Research Article RJ-5

Researches on Multidisciplinary Approaches 2026 (1) ISSN:2791-9099

Cross-Border Digital Threats: Cybercriminal Profile Analysis Based on Gendarmerie Data in Türkiye

Vedat Yılmaz / Asst. Prof. Dr.
Institute of Forensic Sciences, Gendarmerie and Coast Guard Academy
vedat.yilmaz@jsga.edu.tr.

Abstract

In this study, analyses were made by focusing on he concept of cyber crime has created security problems all over the world, and the law enforcement's fight against crime and criminals has evolved into a new structure. In this study, analyses were made by focusing on demographic variables and criminal profiles for cyber crimes registered in the Incident Information System by the Gendarmerie General Command in Turkey between 2014-2024. Based on the cybercrime records in the system, evaluations were made regarding the nationality, gender, age distribution of the perpetrators. Among foreign perpetrators, those with Syrian nationality constitute the majority. Cybercrime perpetrators are mostly males in the transition from adolescence to young adulthood. In particular, perpetrators from Iraq, Iran and Afghanistan have been found to be in older age groups. Cybercrime rates among female perpetrators are higher among Syrian nationals than in other countries. This research highlights the fact that cybercrime has become a borderless, international criminal phenomenon and the importance of international cooperation and data sharing in law enforcement's fight against crime and criminals. As a result, the importance of awareness and cybercrime awareness in the use of technological devices in the prevention of cyber crimes is inevitable.

Keywords: Cybercrime, Digital Threats, Age and Gender Analysis, Law Enforcement.

JEL Codes: K24, K29, F39, O35, O39

Citation: Yılmaz, V. (2026). Cross-border digital threats: Cybercriminal profile analysis based on gendarmerie data in Türkiye. *Researches on Multidisciplinary Approaches (ROMAYA Journal)*, 2026(1).

Submission Date : 27.08.2025
Acceptance Date : 27.11.2025

1. Introduction

Technological developments in the digital world, combined with the ease of accessing the internet from mobile devices, have brought about radical changes in our daily lives and habits. As a result of this transformation, identifying the factors that contribute to cybercrime threats is of great importance for both crime victims and law enforcement agencies in the fight against crime and criminals (Padyab et al., 2024). The unstoppable rapid development in technology, which has become a turning point in human history, has changed our daily habits as well as society.

While the digital world has facilitated access, sharing and transaction methods for all of us, it has also brought cyber risks with it. One of the most important of these emerging risks is cybercrime (Lovan & Lovan, 2016). Cybercrime basically refers to crimes committed through the misuse of technology. With cybercrime, the dark side of the digital world has also emerged. (McGuire & Dowling, 2013). Cybercrime is an important security issue not only for individuals but also for societies and even states. (Gordon & Ford, 2006).

The main difference between cybercrime and traditional crime is that there is no physical boundary to the crime committed in cyberspace. (Cerezo et al., 2007; Onwuadiamu, 2025). Cybercrime crosses physical borders, requiring international cooperation beyond national measures and healthy communication and coordination with other countries for law enforcement. (Neumüller, 2017; Holt et al., 2023). Today, as technology has become a universal tool, it has become easier for individuals and groups to engage in cross-border actions, and it has become common for individuals from different nations to be among the perpetrators of cybercrimes (Holt et al., 2023; Buçaj & Idrizaj, 2025).

The global spread of the internet and the rapid development of digital technologies have made access to information easier and have radically changed our habits. However, this rapid technological change, which has made its impact felt in social life, has also paved the way for exposure to cybersecurity vulnerabilities and unexpected crimes. This vulnerability in cyberspace has been seen as an easy target by criminal elements, and with the increase in the complexity of cybercrimes, the number of victims is increasing day by day (Lusthaus, 2024; Back & LaPrade, 2019). Only as a result of the spread of internet-based applications, it has started to pose serious risks to individuals commercial enterprises and therefore to the entire society, namely the state (Ünver, 2023). One of the biggest factors in this increase in risk is the exponential increase in the volume of trade made over the internet and it has turned into an environment where every form of shopping is done (Apau & Koranteng, 2019). In addition, the field of business and education has become as much a part of our lives as shopping over the internet.

Unlike traditional crime methods, cybercrimes eliminate geographical boundaries and provide criminals with the opportunity to hide their actions regardless of location and to operate internationally (Weulen Kranenbarg et al., 2018; Borwell et al., 2021; Saud, 2025). This situation necessitates that the law enforcement agencies of countries reconsider their strategies to combat cybercrimes and give more importance to international cooperation (Çetin, 2021).

There is a significant amount of research in the literature on cybercrime. For example; Wall (2004) defines cybercrime as “any crime committed over the Internet”, Furnell (2003) defines cybercrime as “any crime that involves the use of a computer” at the most basic level, and Gordon & Ford (2006) define cybercrime as “any crime facilitated or committed using a computer, network, or hardware device” and state that the current definition of cybercrime has developed empirically.

Cybercrimes are crimes committed through the misuse of information technologies, involving attacks on computer systems, networks, and digital data (Taşçı and Can, 2015; Kökkaya, 2022). These crimes mostly include identity theft, social media fraud, personal data breaches, ransomware-based attacks and DDoS attacks (Dawson, 2015; Rao et al., 2018). In cyberspace, perpetrators of these crimes can achieve their goals in the virtual environment without being affected by borders or physical restrictions. This means that perpetrators can take advantage of legal loopholes to commit crimes and find victims outside their own country and escape the punishment for their crimes. (Kökkaya, 2022).

As cybercrime spreads dangerously around the world, international cooperation and crime prevention strategies should be increased to reduce the threat of cybercrime. (Khan, 2024). The rapid increase in cybercrime in the last five years is evident in law enforcement records. (Balqis and Badu, 2025).

In Türkiye, the term "informatics crime" is legally used instead of "cyber crime" for these actions. Cybercrimes are defined in the Turkish Penal Code as entering an information system, blocking or disruptings. (Turkish Penal Code No. 5237, 2004).

Türkiye, located at the intersection of Europe and Asia and facing political instability and conflict in neighboring countries, is a target for cybercrimes. The fight against cybercrime is carried out nationwide by the General Directorate of Security and the General Command of the Gendarmerie, both within the Ministry of Interior.

Cybercrime cases recorded between 2014 and 2024, which were initially classified as a separate crime category by the Gendarmerie General Command in its fight against cybercrime, provide important data on the demographic distribution of crimes and the nationality, gender, and age groups of perpetrators. This data provides important information on the demographic characteristics in which cybercrimes are concentrated and the social groups from which perpetrators come.

The analyses to be made in this study will provide the evaluations to be made regarding the cyberspace where crime has started to shift and the importance and evaluation of the demographic variables that emerge in the fight against crime and criminals.

2. Conceptual Framework / Theory

Demographic analysis is a frequently used and important method in cybercrime research, used to understand the nature of cybercrime and the profile of the perpetrators (Schreuders, 2019; Ndubueze et al., 2013). The literature shows that cybercrime perpetrators are more common among young adults (Näsi et al., 2015). This is related to factors such as predisposition to digital technologies, heavy use of the internet and digital devices, and social media. (Näsi et al., 2015). Additionally, the relationship between the criminal tendencies and education levels of cybercrime perpetrators is emphasized. (Näsi et al., 2015; Schreuders, 2019). The emergence of new opportunities in digital environments, high levels of social media use and personal data sharing, and the tendency of groups in economic distress to turn to cyber crimes are also other issues that are widely discussed in the literature. (Kamal et al., 2012; Ilievski & Bernik, 2016).

The cross-border nature of cybercrime allows perpetrators to operate both within their own countries and internationally. This increases the potential for foreign cybercrime perpetrators to commit crimes in other countries (Neumüller, 2017; Holt et al., 2023; Păduraru, 2025). Foreign cybercrime perpetrators may use legal gaps and technological security infrastructure deficiencies in the countries where they commit crimes as a motivation to commit the crime. The literature cites the reasons for this as different legal regulations, lack of cooperation between countries, problems in cross-border data sharing and differences in security policies in the fight against crime and criminals (Neumüller, 2017; Holt et al., 2023). Further increasing international cooperation, establishing correct data flow mechanisms and carrying out joint activities in the fight against crime are important issues in the fight against cross-border cyber threats (Reitano et al., 2015; Păduraru, 2025).

The following points are among the reasons why cybercrime perpetrators are more likely to commit crimes outside their own countries. First, the rapid spread of digital technologies has facilitated cross-border criminal activities. Differences in national judicial systems and inadequate information sharing make it difficult to catch criminals. Secondly, cyberspace poses challenges in detecting and tracking cybercrime. Thirdly, perpetrators in countries with advanced technological infrastructure tend to operate in countries with less technological development. (Reitano et al., 2015, Chaturvedi et al., 2014, Eldem, 2020).

The main purpose of this article is to analyze the cybercrime cases intervened by the Gendarmerie General Command between 2014-2024 in terms of demographic and crime profiles. The research aims to examine the ages, genders and nationalities of cyber crime perpetrators.

This study attempted to answer the following questions.

- What is the demographic distribution of cybercrimes in Türkiye according to Gendarmerie records?
- What is the distribution of cybercrime perpetrators in Türkiye by country?
- What are the differences between Turkish and foreign nationals when it comes to cyber crime perpetrators?

While searching for answers to these questions, it was also aimed to conduct analyses based on current literature and to present recommendations based on the data obtained.

Developments in cybersecurity and cybercrime have fundamentally altered the traditional understanding of crime (Balqis and Badu, 2025). While traditional crimes are generally assessed through actions that leave tangible traces in physical locations, today's cybercrime has become an invisible and boundary-breaking phenomenon in digital environments (Khan, 2024). This new criminal environment has transformed not only the way crimes are committed but also the perpetrators themselves. Perpetrators are now sufficiently skilled at creating a new criminal environment and effectively utilizing technology through the internet. This has necessitated the reorganization of law enforcement agencies combating crime and criminals, as well as legal systems to punish perpetrators. Therefore, cybersecurity should be considered not only as a technical defense issue but also as a multifaceted socio-technical phenomenon within the modern criminal ecosystem (Özdemir, 2020).

3. Methodology

In this study, cybercrime data processed by the Gendarmerie General Command, a law enforcement agency responsible for public security in the Republic of Türkiye, for the last 10 years were used and detailed analyses were conducted on crime records processed between 2014-2024. The necessary examinations were conducted on a total of 54,842 cybercrime records in 81 provinces of Türkiye, registered in the Gendarmerie General Command Incident Information System, which acts as the Law Enforcement in Türkiye, and committed between 2014-2024. In the study, it was evaluated that 92 crime records were entered incorrectly and were not related to cybercrimes, and the necessary examinations and analyses were conducted on 54,750 records. The research examined in detail the total cybercrime records, including changes in crime rates over the years, gender discrimination and age categories, and records with no nationality data entry for Türkiye national perpetrators and other foreign national perpetrators. The data was examined in three basic demographic dimensions: nationality, gender, and age range. Nationality information covers individuals from 102 different countries. Age data was divided into 7 categories: 15–24, 25–34, 35–44, 45–54, 55–64, 65–75, and undefined (incomplete or incorrect entries). Gender information was classified as "male", "female", and "not specified".

When evaluating the age range, the data set;

- Transition period from adolescence to young adulthood (15-24 years),
- Young adulthood (25-34 years),
- Beginning of middle age (35-44 years),
- Later middle age (45-54 years),
- Late adulthood (55-64 years),
- Old age (65-75 years),
- Incorrect data entry (no data entry, 0-15, 76-over) were divided into 7 different categories.

Primarily, descriptive statistics (frequency and percentage distributions) were used in statistical analyses. Since the data were categorical, parametric tests were not deemed appropriate. Therefore, the Chi-square (χ^2) test of independence was applied to evaluate the statistical significance of the differences between the groups. All analyses were performed using Python's SciPy library.

3.1. Cybercrime Records Committed in Türkiye and Processed by the Gendarmerie

Total criminal records processed in the last 10 years are separated according to the nationality of the person committing the crime and are listed from most to least as presented in Table 1. Foreign nationals with less than 20 records in the last 10 years are considered in the category of citizens of other countries.

3.2. Gender Information of Cyber Crimes

The gender information of the persons processed based on their nationality from the total criminal records is shown in Table 2. Persons whose gender data is not entered are also shown in the list.

3.3. Age Information of Individuals Regarding Cyber Crimes

According to the cyber crime records processed by the Gendarmerie, age ranges were divided into 7 categories, and records not entered for age, and records under the age of 15 and over the age of 75 were considered as incorrect entries and were collected under the Undefined category. Details of the age information of individuals related to cybercrimes are in Table 3.

Table 1. Cybercrime Records Committed in Türkiye and Processed by the Gendarmerie by Years

							Criminal Records						
S.No.	**Country**	**Total**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**
1	Türkiye	45035	381	1495	1659	658	793	1360	3219	5639	9343	12788	7700
2	Syria	7164	0	2	9	12	16	43	159	761	1698	2183	1881
3	Iraq	165	0	0	0	3	2	2	15	28	27	40	48
4	Afghanistan	136	0	0	0	0	2	1	4	19	24	51	35
5	Turkmenistan	118	0	0	0	0	0	3	2	15	13	55	20
6	Iran	123	0	0	0	0	0	3	2	15	26	25	52
7	Uzbek	100	0	0	0	0	1	0	11	14	27	22	25
8	Russia	107	0	0	0	1	1	1	0	4	15	34	51
9	Azerbaijan	64	0	0	1	0	1	0	3	10	10	15	24
10	Nigeria	55	0	0	0	0	0	0	1	3	4	25	22
11	Morocco	55	0	0	0	0	0	0	2	5	8	14	26

12	Bulgaria	40	2	0	0	0	2	0	1	0	11	16	8
13	Germany	37	0	0	0	0	1	1	3	3	5	9	15
14	Libya	37	0	0	0	0	2	0	2	8	10	7	8
15	Algeria	37	0	0	0	0	0	2	2	1	5	12	15
16	Kazakhstan	35	0	0	1	1	0	0	1	5	5	9	13
17	Saudi Arabia	35	0	0	0	0	1	0	1	0	4	11	18
18	Jordan	30	0	0	0	0	0	0	0	8	4	12	6
19	Ukraine	29	0	0	0	0	0	1	1	3	8	9	7
20	China	24	0	0	0	0	0	0	0	3	5	10	6
21	Kuwait	22	0	0	0	0	0	0	0	4	7	6	5
22	Israel	22	0	0	0	0	0	0	0	0	7	10	5
23	Tunisia	22	0	0	0	0	0	0	1	2	4	4	11
24	Cameroon	21	0	0	0	0	0	0	1	3	3	10	4
25	Somalia	21	0	0	0	0	0	0	0	6	8	5	2
26	Angola	21	0	0	0	0	0	0	0	0	9	8	4
27	Georgia	20	0	0	1	0	0	0	1	2	5	9	2
28	Lebanon	20	0	0	0	0	0	0	1	2	5	4	8
29	USA	20	0	0	0	0	0	0	0	0	1	7	12
30	74 Other Countris (less than 20 crime records)	423	0	0	2	4	4	5	14	47	72	117	158
31	Nationality not Entered	712	40	26	154	31	25	37	81	82	87	107	42

Table 2. Gender Information of Cyber Crimes Committed in Türkiye and Processed by the Gendarmerie

			Gender		
S.No.	**Country**	**Total Number of Criminal Records**	**Male**	**Female**	**Gender not Entered**
1	Türkiye	45035	38246	6071	718
2	Syria	7164	4838	2194	132
3	Iraq	165	105	25	35
4	Afghanistan	136	78	43	15
5	Turkmenistan	118	72	44	2
6	Iran	123	64	26	33
7	Uzbekistan	100	51	36	13
8	Russia	107	38	23	46
9	Azerbaijan	64	40	14	10
10	Nigeria	55	40	11	4
11	Morocco	55	14	17	24
12	Bulgaria	40	13	9	18
13	Germany	37	21	7	9
14	Libya	37	21	5	11
15	Algeria	37	13	9	15

16	Kazakhstan	35	16	13	6
17	Saudi Arabia	35	19	3	13
18	Jordan	30	18	4	8
19	Ukraine	29	11	13	5
20	China	24	11	7	6
21	Kuwait	22	9	1	12
22	Israel	22	5	1	16
23	Tunisia	22	8	5	9
24	Cameroon	21	15	5	1
25	Somalia	21	10	7	4
26	Angola	21	18	3	0
27	Georgia	20	7	9	4
28	Lebanon	20	7	3	10
29	USA	20	5	3	12
30	74 Other Countris (less than 20 crime records)	423	205	82	136
31	Nationality not Entered	712	545	59	108

Table 3. Age Information of Individuals Regarding Cyber Crimes Committed in Türkiye and Processed by the Gendarmerie

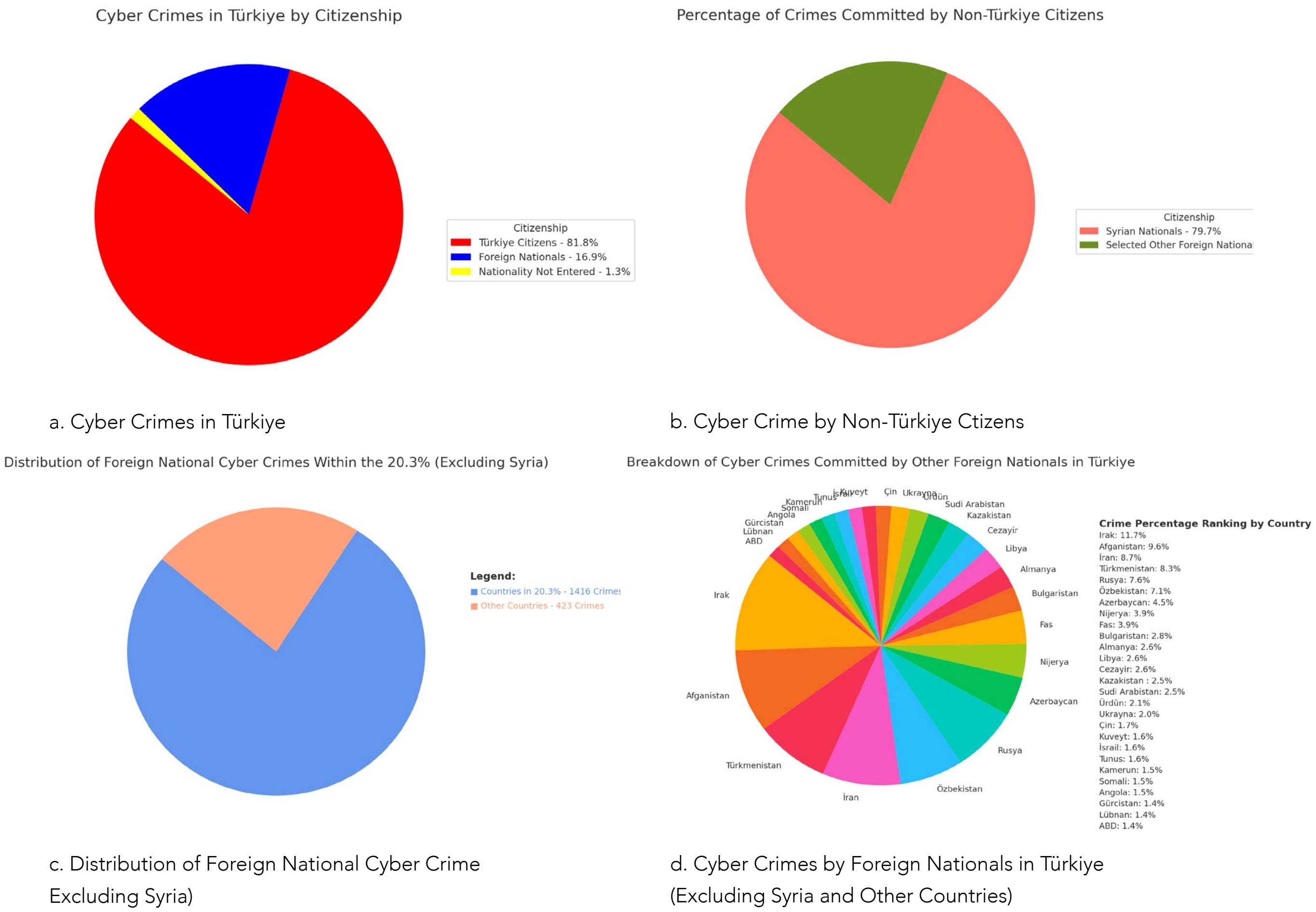
			Age Range						
S.No.	**Country**	**Total**	**15-24**	**25-34**	**35-44**	**45-54**	**55-64**	**65-75**	**Undefined**
1	Türkiye	45035	15149	13008	8797	4886	2036	791	368
2	Syria	7164	1163	2148	1329	847	683	586	108
3	Iraq	165	33	52	36	20	13	3	8
4	Afghanistan	136	28	49	25	16	7	6	5
5	Turkmenistan	118	16	52	32	11	4	0	3
6	Iran	123	14	38	33	18	11	4	5
7	Uzbekistan	100	21	29	24	14	4	1	7
8	Russia	107	21	27	24	16	5	4	10
9	Azerbaijan	64	25	17	15	0	4	1	3
10	Nigeria	55	7	26	18	1	0	0	3
11	Morocco	55	13	17	14	5	1	0	5
12	Bulgaria	40	2	8	13	2	3	2	10
13	Germany	37	3	16	2	10	4	1	1
14	Libya	37	8	6	9	4	4	3	3
15	Algeria	37	8	10	12	2	0	1	4
16	Kazakhstan	35	7	12	7	0	3	0	6
17	Saudi Arabia	35	10	7	9	5	2	2	0
18	Jordan	30	8	10	6	3	2	0	1
19	Ukraine	29	3	11	4	5	3	0	3

20	China	24	5	9	6	0	2	0	2
21	Kuwait	22	1	4	4	2	6	0	5
22	Israel	22	6	5	4	1	2	0	4
23	Tunisia	22	6	7	3	1	2	1	2
24	Cameroon	21	0	11	6	3	0	0	1
25	Somalia	21	5	5	4	1	2	1	3
26	Angola	21	0	8	7	2	1	0	3
27	Georgia	20	4	5	4	4	1	0	2
28	Lebanon	20	3	4	0	4	4	1	4
29	USA	20	4	5	3	2	4	1	1
30	74 Other Countris (less than 20 crime records)	423	83	146	93	37	17	10	37
31	Nationality not Entered	712	42	101	189	192	88	14	86

4. Findings and Discussion

4.1. Cybercrime Records Committed in Türkiye and Processed by the Gendarmerie

Of the 54,750 records recorded, 45,035 were committed by Turkish citizens, and 81.8% of the total cybercrime records were Turkish citizens. 16.9% of the records were committed by foreign nationals, from 102 countries, and no nationality information was entered for 712 crime records, which constitute 1.3% of the records created by security forces. Detailed graphs of the data are presented in Figure 1.



a. Cyber Crimes in Türkiye

b. Cyber Crime by Non-Türkiye Ctizens

c. Distribution of Foreign National Cyber Crime Excluding Syria)

d. Cyber Crimes by Foreign Nationals in Türkiye (Excluding Syria and Other Countries)

Figure 1. Percentage Segments of Countries According to Total Cybercrime Rate

According to the processed cybercrime records, when the criminal records of foreign nationals who committed crimes in Türkiye are examined, it is seen that 7164 records out of 9003 records are Syrian nationals. This constitutes 79.7% of the records among foreign nationals. When Syria is excluded from the foreign nationals side, when 1839 records are examined in percentiles, respectively, Iraq 11.7%, Afghanistan 9.6%, Iran 8.7%, Turkmenistan 8.3%, Russia 7.6%, Uzbekistan 7.1%, Azerbaijan 4.5%, Nigeria 3.9%, Morocco 3.9%, Bulgaria 2.8%, foreign nationals who make up the first 10, comprise 64.2% of the records. Crimes committed by nationals of the remaining 91 countries comprise 35.8% of the records.

According to the studies, the fact that 16.9% of the overall cyber crime rate is made up of foreign nationals shows that the world of cyber crime is globalizing. In addition, the fact that Syrian nationals constitute approximately 80% of foreign nationals is considered to be due to the density of refugees in Türkiye due to the Syrian civil war. When Türkiye's border neighbors, Syria, Iraq, Iran, Azerbaijan, Armenia, Georgia, Bulgaria and Greece are considered, it is striking that Greek and Armenian nationals have less than 20 criminal records. In addition, the records of Turkish Republic citizens from Azerbaijan, Turkmenistan, Uzbekistan and Kazakhstan are noteworthy, but Kyrgyzstan nationals are seen to have less than 20 records. The fact that Afghan nationals are the 3rd most cyber crime-committing foreign nationals is considered to be due to refugee migration to Türkiye. Statistical results are shown in Table 4.

Table 4. Statistical Results

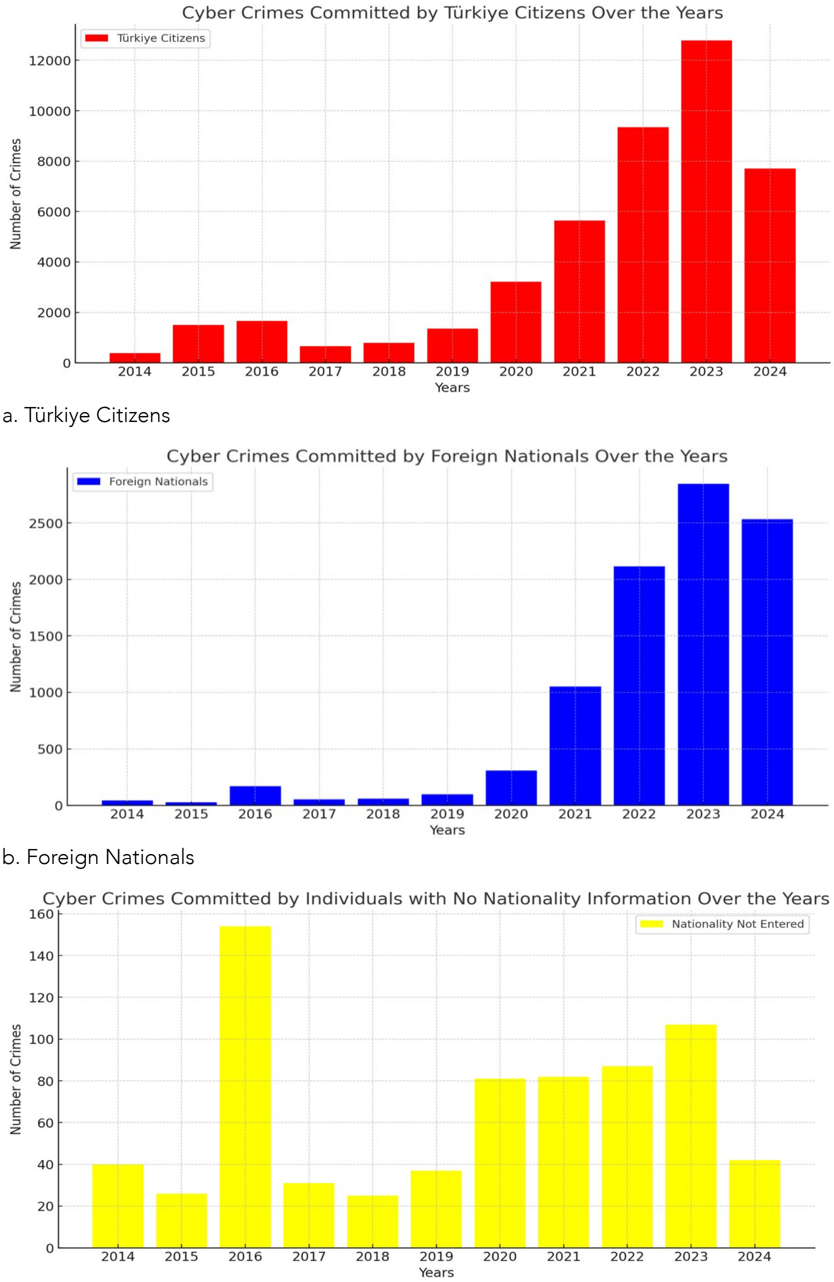
Test	χ^2	df	p-value	Result
Country × Year	3308.20	300	< 0.001	Significant
Country × Gender	7662.99	60	< 0.001	Significant
Country × Age Group	4325.65	180	< 0.001	Significant

4.2. Change In Cybercrime Records Over The Years

When the cybercrime records of the 10-year period between 2014 and 2024, which were processed by the Gendarmerie General Command in Türkiye, are examined according to years; It is seen that the number of individuals processed has increased rapidly since 2020. It is evaluated that the year 2020, when this increase started, was also affected by the detection of the COVID-19 outbreak in Türkiye and the start of remote working activities for quarantine purposes. It is seen that 2023 was the most intense year for cybercrimes detected and processed in Türkiye. In addition to technological advances, it is evaluated that with the pandemic that started in 2020, in an environment where transactions, work environments and even shopping were ordered online from home, victims became more vulnerable due to more intensive internet use. In parallel with the increasing number of cases, it is evaluated that the Gendarmerie General Command has established a new organization to combat crime and criminals within the scope of the increasing threat against Cybercrimes and has started to focus more on this issue, which is another factor in the increase in the number of individuals processed.

Cybercrime records, which have been increasing in the 5-year period since 2019, have decreased in 2024 compared to the previous year. It is evaluated that this decrease is due to the awareness activities carried out by the law enforcement and citizens being more careful in using technology. This similar pattern is valid for both Turkish and foreign national records. An increase was observed in 2016 compared to other recent years, and it is evaluated that this increase may be due to the process experienced after the treacherous coup attempt that was attempted in Türkiye and ended in failure. In addition, when the records in 2016 where no nationality record was entered are examined, the highest values of the last 10-year period are seen. In this case, it is evaluated that the number of law enforcement personnel decreased after the treacherous coup attempt in 2016, and this may be due to the efforts made to catch other criminal elements and members of the Fetullahçı terrorist organization. Cybercrime records committed in Türkiye and kept by the Gendarmerie over the years are shown in Figure 2.

χ^2 Scatter Plot – The red line indicates that the test statistic (χ^2 = 3308.20) lies on the right side of the distribution. This highlights a significant difference at the $p < 0.001$ level. Heat Map (Standardized Residuals) – Color intensities indicate which countries experienced more (red) or less (blue) cybercrime than expected in which years (Figure 3).



a. Türkiye Citizens

b. Foreign Nationals

c. No Nationality Information

Figure 2. Cybercrime Records Committed in Türkiye and Processed by the Gendarmerie by Year

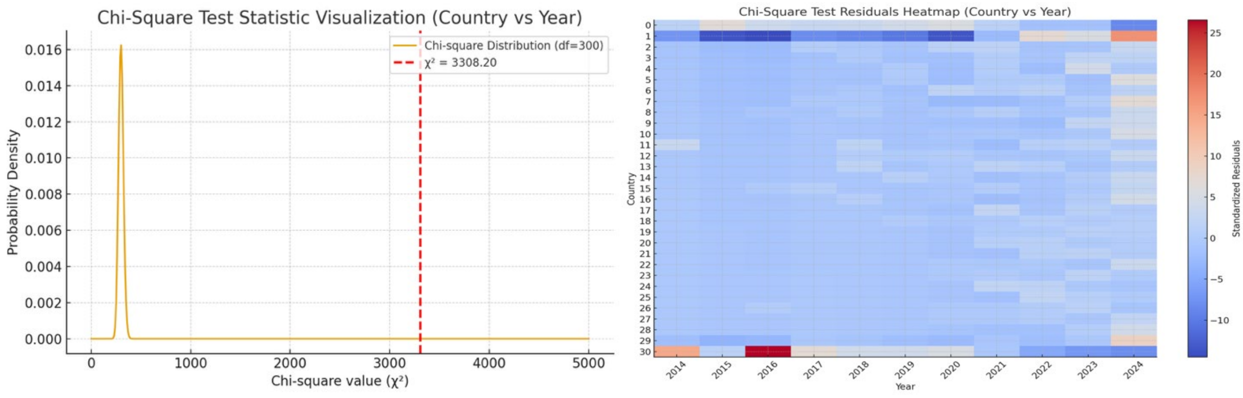


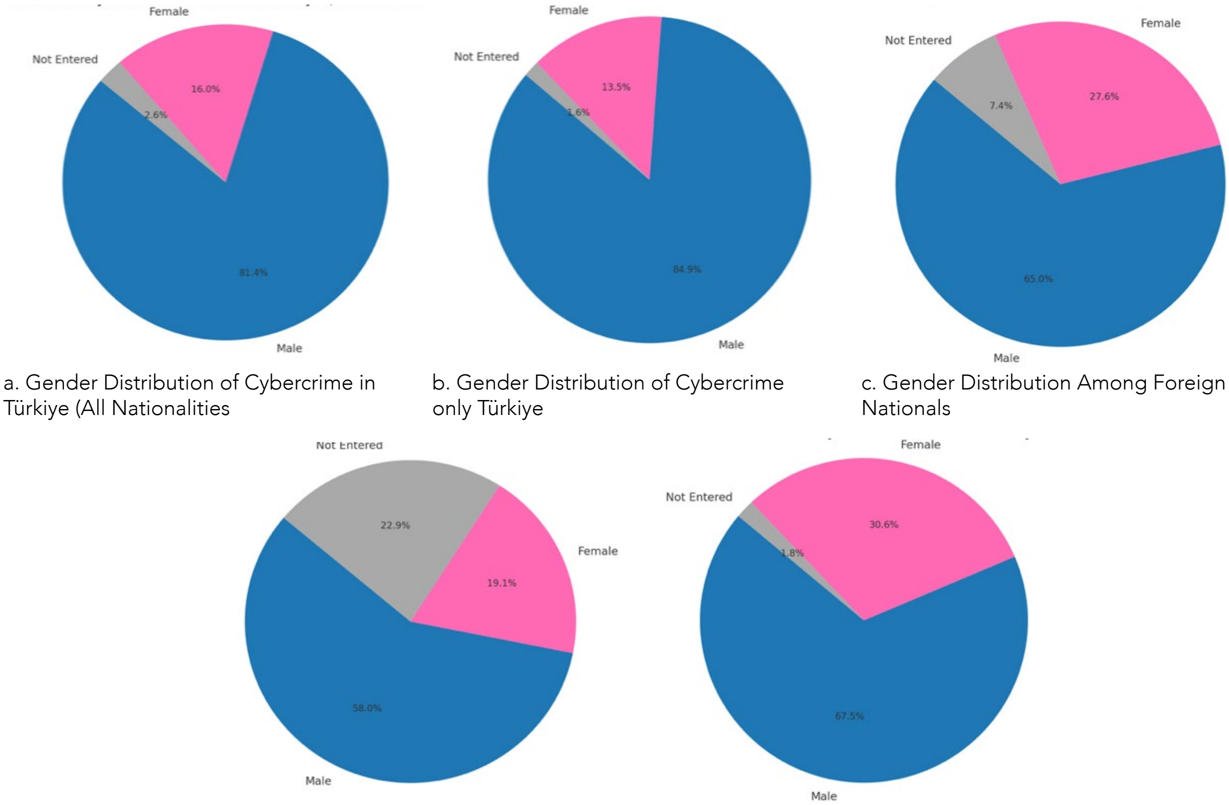
Figure 3. Country and Year χ² Scatter Plot and Heat Map (Standardized Residuals)

4.3. Gender Information of Cyber Crimes

When the records of cybercrime perpetrators are examined, 81.4% of the total number of individuals processed are male, 16.0% are female and 2.6% are individuals whose gender information is not entered. 84.9% of Turkish nationals are male, 13.5% are female and 1.6% are those whose gender information is not entered. When foreign national records are examined, it is seen that this rate is 65.0% for males, 27.6% for females and 7.4% for those whose gender information is not entered. When Syrian nationals are removed from foreign national records, it is seen that 58.0% for males, 19.1% for females and 22.9% for those whose gender information is not entered. In the gender examination of cybercrimes committed by Syrian nationals, it is seen that 67.5% for males, 30.6% for females and 1.8% for those whose gender information is not entered.

As a result of the examinations, it is seen that the number of male perpetrators is approximately 5 times higher than the number of female perpetrators. When only Turkish nationals are examined, it is seen that the number of female perpetrators is much lower than the average, but the number of female perpetrators is higher than the general assessment among foreign nationals. In addition, it is seen that the rate of cybercrime among Syrian women is quite high. Approximately one in every three perpetrators is a woman. When foreign national perpetrators are examined, it is striking that gender data entry is high, excluding Syrian nationals, and the gender of approximately one in every five people is not entered. Details regarding gender-based cybercrimes committed in Türkiye and by the Gendarmerie are shown in Figure 4.

χ^2 Scatter Plot – The red line represents the calculated value of $\chi^2 = 7662.99$. Its location far to the right of the curve confirms high significance at the $p < 0.001$ level. Heat Map (Standardized Residuals) – Red tones indicate higher than expected gender ratios in certain countries, while blue tones indicate lower gender ratios. This suggests, for example, that some countries have higher than expected proportions of female perpetrators or missing records (Figure 5).



a. Gender Distribution of Cybercrime in Türkiye (All Nationalities

b. Gender Distribution of Cybercrime only Türkiye

c. Gender Distribution Among Foreign Nationals

d. Gender Distribution Among Foreign Nationals (Excluding Syria)

e. Gender Distribution of Cybercrime only Suria

Figure 4. Gender Information of Cyber Crimes Committed in Türkiye and Processed by the Gendarmerie

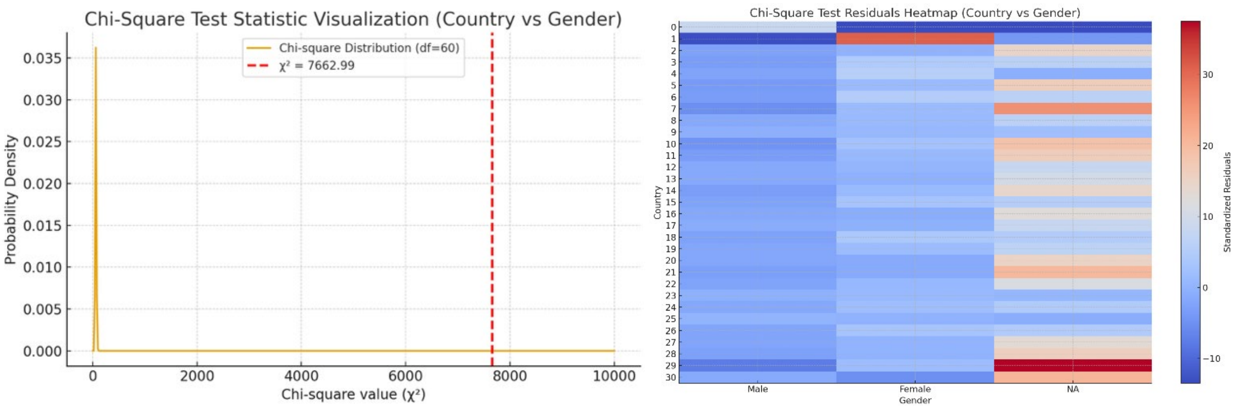


Figure 5. Country and Gender χ² Scatter Plot and Heat Map (Standardized Residuals)

4.4. Age Information of Individuals Regarding Cyber Crimes

When the age assessment dataset in Cyber Crimes is examined by dividing it into 7 different categories; it is seen that the highest rate of 30.7% is in the category specified as the transition period from adolescence to young adulthood. It is known that the individuals in this category have high adaptation to technology, quickly adapt to new technologies and have intensive usage rates with technology.

The rate is 29.1% in the 25-34 age category, called the young adulthood period. It is evaluated that the individuals in this age category are generally in the career start phase, use digital platforms and social media tools intensively, and have gained or are gaining their economic freedom.

The rate of 19.7% is seen in the 35-44 age range, which is evaluated as the beginning of middle age, and this group is a group that has gained experience in using technology but may show differences in adaptation to new trends.

The 45-54 age group, which is called the advanced middle age period, whose adaptations to the digital world vary, is 11.2%.

55-64 years: Late adulthood. People with low technology usage rates, less cyber security awareness and an intermediate period in technology awareness. There are 5.4% of individuals who commit cybercrime in the 55-64 age group, who are in adulthood.

The rate of committing crimes in the old age period between the ages of 65-75 is 2.6%. Those in this age group generally have more limited adaptation to technology and may be more vulnerable to cybercrime.

Records that are 0-15 and 76 and above or do not include an age entry are considered as incorrect data entry. This range includes 1.3% of total individuals who commit crimes. The % Distribution of Cybercrimes by Age Groups is presented in detail in Figure 6. Distribution of Cybercrimes by Age Groups According to All Data is shown in Figure 7.

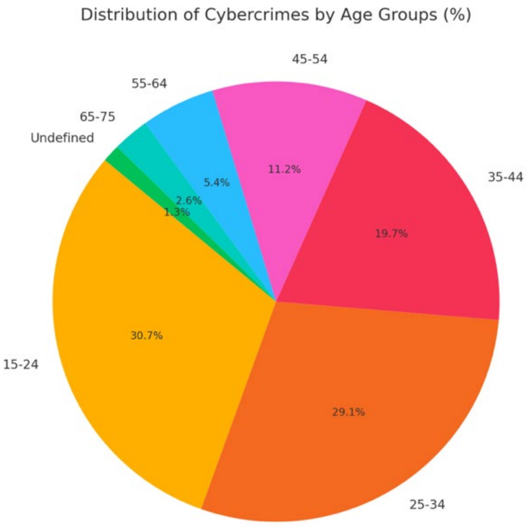


Figure 6. Distribution of Cybercrimes by Age Groups %

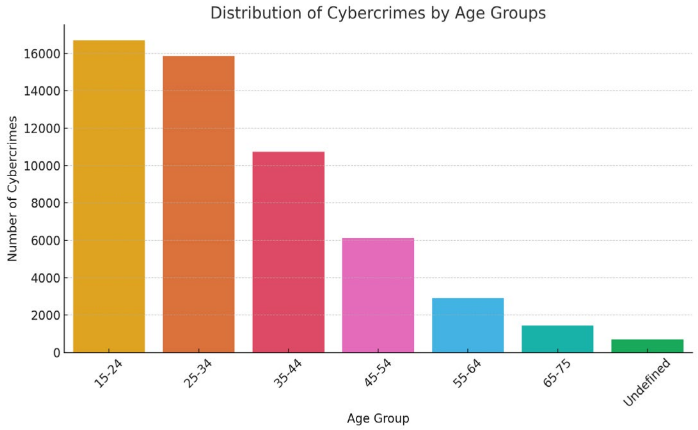
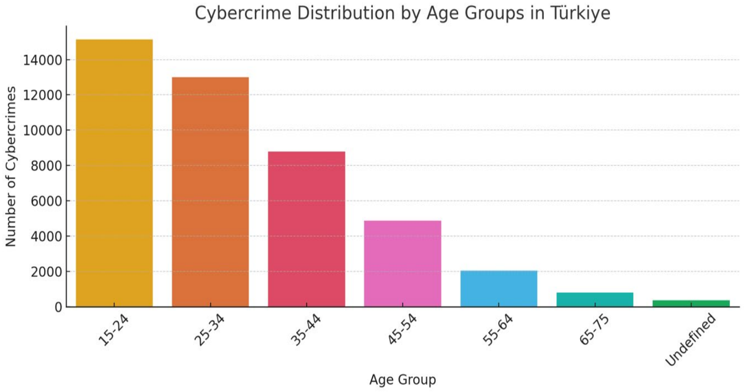


Figure 7. Distribution of Cybercrimes by Age Groups According to All Data

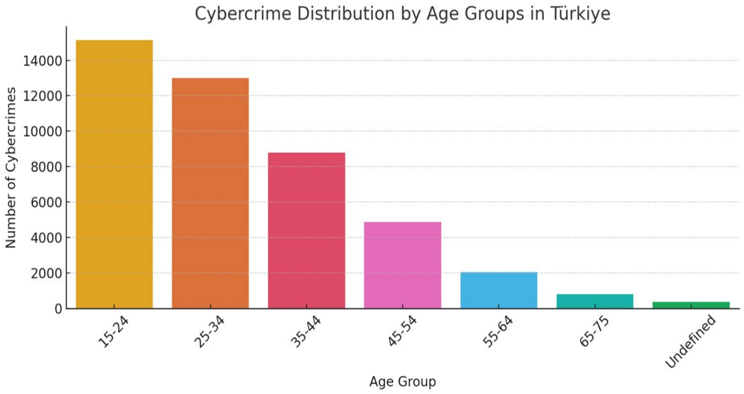
When the evaluations of Turkish cybercrime perpetrators according to age categories are examined, the density of perpetrators who are between the ages of 15-24 and have passed from adolescence to young adulthood draws attention. As the categories of mistake increase, the number of perpetrators gradually decreases and the number of individuals who are identified as age-related or who are defined as erroneous entry is also quite low. Among foreign nationals, the abundance of perpetrators who are at the level of young adulthood between the ages of 25-34 draws attention. As with Turkish nationals, the number of perpetrators decreases as the age category increases in foreign nationals. The reason for this is that the perpetrators in the young category are more proficient in technology and spend more time on open sources, thus taking advantage of the low technological and cyber awareness of cybercrime victims. The number of foreign national perpetrators who commit more crimes in the age range of 35-44, which is considered the beginning of middle age, draws attention, unlike Turkish nationals. In addition, when the Syrian nationals are excluded from the foreign nationals, when the remaining 20.3% of the foreign national perpetrators are examined, it is striking that the undefined category is more prevalent than the Turkish and Syrian national perpetrators. Details of the Distribution of Cybercrimes by Age Groups are shown in Figure 8.

When the crime categories of cybercrime perpetrators who are Turkish citizens are examined, the highest rate is those who are in the transition period from adolescence to young adulthood (15-24 years old) 33.6%. Cybercrime perpetrators who are in young adulthood (25-34 years old) 28.8%, while those who are in the beginning of middle age (35-44 years old) are Turkish citizens and constitute 19.5% of the crime perpetrators in the last 10 years. In other age categories, the number of perpetrators decreases as age increases. When the age ranges of cybercrimes committed by foreign nationals in Türkiye are examined, it is seen that cybercrime perpetrators who are in the young adulthood period (25-34 years old) are the highest with 29.2%. The beginning of middle age (35-44 years old) category comes second with 19.9%. Third in line are those in the transition period from adolescence to young adulthood (15-24 years old) with a rate of 15.9%.

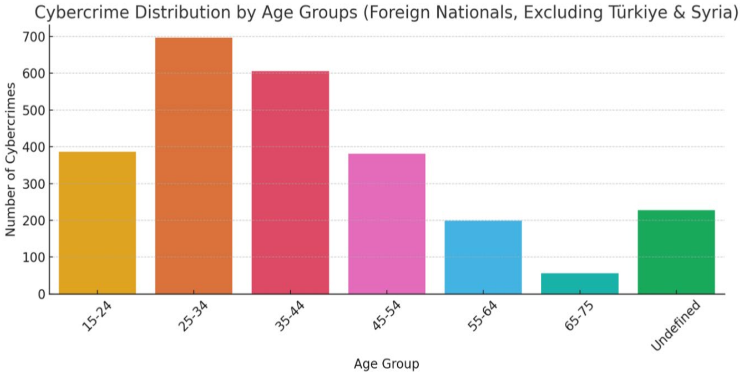
When the 73.7% of the crime perpetrators who constitute the foreign perpetrator category are excluded, and the highest crime perpetrator rate is Syrian nationals, when the age categories of the remaining foreign nationals are examined, it is seen that the age range with the highest rate is 27.3% for cybercrime perpetrators in the young adulthood period (25-34 years old). Second in line is the category of the beginning of middle age (35-44 years old) with a rate of 23.7%. Third in line are those in the transition period from adolescence to young adulthood (15-24 years old) with a rate of 15.1%. In addition, the rate of 14.9% for cybercrime perpetrators in the later middle age period (45-54 years old) is noteworthy.



a. Cybercrime Distribution by Age Groups in Türkiye



b. Cbercrime Distribution by Age Groups Foreign Nationals (Excluding Türkiye)



c. Cbercrime Distribution by Age Groups Foreign Nationals (Excluding Türkiye and Syria)

Figure 8. Distribution of Cybercrimes by Age Groups

It is considered that this difference between Turkish and foreign perpetrators is due to the fact that Turkish perpetrators are in Türkiye at every stage until they grow up and complete higher education, whereas foreign nationals are in Türkiye after a certain period of education or have an immigrant status, and therefore the crime rate is lower than that of Turkish perpetrators between the ages of 15-25, which is the transition category from adolescence to young adulthood.

When foreign cybercrime perpetrators are examined (excluding Syria and other countries with few criminal records), the first 5 nationals in the age categories are presented in Table 4 and Figure 9. Iraqi citizens are in the first place in 5 different categories between the ages of 15-64. It is considered that this is due to the internal unrest in Iraq and Türkiye being a border neighbor. The abundance of cybercrime perpetrators from Iran, another border neighbor of Türkiye, is striking. Especially, the second country with the highest number of perpetrators in the 4 categories between the ages of 35-75 is composed of citizens. It is also striking that Afghanistan, which is among the first 5 countries in every age category, has the most foreign national perpetrators in the 65-75 age category. Libya is in the first five places in the same age category, and Libyan national perpetrators are only in the first 5 countries in this age category. Bulgaria ranks first in the undefined or non-reference category. However, Bulgaria is not in the top 5 rankings in any other age category.

χ^2 Scatter Plot – The red line (χ^2 = 4325.65) lies far to the right of the distribution. This visually confirms that the test is highly significant ($p < 0.001$). Standardized Residual Heat Map – Red regions indicate that certain age groups are overrepresented in some countries than expected, while blue regions indicate that they are underrepresented (Figure 10).

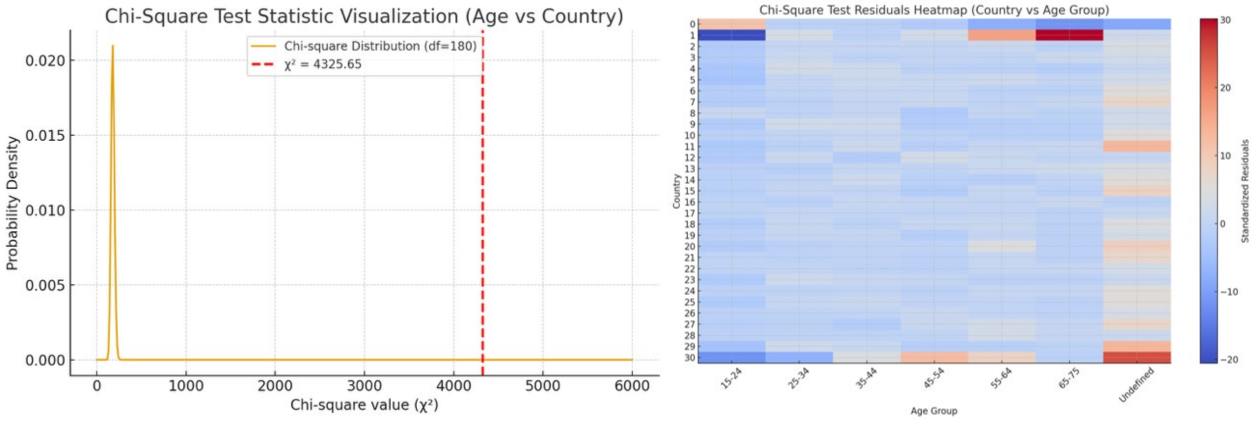


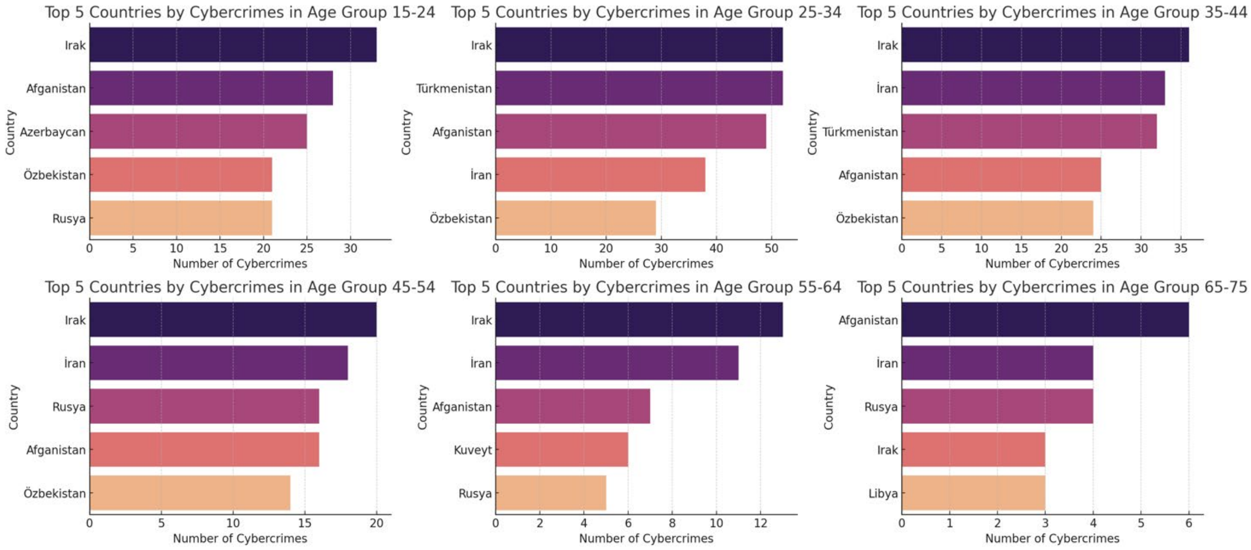
Figure 10. Country and Gender χ² Scatter Plot and Heat Map (Standardized Residuals)

Table 5. Countries with the highest number of criminal records in cybercrime based on the age of individuals (excluding Syria and other countries with low criminal records)

Age Category	Citizen of the country with the highest number of cybercrime perpetrators				
	1	2	3	4	5
15-24	Iraq	Afghanistan	Azerbaijan	Uzbekistan	Russia
25-34	Iraq	Turkmenistan	Afghanistan	Iran	Uzbekistan
35-44	Iraq	Iran	Turkmenistan	Afghanistan	Uzbekistan
45-54	Iraq	Iran	Russia	Afghanistan	Uzbekistan
55-64	Iraq	Iran	Afghanistan	Kuwait	Russia
65-75	Afghanistan	Iran	Russia	Iraq	Libya
Undefined 0-15, 76-over	Bulgaria	Russia	Iraq	Uzbekistan	Kazakhstan

5. Limitations and Future Works

This study has some limitations that need to be considered. Important limitation is that the data used in this study does not include all law enforcement data in Türkiye, but cybercrime data recorded in the Gendarmerie General Command Incident Information System database. In future studies, including Cybercrimes in the database of all law enforcement units operating in Türkiye may make the study more valuable in terms of accuracy and complementarity. The ranking of the Five Countries with the Most Cybercrimes by Age Groups (Excluding Türkiye, Syria and Other Countries) is shown in Figure 9.



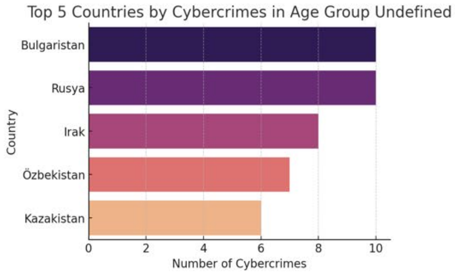


Figure 9. The five Countries with the most Cybercrimes by Age Groups (Exclođing Türkiye, Syria and Other Countris)

6. Conclusions

This study provides a comprehensive demographic and crime profile analysis of cybercrime cases processed by the Gendarmerie General Command in Türkiye over the past decade. The findings reveal a significant increase in cybercrime incidents, especially after 2020, with the COVID-19 pandemic and the resulting increase in digital addiction.

This finding supports the evaluation in the study conducted by Abdullahi and Ismail, stating that cyber crimes have increased during the COVID-19 period. (2025). Additionally, similar to the findings, Olusegun (2025) also shows from his study that the rapid spread of the COVID-19 pandemic in 2020 resulted in an unprecedented level of cybercrime worldwide.

Demographic analysis has revealed that cybercrime perpetrators in Türkiye are predominantly male and aged between 15 and 34.

It is evaluated that the high number of cyber crime perpetrators in this age group is due to factors such as their familiarity with technology, their use of technology at every stage of their lives, their widespread access to social media and digital platforms, and the time they spend on the internet. In contrast, foreign nationals showed a slightly different age distribution. Another finding was the relatively high proportion of female perpetrators among Syrian citizens.

The results revealed that demographic variables play a significant role in cybercrime trends. Based on these differences, law enforcement personnel can plan their activities to combat crime and criminals within the scope of predictive law enforcement.

Cybercrime, which has transcended national borders and become an international threat, is a growing problem facing law enforcement today. In this context, law enforcement agencies must develop new strategies to combat crime.

Given the vulnerability of migrants from countries experiencing socio-political instability or conflict/war to many crimes, especially cybercrime, and their criminal tendencies, international cooperation and joint efforts must be further strengthened. In this context, law enforcement agencies must be restructured to meet current needs and increase their capacity to combat cybercrime in the fight against crime and criminals.

The findings demonstrate that cybercrime is not merely a technical problem but also a sociological and behavioral phenomenon. Therefore, interdisciplinary studies should be expanded to combat these emerging and ever-increasing cybercrime rates. This approach can help better understand the motivations, behavioral patterns, and demographic characteristics of cybercriminals. The significant cross-country differences revealed by chi-square tests highlight the need for international cooperation. Cyber threats are not the concern of a single state but have become a global, transnational problem. This research demonstrates that cybercrime is a multifaceted and rapidly evolving field that requires a dynamic and data-driven response.

Future studies should utilize data from all law enforcement units to obtain a more holistic perspective on cybercrime in Türkiye. Thus, the results will support the development of national and international strategies against cyber threats.

References

Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. International Journal of Cyber Criminology, 13(2).

Abdullahi, A. S., & Ismail, U. (2025). Cybercrime During COVID-19 Pandemic in Urban Kano, Nigeria. In Cybercrime Unveiled: Technologies for Analysing Legal Complexity (pp. 309-327).

Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 1-4.

Balqis, A. A. A., & Badu, L. W. (2025). The Influence of Digitalization in Encouraging Crime: A Criminological Perspective. Estudiante Law Journal, 7(1), 139-148.

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime. Journal of Digital Social Research, 3(3), 85–110. https://doi.org/10.33621/jdsr.v3i3.66

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 2025024-2025024

Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In Second international workshop on digital forensics and incident analysis (WDFIA 2007) (pp. 13-27). IEEE.

Chaturvedi, M., Unal, A., Aggarwal, P., Bahl, S., & Malik, S. (2014, June). International cooperation in cyber space to combat cyber crime and terrorism. In 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW) (pp. 1-4). IEEE.

Çetin, M. S. (2021). Yargıtay Kararlar Işığında Bilişim Sistemine Girme Suçu (TCK m. 243). Türkiye Adalet Akademisi Dergisi, (45), 1-28.

Dawson, M. (2015). A brief review of new threats and countermeasures in digital crime and cyber terrorism. New Threats and Countermeasures in Digital Crime and Cyber Terrorism, 1-7.

Eldem, T. (2020). The governance of Turkey's cyberspace: between cyber security and information security. International Journal of Public Administration, 43(5), 452-465.

Furnell, S. (2003, June). Cybercrime: vandalizing the information society. In International conference on web engineering (pp. 8-16). Berlin, Heidelberg: Springer Berlin Heidelberg.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Holt, T. J., Chermak, S. M., Freilich, J. D., Turner, N., & Greene-Colozzi, E. (2023). Introducing and exploring the extremist cybercrime database (ECCD). Crime & Delinquency, 69(12), 2411-2436.

Kamal, M. M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. (2012). Nature of cyber crime and its impacts on young people: A case from Bangladesh. Asian Social Science, 8(15), 171.

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. Laws, 13(4), 44.

Kökkaya, F. (2022). Siber suçlarla mücadelede Türkiye-Avrupa Birliği arasındaki işbirliği [Yüksek lisans tezi, Fırat Üniversitesi]. Ulusal Tez Merkezi.

Ilievski, A., & Bernik, I. (2016). Social-economic aspects of cybercrime. Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences, 9(3), 8-22.

Iovan, S., & Iovan, A. A. (2016). From cyber threats to cyber-crime. Journal of Information Systems & Operations Management, 425.

Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?. Annual Review of Law and Social Science, 20(1), 369-385.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75, 1-35.

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.

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cyber crime victimization among Internet active Nigerians: An analysis of socio-demographic correlates. International Journal of Criminal Justice Sciences, 8(2), 225.

Neumüller, A. S. (2017). Cybercrime Centres: Analysis and Recommendations. Unpublished Master's thesis], University College Dublin.

Onwuadiamu, G. (2025). Cybercrime in criminology; a systematic review of criminological theories, methods, and concepts. Journal of Economic Criminology, 100136.

Olusegun-Joseph, Y. (2025). Urbanity, Transgressive Digitality, and COVID-19: Hierarchical Cybercrime (s) and the Subaltern Nigerian Urban Youth in a Global Pandemic. Journal of Asian and African Studies, 60(4), 2549-2563.

Păduraru, I. (2025). Forensic analysis of fraudulent messages: translation as a tool in combating cross-border cybercrime. Legea şi Viața, (S), 283-293.

Padyab, M., Padyab, A., Rostami, A., & Ghazinour, M. (2024). Cybercrime in Nordic countries: a scoping review on demographic, socioeconomic, and technological determinants. SN Social Sciences, 4(11), 205.

Rao, N. S., Sekharaiah, C., & Rao, A. (2018). An approach to distinguish the conditions of flash crowd versus DDoS attacks and to remedy a cyber crime. Technology, 9(2), 110-123.

Reitano, T., Oerting, T., & Hunter, M. (2015). Innovations in international cooperation to counter cybercrime: The joint cybercrime action taskforce. The European Review of Organised Crime, 2(2), 142-154.

Schreuders, C. (2019). Understanding cybercrime victimisation: modelling the local area variations in routinely collected cybercrime police data using latent class analysis. International Journal of Cyber Criminology, 13(2), 493-510.

Saud, C. P. (2025). Cyber Crime in Nepal: An Analysis of Case Status and Trends.

Ünver, G. N. (2023). Comparison of Cyber Security Policies of Türkiye and England. Cyberpolitik Journal, 8(16), 49-84.

Taşçı, U., & Can, A. (2015). Türkiye'de Polisin siber suçlarla mücadele politikası: 1997-2014. Fırat Üniversitesi Sosyal Bilimler Dergisi, 25(2), 229-248.

Turkish Penal Code No. 5237, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5.

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

Weulen Kranenbarg, M., Ruiter, S., van Gelder, J. L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. Journal of developmental and life-course criminology, 4(3), 343–364. https://doi.org/10.1007/s40865-018-0087-8