Sinop Üniversitesi
Sosyal Bilimler Dergisi
Araştırma Makalesi
ISSN 2547-989X

Sinop Üniversitesi Sosyal Bilimler Dergisi, 9 (1), 27-54
Geliş Tarihi:21.01.2025 Kabul Tarihi:15.04.2025
Yayın: 2025 Yayın Tarihi:31.05.2025
https://doi.org/10.30561/sinopusd.1624223
https://dergipark.org.tr/sinopusd

CYBERCRIME RATES ASSESSMENT IN TÜRKIYE BY POPULATION: EVALUATION FOR 81 PROVINCES

Vedat YILMAZ*

Abstract

The rapid increase in digitalization and accessibility of technology has significantly changed the way of life in societies. This change has led to the emergence of new threats such as cybercrime. Cybercrime has become a complex problem that affects the security of not only individuals but also institutions and states. This study examined the dynamics of cyber-crimes committed by foreign nationals in Türkiye between 2014 and 2024. The research analyzes how crime rates are related to population density, migration, and regional differences by considering a total of 54.842 cybercrime records in 81 provinces of Türkiye, registered in the Gendarmerie General Command Incidents Information System. Statistical analysis revealed a positive correlation between the total population and cybercrime rates, while a weak positive correlation was identified between the immigrant population and crime rates. Additionally, it has been determined that cybercrime rates show regional differences and are especially concentrated in tourism regions. This situation reveals the impact of economic and social factors on cybercrime trends. As a result, the study emphasizes the importance of cooperation at national and international levels in the fight against cybercrime and suggests that digital security awareness should be increased. Additionally, supporting the economic and social integration of immigrants has been considered an effective tool in reducing crime rates. This research aims to contribute to the development of Türkiye's digital security strategies.

Keywords: Cyber Crime, Cyber Security, Gendarmerie, Immigrants, Law Enforcement.

Türkiye'de Siber Suç Oranlarının Nüfusa Göre Değerlendirilmesi: 81 İl için Değerlendirme

Öz

Dijitalleşmenin ve teknolojinin ulaşılabilirliğinin hızla artması, toplumların yaşam biçimini önemli derecede değiştirmiştir. Bu değişim, siber suçlar gibi yeni tehditlerin de ortaya

* Doktora Öğrencisi, JSGA, Adli Bilimler Enstitüsü, Kriminalistik Anabilim Dalı, vedat.yilmaz@jsga.edu.tr, https://orcid.org/0000-0002-3112-9371

çıkmasına yol açmıştır. Siber suçlar, yalnızca bireylerin değil, kurumların ve devletlerin güvenliğini de etkileyen karmaşık bir sorun haline gelmiştir. Bu çalışma, Türkiye'de 2014-2024 yılları arasında yabancı uyruklular tarafından işlenen siber suçların dinamiklerini incelemiştir. Araştırma, J.Gn.K.lığı Olaylar Bilgi Sisteminde kayıtlı, Türkiye'nin 81 ilindeki toplam 54.842 siber suç kaydını ele alarak, suç oranlarının nüfus yoğunluğu, göç ve bölgesel farklılıklarla nasıl ilişkilendiğini analiz etmektedir. İstatistiksel analizler, toplam nüfus ile siber suç oranları arasında pozitif bir ilişki olduğunu ortaya koyarken, göçmen nüfusu ile suç oranları arasında zayıf bir pozitif korelasyon tespit edilmiştir. Ayrıca, siber suç oranlarının bölgesel farklılıklar gösterdiği ve özellikle turizm bölgelerinde yoğunlaştığı belirlemiştir. Bu durum, ekonomik ve sosyal faktörlerin siber suç eğilimleri üzerindeki etkisini gözler önüne sermektedir. Sonuç olarak, çalışma, siber suçlarla mücadelede ulusal ve uluslararası düzeyde iş birliğinin önemini vurgulamakta ve dijital güvenlik farkındalığının artırılması gerektiğini önermektedir. Ayrıca, göçmenlerin ekonomik ve sosyal entegrasyonunun desteklenmesi, suç oranlarını azaltmada etkili bir araç olarak değerlendirilmiştir. Bu araştırma, Türkiye'nin dijital güvenlik stratejilerinin geliştirilmesine katkı sağlamayı hedeflemektedir.

Anahtar Kelimeler: Siber Suç, Siber Güvenlik, Jandarma, Göçmenler, Kolluk

1. Introduction

The rapid change and development in information and communication technologies has affected many areas such as social structures, economic systems, etc. While digitalization has made access to and sharing of information more efficient for both individuals and institutions, it has also revealed threats and risks on a global scale (Özel, 2016).

Technology is advancing rapidly penetration of the Internet into all areas of modern life have radically transformed the activities of individuals, institutions, and states (Salahshour et al., 2018). However, this transformation has also revealed the darker side of digitalization, most notably the growing prevalence of cybercrime (Goni et al., 2022). Cybercrimes, which span a wide spectrum from identity theft to financial fraud, hacking to cyber terrorism, are among the priority issues of policymakers, law enforcement officers, and academics today (Goni et al., 2022). Cybercrime is defined by Wall (2004) as "any crime committed over the Internet." Gordon and Ford (2006) define cybercrime as "a crime facilitated or committed using a computer, network or hardware device". Considering these definitions, cybercrimes refer to crimes committed by technology

misuse and reveal the digital world's dark side. Cybercrime is an important security issue that causes economic and social damage not only to individuals but also to companies and states, as mentioned in the Council of Europe Convention on Cybercrime (Council of Europe, 2024).

The main difference between cybercrimes and traditional crimes is that they have a cross-border nature (Jahankhani et al., 2014). Therefore, combating cybercrime requires international cooperation and coordination, beyond national-level measures (UNCTAD, 2024). Nowadays, as technology has become a universal tool, it has become easier for individuals and groups to commit cross-border actions, and it has become common for individuals from different nationalities to be among the perpetrators of cybercrimes.

Unlike traditional crimes, cybercrimes can produce much more comprehensive, rapid, and effective results by using the opportunities offered by the digital environment (Goni et al., 2022). This situation necessitates the development of more complex and multidimensional approaches to preventing and punishing cybercrimes. Being aware of these differences will enable both individuals and states to deal more effectively with the threats they face in the digital world.

Cybercrimes are inherently based on digital technology and internet infrastructure (Gordon & Ford, 2006; Saini et al., 2012). This situation has enabled cybercrimes to gain many features that distinguish them from traditional crimes (Saini et al., 2012). While traditional crimes usually occur in a physical environment, cybercrimes are committed in a virtual environment. This crime committed in cyberspace can have an impact that transcends national borders (Das & Nayak, 2013; Saini et al., 2012). The main points where cybercrimes differ from traditional crimes can be listed as follows (Borwell et al., 2021; Montoya et al., 2013; Schiks et al., 2022):

a. Anonymity and Identity Privacy: Cybercrimes offer great advantages in providing anonymity to criminal perpetrators. Due to the nature of the Internet, a person can hide their identity in the virtual world, create fake profiles, or use

techniques that are difficult to trace. While it is more difficult for criminals to hide their identities in traditional crimes, this is much easier in the cyber world. For example, an attacker can use tools such as VPN, proxy servers, or the darknet to hide their identity.

b. Speed and Area of Effect: Cybercrimes can have a wide area of impact in a very short time. Traditional crimes are generally targeted, and their effects may be limited to a limited area. However, cybercrime can have rapid and far-reaching consequences, such as the global spread of a virus or the compromise of a database in seconds. This speed also makes it difficult to detect and prevent cybercrime.

c. Digital Harm Instead of Physical Violence: While traditional crimes often involve physical violence or property damage, cybercrimes focus on digital harm. This damage may take the form of data theft, rendering systems dysfunctional, loss of reputation, or economic losses. For example, the leak of a company's database containing customer information could seriously damage the company's reputation and lead to financial losses.

d. Processing Tools and Techniques: Cybercrimes are carried out with advanced technologies such as complex software, malicious codes, social engineering methods, and artificial intelligence. Traditional crimes generally require physical means and methods. This makes the detection and prevention of cybercrime a matter that requires more technical expertise.

e. International Legal Problems: Cybercrimes generally have a structure that concerns more than one country. The fact that the perpetrator of the crime is in one country, the victim is in another country and the effects of the crime are in different regions brings about international legal problems. While traditional crimes are usually handled within a single jurisdiction, international cooperation and coordination become a major necessity in cybercrime. However, differences in the legal regulations of different countries may further complicate this cooperation.

f. Continuous Evolution and Adaptability: Cybercrimes have a constantly changing structure in parallel with developments in technology. New technologies

enable new types of crimes to emerge. For example, the proliferation of cryptocurrencies has caused types of crimes such as money laundering and fraud to move to digital platforms. This rapid evolution may cause traditional methods to become insufficient in the fight against cybercrime.

Migration is one of the oldest phenomena in human history and is shaped by the search for better living conditions, security, and opportunity (Karakaya, 2020). Throughout the centuries, migration; has shaped countries, economies, and cultures, presenting both opportunities and challenges. In recent years, Turkey's strategic geographical location at the crossroads between Europe and Asia has made it one of the focal points of migration movements. The relationship between migration and cybercrime rates stands out as one of the most important debates today (Buoncompagni, 2020; Näsi et al., 2015). In an era where digitalization is accelerating and cyber threats are increasing in diversity, the potential for immigrant communities to be involved in these new types of crimes and their risks of exposure are an important topic of discussion.

Due to its geographical location and strategic importance, Türkiye has been both the target and one of the perpetrators of cybercrime activities (Drent et al., 2022). The increase in cybercrimes, especially between 2014 and 2024, shows that these crimes are also committed by foreign perpetrators. Foreign criminals can use Türkiye as an operation centre or target area, especially with the facilities provided by the internet infrastructure and digital resources. This situation has made the legal, political, and economic aspects of cybercrime more complex. Understanding the dynamics of cybercrime committed by foreign nationals in Türkiye is of critical importance to protect the country's digital assets and maintain public trust in online systems.

Cybercrime is not only a technical issue, but also a social, legal, and political problem (Goni et al.,2022). In this context, the findings of the study aim to provide important suggestions for Türkiye to strengthen its digital security infrastructure and increase international cooperation in the fight against cybercrime. Additionally, the

results of the paper may contribute to the development of new policies for the prevention of cross-border cybercrime. Unlike traditional crimes, cybercrimes can produce much more comprehensive, rapid, and effective results by using the opportunities offered by the digital environment. This situation necessitates the development of more complex and multidimensional approaches to preventing and punishing cyber-crimes. Being aware of these differences will enable both individuals and states to deal more effectively with the threats they face in the digital world.

In this study, the rates of cybercrimes committed by foreign nationals in Türkiye between 2014 and 2024 will be discussed in detail in terms of city and population. The main purpose of the article is to analyse in which cities and by whom these crimes are committed and to determine the criminal tendencies of immigrants in this regard. In this context, it is to evaluate Türkiye's capacity to combat cybercrime and international cooperation strategies. In particular, it will focus on how foreign perpetrators are involved in cybercrime activities in Türkiye, what methods they use, and the effects of these crimes at the regional level.

In this context, the study will seek answers to three basic questions:

1. What is the rate of cybercrimes committed by foreign nationals compared to the general rate?
2. Is there a connection between provincial populations in Türkiye and detected cybercrime rates?
3. Is there a connection between province-based immigrant numbers and crime rates?

2. Materials and Methods

2.1. Data Analysis

In the study, cybercrime records between 2014 and 2024 in the incidents information system of the Gendarmerie General Command, which acts as a law enforcement force, were used. In this context, detailed analyses were carried out on a total of 54.842 cybercrime records committed in 81 provinces. During these 10

years, the evaluation was made on a provincial basis, based on 45.035 cybercrime records committed by Türkiye citizens, 9095 criminal records of foreign nationals, and 712 records whose nationality was not entered. In addition, evaluations were made by Türkiye Statistical Institute regarding cybercrimes committed according to the total population, using the Türkiye and immigrant population values of 2023 (TÜİK, 2023).

2.2. Statistical Analysis

Pearson Correlation Analysis was used to measure linear relationships between immigration rate and crime rate. Pearson correlation coefficient (r) value was calculated between +1 and -1. ($r>0$ Positive relationship, $r<0$ Negative relationship, $r=0$ No relationship). P-value was used to test the statistical significance of the correlation. $p < 0.05$ indicates a significant relationship. Linear Regression Analysis was used to visualize the relationship between immigration rate and crime rate and determine the trend line. A first-order (linear) polynomial was constructed on the data. Coefficients for the trend line were calculated using the numpy.polyfit function in Python. The trend line is visualized on the data.

3. Results

When the data used in this study is examined, the overall crime distribution across all cities for 54,842 records of transactions made against Türkiye and foreign nationals in 81 provinces of Türkiye is presented in Figure 1. According to the cybercrime data of the cities, Crime rates per 100.000 people by city values are shown in Figure 2.

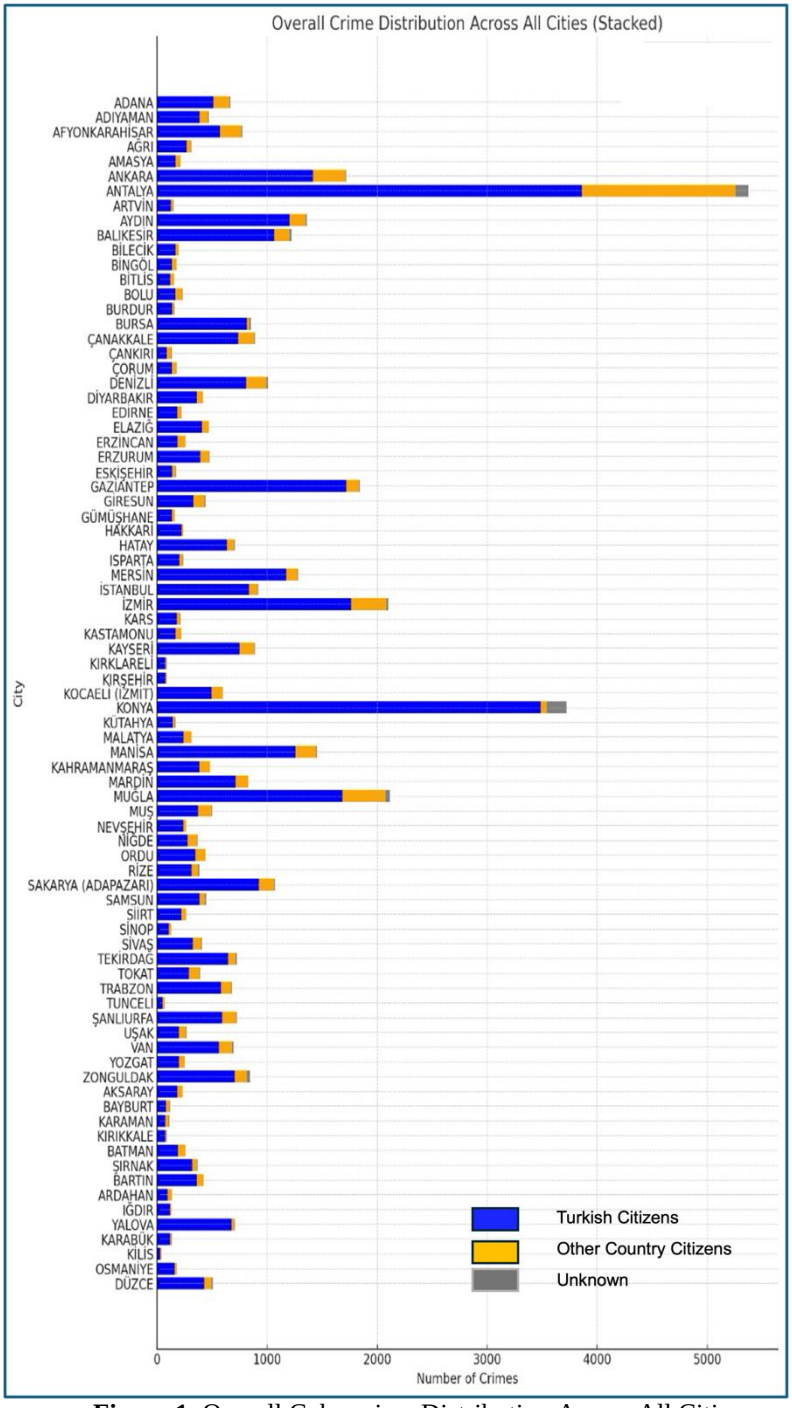


Figure 1. Overall Cybercrime Distribution Across All Cities

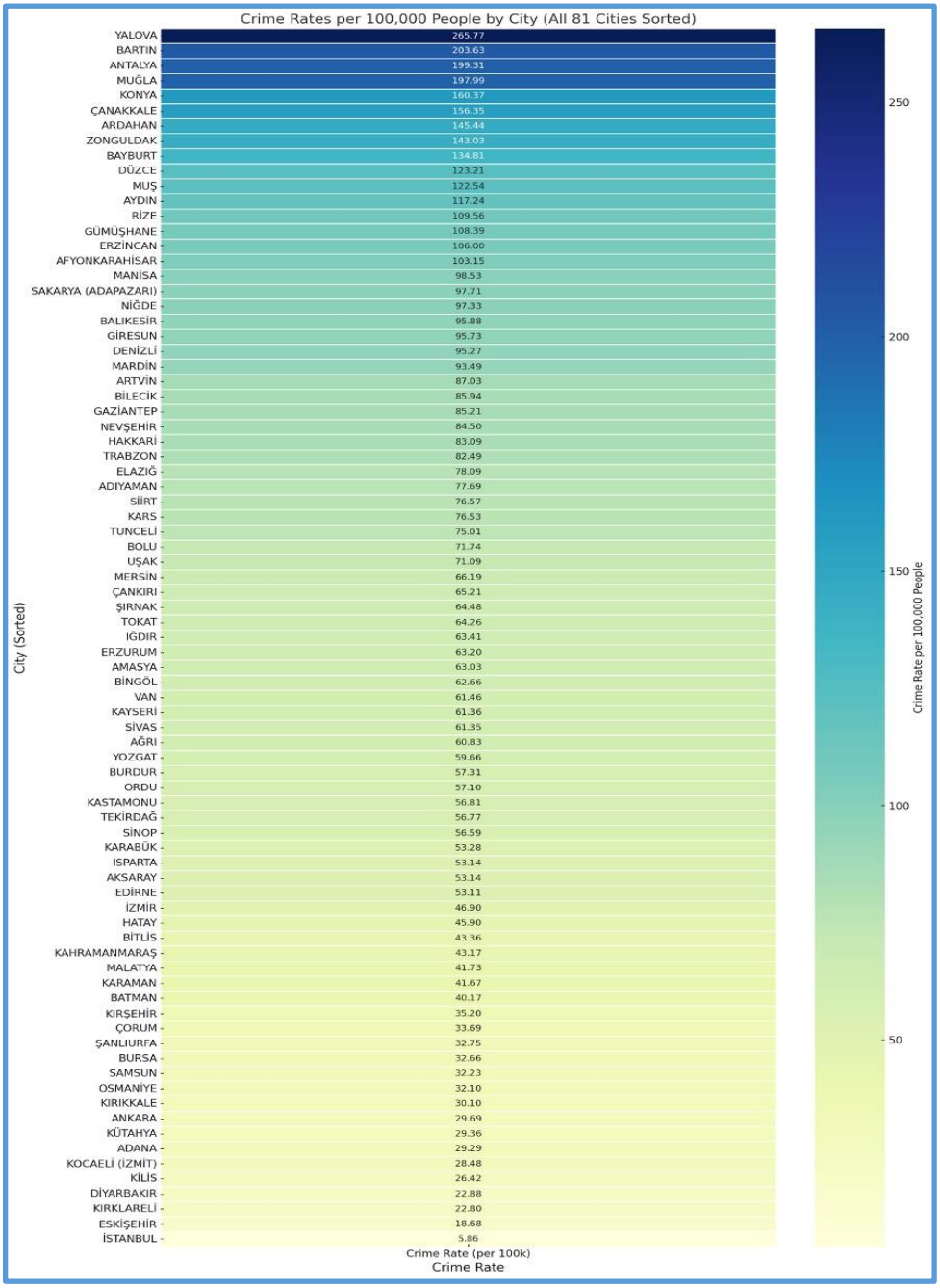
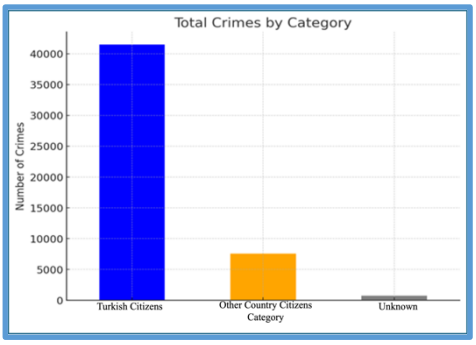
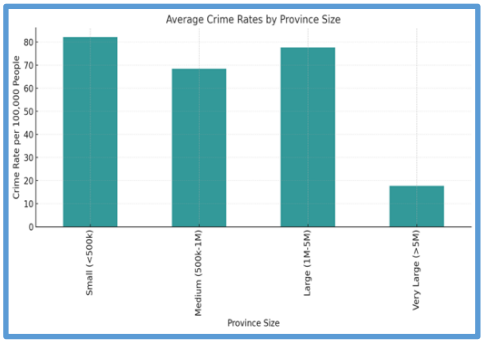


Figure 2. Cybercrime Rates Per 100.000 People by City.

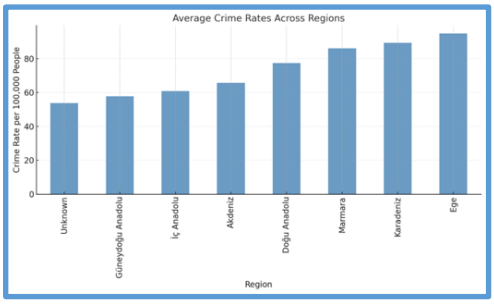
Total Crime Rates are discussed in 4 different graphs and the graphs are presented in Figure 3. Total Crimes by Category, including Türkiye citizens, foreign, and unspecified, have been prepared for use in general evaluation. Average Crime Rates by Province Size shows the average crime rates per 100.000 people according to the population size of the provinces. Provinces are divided into four categories according to their population size. Average Crime Rates Across Regions: This shows the average crime rates (crime rate per 100.000 people) for different regions in Türkiye. This visualization was used to analyse how crime rates vary by region. Average Migration Rate Across Regions: This shows the average immigration rates in different regions of Türkiye. Significant differences in immigration rates can be observed between regions. This visualization was used to understand the geographical distribution of the immigrant population.



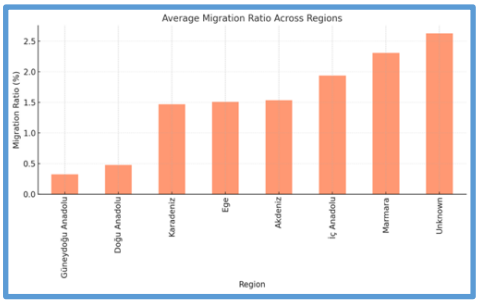
a. Total Crimes by Category



b. Average Crimes Rates by Province Size



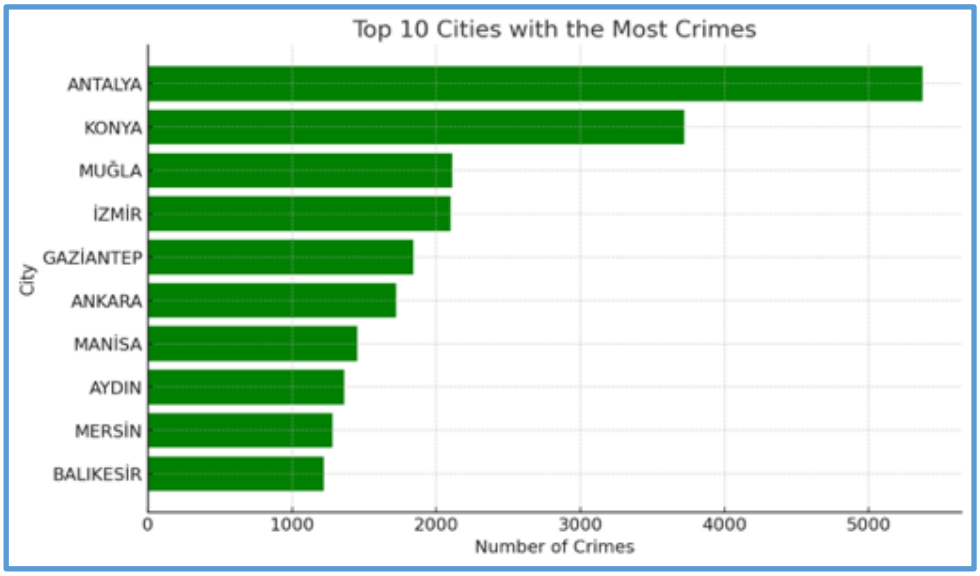
c. Average Crimes Rates Across Regions



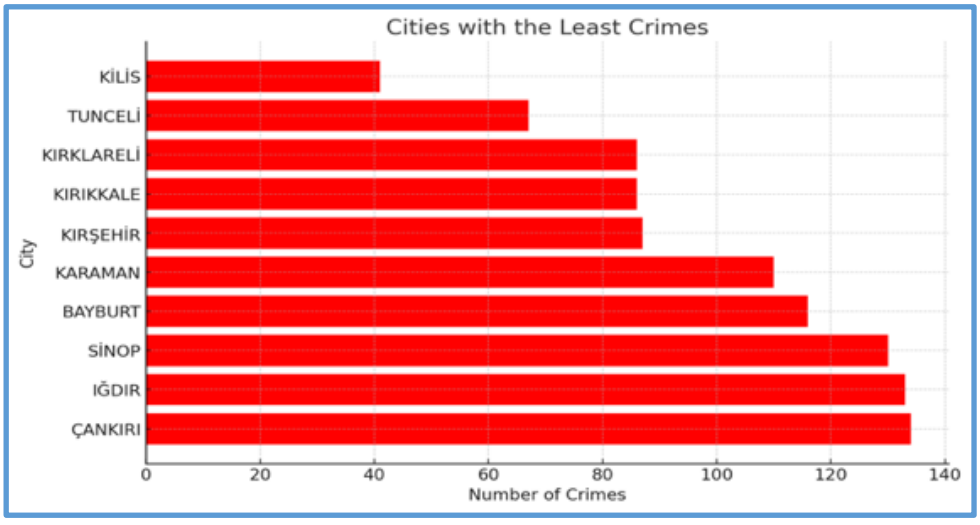
d. Average Migration Rate Across Regions

Figure 3. Total Cybercrimes Rates

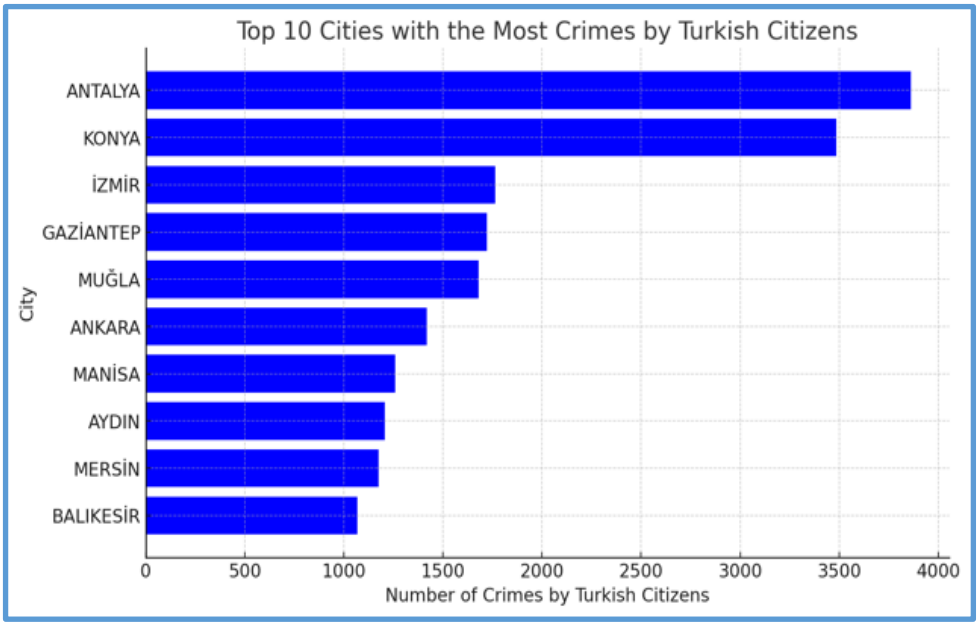
Cities with the most and the least Crime Rates were evaluated through 6 different graphs included in Figure 4.



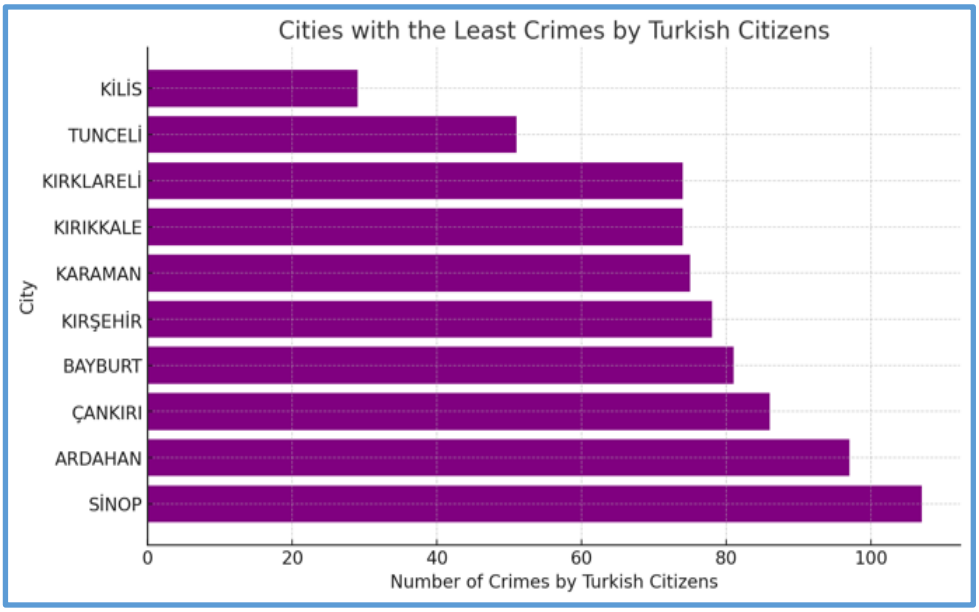
a. Top 10 Cites With The Most Cybercrimes



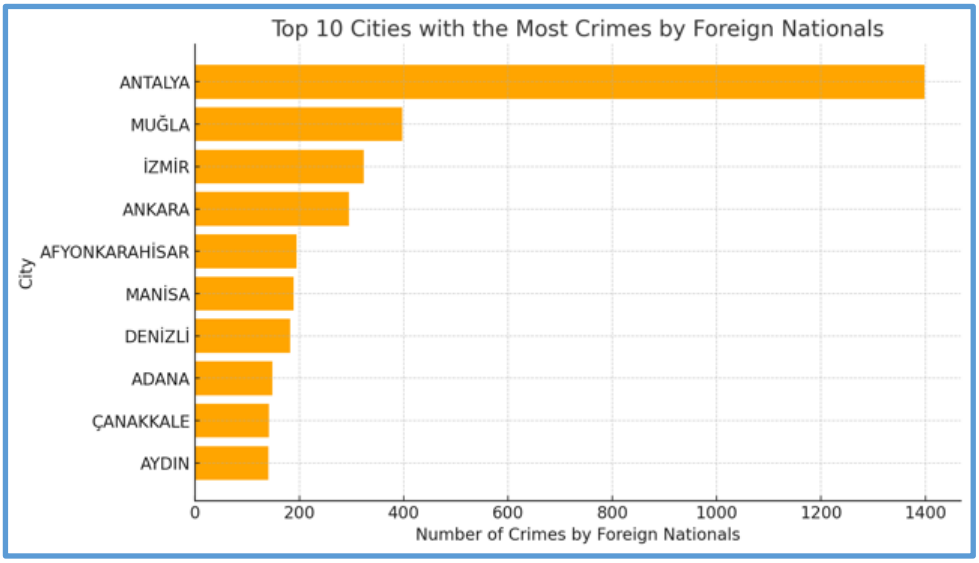
b. Cities With The Least Cybercrimes



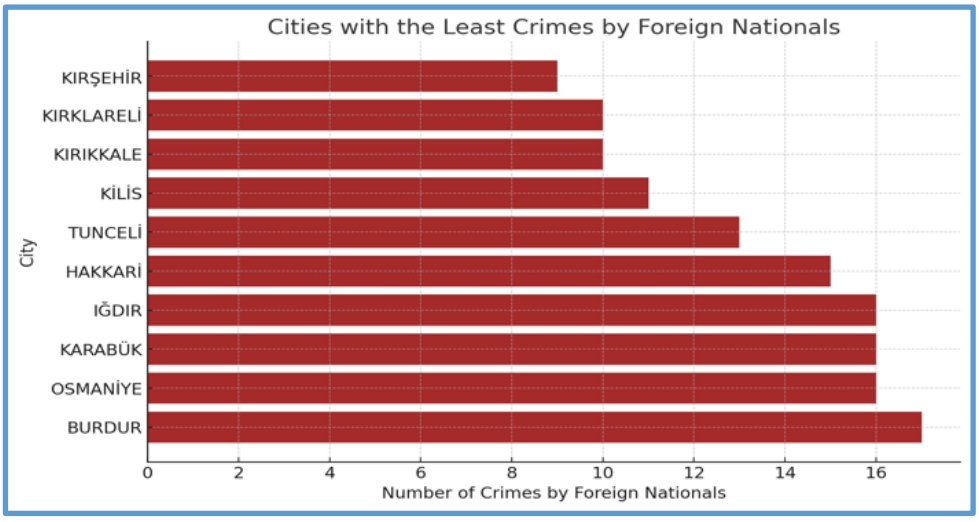
c. Top 10 Cities With The Most Cybercrimes by Türkiye Citizens



d. Cities With The Least Cybercrimes by Türkiye Citizens



e. Top 10 Cities With The Most Cybercrimes by Foreign Nationals

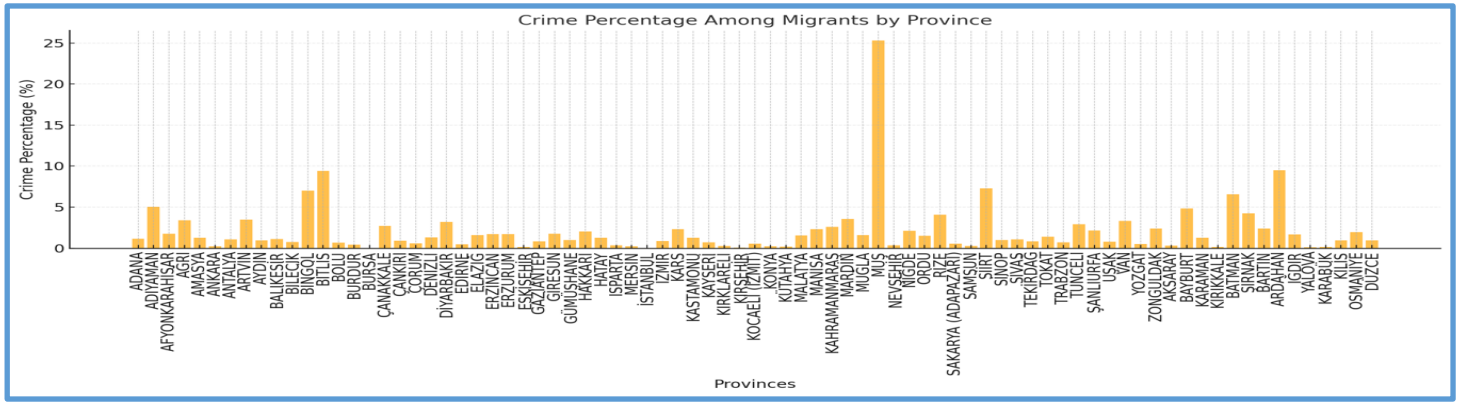


f. Cities With The Least Cybercrimes by Foreign Nationals

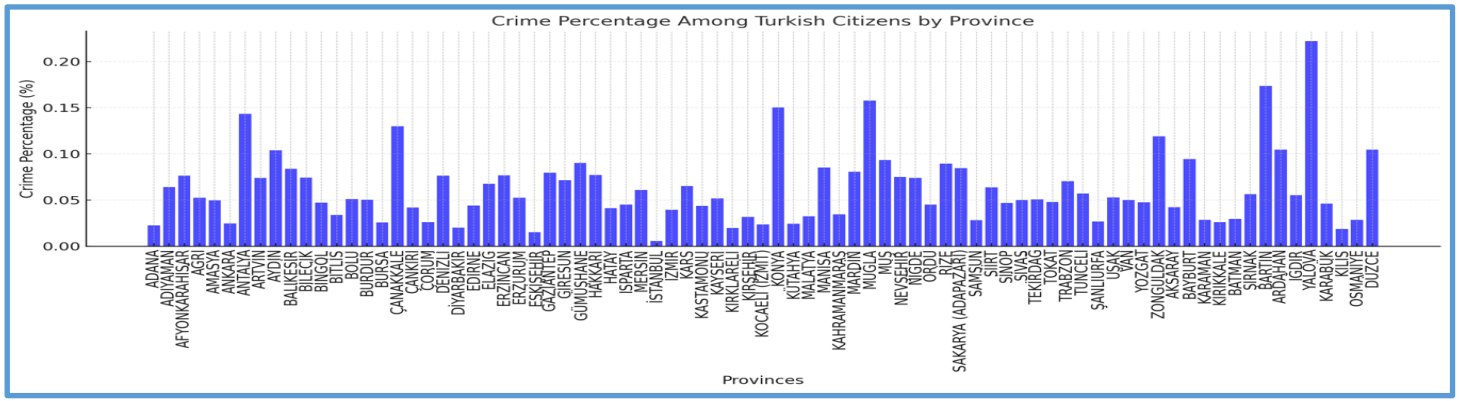
Figure 4. Cities with the most and the least Cybercrimes Rates

Figure 5 shows the Crime Percentage by Province. The first chart shows the crime percentages of the immigrant population within their population on a provincial basis. The second chart shows the crime percentages of Türkiye citizens relative to the population by province.

Trend Crime Data by Province is presented in Figure 6. The first chart shows the ratio of crimes committed by Türkiye citizens to total crimes on a provincial basis (in %). This analysis was used to visualize how crime rates for Türkiye citizens vary between provinces and in which provinces they are higher or lower. In the secondary chart, the ratio of immigrant crimes to total crimes (in %) on a provincial basis is visualized. This analysis was used to observe how immigrant crime rates vary between provinces and in which provinces they are higher or lower.

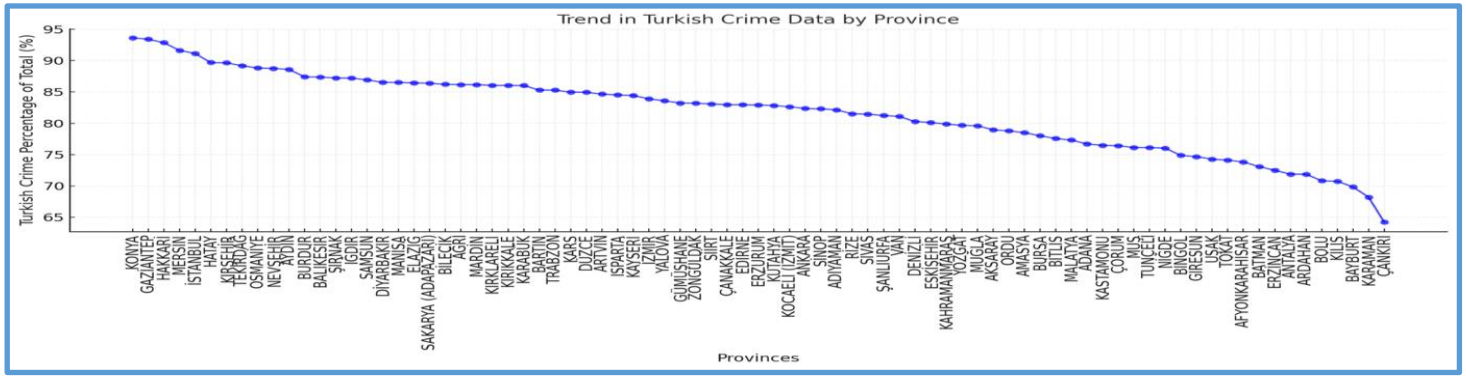


a. Cybercrimes Percentage Among Migrants by Province

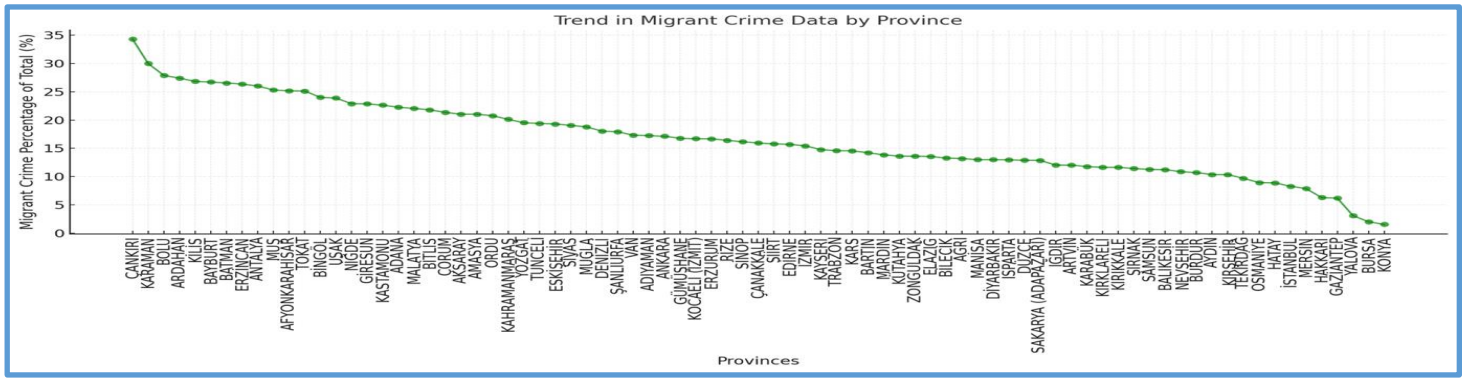


b. Cybercrimes Percentage Among Türkiye Citizens by Province

Figure 5. Cybercrime Percentage by Province



a. Trend in Türkiye Cybercrimes Data by Province



b. Trend in Migrant Cybercrimes Data by Province

Figure 6. Trend Cybercrimes Data by Province

Figure 7 was used to statistically explain the impact of immigrants on cybercrime.

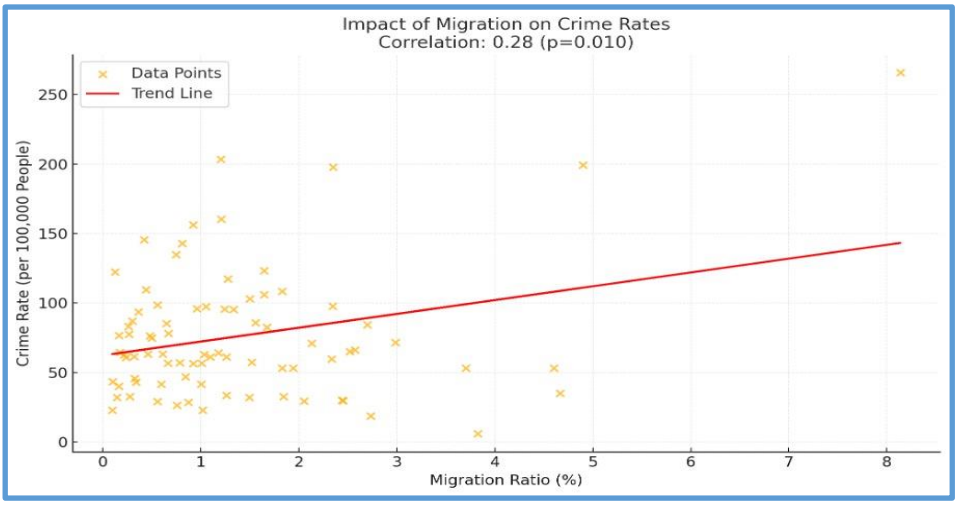


Figure 7. İmpact of Migration on Cybercrimes Rates Correlation

4. Discussion

This section analyses in detail the results presented in the previous sections. Using the statistical and graphical data of the study, the relationship between population dynamics and cybercrime trends across Türkiye, especially the role of immigrants and regional differences, was emphasized.

4.1. Effect of Total Population on Cyber Crime Rates

Analysis shows that there is a statistically significant positive correlation between the total population and the number of cybercrimes ($p<0.01$). This finding reveals that higher crime rates are seen in more densely populated areas. This relationship shows that each increase in population leads to an increase of approximately 0.0004 in crime. Although this rate may seem low at the individual level, its overall effect is significant in densely populated areas.

According to the statement of the Türkiye Statistical Institute, as of December 31, 2023, the population of Türkiye is 85 million 372 thousand 377.

According to cybercrime data between 2014-2024, according to Figure 3a, 83.32% of the perpetrators are Türkiye citizens, 15.28% are foreign nationals, and 0.014% are those of unknown nationality. According to the total population of 2023, cybercrime was committed at the rate of approximately 1.7% of the total population in the last 10 years. Approximately 1.42% of this value consists of Türkiye citizens and 0.26% is foreign nationals.

Effect of Total Population: There is a significant positive relationship between total population and total number of crimes ($p<0.01$). Each increase in population increases the number of crimes by approximately 0.0004. Although this may seem a low value, its effect is significant considering the size of the population.

Effect of Immigrant Population: A negative relationship is observed between the immigrant population and the total number of crimes, but this relationship is not statistically significant ($p=0.075$). The increase in the immigrant population may indicate a slight decrease in the number of crimes.

Overall Fit of the Model: The R-square value is 0.161, meaning the independent variables (total population and immigrant population) explain 16% of the total crimes. The explanatory power of the model is low, other factors should also be considered to affect crime rates.

When the general crime distribution in all cities (according to Figure 1) is evaluated independently of the population, the cybercrime density of Antalya province is remarkable. Antalya is one of the most popular tourism spots in Türkiye. According to TUİK data, 16 million 925 thousand 349 foreign nationals came to Antalya in 2024 (Tourist Business Association, 2025). When the heavy visitor traffic of both Türkiye and foreign nationals in the summer months is taken into account, the high crime rates can be understood. In addition, the geographical location and proximity of Konya, which is the second province with the highest total crime rate, to Antalya province also support this issue. While the abundance of Türkiye citizen perpetrators in Konya province is striking, the scarcity of other country national

perpetrators is striking. Among the individuals committing cybercrimes in Konya, the number of those whose nationality information was not entered is also quite high.

After the crimes in Antalya and Konya, the provinces with the highest crime rates, Muğla and İzmir, are also Türkiye's leading provinces in tourism, just like Antalya, and this is also considered to be related to the number of tourists coming for vacation.

Türkiye's geographical location has opened the Mediterranean and Aegean coasts as a migrant transit point for many countries working towards the European continent with a dream of a new life (Arslan and Taş, 2022). This means that these people are exhausted in terms of cybercrime and can be the target of those who fail as easy targets.

4.2. The Role of the Immigrant Population in Cyber Crime Dynamics

The study showed a weak negative correlation between the immigrant population and total crime rates ($p=0.075$). This suggests that an increase in the immigrant population does not necessarily lead to higher crime rates and may even indicate a slight decrease. This observation supports the conclusion that immigrants are not a key component of cybercrime trends in Türkiye. This may be because immigrants who are engaged in stable employment or education are less likely to engage in criminal activities. Immigrants are often more likely to be targets of cybercrime than perpetrators of these crimes. This may change the focus of response efforts. Strong social support among immigrant communities can further reduce crime rates by increasing stability and resilience.

4.3. Regional and Provincial Differences in Cyber Crimes

Regional analyses reveal significant differences in cybercrime rates between provinces. Migration rates show variable effects depending on the region.

Figure 3b. As can be seen, when the provinces are evaluated according to population, cybercrime rates per 100,000 people are higher in provinces with a population of less than 500 thousand. Metropolitan provinces with a population between 1 million and 5 million are in second place, and provinces with a population

of 500 thousand to 1 million are in third place. Is ranked. Values covering the provinces of Istanbul and Ankara, whose population data is more than 5 million, are in the last place. It is considered that the effect of this is because crime detection in the two provinces with the highest population is at a similar level to other provinces.

When Türkiye's geographical regions are examined, total cybercrime rates per 100,000 people are examined, as seen in Figure 3c, the highest cybercrime rate is in the Aegean region, respectively, Black Sea, Marmara, eastern Anatolia, Mediterranean, central Anatolia, and Southeastern Anatolia.

According to the graph presented in Figure 3d, when the cybercrime rates committed by immigrants per 100 thousand people are examined by region, the Marmara region, where the Türkiye population lives most, ranks first, followed by Central Anatolia, Mediterranean, Aegean, Black Sea Eastern Anatolia, and Southeastern Anatolia, respectively. It is noteworthy that while the Black Sea region has the highest density of all cybercrime rates, it is the Marmara region for immigrants. It is considered that this situation may be due to immigrants trying to settle in provinces where job opportunities are more, and the population density is higher.

When the density of cybercrime per 100,000 people is examined, it is seen that Yalova is the province with the highest city-based cybercrime rate, according to the graph presented in Figure 2. Due to its geographical location, Yalova's proximity to Türkiye’s largest city, Istanbul, and its 4th largest city, Bursa, is remarkable. After Yalova, Bartın has the highest crime rate, followed by Antalya, Muğla, and Konya, respectively. The rate of cybercrime in Bartın, which has a low population density, is high compared to the population. It is noteworthy that Antalya, Konya, and Muğla are the leading provinces of Türkiye in terms of tourism. The lowest provinces are Istanbul, Eskişehir, Kırıkkale, Diyarbakır and Kilis. Considering the population density of Istanbul, it is an expected result that the cybercrime rate per 100 thousand people is low. However, it is considered that the low rate in Eskişehir, one of the medium-sized provinces, is due to the high level of education and the large student

population, which will reduce the number of victims and the fact that there may be a high number of conscious technology users.

If an evaluation is made based on the total crime rate of Türkiye's provinces, regardless of their population density, the province with the most cybercrime data is Antalya, followed by Konya, Muğla, İzmir, Gaziantep, Ankara, Manisa, Aydın, Mersin and Balıkesir, respectively. It is noteworthy that the majority of these provinces are coastal tourism provinces (Figure 4a). The province with the lowest cybercrime rate is Kilis. Considering the ratio of Kilis province to population, it is also considered that it is one of the cities with the least cybercrime, which may be due to its geographical location and proximity to the metropolitan cities of Gaziantep and Adana. These are, respectively, Tunceli, Kırklareli, Kırıkkale, Kırşehir, Karaman, Bayburt, Sinop, Iğdır and Çankırı (Figure 4b). Antalya, Türkiye's tourism paradise, is one of the cities where Türkiye citizens commit the most crimes, regardless of population. These are Konya, İzmir, Gaziantep, Muğla, Ankara, Manisa, Aydın, Mersin, and Balıkesir, respectively (Figure 4c). According to cybercrime rates, the provinces with the least crime are Kilis, Tunceli, Kırklareli, Kırıkkale, Karaman, Kırşehir, Bayburt, Çankırı, Ardahan, Sinop (Figure 4d).

Antalya is one of the cities where the most crimes are committed by foreign nationals, regardless of population. They are Muğla, İzmir, Ankara, Afyonkarahisar, Manisa, Denizli, Adana, and Aydın, respectively (Figure 4e). According to cybercrime rates, the provinces with the least crime are Kırşehir, Kırklareli, Kırıkkale, Kilis, Tunceli, Hakkari, Iğdır, Karabük, Osmaniye and Burdur (Figure 4f). It is noteworthy that the highest crime rate is in the Aegean region.

Immigrant concentration may be a factor influencing crime rates in these cities, but these effects are generally limited and more associated with specific types of crime. When foreign national crime perpetrators are taken into consideration, it should not be forgotten that it does not only originate from immigrants but also includes short-term citizens of other countries who come to Türkiye for tourism or other purposes.

It should not be forgotten that the evaluations made based on these data may be because the capacity of law enforcement forces to detect and prevent digital crimes varies between provinces.

4.4. The relationship between Türkiye citizens **and immigrant populations of provinces in cyber crimes**

In Figure 5, the Crime Percentage by Province is shown according to the Türkiye citizens and immigrant population in that province. When we evaluate the crime percentages of the immigrant population within their population on a provincial basis, the provinces of Ardahan, Bitlis, Bingöl, and Siirt, especially Muş, attract attention. In addition, considering that these provinces are in the east of Türkiye and their developed levels and small population, it is considered to be because they receive fewer immigrants than other provinces. It is noteworthy that crime rates are lower in the eastern provinces. The reasons for this include limited digital infrastructure and relatively less complex economic activities.

When the crime percentages of Türkiye citizens relative to the population are examined by province, Yalova, Muğla, Konya, Antalya, and Çanakkale constitute the top 5 provinces. When only the Türkiye citizens population and cybercrimes committed by Türkiye citizens are evaluated, Çanakkale province is different from the general evaluation. Crime rates can be expected to increase in areas with high economic activity. Digital security awareness should be increased for both Türkiye citizens and immigrants. Moreover, Understanding the distribution of crime by province can enable Law Enforcement Forces to evolve their organizational structures accordingly. Awareness-raising activities should be carried out at local and national levels, especially in tourist areas.

4.5. Evaluation of cybercrime trends by the province in terms of Türkiye citizens **and Immigrant Populations**

In Figure 6, Trend Crime Data by Province is presented. When the first graph is examined in terms of the ratio of crimes committed by Türkiye citizens to the total crime committed in that province (%), it is seen that most Türkiye citizens commit

cybercrimes in Konya. This rate is approximately 94%. This rate is followed by Gaziantep with 93%. After Konya and Gaziantep provinces, Hakkari, Mersin and Istanbul provinces come. Proportionally, Çankırı is the province where the least of the total crimes in that province are committed by Türkiye citizens. In Çankırı province, the rate is approximately 63%.

In the secondary chart, when the percentage values of cybercrimes committed by foreign nationals on a provincial basis are examined according to the total cybercrime rate of that province, Çankırı province, which has the lowest rate for Türkiye citizens, has the highest rate for foreign national perpetrators. This rate is approximately 34%. Çankırı is followed by Karaman, Bolu, Adıyaman and Kilis provinces. It shows that crime rate trends between different provinces differ according to geographical and economic conditions. Crime rates are generally higher in western regions, while these rates are lower in eastern regions. This reveals the impact of regional economic inequalities and digital access differences.

4.6. Statistical Analysis Results between immigration rate and crime rate

Correlation Analysis was used to statistically explain the impact of immigrants on cybercrimes, as seen in Figure 7. Pearson correlation coefficient: 0.28, with a p-value of 0.01, shows that there is a statistically significant but weak positive relationship between the immigration rate and the crime rate. The red line on the graph shows the trend between the immigration rate and the crime rate. The increase in the rate of immigration has been associated with a slight upward trend in the crime rate. Since the statistical relationship is weak, it is considered that other factors affecting crime rates play a stronger role.

4.7. Broader Implications and Recommendations

These findings have important implications for policy and law enforcement strategies:

a. Increasing Resource Allocation: Increasing cybersecurity resources in high-risk areas can contribute to effectively reducing crime rates.

b. Targeted Awareness-Raising Programs: Awareness-raising programs on digital security can be created for both citizens and immigrants.

c. Policy Reforms: Policies aimed at the economic and social integration of immigrants can help reduce crime trends.

d. Technological Interventions: Using advanced analytics tools to monitor and predict cybercrime trends can optimize prevention strategies.

e. International Cooperation: Due to the transnational nature of cybercrime, strengthening cooperation at the international level is of great importance.

4.8. Limitations and Future Research Directions

Although this study provides valuable findings, it has some limitations. The most important limitation is that the data used in this study includes cybercrime data recorded in the Gendarmerie General Command Incidents Information System database. Including Cyber Crimes in the database of the General Directorate of Security in future studies may make the study more valuable in terms of accuracy and complementarity. The low explanatory power of the statistical model (R^2 = 0.161) indicates that additional variables such as economic status, education level, technological literacy, age, and gender should be included. More detailed data on specific crime types and methods could further deepen the analysis. Future studies could use longitudinal data to examine the effects of policy interventions.

5. Conclusions

It highlights the complexity of cybercrime dynamics in Türkiye and draws attention to the importance of interactions between population characteristics, regional factors, and the role of immigrants. Addressing these factors with comprehensive and inclusive strategies can increase Türkiye's resilience against cyber threats and contribute to the creation of a safe and inclusive digital environment.

This study provides a comprehensive analysis to understand the demographic, regional, and social dynamics of cybercrimes committed in Türkiye between 2014 and 2024. The findings show a significant positive relationship

between the total population and cybercrime rates. However, it has been determined that the increase in the immigrant population does not lead to a significant increase in cybercrime rates, on the contrary, immigrants are among the victims rather than the perpetrators of cybercrime. The fact that immigrants tend to be less involved in criminal activities has been linked to their engagement in stable activities such as employment or education.

Regional analyses reveal that the density of cybercrime varies significantly between provinces. While crime rates are higher in the western regions, these rates are relatively low in the eastern regions. High crime rates, especially in tourist areas, attract attention. However, in provinces such as Istanbul and Ankara, where population density is high, the low crime rates per 100 thousand people are attributed to the technology and security awareness in these provinces.

Although the impact of regional and economic factors on the participation of immigrants in cybercrimes is limited, increasing the digital security awareness of these people is critical in preventing victimization. In addition, the fact that crime rates committed by Türkiye citizens are concentrated in regions where economic and social mobility is high indicates that special measures should be taken in these areas.

In light of these findings, the following strategic measures are recommended in Türkiye's fight against cybercrime:

Resource Allocation and Training: More resources should be provided to security units in high-risk areas and digital security training should be expanded.

Immigrant Integration: Policies that support the economic and social integration of immigrants can be effective in reducing crime trends.

Advanced Technological Tools: Artificial intelligence and advanced data analytics tools should be used to monitor and prevent cybercrime trends.

International Cooperation: Considering the international nature of cybercrime, transnational cooperation mechanisms should be strengthened.

Regional Approaches: Province-specific policies should be developed that take into account geographical and economic differences.

A holistic and multidimensional approach should be adopted in the fight against cybercrime. This study provides an important basis for the development and implementation of strategies that will increase Türkiye's digital security. Future research can expand knowledge in this area by using different data sets and variables.

References

Arslan, T., & Taş, B. (2022). Türkiye'de uluslararası göç-suç ilişkileri. [International migration-crime relations in Turkey.] Çankırı Karatekin University Karatekin Faculty of Letters Journal, 10(1), 1-28.

United Nations Conference on Trade and Development (UNCTAD), "Cybercrime Legislation Worldwide", https://unctad.org/page/cybercrime-legislation-worldwide Access date: 18.12.2024.

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, *3*(3), 85-110.

Buoncompagni, G. (2020). Cyber-risk, cyber-migration. For a new human geography and security. *SICUREZZA, TERRORISMO E SOCIETÀ*, *11*, 157-177.

Council of Europe, Convetion on Cybercrime, https://www.coe.int/tr/web/impact-convention-human-rights/convention-on-cybercrime#/ Access date:16.12.2024)

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging Technologies*, *6*(2), 142-153.

Drent, M., Dinnissen, R., van Ginkel, B., Hogeboom, H., Homan, K., Zandee, D., & Meijnders, M. (2022). *Relationship between external and internal security*. Clingendael Institute.

Goni, O., Ali, M. H., Showrov, M. M. A., & Shameem, M. A. (2022). The basic concept of cybercrime. *Journal of Technology Innovations and Energy*, *1*(2), 16-24.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology*, *2*, 13-20.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber crime and cyber terrorism investigator's handbook* (pp. 149-164). Syngress.

Karakaya, H. (2020). Göç ve Türkiye'deki etkileri. [Migration and its effects in Turkey.] Fırat University International Journal of Economics and Administrative Sciences, *4*(2), 93-130.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203-210.

Montoya, L., Junger, M., & Hartel, P. (2013, August). How" Digital" is Traditional Crime? In *2013 European Intelligence and Security Informatics Conference* (pp. 31-37). IEEE.

Özel, N. (2016). Bilgi ve İletişim Teknolojilerinin Etkisiyle Değişen Bilgi Kaynakları, Hizmetleri ve Öğrenme Ortamları [Changing Information Resources, Services and Learning Environments with the Impact of Information and Communication Technologies.] National Education Journal, *45*(209), 270-294.

Salahshour Rad, M., Nilashi, M., & Mohamed Dahlan, H. (2018). Information technology adoption: a review of the literature and classification. *Universal Access in the Information Society*, 17, 361-390.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Schiks, J. A., van de Weijer, S. G., & Leukfeldt, E. R. (2022). High-tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals, and non-criminals. *Computers in Human Behavior*, *126*, 106985.

Tourist Business Association (2025), https://www.altid.org.tr/bilgi-hizmetleri/antalya-ziyaretci-sayilari-2024-2/ Access date:27.03.2025.

TÜİK, International Migration Statistics, (2023), https://data.tuik.gov.tr/Bulten/Index?p=Uluslararasi-Goc-Istatistikleri-2023-53544 Access date:30.12.2024.

Wall, D. (2004). What are cybercrimes? *Criminal Justice Matters*, *58*(1), 20-21.