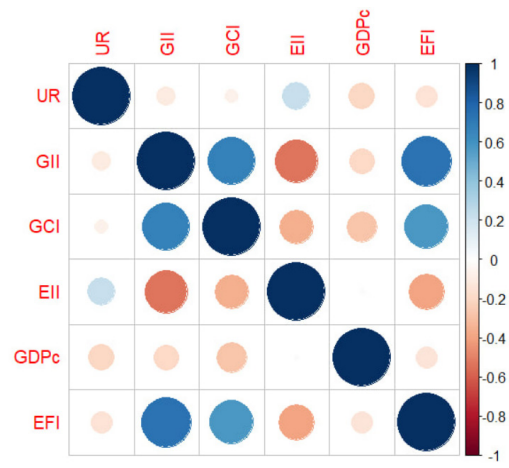

Table 2

Correlation matrix

	UR	GII	GCI	EII	GDPc	EFI
UR	1	-0.1091335	-0.0602019	0.2280698	-0.20087374	-0.1403777
GII	-0.1091335	1	0.6701865	-0.53865332	-0.19488524	0.7396576
GCI	-0.0602019	0.6701865	1	-0.35052724	-0.27615767	0.5710038
EII	0.2280698	-0.5386533	-0.3505272	1	0.01243542	-0.3904422
GDPc	-0.2008737	-0.1948852	-0.2761577	0.01243542	1	-0.1378184
EFI	-0.1403777	0.7396576	0.5710038	-0.39044221	-0.13781837	1

The correlation matrix displayed in Table 2 shows that very strong correlations between independent variables are not found. The highest correlation is between variables Economic Freedom Index and Global Innovation Index, indicating that states with higher economic freedom (more market-oriented economy) tend to have higher levels of innovation. Also, a moderate correlation can be found between the Global Cybersecurity Index and the Global Innovation Index, hinting that states with higher rates of innovation tend to have stronger cybersecurity. Moreover, a degree of correlation exists between economic freedom and cybersecurity strength. Such results show that economic freedom, cybersecurity strength, and rate of innovation are somewhat correlated with each other.

Regression Findings

The present section presents regression analysis with the application of robust standard errors. F-test statistic with a value of 1.713 and p-value of 0.1292 (higher than 0.05) displays that the chosen independent variables (IVs) are not the best in explaining the outcome variables of cybercrime. This finding is supported by an adjusted R-square score of 0.04902 which indicates that the model explains only 4.9 % of the variation of the dependent variable.

Table 3

Regression output

Coefficients:	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	10.02787	11.61819	0.863	0.3908
UR	-0.16519	0.20389	-0.81	0.4203
GII	0.23134	0.13082	1.768	0.0809
GCI	0.07024	0.04851	1.448	0.1517
EII	11.78253	12.72956	0.926	0.3575
GDPc	-0.00136	0.00514	-0.265	0.792
EFI	-0.39756	0.15771	-2.521	0.0138
R-squared	0.1178			
Adjusted R-squared	0.04902			
F-statistic	1.713			0.1292

As Table 3 displays, there is only a single significant variable predicting the World Cybercrime Index score – the Economic Freedom Index. EFI has the appropriate p-value of 0.0138, with a negative estimate score which indicates that higher EFI results in lower cybercrime scores. Another variable that is close to statistical significance with a p-value of 0.0809 is the Global Innovation Index. The estimate of GII is positive, indicating that higher GII scores might result in higher scores in WCI.

Discussion

The results of regression analyses provide ground for understanding the factors influencing the country's contribution to global cybercrime. Firstly, the analysis was held to test the theoretical proposition established based on the literature on cybercrime and crime rates. The first theoretical proposition (TP1) based on Karl Marx's theory of international political economy highlighted two significant factors determining higher crime rates – economic inequality and economic freedom (economic structure). Based on the results of the regression output, the first theoretical proposition was rejected. Analysis shows that economic inequalities do not play a role in determining the cybercrime rate as variable EII was statistically insignificant. Moreover, while Marxian theory explains that a more market-based economic structure leads to higher crime rates, the regression results suggested the opposite – a higher degree of economic freedom leads to decreased levels of cybercrime. One of the claims of the second theoretical proposition (TP2), which is based on Rational Choice and Routine Activity theories, is that increasing innovation rates lead to higher cybercrime rates. This claim can be considered valid, though with a probability value lower than the standard threshold. However, the TP2 is partially rejected as claims on the influence of low cybersecurity levels and higher unemployment rates were not statistically significant.

One of the main reasons for rejecting suggestions proposed by Marxian theory on international political economy might be the different scope and external context of the theory. Although Marxian theories still have a large supporter base and can be relevant in explaining some global events, they are built based on the context of an international order of the 19th century. Apart from the context of the international system, the theory is mainly focused on explaining other types of crime rather than cybercrime. Despite having similar bases, cybercrime conceptually differs from other types of crimes and is a phenomenon developed with the development of technology. The scope and context in which international political economy theory was created might just be irrelevant to modern political, economic, technological, and social contexts.

Moreover, an explanation of the inverse relationship between the Economic Freedom Index and World Cybercrime Index identified by the regression model might be rooted in the results of the correlation test. The correlation matrix displayed that EFI, GII, and GCI have a positive correlation. This means that countries with more free market economies tend to have higher rates of innovation, technological advancement, and cybersecurity rates. Moreover, a more liberal approach to an economic system can be connected to a higher overall level of democracy, hence a better rule of law, and technological literacy. Good rule of law introduces a better legal framework for dealing with cybercrime, while technological literacy enables citizens to use the internet more carefully and acknowledge potential threats. All of the above-mentioned factors hinder levels

of cybercrime because based on the rational choice theory, when the potential risk exceeds financial gains, it becomes irrational for a person to commit a crime.

The potential reason behind the insignificance of the unemployment rate and cybersecurity level might lie in the complex, dynamic nature of cybercrime. It is unlike that such a multifaceted social phenomenon as cybercrime can be predicted by isolated factors like UR and GCI. The predictors specifying high levels of cybercrime might include a mix of various factors.

Limitations and Recommendations

Through the process of executing the research, various limitations arose. As the essence of the analysis is based on the first-ever World Cybercrime Index, it is expected to have a limited dataset. Also, as adjusted R-squared and F-test showed, the analysis does not explain the whole scope of WCI. This indicates that research should be missing some of the key variables in explaining the cybercrime rates. The research focuses mainly on the economic factors and introduces some social factors; however, the explanation of cybercrime rates might be rooted in different areas of study like politics or sociology. Theories taken as a basis of theoretical propositions do not provide enough explanation of cybercrime levels (which was proved by the analysis). Moreover, the complex nature of social phenomena like cybercrime limits the scope of quantitative research due to the inability to establish valid predictors in isolated tests. The incorporation of forensic science into cybersecurity strategies may address some of these gaps. By identifying patterns in digital evidence and providing deeper insights into offender tactics, forensic methodologies can complement traditional predictors to create a more comprehensive understanding of cybercrime.

The researchers wanting to deepen the findings of the present paper or offer a different approach for exploring cybercrime must be attentive to future issues of the World Cybercrime Index, as it presents a great tool for quantitative analysis of the phenomenon. Firstly, the time-series analysis is suggested to be executed in the future. Moreover, to consider the multifaced nature of social occurrences like cybercrime, qualitative in-depth analysis is suggested. The findings of the present paper offer the theoretical basis for scholars and policymakers to focus on exploring the effects of economic systems, freedom, and innovation on cybercrime rates.

Conclusion

The present paper investigates the economic and social factors and their influence on cybercrime rates. The work presents relevant findings for scholars and policymakers by quantitatively testing the theoretical framework existing around the topic.

Literature explores some of the most relevant theories emphasizing the social and economic reasons behind cybercrime and patterns of crime occurrence. Some of the most relevant theories highlighting the interaction of cybercrime and applicable factors are the Marxian theory of political economy, rational choice theory, and routine activity theory. Marxian theory emphasizes the inherent issues of a capitalist system which lead to social inequalities and might result in increased crime rates. Rational Choice theory perceives people as rational actors and tries to explain patterns where cybercrime would be rational and profitable to pursue. Routine Activity theory identifies three pillars in the motivation behind criminal activity: motivated criminals, suitable targets, and absence of guardianship. Two theoretical propositions were formulated based on these three the-

ories. The first, based on Marxian views, stated that a more capitalistic structure and high economic inequality will lead to increased levels of cybercrime. The second, based on Rational Choice and Routine Activity theories, emphasized that low cybersecurity, high technological advancement, and high unemployment levels would lead to increased cybercrime.

To test the propositions, a regression analysis of 94 sample countries was executed. The dependent variable of analysis was based on the World Cybercrime Index. Predictor variables were based on the Unemployment Rate, Global Innovation Index, Global Cybersecurity Index, Economic Inequality Index, Gross Domestic Product per capita, and Economic Freedom Index.

The test results displayed only one significant (EFI) and one borderline significant variable (GII). Key findings indicated an inverse relation between the Economic Freedom Index and the Cybercrime rate. Moreover, the Global Innovation Index is a positive predictor of Cybercrime with a probability of around 92 %. Some other interesting findings arose from the correlation matrix that displayed a positive correlation between EFI, GII, and GCI. Based on findings, TP1 was rejected and TP2 was partially rejected.

Appendix

Figure 2

Shapiro-Wilk test

Descriptive Statistics

	UR	GII	GCI	EII	GDPc	EFI	WCI Score
Shapiro-Wilk	0.861	0.956	0.853	0.977	0.433	0.894	0.377
P-value of Shapiro-Wilk	< .001	0.006	< .001	0.102	< .001	< .001	< .001

Table 4

Breusch-Pagan test

	BP	df	P-value
Breusch-Pagan test	4.2325	6	0.6452

Table 5

Variance Inflation Factor

	UR	GII	GCI	EII	GDPc	EFI
VIF	1.114279	3.231400	1.938558	1.477384	1.148550	2.282352

Table 6

Full dataset

Country	UR	GII	GCI	EII	GDPc	EFI	WCI Score
Russia	4.715	36.6	98.06	0.58	12,532	61.5	58.39
Ukraine	9.834	35.6	65.93	0.5	4,828	56.2	36.44
China	4.55	54.8	92.53	0.57	12,618	58.4	27.86
United States	5.349	61.3	100	0.63	70,219	74.8	25.01

Continued from Table 6

Country	UR	GII	GCI	EII	GDPc	EFI	WCI Score
Nigeria	5.393	20.01	84.76	0.55	2,066	58.7	21.28
Romania	5.59	35.6	75.78	0.5	14,947	68.8	14.83
North Korea	3.134		1.35	0.5		5.2	10.61
United Kingdom	4.826	59.8	99.54	0.46	46,870	78.4	9.01
Brazil	13.159	34.2	96.6	0.68	7,697	53.4	8.93
India	6.38	36.4	97.5	0.63	2,238	56.5	6.13
Iran	9.282	32.9	81.07	0.61	4,084	47.2	4.78
Belarus	3.9	32.6	50.57	0.39	7,490	61	3.87
Ghana	3.338	22.3	86.69	0.61	2,422	59.2	3.58
South Africa	28.77	32.7	78.46	0.75	7,074	59.7	2.58
Moldova	0.794	32.3	75.78	0.46	5,275	62.5	2.57
Israel	4.812	53.4	90.93	0.59	52,130	73.8	2.51
Poland	3.363	39.9	93.86	0.47	18,050	69.7	2.22
Germany	3.638	57.3	97.41	0.46	51,427	72.5	2.17
Netherlands	4.21	58.6	97.05	0.45	58,728	76.8	1.92
Latvia	7.513	40	97.28	0.48	20,930	72.3	1.68
Kazakhstan	5.556	28.6	93.15	0.47	10,374	71.1	1.67
Viet Nam	2.385	37	94.59	0.58	3,756	61.7	1.59
Estonia	6.178	49.9	99.48	0.5	27,944	78.2	1.59
United Arab Emirates	3.105	43	98.06	0.59	44,332	76.9	1.55
Canada	7.527	53.1	97.67	0.5	52,515	77.9	1.34
Malaysia	4.64	41.9	98.06	0.59	11,135	74.4	1.33
Philippines	3.398	35.3	77	0.6	3,461	64.1	1.24
Turkey	11.969	38.3	97.49	0.6	9,743	64	1.22
France	7.874	55	97.6	0.46	43,671	65.7	1.17
Indonesia	3.827	27.1	94.88	0.53	4,334	66.9	1.17
Bulgaria	5.267	42.4	67.38	0.55	12,219	70.4	1.07
Thailand	1.215	37.2	86.5	0.64	7,061	69.7	1.0
Mexico	4.019	34.5	81.68	0.75	10,359	65.5	0.98
Australia	5.116	48.3	97.47	0.48	60,697	82.4	0.95
Italy	9.497	45.7	96.13	0.53	36,449	64.9	0.8
South Korea	3.639	59.3	98.52	0.43	35,142	74	0.79
Cameroon	3.951	19.7	45.63	0.64	1,654	53.4	0.7
Colombia	13.898	31.7	63.72	0.72	6,183	68.1	0.7
Gambia	6.206		32.12	0.56	772	58.8	0.62
Czech Republic	2.803	49	74.37	0.41	26,823	73.8	0.59
Switzerland	5.097	65.5	86.97	0.42	93,446	81.9	0.55

Continued from Table 6

Country	UR	GII	GCI	EII	GDPc	EFI	WCI Score
Cyprus	7.513	46.7	88.82	0.45	32,746	71.4	0.52
Myanmar	4.34	18.4	36.41	0.62	1,232	55.2	0.51
Pakistan	6.338	24.4	64.88	0.55	1,506	51.7	0.51
Sierra Leone	3.516		25.31	0.57	505	51.7	0.5
Laos	1.997	20.2	20.34	0.57	2,536	53.9	0.49
Haiti	15.253		6.4	0.65	1,824	50.8	0.48
Morocco	10.539	29.3	82.41	0.6	3,768	63.3	0.45
Panama	10.453	28	34.11	0.65	15,491	66.2	0.45
Belize	10.157		10.29	0.65	6,061	57.5	0.44
Cambodia	0.396	22.8	19.12	0.68	1,625	57.3	0.42
Armenia	10.012	31.4	50.47	0.59	4,973	52.7	0.41
Lithuania	7.112	39.9	97.93	0.62	23,850	76.9	0.38
Chile	9.325	35.1	68.83	0.71	16,241	75.2	0.38
Ecuador	4.552	25.4	26.3	0.61	5,965	52.4	0.36
Ivory Coast	2.59	21	67.82	0.64	2,163	61.7	0.35
Afghanistan	11.934		5.2	0.52	356	53	0.35
Angola	15.799	15	12.99	0.69	1,927	54.2	0.35
Peru	5.097	31.2	55.67	0.69	6,635	67.7	0.35
Algeria	13.607	19.9	33.95	0.49	3,700	49.7	0.34
Lebanon	12.621	25.1	30.44	0.65	4,136	51.4	0.33
Benin	1.694	18	80.06	0.58	1,361	59.6	0.31
Kenya	5.693	27.5	81.7	0.6	2,070	54.9	0.31
Georgia	11.794	32.4	81.06	0.57	5,023	77.2	0.27
Spain	14.781	45.4	98.52	0.46	30,489	69.9	0.27
Senegal	3.368	23.3	35.85	0.58	1,634	58	0.25
Tunisia	16.505	30.7	86.23	0.53	3,807	56.6	0.22
Slovenia	4.747	44.1	74.93	0.42	29,331	68.3	0.22
Sweden	8.722	63.1	94.55	0.44	61,418	74.7	0.21
Cuba	1.373		58.76	0.58	9,139	28.1	0.2
Greece	14.657	36.3	93.98	0.46	20,311	60.9	0.2
Uganda	3.422	20	69.98	0.63	883	58.6	0.19
Belgium	6.264	49.2	96.25	0.41	51,850	70.1	0.19
Togo	2.285	19.3	33.19	0.61	977	57.5	0.18
Malta	3.403	47.1	83.65	0.47	34,881	70.2	0.18
Mauritius	7.719	35.2	96.89	0.57	9,069	56.1	0.17
Equatorial Guinea	9.194	16.7	1.46	0.63	7,406	49.2	0.17
Hungary	4.045	42.7	91.28	0.44	18,753	67.2	0.17
Serbia	10.061	35	89.8	0.48	9,233	67.2	0.15

Continued from Table 6

Country	UR	GII	GCI	EII	GDPc	EFI	WCI Score
Argentina	8.736	29.8	50.12	0.56	10,651	52.7	0.15
Jamaica	5.188	29.6	32.53	0.65	5,184	69	0.14
Bosnia and Herzegovina	14.897	29.6	29.44	0.48	7,230	62.9	0.14
Central African Republic	6.676		3.24	0.73	461	48.8	0.13
Botswana	23.106	22.9	53.06	0.7	7,239	67.6	0.13
Ethiopia	3.935	18.6	27.74	0.55	925	51.7	0.13
Zambia	5.195	19.8	68.88	0.72	1,135	50.4	0.13
Azerbaijan	6.04	28.4	89.31	0.56	5,408	70.1	0.13
Dominican Republic	7.702	25.1	75.05	0.62	8,477	62.1	0.13
Luxembourg	5.247	49	97.41	0.44	133,712	76	0.11
Japan	2.828	54.5	97.82	0.54	40,059	74.1	0.09
Mali	2.29	19.5	10.14	0.56	882	55.6	0.09
Syria	14.796		22.14	0.65	421		0.09
Guinea-Bissau	3.628		9.85	0.55	795	54.9	0.09
Egypt	7.441	25.1	95.48	0.57	3,887	55.7	0.08

Економічні та соціальні чинники кіберзлочинності

Теодор Джорджобіані

Ця стаття має на меті сприяти розумінню такого доволі нового соціального явища, як кіберзлочинність. Сучасні глобальні реалії технологічного прогресу та значна залежність від цифрових інструментів фокусують увагу на загрозах кіберзлочинності. Для того щоб створити ефективні превентивні механізми, важливо дослідити чинники, що впливають на рівень кіберзлочинності. Для досягнення поставленої мети застосовано регресійний аналіз, побудований на нещодавно оприлюдненому вперше в історії Світовому індексі кіберзлочинності. Проаналізовано показники кіберзлочинності 94 країн на основі впливу 6 предикторних змінних. Аналіз показав, що ступінь економічної свободи має зворотний вплив на рівень кіберзлочинності, а рівень інновацій прямо збільшує цей рівень, хоча й із меншою ймовірністю. Дослідникам, які цікавляться цією темою, рекомендуємо уважно стежити за майбутніми випусками Світового індексу кіберзлочинності, щоби мати змогу більш масштабно аналізувати часові ряди.

Ключові слова: *економічні чинники; кіберзлочинність; регресійний аналіз; індекс економічної свободи.*

Financing
This research did not receive any specific grant from funding institutions in the public, commercial or non-commercial sectors.

Disclaimer
Founders had no role in the research design, data collection and analysis, decision to publish or manuscript preparation.

Participants
The author has contributed solely to intellectual discussion underlying this document, case law research, writing and editing, and assumes responsibility for its content and interpretation.

Declaration of Competing Interest
Author declare no conflict of interest.

References

Abell, P. (2000). *Sociological Theory and Rational Choice Theory*. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5d987c7e4ad51f12a64ed5163c6bbbd7a4cfe07b.

Agnew, R. (1992). Foundations for a general Strain Theory of crime and delinquency. *Criminology*. Vol. 30. Is. 1. DOI: 10.1111/j.1745-9125.1992.tb01093.x.

Agnew, R., & Brezina, T. (2019). General Strain Theory. In: Krohn, M., Hendrix, N., Penly Hall, G., Lizotte, A. (eds) *Handbook on Crime and Deviance. Handbooks of Sociology and Social Research*. Ed. R. T. Serpe. Springer, Cham. DOI: 10.1007/978-3-030-20779-3_8.

Ahmad, R., & Thurasamy, R. (2022). A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes. *Journal of Cyber Security and Mobility*. Vol. 11. Is. 3. DOI: 10.13052/jcsm2245-1439.1133.

Albritton, R. (1993). Marxian Political Economy for an Age of Postmodern Excess. *Rethinking Marxism. A Journal of Economics, Culture & Society*. Vol. 6. Is. 1. DOI: 10.1080/08935699308658041.

Arthur, J. (1991). Development and crime in Africa: A test of modernization theory. *Journal of Criminal Justice*. Vol. 19. Is. 6. DOI: 10.1016/0047-2352(91)90062-Z.

Bernburg, J. G. (2002). Anomie, Social Change and Crime: A Theoretical Examination of Institutional-Anomie Theory. *The British Journal of Criminology*. Vol. 42. No. 4. URL: http://www.jstor.org/stable/23638963.

Bjerregaard, B., & Cochran, J. K. (2008). A Cross-National Test of Institutional Anomie Theory: Do the Strength of Other Social Institutions Mediate or Moderate the Effects of the Economy on the Rate of Crime? *Western Criminology Review*. Vol. 9. Is. 1. URL: http://www.westerncriminology.org/documents/WCR/v09n1/bjerregaard.pdf.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLoS ONE*. 19(4):e0297312. DOI: 10.1371/journal.pone.0297312.

Chambliss, W. J. (1975). Toward a Political Economy of Crime. *Theory and Society*. Vol. 2. No. 2. URL: http://www.jstor.org/stable/656788.

Chamlin, M. B., & Cochran, J. K. (1995). Assessing Messner and Rosenfeld's Institutional Anomie Theory: A Partial Test. *Criminology*. Vol. 33. Is. 3. DOI: 10.1111/j.1745-9125.1995.tb01184.x.

Chism, K. A., & Steinmetz, K. F. (2017). Technocrime and Srain Theory. In: *Technocrime and Criminological Theory*. Ed. Steinmetz, K. F., & Nobles, M. R. London : Routledge. DOI: 10.4324/9781315117249-5.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*. Vol. 44. No. 4. URL: https://www.jstor.org/stable/2094589?origin=crossref.

Comparative economic systems (1969). Ed. by Prybyla, J. S. Boston : Allyn and Bacon.

Dearden, Th. E., Parti, K., & Hawdon, J. (2021). Institutional Anomie Theory and Cybercrime – Cybercrime and the American Dream, Now Available Online. *Journal of Contemporary Criminal Justice*. Vol. 37. Is. 3. DOI: 10.1177/10439862211001590.

Felson, M. (1987). Routine Activities and Crime Prevention in the Developing Metropolis. *Criminology*. Vol. 25. Is. 4. DOI: 10.1111/j.1745-9125.1987.tb00825.x.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief: Practical Theory for Crime Prevention. *Policing and Reducing Crime Unit: Police Research Series. Paper 98*. Ed. Webb B. URL: https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf.

Hay, C., & Ray, K. (2020). General Strain Theory and Cybercrime. In: *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Eds.: Holt Th. J., Bossler A. M. Springer eBooks. DOI: 10.1007/978-3-319-78440-3_21.

Hechter, M. (1992). Should Values Be Written Out of the Social Scientist's Lexicon? *Sociological Theory*. Vol. 10. No. 2. URL: https://www.jstor.org/stable/201961.

Heilbroner, R. L. (1984). Economics and Political Economy: Marx, Keynes, and Schumpeter. *Journal of Economic Issues*. Vol. 18. No. 3. URL: http://www.jstor.org/stable/4225467.

Hodgson, G. M. (2012). On the Limits of Rational Choice Theory. *Economic Thought. World Economics Association*. Vol. 1. URL: http://et.worldeconomicsassociation.org/files/ETHodgson_1_1.pdf.

Holt, Th., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior.* Vol. 35. Is. 1. DOI: 10.1080/01639625.2013.822209.

Inglehart, R., & Baker, W. E. (2000). Modernization, Cultural Change, and the Persistence of Traditional Values. *American Sociological Review*. Vol. 65. Is. 1. DOI: 10.1177/000312240006500103.

Kawachi, I., Kennedy, B. P., & Wilkinson, R. G. (1999). Crime: social disorganization and relative deprivation. *Social Science & Medicine*. Vol. 48. Is. 6. DOI: 10.1016/s0277-9536(98)00400-6.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*. Vol. 30. Is. 4. DOI: 10.1177/0894439311422689.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy Magazine*. Vol. 4. Is. 1. DOI: 10.1109/MSP.2006.27.

Kshetri, N. (2010). Structure of Cybercrime in Developing Economies. In: *The Global Cybercrime Industry*. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-11522-6_8.

Laszka, A., & Schwartz, G. (2016). Becoming Cybercriminals: Incentives in Networks with Interdependent Security. In: *Decision and Game Theory for Security*. 7th International Conference, GameSec, New York, NY, USA, Nov 2–4. DOI: 10.1007/978-3-319-47413-7_20.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*. Vol. 37. Is. 3. DOI: 10.1080/01639625.2015.1012409.

Li, X., & Whinston, A. B. (2020). The Economics of Cyber Crime. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3603694.

Lynch, M. J., Groves, W. B., & Lizotte, A. (1994). The rate of surplus value and crime. A theoretical and empirical examination of Marxian economic theory and criminology. *Crime, Law and Social Change*. Vol. 21. Is. 1. DOI: 10.1007/bf01307806.

Milgrom, P., & Roberts, J. (1988). An Economic Approach to Influence Activities in Organizations. *American Journal of Sociology*. Vol. 94. DOI: 10.1086/228945.

Mishra, S., & Novakowski, D. (2016). Personal relative deprivation and risk: An examination of individual differences in personality, attitudes, and behavioral outcomes. *Personality and Individual Differences*. Vol. 90. DOI: 10.1016/J.PAID.2015.10.031.

Rowlinson, M., & Hassard, J. (2000). Marxist Political Economy, Revolutionary Politics, and Labor Process Theory. *International Studies of Management & Organization*. Vol. 30. No. 4. URL: http://www.jstor.org/stable/23316303.

Schumpeter, J. A. (2021). *The Theory of Economic Development*. London : Routledge. DOI: 10.4324/9781003146766.

Smith, H. J., Pettigrew, T. F., & Huo, Y. J. (2020). Relative deprivation theory: Advances and applications. In: J. Suls, R. L. Collins, & L. Wheeler (Eds.). *Social comparison, judgment, and behavior*. Oxford University Press. DOI: 10.1093/oso/9780190629113.003.0018.

Srivastava, Sh. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*. Vol. 23. Is. 2. DOI: 10.1080/1097198X.2020.1752084.

Sweezy, P. M. (1943). The Theory of Capitalist Development: Principles of Marxian Political Economy. *The Canadian Journal of Economics and Political Science*. DOI: 10.2307/137444.

Webber, C. (2007). Revaluating relative deprivation theory. *Theoretical Criminology*. Vol. 11. Is. 1. DOI: 10.1177/1362480607072737.

Giorgobiani, T. (2024). Economic and Social Drivers of Cybercrime. *Theory and Practice of Forensic Science and Criminalistics.* Issue 4 (37). P. 158—174. DOI: 10.32353/khrife.4.2024.10.