2022

1-2.

CRIMINAL GEOGRAPHICAL JOURNAL

Number 1-2 Volume IV. November 2022 ISSN 2676-9778

Hungarian Association of Police Science – International Criminal Geographical Association

CGJ

CRIMINAL GEOGRAPHICAL JOURNAL

ACADEMIC AND APPLIED RESEARC IN CRIMINAL GEOGRAPHY SCIENCE

VOLUME IV. / NUMBER 1-2 / November 2022

Academic and applied research in criminal geography science.
CGR is a peer-reviewed international scientific journal.
Published four times a year.

All correspondence should be addressed to chair of the editorial board
criminalgeography@gmail.com
Vol. IV. 2022/1-2.
Designed by Antal Forró

CONTENTS

LECTORI SALUTEM!

Dear Readers,

It is no exaggeration to say that domestic and international criminal geography life has significantly "spin up" in the last few years, and more and more quality studies are being published.

The International Criminal Geographical Association was founded. The Association announced a number of tenders, for which applications were received from several countries. Several tenders are currently underway.

We are happy to state that the fourth year of our journal is being published. The editorial board is determined to make the Criminal Geographical Journal a noted and qualified journal at the international level, which is why it considers it important to publish quality articles. For this purpose, the received studies are first reviewed by the editor-in-chief and the chairman of the editorial board, and if necessary, they are rejected. Starting in 2022, we also introduced double-blind proofreading, which promotes the publication of quality articles even more. The editorial board pays particular attention to the use of correct, stylistically and grammatically impeccable professional language, therefore due to the linguist members of the editorial board, the journal also employs two reader editors.

If you have any comments or suggestions regarding the journal, please write them to the editorial board.

I wish you a pleasant time for reading the journal!

Szabolcs Mátyás
Chair of the editorial board

Authors of this issue

Avramov, S. Arseniy Master of law, Synergy University (Moscow, Russia)

Ivan, Dominik Ph.D. student, University of Public Service (Budapest, Hungary)

Kobets, N. Peter Ph.D. chief researcher, All-Russian Scientific-research Institute of the Russian Ministry of Internal Affairs (Moscow, Russia)

Krasnova, Aleksandrovna Kristina Ph.D. associate professor, the North Western branch of the Russian State University of Justice, Russia (Saint Petersburg, Russia)

Volkova A. Maria associate professor, Synergy University (Moscow, Russia)

Zhao, Chunyang Ph.D. criminal law major student, Beijing Normal University (Beijing, China)

Lectors of this issue

Tibor Kiss Ph.D. assistant professor (University of Public Service, Hungary)

Máté Sivadó Ph.D. assistant professor (University of Public Service, Hungary)

Miklós Tihanyi Ph.D. associate professor (University of Public Service, Hungary)

Mihály Tömöri Ph.D. associate professor (University of Nyregyháza, Hungary)

Vince Vári Ph.D. associate professor (University of Public Service, Hungary)

Gabriella Simon Ürmösné Ph.D. associate professor (University of Public Service, Hungary)

Avramov S. Arseniy Master of law

Synergy University

arseniyavramov@gmail.com

Volkova A. Maria Ph.D. associate professor

Synergy University

mvolkova2013@bk.ru

CYBER ATTACKS ACROSS THE WORLD, INVESTIGATING AND DEALING VS, LEGAL AND TECHNOLOGICAL CHALLENGES

Abstract

The twenty first century is often called the century or even the era of technology, where people meet all kinds of technology in every minute on a daily basis. It starts from a usual worker's smartphone and ends up in larger scale, where some massive companies' software is simply doing its job and yet can meet a not very simple issue – called cyber attack. Cyber attacks have been existing for some years now, but just like technology, they grow and evolve into something bigger, as nowadays they are usually not just a "little hack", as they became big on a national and international levels and they are exactly like that this article will investigate.

Keywords: cyber attack, security, internet, modern situation, cyber crime

1. Introduction

Cyber attacks can affect the information space in which the resources of a physical device are concentrated, it usually requires verification of data carriers, specifically designed for their storage, processing and transmission of the user's personal information (Z Zhesterov, P.V. 'From visible past to an invisible presence: new criminological reality after planetary cyber attack 12/05/17 WannaCry', East European Review, 2018, volume 9, issue 2, pp. 57). The most common kinds of cyber attacks include: DDoS attacks, which are distributed denial of service attacks that are implemented by using several compromised computer systems as sources of attack traffic, they flood systems with a large number of requests, resulting in reduced throughput and systems becoming overloaded and unavailable, bots, that are software robots who mimic or replace human behaviour and perform simple tasks at a speed that exceeds user activity, as well as fishing and brute force, where attackers use apps and scripts as “brute-force tools” that try multiple password combinations to bypass authentication processes. The main targets of cyber attacks are credit and financial sector, public authorities, defence industry and space, science and education and others, where the obvious goals are to either steal information and money or to make the processes work much worse than at the base level. It is very tough to fight against cyber attacks, and it is indeed extremely hard to actually find those “attackers” in real life, since they do everything in their power to secure their “irl” (*in real life*) location (Kobets, P.N. – Krasnova, K.A. Criminal-legal measures to ensure cyber security in the conditions of exponent growth of cyber-crime. In the collection: Ensuring public safety and combating crime: tasks, problems and prospects. Materials of the All-Russian Scientific and Practical Conference in 2 volumes. Krasnodar, 2017, p.207). By knowing all of those information some questions appear: How do governments fight against it? How do countries classify cyber attacks from the perspective of legislation?

2. Methods around the world and the legislations of fighting against cyber crimes

Let us try to figure out the answers to those questions in various countries.

In the U.S.A. for instance, on 14th February 2003 there was a publication of the "National Cyber Security Strategy, which became part of the "National Strategy for the Physical Protection of Critical Infrastructure and Key Assets" (Kovaleva T.K.Critical Infrastructure in the US // National Security innovation and investment. 2019. P.81). The American authorities recognized that the country's infrastructure completely depended on information systems and networks that were vulnerable to external cyber attacks. The main goal of the strategy was the creation of a unified national system for responding to such attacks.

In May 2011, the "International Strategy for Action in Cyberspace" (https://medialaw.asia/node/9003) was published in which it announced its readiness to use military means to neutralize threats in the information space. In July, the Pentagon's own cyberspace strategy became known (The Computer Fraud and Abuse Act (USA-CFAA), 18 U.S.C. 1030.). By using legal steps, the US has put up sanctions for cybercrime that include monetary fines and imprisonment. The punishment depends on many factors: the severity of the crime committed, the amount of economic damage caused by the act, the defendant's criminal past, and many others. Currently, the US Congress is considering a new law on cybersecurity, which provides tougher penalties for cybercrimes and the actual equalization of the definition of their public danger with real crimes.

In February 2011, the *German* government adopted the "Cyberspace Security Strategy", which sets goals for increasing the cybersecurity of government structures, the economy and private users (https://digital.report/kibergotovnost-germanii-2-0-natsionalnaya-strategiya/). In the German strategy, just like in the American one, the secret part remains unknown, apparently concerning the system of countermeasures against information attacks. Considering the legal part, the German Penal Code uses a special term – “Daten”, which is defined in article 202 of the German Criminal Code – data that is stored or transmitted electronically, magnetically or in another way that is not directly visually perceptible, i.e. computer data. Illegal receipt by a person of computer data that was not intended for him, which is under special protection against unauthorized access, in order to gain benefits for himself or for a third party shall entail imprisonment for up to three years. Erasing, destroying, rendering unusable, altering data or attempting to do so is punishable by a fine or imprisonment for up to two years. Paragraph "B" of article 303 of the Criminal Code covers such crimes as DNS attacks (computer sabotage) and the creation of malware (Federal Ministry of Justice (Ger), Prof. Dr. Michael Bohlander). The article contains a provision that computer sabotage - interference with the processing of data that is essential to a business, government agencies, or someone else's way of doing business, is a crime. Interference can be carried out by destroying, damaging, rendering unusable, altering a computer system, or interfering with data transmission. These acts are punishable by imprisonment for up to five years.

In the *Netherlands*, “*the intentional use of technical devices for intercepting or recording data flowing through telecommunication systems or connected equipment, for the purpose of deriving benefit for himself or for a third party, if the data is not intended only for him, provides for a fine or imprisonment for up to 1 year*” states Article 139c of the Criminal Code. While *“a person who provides the means to unlawfully intercept and record data flowing through telecommunications or automated systems may be subject to a fine or imprisonment for up to 6 months”* (Article 139d) (Die Verfassung des Königreichs der Niederlande, 2018). In 1993, the Netherlands adopted the Law on Computer Crimes, supplementing the Dutch Criminal Code with new compositions: unauthorized access to computer networks; unauthorized copying of data; computer sabotage; the spread of viruses; computer espionage. Additions and clarifications were made to a number of articles of the Dutch Criminal Code that provide for liability for committing traditional crimes (extortion, fraud, forgery, etc.), which allows using these elements of crime, in appropriate cases, to combat computer crimes.

Similar documents have been adopted in Great Britain and India.

In the Russian Federation, the situation with qualified personnel in the field of cybersecurity in Russia is rather the same as in the United States, but has more acute character. Therefore, it is proposed to introduce and develop special courses on the investigation of such crimes at law faculties in the field of telecommunication technologies, cybersecurity and information security. Russian professors think that it is necessary that every graduate of the Faculty of Law possess not only legal knowledge, but also proper digital literacy (Zhurmukhambetova 2021). It is necessary to improve the digital literacy of the population in order to avoid the emergence of new cybercrime, to develop this literacy among law enforcement officers in order to prevent cybercrime. Without a proper regulatory framework, there can be no effective fight against cybercrime by law enforcement agencies. The fact that the state is pursuing an active policy is not denied to solve the above problems. However, at the moment the intensity of the development of this issue is still insufficient. According to the Ministry of Internal Affairs, over the period of 2020, the number of crimes committed using information and communication technologies has increased by 94.6%, grave and especially grave – by 129.7%. It should be noted that payment cards for criminal purposes were actually used 6 times more often than in 2019, when there was no danger of a pandemic, and mobile communications were used for the same purposes 2 times more often and more. According to statistics on cybercrime, for example, the Bryansk prosecutor's office for 2019 indicated that 1372 crimes were committed using information and telecommunication technologies, which is almost 2 times more than in the same period in the past (Ministry of Internal Affairs of the Russian Federation^ Brief description of the state of crime in Russia, 2020).

3. The COVID-19 and 2022 situations' impact on cybercrimes

The COVID-19 pandemic has made significant changes in the life of all (Reshnyak, M.G. – Botasheva, Z.H. Addressing some of the legal challenges posed by the coronavirus infection control system (COVID-19), Gaps in Russian legislation, 2021, volume 14, number 4, p269; Krasnova, K.A. – Topilskaya, E.V. Pandemic is not a barrier for student science. In the collection: Cybercrime: risks and threats, materials of the all-Russian student round scientific and practical table with international participation. St. Petersburg, 2021. p. 9). First of all, those changes are associated with various kinds of restrictions, like the cancelling of mass events, compliance with masks and gloves regime and social distancing. Talking about the situation in Russia, due to the fact that a huge number of citizens were ordered to stay at home, the load force on the internet has been very significant. As a result, there have been multiple interruptions in the internet connection for a long time. At the moment on one hand, scammers have become more active and have begun to act even more sophisticated than before the pandemic. Both the internet service providers and the ordinary users were not ready for such global changes in their lives and activities, so the attackers took advantage of this.

Government forces have tried to fight against it, but who was ready for such a powerful shot? It is unacceptable to assume that law enforcement agencies and representatives of state structures did not take any action. On the contrary, they did in fact respond very quickly to any offenses in the area related to information and communication services. Moreover, long before that, in order to implement preventive measures, Russia during the 74th session of the United Nations proposed, under the auspices of the UN, agreed on and approved a convention on combating crimes in the field of the use of information and communication technologies, which would allow for effective international cooperation in the field of combating cybercrime. Analysing this situation, we can conclude that in addition to strengthening legal regulation, the main method of combating cybercrime is to increase the legal culture of the population, including educating citizens in the field of computer literacy. The fact is that one of the most frequently committed crimes on the Internet is extortion, including personal data. And if citizens are warned about the danger of providing their data and other actions by which fraudsters can deceive them, then the number of crimes in the corresponding category will significantly decrease. Unfortunately, with all the varieties of legal instruments, available to public authorities, at the moment there are still some difficulties in their application to combat the activities of criminal elements in the internet websites. At the same time, the leadership of the authorized bodies of state power is taking a lot of efforts to optimize the organizational structure and increase the efficiency of their work, which is a prerequisite for systematic and efficient activities to prevent and combat cybercrime. In the light of these arguments, it is impossible not to mention Mikhail Mishustin reforms of the state apparatus. As part of its implementation, the staff of civil servants in central and territorial government bodies will be optimized, which, as the Head of the Government Staff Dmitry Grigorenko notes, will allow the public administration system to become “more clear, logical, up-to-date” (Countering the use of information and communication technologies for criminal purposes // United Nations Office on Drugs and Crime, 2019).

Russian newspaper “Izvestie” tells its readers about many cyber crimes happening on a daily basis, starting from February of 2022. Apart from the propaganda from both sides, it is very clear that “special military operation” happens not only at the battlefield of both ground and skies, but on cyber level as well. It is almost impossible to find the truth, therefore it is understandable that several acts are happening big and small providing its impact. According to “Izvestie” Ukrainian hackers have launched a large-scale attack on the “Mir” payment system and its operator, the National Payment Card System (NSPK). This was reported on September 23 by the Kommersant newspaper, citing its source in the field of information security. “The goal of the attack is to overload the system and cause a failure in card servicing. Since the beginning of the military operation in Ukraine, the entire Russian IT infrastructure has been subjected to massive hacker attacks. Until now, there has been no information about vulnerabilities in the Mir system”, the newspaper says. Cyber activists generate traffic to systems using browsers or primitive DDoS tools to disrupt payments and terminals. The source of the newspaper has also noted that in the current situation, the attackers may be able to succeed in the attacks. In this case, it is possible to disable cashless payments for several hours. The Ministry of Digital Development reported that this issue is within the competence of the National Coordination Centre for Computer Incidents, as well as within the competence of the Central Bank. However, at the moment, representatives of the Central Bank did not answer the newspaper, and the NSPK declined to comment. Earlier that day, Sergei Solovykh, head of the department for working with wealthy clients at Fontvielle Investment Company, told Izvestia that the topic of using “Mir” payment cards had become speculative abroad, since it had more political overtones than economic ones. On the same day, the United States was threatening to impose sanctions on those Turkish credit organizations that would continue to work with the Mir payment system. According to the Turkish media, the banks most often used by “Mir” card holders in Turkey continue to work with them. Earlier in September, some hotels in Turkey stopped accepting payments through Mir due to the threat of sanctions. One of the major chains confirmed that since September 15, it was recommended in the country not to accept cards, but each hotel can decide for itself whether to follow these recommendations or not. This is just a fresh example of many cyber crimes happening right now. From the scientific point of view, it is hard to find the right thing to do, especially from the legal perspective.

Conclusion

In such circumstances and conditions, it is rather necessary that the legal regulation of cybersecurity is carried out not only at the regional level. Safety efficiency can only be achieved through the unification of international and foreign norms, which will grant a better result. At the same time, it would be right to carry out more detailed regulations of all areas of public relations, such as: property, advertising, information, financial and other areas.

References

Dolgopolov, A. ‘Impact of the COVID-19 pandemic on cybercrime’. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.13-16.

Kobets, P.N. – Krasnova, K.A. ‘Criminal-legal measures to ensure cyber security in the conditions of exponent growth of cyber-crime’. In Ensuring public safety and combating crime: tasks, problems and prospects. Materials of the All-Russian scientific and practical conference in 2 volumes. Krasnodar, 2017, pp. 205-208.

Kovaleva, T.K. ‘Critical Infrastructure in the US’. National Security innovation and investment, 2019, pp. 78-85.

Krasnova, K.A. – Topilskaya, E.V. ‘Pandemic is not a barrier for student science’. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. St. Petersburg, 2021, pp. 8-10.

Reshnyak, M.G. – Botasheva, Z.H. ‘Addressing some of the legal challenges posed by the coronavirus infection control system (COVID-19)’, Gaps in Russian legislation, 2021, volume 14, number 4, pp. 266-270.

Prashant, M. Classification of Cyber Crimes, LCI, 2020.

Synkov, V.V. ’Cybercrime is the challenge of the 21st century’. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.208-212**.**

Tamrazov, G.O. ‘Fraud in the field of computer information: qualification problems’. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp. 63-68.

Voinov, N.E. ‘Cybercrime in the Russian Federation: current state and current problems’.
In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.142-147.

Zhesterov, P.V. ’From visible pasts to an invisible presence: new criminological reality after planetary cyber attack 12/05/17 WannaCry’, East European Review, 2018, volume 9, issue 2, pp. 55-67.

Zhurmukhambetova, S. ‘Cybersecurity Trends in the fight against cybercrime’. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.167-172.

Dominik Iván Ph.D. student

University of Public Service Doctoral School of Police Sciences and Law Enforcement

ivan.dominik1996@gmail.com

THE NEW POSSIBILITIES OF GEOGRAPHIC INFORMATION SYSTEMS DURING CRIMINAL INVESTIGATION

Abstract

The use of visual aids (maps) to determine criminal activity is not a new concept in the world of law enforcement. In the beginning, the common practice meant putting pins into paper maps displayed on the walls, then entering the data into a spreadsheet. Currently, the number of different software companies providing Geographic Information System (GIS) services are growing each year. This increase is accompanied by the development of the data entry process, the maintenance costs of the system, and the increase in the number of users using the system. When we look at the challenges that law enforcement agencies face daily, the implementation of the GIS can provide another strategic tool for the police force against crime. This study aims to present and analyze the methods offered by GIS and their applications. Furthermore, the aspects of GIS related to crime analysis will be examined, and its concrete application in practice will be presented.

Keywords: geographic information system, geography of crime, predictive policing, geoinformatics, crime

1. Introduction

Geographic profiling basically requires the use of GIS, which is an automated system for recording, storing, retrieving, analyzing, and displaying spatial data. (Márkus 2020)

The data describe both the location and the attributes of spatial features. For example, describing a road requires reference to its location (i.e., where it is) and its attributes (e.g., length, name, speed limit, and direction). GIS enables the user to manage road information and many other geospatial data, thus distinguishes them from corporate management and other IT systems dealing with non-spatial data. Commercial or open-source GIS software includes programs and applications that a computer can run for data management, data analysis, data visualization, and other tasks. In a GIS, additional applications can be used for special data analyses. (Steele 2018, Chang 2016).

GIS is a complex database system that contains information about the coordinates of the location of spatial objects and allows various procedures to be performed. In addition, GIS is a tool for micro-, meso-, and macro-scale geographic research, which leads to visualization, but also to the solution of spatial planning, management, and modeling problems (Bujdosó 2009).

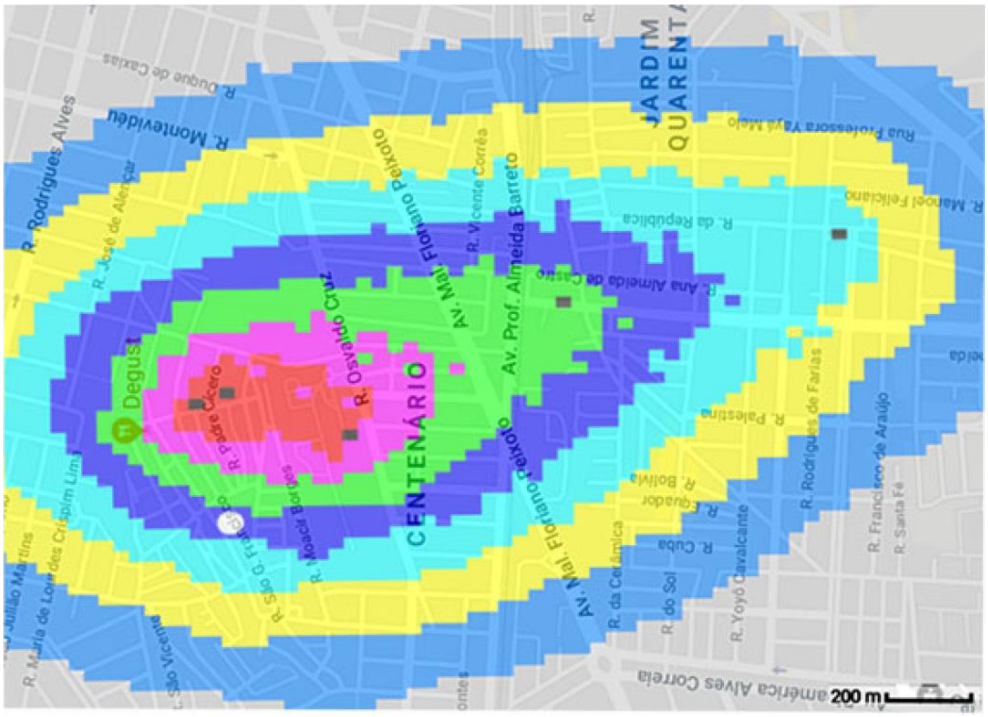
It should be added that the ways and methods of processing data on geographic objects, as well as the goals of the systems, can differ significantly. The created model of the geographic environment included in the database is the starting point for the analysis of the objects, after determining their characteristics, location, class, quantitative and qualitative characteristics but also the relationships among them. GIS provides an insight into crime prevention efforts by predicting hot spots. These hot spots are key to taking a proactive stance to stop crimes before they happen. The collected data are useful in identifying trends (Goniewicz 2021).

2. Geographic Information Systems in Law Enforcement

2.1. The Dragnet Geographic Information System

Currently, there are four popular GIS systems used for profiling (Dragnet, Rigel, CrimeStat, Predator), which are used by law enforcement agencies in many countries. These systems can be considered as useful estimation tools for the probable determination of crime areas (Willmott et al. 2021).

For example, Dragnet is a GIS that was developed specifically as an operational decision support tool in response to the need to provide investigators with greater opportunities to identify and apprehend serial offenders. Based on the principle of minimum effort, Dragnet uses a negative exponential algorithm based on the distance decreasing function. If crime location information within a given crime sequence has been once calculated and entered into the GIS, Dragnet creates mathematically based models of crime scenes, allowing potential search regions to be determined (Figure 1) (Steele 2018).



1. Figure: Dragnet in practice

Source: Willmott et al. 2021

The software is able to present the results of this mathematical algorithm projected onto the identified crime scenes even more significant from the detective's point of view, with the help of such an empirically generated model (Figure 1). It is worth noting to Dragnet, that there are several alternative geographic profiling systems, such as the Rigel Criminal geographic system and the Predator system, which are based on similar mathematical algorithmic principles as Dragnet (Willmott et al. 2021). As with any predictive modeling technology or system, results depend on the accuracy and relevance of the data. As the nature and context of crime and forensics continue to evolve and change, so must the empirical evidence supporting geographic profiles from these systems to ensure accuracy and effectiveness. As the probability regions move outward through the green, purple, blue, and yellow regions, the likelihood that the offender lives in these areas decreases. It is therefore necessary to consider the factors that can influence the offender's lifestyle or activities, regardless of the expected value (Lino et al 2018). Currently, the study area of systems that are based on geographic profiling are all based on data found in the tangible world, so the geographic profiling of perpetrators of crimes committed in cyberspace is more difficult to solve.

2.2. The hardship of Geographic Information Systems

The construction of a GIS system is a complex task, in addition to the cost of the hardware, there is also the cost of training. Frequent updating of the database can lead to errors in the results. Managing growing data sets is a comprehensive challenge for the GIS system. It was mentioned earlier that the accuracy of the map depends on the quality of the input data. As a result, the quality of the collected data directly affects the accuracy of the final system. Geographical errors also affect the final results, since the GIS system handles large-scale data. Not to mention that non-spatial data related to location can also be inaccurate. Inaccuracies can be caused by a variety of errors. The accuracy of non-spatial data can also show large differences. The user group is not limited to authorized persons. Therefore, the use of data displayed from the GIS system is at risk. Incorrect interpretation can lead to the failure of the implementation of the result, and errors may occur at the start, so additional efforts may be needed for the full implementation of the GIS system (Goniewicz 2021).

3. The connection between GIS and crime analysis

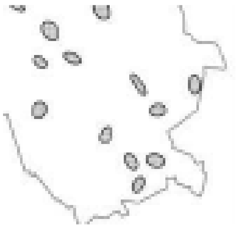
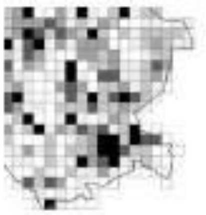
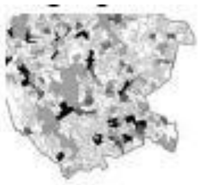
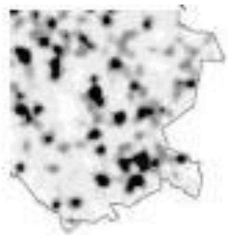
Geospatial information plays a fundamental role in mapping and analyzing crime. The ability to connect and process information, and to display it spatially and visually, allows law enforcement agencies to be faster and more successful. A GIS transforms the physical elements of the real world, such as roads, rivers, mountains, buildings, into forms that can be visualized and analyzed. GIS uses two types of models, vector and raster. The vector deals with discrete objects, and the raster deals with continuous objects (Zahra 2018).

Computer crime maps were created for the first time in the 1960s and 1970s. In the 1990s, Geographic Information Systems became widely available on the market, and in the late 1990s, criminologists and police units began GIS analysis. Spatial analysis of crime using a geographic system and spatial statistics is now widely used to analyze the mass occurrence of crimes to reveal the unequal distribution of crime risks and the spatial interactions between crimes. In 1978, Robert A. Baron and his colleagues found a correlation between violent crime and temperature. A series of experiments were conducted on the effects of high temperatures on aggressive behavior. These researches suggest that there is a connection between aggression and high temperatures, i.e. aggression increases under the influence of heat. The use of modern techniques, machines and computers presents new challenges to the police in every country. With the help of the GIS module, the police and investigative authorities can assess the geographical location of crimes and predict the place where the crime was committed.

4. Hotspot analysis

The concept of hotspot is used by science in two areas. In geological science, the meaning of a hot spot is nothing more than an area on the tectonic plate where magma from the depths of the mantle pierces to the surface. Criminology, on the other hand, uses the term hotspot for small areas where crime is more frequent than in neighboring areas (Mátyás 2020). The hotspot technique is basically used to identify areas with high crime rates. The analysis tool identifies spatial groups of statistically significant high or low value attributes. Hotspot mapping is based on the hypothesis that high crime region points will appear as groups in a spatial distribution. Hotspots provide crime analysts with a graphical representation of crime-related problems. Detecting the location and cause of crime can improve the fight against crime. In the near future, hot spot mapping and geospatial information may support law enforcement activities. Geospatial informatics and crime analysis can show a comprehensive connection between the crime, the victim and the perpetrators (Zahra 2018).

Commonly used types of hotspot analysis are:

Name	Method	Advantages
Spatial Ellipse 	It uses spatial and temporal analysis of crime to identify hotspot areas and fits an ellipse to each hotspot.	The size and location of each hot spot becomes easily visible. There is no need to rely on defined geographical boundaries.
Grid Based Mapping 	By drawing uniform grids over a survey area, it shades the area within each grid square according to crime data.	Grid squares of the same size mean that hotspot areas can be easily identified without risk of misinterpretation.
Geographic Area Based Mapping 	Hotspots are based on specific administrative or political areas. Each is thematically mapped based on the number of crimes that occur in them.	It reflects the areas and boundaries used by organizations. The prepared thematic maps are logical and easy to understand.
Density Estimation 	Creates a spatially distributed plot by aggregating point data within a defined search radius.	It represents the spatial distribution of criminal events. There is no need to rely on specific geographical boundaries.

The analysis of hotspots has become the most widespread application method used by GIS with regard to criminal data, which can be used in a variety of ways these days. For example, crime hotspot maps can be presented during strategic or tactical planning meetings so that decision makers know where to deploy resources such as patrols. Furthermore, police analysts are able to use hotspot analysis when creating a profile of a given crime problem in order to better understand the criminological background that causes it. The better a problem is understood, the better prepared decision makers are to implement successful crime prevention interventions. In addition to the previously mentioned applied forms of criminal analysis, GIS data can be used in various ways in criminological and criminal justice research (Zahra 2018).

4.1. The importance of geographical factors

Geographical knowledge is also necessary for an eligible GIS analysis. The first standpoint is how to represent the data on a two-dimensional map. This involves the use of a projection system, which is a method of projecting the spherical surface of the earth onto a flat plane. Distortions may occur if the projection is not done correctly. Furthermore, in countries with large territories, such distortions can be large. It is not possible to map all data in its original format; sometimes geocoding is required. Geocoding is the process of finding related geographic coordinates from other geographic data, such as street addresses or zip codes. Data useful for criminological and criminal justice work are often collected at the level of administrative areas. Thematic figures, which are shaded in polygonal shapes according to state, county or administrative boundaries, are generally more popular because it is easier for the user to find the connection points.

5. Summary

Computerization and the development of geographic information systems enabled the digital representation of space for the interactive analysis of multiple data in the form of models or simulations. On the other hand, the computerization of the environment has become a new source of danger for the state, society and the individuals themselves, especially in the area of personal data protection. However, technical and technological development seems indispensable nowadays, due to the many possibilities it provides, for example in the field of geographic information. Even today, the GIS system enables the collection, storage, processing, and display of spatial data, which adds a new dimension to public administration activities. For example, in crisis management, the preparedness of the services, inspections, and guards in the event of a disaster is now incomparable compared to previous years. Unfortunately, a GIS system requires appropriate hardware, software, spatial databases, and appropriate procedures for processing and sharing information. This requires not only expensive modernization, but also the maintenance of professional human resources.

The most obvious limitation to the reliability and accuracy of the geographic profiles produced is based on the underlying assumptions that, if inaccurate, can distort or change the likely location of the featured offender and the recommended investigative strategies.

Another limitation of systems that support geographic profiling, such as Dragnet, is that they do not contain information known about the actions of criminals during the commission of their crimes. Computer systems for geographic profiling are generally not able to directly integrate with important information about large numbers of offenders stored in police databases. The combination of such information would undoubtedly offer greater investigative value than analysis of crime geography alone. Even though geographic information systems that also use geographic profiling make it possible to significantly narrow the range of suspects or to predict the crime itself, investigators must keep in mind the limitations of the method. Any geographic profile should be treated as a possible direction of investigation, while keeping an open eye on other avenues of investigation. Notably, offenders may also be commuter criminals or, because of factors such as limited data sharing between different police forces or agencies, the additional information may result in a slightly different geographic profile.

References

Bujdosó, Zoltán (2009): A megyehatár hatása a városok vonzáskörzetére Hajdú-Bihar megye példáján**,** Debreceni Egyetemi Kiadó, Debrecen, 211 p.

Goniewicz, Krzysztof (2021): Geographic information system technology: Review of the challenges for its establishment as a major asset for disaster and emergency management in Poland. Disaster medicine and public health preparedness

Kang-Tsung, Chang (2016): Geographic information system. International Encyclopedia of Geography: People, the Earth, Environment and Technology: People, the Earth, Environment and Technology

Lino, D. – Calado, B. – Belchior, D – Cruz, M. Lobato (2018): Geographical offender profiling: Dragnet's applicability on a Brazilian sample. J Investig Psychol Offender Profil

Márkus Béla (2002) (szerk.): Mi a térinformatika? (http://gisfigyelo. geocentrum.hu/ncgia/ncgia_1.html - letöltés ideje: 2015. szeptember 10.)

Mátyás Szabolcs (2020): Az elemző-értékelő munka gyakorlati aspektusai. Ludovika Kiadó, Budapest

Steele, Robert L. (2018) GIS: The Solution for Real-Time Crime Mapping And Crime Predicting in a Police Agency

Willmott, Dominic – Hunt, Daniel – Mojtahedi, Dara (2021): Criminal Geography and Geographical Profiling within Police Investigations – A Brief Introduction Internet Journal of Criminology

Zahra, Syeda Ambreen (2018): Crime Mapping in GIS by Using Hotspot. 2(1)

Peter N. Kobets Ph.D. professor, chief researcher

All-Russian Scientific-research Institute of the Russian Ministry of Internal Affairs

pkobets37@rambler.ru

Kristina A. Krasnova Ph.D. associate professor

The North Western branch of the Federal State Budget-Funded Educational Institution of Higher Education (The Russian State University of Justice)

krasnova.spb.rpa-mu@mail.ru

GEOGRAPHICAL ASPECTS OF TOURISM SECURITY IN RUSSIA. LEGAL AND ORGANIZATIONAL CHALLENGES

Abstract

Tourism plays an increasingly important role in the economy of all countries, including Russia. Guaranteeing the safety of tourists arriving in the country is in the basic interest of every country, as it has a serious economic interest. One way to ensure a high level of tourism security is to create a "tourist police". Russia and several former Soviet states are following this path. The study shows how these special police units were set up in Russia and what their characteristics are. In a country the size of a continent, police forces for the protection and assistance of tourists were established primarily in those destinations that are visited by millions of tourists annually.

Keywords: tourism, security, Russia, law enforcement

1. Introduction

Tourism is a complex system that depends on many factors. Among them, the human one takes the lead; therefore, tourism is one of the vulnerable areas of human activity regarding its security, including against terrorism (Kobets 2020). In 2020 Insurly, a French insurance aggregator, ranked Russia 86th among 180 countries included in the safety rating for tourists with the level of risk classified as “significant”. Insurly assessed a total of 180 countries. The rating allows us to find out the level of risk for travelling to a particular country. The rating includes either data on violence (murders, terrorist attacks) or information on safety for tourists’ health (such as epidemic outbreaks, basic sanitation and air quality) as well as transport safety. The rating was compiled on a 100-point scale. Russia was given the lowest rating in the category of “Violence” (only 17 points out of 100) based on two indicators: intentional killings and acts of terrorism. “Transport security” in Russia was awarded 41 points. The highest score (83 points) was given to health protection. Emergency protection received 74 points out of 100. The other CIS countries were ranked as follows: Belarus (48th place), Azerbaijan (52nd place), Turkmenistan (60th place), Moldova (66th place), Georgia (68th place), Kazakhstan (71st place), Armenia (72nd place), Ukraine (83rd place), Russia (86th place), Tajikistan (93rd place) and Kyrgyzstan (106th place) (https://www.tourismsafety.ru).

Therefore, the safety of tourism at a time of the first 22 years of the 21st century is a prerequisite for the tourism industry development and enables tourist services (Kobets 2018, 22-25.). Nevertheless, so far in the Russian Federation, the relevant federal authority responsible for this area has not been determined, and the regions have quite mysterious and incomprehensible powers (Kobets – Krasnova 2022). While crimes, incidents with and against tourists occur, and until they are sure that they will not be robbed at the hotel, deceived by taxi drivers, blown up and raped, or that in the case of any emergency or fire a person with disabilities will not be left without help and will not die, no infrastructure, advertising and promotion of tour products will help (Tihanyi 2017).

2. The role of tourism security in Russia

The safety of tourism directly depends on the state policy and its measures for protecting tourists. In Russia, the rights and obligations of a tourist that prepares and makes a trip are determined by the federal law on the bases of tourist activity in the Russian Federation. In particular, according to the law, a tourist has the right to be guaranteed the personal safety, safety of his property, unhindered receipt of emergency medical care, as well as to receive reliable information about the rules of entry into the host country and the peculiarities of behaviour in it, such as customs, various rites of the local population, sanitary and epidemiological conditions. Clearly, during the journey, the tourist is obliged to comply with the host country legislation, respect its customs, traditions, religious beliefs and social structure and follow personal safety rules. Information about the threat to tourists’ safety in the host country should come from the national tourist administration and tour operators.

Russia also takes the necessary steps to issue regulatory documents to ensure tourists’ safety. The adopted legislative acts oblige the federal executive authorities to inform tour operators and tourists about the security threats, including through the state media. The Service of the Chief Sanitary Physician of Moscow seeks to prevent quarantine and parasitic infections during tourist trips. Managers of travel agencies must instruct each tourist that travels to countries with life-threatening diseases (such as plague, cholera, yellow fever and malaria) and provide them with a memo and antimalarial drugs.

The safety of tourism and the reduction of travel risks relate to a wide range of challenges, including the creation of a special police service to protect visitors and the local population, checking the safety of tourist accommodation establishments and their licenses and certificates, organizing emergency communication lines, receiving complaints from tourists, protecting monuments, the environment, combating drugs and prostitution.

At the WTO's initiative, the First Global Research and Travel Trade Conference on Security and Risks in Travel and Tourism was held in Österund (Sweden) back in 1995 (https://studwood.ru). The findings of a survey among 73 countries on the safety and protection of travellers, tourists and tourist sites showed that in 71% of the countries the special tourist police or security service guarded tourists' spots and attractions. In more than half of the countries, such a service is part of the state or municipal police; 21% of the countries have a special tourist police service; in half of the countries, this service helps tourists solve their problems, and in 40% of the countries the police inform the relevant consulates and tourists. The tourist police are also mandated to preserve cultural monuments and the environment, combat drugs, provide information to tourists and protect local ethnic groups. However, at that time, only nine countries had laws on tourist police. Tourist police officers in 41% of the countries study foreign languages, and in 26% of the countries are trained in specific tourism disciplines. In 37% of the countries, they maintain regular communication with tourism agencies, firms and ordinary police (https://www.tourismsafety.ru).

The tourist police serve as a powerful argument in assessing the tourist destination's reliability for visiting by foreign tourists. The tourist police mainly exist in countries where the tourism industry is of great importance (Kobets 2017, 9-11). As an ambulance service in medicine, this unit helps foreigners solve problems in a different country. If this fact is a novelty in our country, then for several countries of the Middle East and South-East Asia (Kobets 2019, 22-24) as well as some Member States of the Commonwealth of Independent States (Kobets 2020, 31-32) it is a practice with the concept already formed and experience accumulated. In these countries, the tourist police perform the functions of patrolling active recreation areas. If necessary, it is obliged to assist foreign citizens.

3. Foundation of the Russian tourist police

During a telephone survey, in which 1600 thousand Russians over 18 years old took part, 75% of respondents answering the question of "whether the tourist police in the Russian Federation are more likely needed or not needed" chose the option of "more likely needed" (https://ria.ru).

The decision to create temporary specialized units of the tourist police was announced on April 2, 2018 (https://мвд.рф). The tourist police began to function in Moscow in July 2018. Its creation was initiated by the Ministry of Internal Affairs of the Russian Federation. This unit's duties are to ensure the safe stay of guests of the capital and maintain Moscow's positive image. The tourist police officers' duties include actions to ensure security and provide assistance to tourists and other capital guests. This unit staff speaks foreign languages and has received special training in communicating with foreigners. The tourist police are also tasked to quickly respond to thefts and robberies that involve tourists as victims, to help foreign citizens caught up in criminal situations (https://fb.ru).

Russian regions assess differently the need to introduce such units and see the possible tourist police's functions in various ways. Most tourist industry representatives say that the special tourist police are essential for mass tourism destinations, for example, St. Petersburg and Crimea, which are visited every year by millions of Russians and foreigners. In Crimea, the idea of creating the tourist police finds local support. Places of mass recreation often require the constant presence of people in uniform, because it happens that people walk with children while someone drinks, swears, begs, does illegal business or actively litters the spot. Such violations spoil the whole picture. The Republic of Dagestan, where the number of tourists is increasing, also supports creating the tourist police. In Veliky Novgorod, the idea is considered especially timely with the number of foreign tourists being on the rise. Some regions, including those included in traditional tourist routes (for example, the Golden Ring of Russia), believe that the tourist police's creation is still irrelevant because there are other problems (https://travel.rambler.ru).

Another issue that requires discussion is the integration of the tourism industry into the digital economy. Concerning the safety of tourism, the introduction of innovative practice-oriented technologies is essential. In particular, machine vision technologies, or so-called facial biometrics, can identify a person in transport security systems during operational activities (Morozov – Morozova, 139.).

4. Conclusion

Despite some restrictions on inbound tourism caused by the COVID-19 pandemic (air traffic takes place with only 15 countries), the improvement of tourism security is a promising area for both lawmakers and the police. The idea of the tourist police's creation is generally correct, but it is necessary to clarify such a service's functions, explain its tasks and convey this information to tour operators working with foreign tourists. For a foreign tourist, the presence of an approachable policeman who can speak a foreign language and explain something means additional comfort. With the rapid development of domestic tourism, one should predict the demand for such a service to ensure the Russians' safe rest. As a consequence, the appearance of the tourist police in Russian cities can only be welcomed.

References

Kobets, P.N. (2020): ‘Sovershenstvovanie antiterroristicheskikh mer bezopasnosti na ob"ektakh transporta’, Nauchnyi portal MVD Rossii, (1):49, pp. 35–45.

86th place: that is how the French insurance aggregator ranked Russia in terms of tourists’ safety. (https://www.tourismsafety.ru/news_one_3500.html – 14. 1. 2021)

Kobets, P.N. (2018): ‘Sovremennye pravovye podkhody k regulirovaniyu bezopasnosti v sfere turizma v Rossiiskoi Federatsii’, Turizm: pravo i ekonomika, 2018/3, pp. 22–25.

First Global Research and Travel Trade Conference on Security and Risks in Travel and Tourism (Östersund) (https://studwood.ru/1144781/turizm/estersundskaya_konferentsiya_bezopasnosti_turizma_umensheniyu_riskov_puteshestviyah – 14.1.2021).

Tourism Safety: International Practice (https://www.tourismsafety.ru/news_one_2415_44.html – 14.12021)

Kobets, P.N. (2017): ‘O probleme bezopasnosti i zashchity v turizme v usloviyakh serediny vtorogo desyatiletiya XXI stoletiya’, Turizm: pravo i ekonomika, 2017/1, pp. 9–11.

Kobets, P.N. (2019): ‘Osobennosti obespecheniya bezopasnosti turizma podrazdeleniyami turisticheskoi politsii ryada gosudarstv Blizhnego Vostoka i Yugo-Vostochnoi Azii’, Turizm: pravo i ekonomika, 2019/1, pp. 22–24.

Kobets, P.N. (2020): ‘Stanovlenie podrazdelenii turisticheskoi politsii (militsii) v gosudarstvakh – uchastnikakh Sodruzhestva nezavisimykh Gosudarstv’, Turizm: pravo i ekonomika, 2020/1, pp. 30–32.

Kobets, P.N. – Krasnova, K.A. (2022): A turizmusbiztonság földrajzi vetületei Oroszországban. Jogi és szervezeti kihívások, *Bűnözésföldrajzi közlemények*, (3):1-2, pp. 17-22.

Russians believe that the country needs the tourist police (https://ria.ru/20181109/1532418813.html – 14.1.2021)

Vladimir Kolokoltsev decided to create tourist police units in the cities where the World Cup matches will be held (https://мвд.рф/news/item/12682997- 14.1.2021)

What is a tourist police? Tourist police in Moscow (https://fb.ru/article/189758/chto-takoe-turisticheskaya-politsiya-turisticheskaya-politsiya-v-moskve - 14.1.2021)

Regions appreciated the idea of introducing tourist police (https://travel.rambler.ru/news/37458700/?utm_content=rtravel&utm_medium=read_more&utm_source=copylink – 14.1.2021)

Morozov, M.A. – Morozova, N.S. (2018): ‘Novaya paradigma razvitiya turizma i industrii gostepriimstva v usloviyakh tsifrovoi ekonomiki’, Vestnik Rossiiskogo novogo universiteta. seriya: Chelovek i obshchestvo, 2018/1, pp. 135–141

Tihanyi Miklós (2017): ’The Tools of the Police for the Improvement of the Citizens' Subjective Sense of Security in Hungary’ In: Hadtudományi Szemle, (10):2, pp. 284-294

Zhao Chunyang Ph.D. criminal law major, student

Beijing Normal University

chunyang.zhao0314@foxmail.com

AN EMPIRICAL STUDY OF GEOGRAPHICAL DIFFERENCES IN CRIMES OF AIDING INFORMATION NETWORK CRIMINAL ACTIVITIES — SAMPLE OF 1,081 JUDGMENTS

Abstract

The crime of aiding information network criminal activities is a new crime added by the "Criminal Law Amendment (IX)", which shows significant geographical differences in practice. In the Chinalawinfo database of Peking University, a total of 1,081 judgments and 2,131 defendants were obtained by searching with this crime as the keyword. Taking the seven regions of North China, Northeast China, East China, Central China, South China, Southwest China, and Northwest China as the empirical research, it is concluded that this crime mainly presents the characteristics of progressively severe crime situation from North to South and progressively diverse types of criminal acts. There is a problem that the sentencing around the crime situation does not match the problem, and put forward four suggestions: the three northern regions should moderately relax the application of probation for this crime; Central China should focus on combating the "two cards" type of help; East, Southwest and South China should focus on the prevention of technical support type of help, combat; Southwest China should moderately increase the punishment for this crime.

Keywords: Crime of aiding information network criminal activities, Network complicity, Geographical differences, Empirical study

Introduction

According to the "Characteristics and Trends of Cybercrime in Judicial Data Special Report" released by the Supreme People's Court on November 19, 2019, the volume of cybercrime cases has been increasing year by year in recent years, and they are mostly found in the southeastern coastal areas, followed by the eastern non-coastal areas and the northeastern coastal areas and central areas, with significant geographical differences[1]. Among the increasingly frequent cybercrimes, the crime of helping information network criminal activities, as a new crime added

[1] See China Judicial Big Data Service network (http://data.court.gov.cn)

by the Criminal Law Amendment (IX) enacted in 2015, belongs to the predicate crimes of many cybercrimes in terms of crime positioning. The three main forms of "technical support", "advertising promotion" and "payment settlement" regulated by its elements are all necessary links of network fraud, online gambling, and other mainstream network crimes.

Therefore, an analysis of the characteristics of the geographical differences of the crime of aiding information network criminal activities can demonstrate the overall geographical differences of the current Chinese cybercrime to a degree, and provide a practical basis for each region to formulate the corresponding criminal policy in response to the specific crime situation in its region.

I. Research Methodology

1.1. Sample Selection

The sample selected for this paper was taken from the Peking University Chinalawinfo Database (http://www.lawinfochina.com/search/SearchCase.aspx). The reason why the Peking University Chinalawinfo Database is chosen as the source of the research object instead of the official Magistrate's Document website is mainly because the former has certain advantages in terms of the number of cases. Moreover, its cases can include the cases provided by the Magistrate Document Network completely. At the same time, to maximize the sample size and improve the credibility of the research results, all the judgments obtained from Peking University Chinalawinfo Database were selected in this paper, and no sampling method was used.

A search using the keyword "Crime of aiding information network criminal activities" showed that as of January 4, 2021, the database contained a total of 1,124 verdicts. After eliminating the duplicate content, a total of 1081 judgments were obtained, with a total of 2131 defendants, including units and natural persons. The reason for counting the number of defendants is that, in terms of the definition of the specific sample, there are a large number of accomplices in the "crime of aiding information network criminal activities", the subject of the study. At the same time, compared with the statistical method of using cases or judgments as samples, the statistical method of using specific defendants as samples can more clearly show the application of this crime in practice, and also help to analyze the regional differences in the specific conviction and sentence of this crime.

1.2. Variable Design

After determining the statistical criteria for the sample of defendants, the paper further designed the variables. Specifically, this paper designed the research variables in the following dimensions:

Firstly, Basic information, including a total of seven variables: case title, trial level, time, geographic area, name of the perpetrator, nature of the perpetrator, and the perpetrator's complicity status. ①Case name refers to the name of the case explicitly stated in the judgment, which is used to identify the specific case so that it can be easily compared with the perpetrator as a sample in the subsequent study, and to facilitate finding the specific case and checking the accuracy of data entry. ②Trial level refers to whether the case is a criminal case of first or second instance, and is a record of the specific trial procedure to which the actor belongs. ③Time refers to the specific time of the verdict, in years. ④Geography refers to the specific geographical area where the perpetrator was sentenced. For the sake of statistics, this paper takes seven geographical regions, namely, North China, Northeast China, East China, Central China, South China, Southwest China, and Northwest China, instead of all provincial administrative regions, as the statistical standard for the geographical area.（The regions are referred to in following as N, NE, E, C, S, SW, NW. ⑤The name of the actor is the name or designation of the perpetrator, which is similar to the name of the case. The main purpose of the statistics of this variable is to facilitate subsequent data processing.

Secondly, the variables related to the circumstances of the crime include seven variables: the number of objects to help, and the amount of payment and settlement, the number of funds provided, the amount of illegal income, the specific sentencing circumstances, the type of positive offense behavior and the type of helping behavior. Among them, the number of objects in order to help, the amount of payment and settlement, the number of funds provided, and the amount of illegal income are the "Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Network and Aiding Criminal Information Network Activities" published by the Supreme People's Court and the Supreme People's Procuratorate on October 21, 2019, which stipulates in Article 12 the determination of "serious circumstances" criteria[2]. The specific sentencing circumstances include confession,

[2] This law also provides for three sentencing circumstances: those who have received administrative punishment within two years for illegal use of information network, aiding criminal information network activities, or endangering computer information system security and aiding criminal information network activities; those who have been helped to commit crimes with serious consequences; and other circumstances of seriousness. However, the above three are difficult to count purely from the perspective of the judgment, and thus are not included in the statistical variables.

surrender, merit, guilty plea, active refund, special subject, other mitigating circumstances, recidivism, other aggravating circumstances, a total of 10 statistical standards. The statistical criteria for the types of principal offender behaviors include failure to mention, network fraud, network gambling, infringement of citizen information, dissemination of obscene pornography, destruction of computer information systems, and other positive offense behaviors. In addition, since this crime explicitly specifies four types of specific behaviors to provide technical support, advertising promotion, payment settlement, or other helping behaviors for others, by designing the variable of specific behavioral types, the above four main behavioral types of this crime are counted, and the specific practical application of the four types can be derived.

Thirdly, the variables related to penalty disposition include only three variables: the type of free sentence, the length of free sentence, and the amount of fine sentence. Among them, the types of free sentences include free sentences, custodial sentences, fixed-term sentences, and suspended sentences. The duration of the free sentence is calculated in months of fixed-term imprisonment, and for the convenience of statistics, every two month is calculated as one month of fixed-term imprisonment, and one month of detention is calculated as one month of fixed-term imprisonment, that is, three years of probation is calculated as 18 months of the free sentence. The fine sentence is calculated in RMB.

2. Data Basic Overview and Geographical Variation Characteristics

Based on the above-mentioned sample selection and variable design, the data obtained can be processed by using SPSS software to paint a broad picture of the judicial application of this crime. In the following section, we intend to analyze the data in terms of the general application and the main differences in the application of the crime among the regions, to verify the conclusions of the above-mentioned official reports and find answers to the theoretical disputes in practice.

2.1. General Overview

Here, the overall temporal and spatial distribution of judicial practice is outlined based on three main scalars: time of trial completion, geographic area of trial completion, and the number of cases, to facilitate subsequent analysis of the status of geographic differences.

2.1.1. Time of trial completion

Figure 1 clearly shows that in 2020, a total of 1,797 defendants, 84.3% of the total, were tried for the crime of aiding information network criminal activities; in 2019, only 219, 10.28% of the total, were tried; and only 115, 5.40% of the total, were tried in the previous three years. This trend is largely consistent with the aforementioned findings reported by the Supreme Court and the Supreme Prosecutor. This trend is not surprising considering that the "Criminal Law Amendment (IX)" Act has only been in force since November 1, 2015, a relatively short period of time, and that it was treated as an act of complicity under the heavier statutory penalty when it occurred.

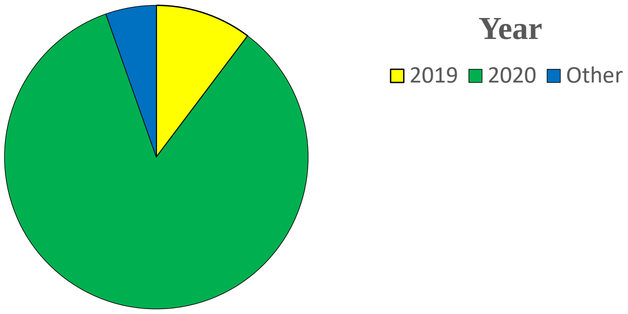


Figure 1 Statistical chart of the year of trial completion for each defendant

2.1.2. Geographic distribution of trial completion

It can be easily seen from Figure 2 that the 2,131 defendants counted in this paper were mainly tried in E and C, with a total of 1,584 defendants in both, accounting for 74.3% of all defendants. NW accounted for only 2.1% of the total number of cases, and was the region with the lowest number of cases; NE was the second, with 3.6%; followed by N with 4.8%. The total number of cases in S and SW is similar, accounting for 8.1% and 7.2% respectively. This proportional distribution is consistent with the data released by the Supreme People's Court, once again proving that crimes of aiding criminal information network activities are mainly concentrated in E and C, with more significant geographical concentration characteristics.

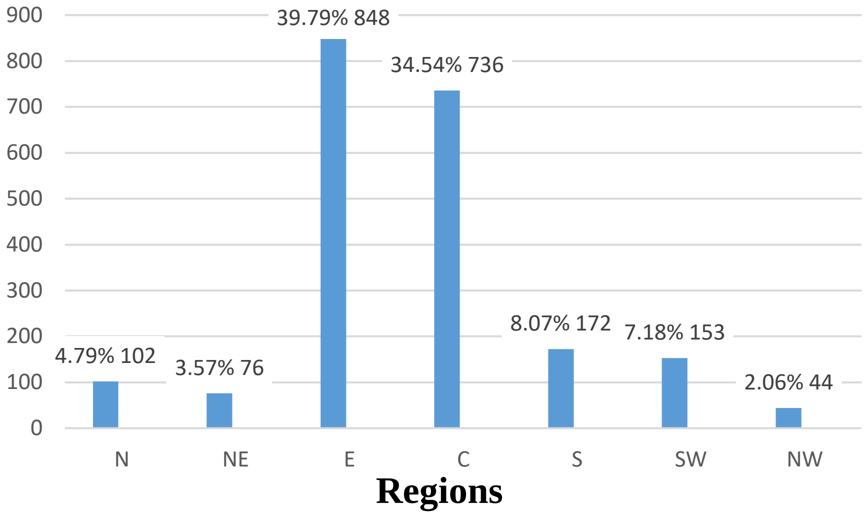


Figure 2 Statistical map of the geographical distribution of the defendants

2.2. The main characteristics in geographical differences

Several key differences in the application of this crime in practice are found through statistical analysis of the specific sentencing status, the application of sentencing circumstances, and the differences in the performance of the crime circumstances in each region.

2.2.1. Differences in sentencing situations between geographic regions

As can be seen from Table 1, in terms of the average value of free sentences, NW and N has the highest value of about 12.7 months, followed by NE with about 12.5 months, and SW has the lowest value of about 9.6 months, and the difference in its average value is more than three months, which shows that there is a large variability in free sentence disposition among regions. Similarly, the highest average value of fine sentences was in N at about RMB 21,971, followed by E, at about RMB 19,603, and the lowest in NW, at RMB 12,125, with a difference of nearly RMB 10,000. Even taking into account the fact that compared to the NW, N and E are more economically developed, and there is a tendency for their fine sentences to change according to the regional economic development, this difference is still too large. In particular, the average value of fines in the NE, which is also relatively underdeveloped, still reaches about 18,553 yuan, which is not only much higher than that in the NW but also higher than that in S and SW, which shows that there is also a large variation in the punishment of fines between regions.

Table 1 Statistics on the differences in sentencing mean values

Region		N	Minimal value	Maximum value	Average value	Standard deviation
N	Sentence to freedom penalty	102	.0	24.0	10.480	6.2896
	Sentence to fine punishment	102	0	980000	21970.59	96687.560
NE	Sentence to freedom penalty	76	3.0	23.0	12.520	5.6707
	Sentence to fine punishment	76	1000	380000	18552.63	56037.462
E	Sentence to freedom penalty	848	.0	34.0	9.719	5.4519
	Sentence to fine punishment	848	0	650000	19602.59	42911.162
C	Sentence to freedom penalty	736	.0	36.0	9.781	5.1338
	Sentence to fine punishment	736	1000	600000	13043.81	31502.100
S	Sentence to freedom penalty	172	.0	33.0	10.680	5.0546
	Sentence to fine punishment	172	1000	60000	11566.86	11788.333
SW	Sentence to freedom penalty	153	3.0	24.0	9.552	4.2229
	Sentence to fine punishment	153	1000	200000	14728.76	25626.876
NW	Sentence to freedom penalty	44	5.0	30.0	12.659	5.1847
	Sentence to fine punishment	44	2000	150000	12125.00	22965.375

As for the differences between the types of liberal sentences applied between regions, as shown in Table 2, the highest proportion of probation was applied in SW, accounting for 37.7%, and the lowest in S, where only 9 defendants out of a total of 172 were applied to probation, accounting for 5.2%, with a difference of more than 20%, again significantly reflecting the large differences in the application of probation between regions.

Table 2 Statistical table of differences in the types of freedom penalty

Region			Frequency	Percentage
N	Effective	Not sentenced to freedom penalty	11	10.8
		Probation	15	14.7
		Detention	3	2.9
		Fixed-term imprisonment	73	71.6
		Total	102	100.0
NE	Effective	Probation	8	10.5
		Detention	7	9.2
		Fixed-term imprisonment	61	80.3
		Total	76	100.0
E	Effective	Not sentenced to freedom penalty	16	1.9
		Probation	245	28.9
		Detention	69	8.1
		Fixed-term imprisonment	518	61.1
		Total	848	100.0
C	Effective	Not sentenced to freedom penalty	17	2.3
		Probation	128	17.4
		Detention	33	4.5
		Fixed-term imprisonment	558	75.8
		Total	736	100.0
S	Effective	Probation	9	5.2
		Detention	10	5.8
		Fixed-term imprisonment	153	89.0
		Total	172	100.0
SW	Effective	Probation	57	37.3
		Detention	1	.7
		Fixed-term imprisonment	95	62.1
		Total	153	100.0
NW	Effective	Probation	6	13.6
		Detention	3	6.8
		Fixed-term imprisonment	35	79.5
		Total	44	100.0

2.2.2. Regional differences in sentencing circumstances and circumstances of the crime

Table 3 provides statistics on the application of the major sentencing circumstances of this crime in seven regions. It can be seen that in most regions, the three sentencing circumstances that account for the highest proportion are confession, guilty plea, and active return of stolen goods. This shows that these three mitigating circumstances are the high proportion of this crime in practice, the judicial authorities mainly consider the sentencing circumstances. In all regions, the highest percentage of confessions for the northwest region, accounting for 75.0%, followed by E, accounting for 74.6%; the lowest in SW, accounting for 15.7%; S second, accounting for 30.8%. The highest percentage of guilty pleas was in NW, accounting for 88.6%, followed by SW, accounting for 84.3%; the lowest percentage was in NE, accounting for 61.8%, followed by S, accounting for 76.2%. In the positive return of stolen goods, the highest proportion of the region is C, accounting for 38.3%; followed by E, accounting for 33.7%; the least region is S, accounting for only 4.1%; NW is the second, accounting for 11.4%. Comprehensive three sentencing circumstances, the SW region in the confession and surrender of two sentencing circumstances on a more special performance, is the only surrender accounted for a higher proportion than probation, reaching 58.8% of the region. And the proportion of guilty pleas in this region is also higher, indicating that the attitude of the perpetrators in this region is more favorable than that in other regions, or the judicial authorities in this region are more lenient in determining the above-mentioned mitigating circumstances. In S, the proportion of confession, surrender, guilty plea, and active return of stolen goods is low, which indicates that the attitude of the perpetrators in this region is poorer, or the judicial organs in this region are harsher in determining the above mitigating circumstances.

Table 3 Statistical table of the differences in sentencing circumstances

Region	Types of sentencing circumstances	Frequency	Percentage
N	Confession	60	58.8
	Surrender	18	17.6
	Merit	2	2.0
	Plead guilty to a fine	80	78.4
	Actively return stolen goods	32	31.4
	Other leniencies	2	2.0
	Recidivism	5	4.9
	Other severe punishment	2	2.0
NE	Confession	38	50.0
	Surrender	14	18.4
	Merit	2	2.6
	Plead guilty to a fine	47	61.8
	Actively return stolen goods	24	31.6
	Other leniencies	3	3.9
	Recidivism	3	3.9
	Other severe punishment	3	3.9
E	Confession	633	74.6
	Surrender	134	15.8
	Merit	13	1.5
	Plead guilty to a fine	662	78.1
	Actively return stolen goods	286	33.7
	Other leniencies	18	2.1
	Recidivism	32	3.8
	Other severe punishment	18	2.1

C	Confession	488	66.3
	Surrender	154	20.9
	Merit	12	1.6
	Plead guilty to a fine	600	81.5
	Actively return stolen goods	282	38.3
	Other leniencies	3	.4
	Recidivism	18	2.4
	Other severe punishment	3	.4
S	Confession	53	30.8
	Surrender	18	10.5
	Merit	3	1.7
	Plead guilty to a fine	131	76.2
	Actively return stolen goods	7	4.1
	Other leniencies	9	5.2
	Recidivism	3	1.7
	Other severe punishment	9	5.2
SW	Confession	24	15.7
	Surrender	60	58.8
	Merit	7	4.6
	Plead guilty to a fine	129	84.3
	Actively return stolen goods	44	28.8
	Other leniencies	0	0
	Recidivism	7	4.6
	Other severe punishment	0	0
NW	Confession	33	75.0
	Surrender	4	9.1
	Merit	2	4.5
	Plead guilty to a fine	39	88.6
	Actively return stolen goods	5	11.4
	Other leniencies	0	0
	Recidivism	0	0
	Other severe punishment	0	0

Table 4 shows the regional differences in the mean values of the main crime circumstances of this crime, which can depict the differences in the severity of the crime situation between regions. First of all, from the viewpoint of the number of objects of help, the SW region has the highest mean value of the number of objects of help, which is 7.67; S region is the second-highest, which is 7.06; N region and NW region both have the lowest, which is 1.4. On the whole, the number of people helped by this crime varies greatly from region to region, among which the mean value of SW and S regions is significantly higher than other regions, while N and NW regions are significantly lower than other regions, which shows that the manifestation of the help of this crime is significantly different among regions.

Second, in terms of the payment settlement amount, the difference between regions is more obvious. Among them, the region with the largest average payment settlement amount is C with

RMB 339,301,963.62, followed by SW with RMB 173,809,661.7, while the lowest region, N has an average payment settlement amount of only RMB 627,145.08, with a difference of more than 300 million yuan. Even considering that a few cases with high payment settlement amounts raised the regional average, this difference is still too large.

Again, in the amount of illegal income, each region also showed a large variation. Among them, the E region is the highest average value of illegal income, the average value of more than 150,000 yuan; the SW region is the second, more than 148,000 yuan; the lowest average value of illegal income is NW region, the average value of only 9,500 yuan.

In general, Table 4 shows the differences in the circumstances of the crimes committed by the perpetrators in each region: SW region not only has the highest average value of the number of objects helped, but also has a higher amount of payment and settlement and the amount of illegal income, which is the most serious crime situation among all regions. In contrast, N and NW regions have lower average values of the number of targets helped and lower average values of payment and settlement amounts and illegal income amounts. In addition, the two regions are characterized by a low caseload, which means that this crime is less frequent and less serious.

Table 4 Statistical table of differences in crime circumstances

Region		Minimal value	Maximum value	Average value	Standard deviation
N	Number of people helped	1	6	1.40	1.194
	Payment settlement amount	0	13295904	627145.08	1716016.692
	Amount of illegal proceeds	0	987304	56294.50	176635.049
NE	Number of people helped	1	25	2.98	4.997
	Payment settlement amount	0	274781070	5535731.50	35470249.502
	Amount of illegal proceeds	0	3745350	102878.92	488099.253
E	Number of people helped	1	100	3.06	8.459
	Payment settlement amount	0	657256486	7239152.32	43877729.920
	Amount of illegal proceeds	0	7700000	153765.99	603007.076
C	Number of people helped	1	59	4.15	9.526
	Payment settlement amount	0	219535921972	339301963.62	8525853767.331
	Amount of illegal proceeds	0	13400000	109185.91	996834.562
S	Number of people helped	1	60	7.06	14.408
	Payment settlement amount	0	28876000000	173809661.70	2221016662.063
	Amount of illegal proceeds	200	2000000	60838.47	238854.201
SW	Number of people helped	1	300	7.67	28.710
	Payment settlement amount	0	90000000	4511258.95	15727780.811
	Amount of illegal proceeds	100	4764397	148443.96	630768.586
NW	Number of people helped	1	3	1.40	.737
	Payment settlement amount	0	4000000	714666.02	1366877.948
	Amount of illegal proceeds	600	42000	9526.19	11452.878

Table 5 shows the differences in the principal offender behavior facilitated by this crime across regions. Overall, Internet fraud is the most predominant type of principal offender behavior facilitated by this crime, with Internet gambling coming in second and other types of principal offender behavior accounting for a lower percentage. Specifically, the highest percentage of Internet fraud was in NW and NE, both of which exceeded 80%, showing significant differences from other regions, especially in NW, where all of the principal offenders explicitly mentioned in the verdicts were Internet fraud; while E had the lowest percentage, 62.6%, but the difference is not significant compared to other regions.

Table 5 Statistical table of the differences in the types of principal offender behaviors

Region			Frequency	Percentage	Cumulative percentage
N	Effective	Not mentioned	11	10.8	10.8
		Internet fraud	66	64.7	75.5
		Internet gambling	21	20.6	96.1
		Dissemination of obscene and pornographic information	1	1.0	97.1
		Damage to computer information system	3	2.9	100.0
		Total	102	100.0	
NE	Effective	Not mentioned	2	2.6	2.6
		Internet fraud	61	80.3	82.9
		Internet gambling	8	10.5	93.4
		Infringement of citizens' information	1	1.3	94.7
		Damage to computer information system	2	2.6	97.4
		Other crimes and violations using the network	2	2.6	100.0
		Total	76	100.0	
E	Effective	Not mentioned	92	10.8	10.8
		Internet fraud	531	62.6	73.5
		Internet gambling	109	12.9	86.3
		Infringement of citizens' information	17	2.0	88.3
		Dissemination of obscene and pornographic information	30	3.5	91.9
		Damage to computer information system	19	2.2	94.1
		Other crimes and violations using the network	50	5.9	100.0
		Total	848	100.0	
C	Effective	Not mentioned	102	13.9	13.9
		Internet fraud	500	67.9	81.8
		Internet gambling	89	12.1	93.9
		Dissemination of obscene and pornographic information	18	2.4	96.3
		Damage to computer information system	1	.1	96.5

		Other crimes and violations using the network	26	3.5	100.0
		Total	736	100.0	
S	Effective	Not mentioned	12	7.0	7.0
		Internet fraud	111	64.5	71.5
		Internet gambling	30	17.4	89.0
		Infringement of citizens' information	2	1.2	90.1
		Dissemination of obscene and pornographic information	13	7.6	97.7
		Other crimes and violations using the network	4	2.3	100.0
		Total	172	100.0	
SW	Effective	Not mentioned	16	10.5	10.5
		Internet fraud	101	66.0	76.5
		Internet gambling	24	15.7	92.2
		Dissemination of obscene and pornographic information	2	1.3	93.5
		Damage to computer information system	3	2.0	95.4
		Other crimes and violations using the network	7	4.6	100.0
		Total	153	100.0	
NW	Effective	Not mentioned	8	18.2	18.2
		Internet fraud	36	81.8	100.0
		Total	44	100.0	

Table 6 shows the differences in the types of conduct aided by this crime across regions. Similar to the aforementioned fraudulent acts, payment settlement acts also dominate all regions, followed by technical support acts, and advertising promotion is a lesser type of act. Specifically, the highest percentage of payment settlement type is in C, which is consistent with its high average value of payment settlement amount; the percentage of technical support acts exceeds that of payment settlement acts in S and SW regions, with SW region S and SW regions, have a higher share of technical support than payment settlement, with SW region having the highest share of technical support and the lowest share of payment settlement.

Table 6 Statistical table of differences in types of aiding behaviors

Region			Frequency	Percentage	Cumulative percentage
N	Effective	Technical support	25	24.5	24.5
		Advertising promotion	8	7.8	32.4
		Payment settlement	63	61.8	94.1
		Other aiding behaviors	6	5.9	100.0

		Total	102	100.0	
NE	Effective	Technical support	19	25.0	25.0
		Advertising promotion	5	6.6	31.6
		Payment settlement	52	68.4	100.0
		Total	76	100.0	
E	Effective	Technical support	221	26.1	26.1
		Advertising promotion	64	7.5	33.6
		Payment settlement	509	60.0	93.6
		Other aiding behaviors	54	6.4	100.0
		Total	848	100.0	
C	Effective	Technical support	138	18.8	18.8
		Advertising promotion	26	3.5	22.3
		Payment settlement	542	73.6	95.9
		Other aiding behaviors	30	4.1	100.0
		Total	736	100.0	
S	Effective	Technical support	79	45.9	45.9
		Advertising promotion	12	7.0	52.9
		Payment settlement	73	42.4	95.3
		Other aiding behaviors	8	4.7	100.0
		Total	172	100.0	
SW	Effective	Technical support	72	47.1	47.1
		Advertising promotion	20	13.1	60.1
		Payment settlement	61	39.9	100.0
		Total	153	100.0	
NW	Effective	Technical support	6	13.6	13.6
		Advertising promotion	6	13.6	27.3
		Payment settlement	27	61.4	88.6
		Other aiding behaviors	5	11.4	100.0
		Total	44	100.0	

2.2.3 Analysis of the effect of geographic regions sentencing circumstances and crime circumstances on sentencing

Table 7 and Table 8 analyze the effects of sentencing and offense circumstances on the sentencing of the two types of penalties in each region by linear regression using the aforementioned sentencing and offence circumstances as independent variables and the freedom penalty and fine punishment as dependent variables, respectively (due to space limitations, variables that are not significant, i.e., sig. > 0.05, are excluded from both tables, and only significant factors other than constants are retained). In addition, due to the small sample size in NW, the variables in this study are not statistically significant in this region, while in N the only significant factor is the number of illegal proceeds in Table 7 and Table 8 analyze the effects of sentencing and offense circumstances on the sentencing of the two types of penalties in each region by linear regression using the aforementioned sentencing and offense circumstances as independent variables and the freedom penalty and fine punishment as dependent variables, respectively (due to space limitations, variables that are not significant, i.e., sig. > 0.05, are excluded from both tables, and only significant factors other than constants are retained). In addition, due to the small sample size in NW, the variables in this study are not statistically significant in this region, while in N the only significant factor is the number of illegal proceeds in the fine punishment.

Table 7 shows that, among the five regions with significant factors, the E region has the most significant factors in imposing the freedom penalty. This includes payment settlement amount, amount of illegal proceeds, whether it constitutes surrender, and whether it constitutes recidivism, all of which have a significant effect on the imposition of freedom penalty; C follows, except for the number of illegal proceeds and whether it constitutes Recidivism, which also has a significant effect in this region. In C, except for the number of illegal proceeds and whether it constitutes recidivism, whether to actively return stolen goods also has a significant impact on the freedom penalty in this region. On the whole, the number of illegal proceeds and whether it constitutes surrender are the most influential factors in determining freedom penalty in most districts, while payment settlement amount and whether it constitutes plead guilty to a fine, actively return stolen goods, and recidivism are the most influential factors in determining freedom penalty in most districts. On the whole, the number of illegal proceeds and whether it constitutes Surrender are the most influential factors in determining liberty sentences in most districts, while payment settlement amount and whether it constitutes plead guilty to a fine, actively return stolen goods, and recidivism are the most influential factors in determining liberty sentences in most districts. The payment settlement amount and whether it constitutes plead guilty to a fine, actively return stolen goods, and recidivism are the elements that have a significant effect in a few areas, while the number of people helped, confession, and both elements do not have a significant effect in all areas. Although there is also no significant effect of merit, the conclusion is not representative because the sample size of the existence of merit circumstances is too small.

Table 7 Statistical table of the differences in sentencing and crime circumstances on the disposition of freedom penalty

Region	Model		Non-standardized coefficient		t	Sig.
			B	Standard Error		
N	1	No significant factors				
NE	1	Plead guilty to a fine	-4.189	1.642	-2.550	.016
		Actively return stolen goods	-8.365	1.451	-5.763	.000
E	1	Payment settlement amount	3.204E-008	.000	6.343	.000
		Amount of illegal proceeds	8.936E-007	.000	2.040	.042
		Surrender	-2.843	.930	-3.057	.002
		Recidivism	3.311	1.195	2.771	.006
C	1	Amount of illegal proceeds	6.581E-006	.000	2.187	.029
		Actively return stolen goods	-1.967	.530	-3.715	.000
		Recidivism	3.524	1.490	2.365	.019
S	1	Surrender	-3.793	1.569	-2.417	.019
SW	1	Amount of illegal proceeds	2.281E-006	.000	5.019	.000
		Surrender	-3.990	2.002	-1.993	.050
NW	1	No significant factors				

Table 8 shows that E and SW regions have the most significant factors in influencing fine punishment. Among them, the number of people helped, payment settlement amount, amount of illegal proceeds, and recidivism are the factors that have a significant influence on the imposition of fine punishment in E. While SW has the same number of people helped and amount of illegal proceeds as E. In the SW region, except for the number of people helped and the amount of illegal proceeds, whether the perpetrator constitutes plead guilty to a fine and actively return stolen goods are the factors that have a significant impact on the fine punishment in the region. The regression coefficients of amounts of illegal proceeds (i.e., B) are the same as those of E. The regression coefficient (i.e., B-value) of the number of illegal proceeds in each region shows that N is the region with the largest increase of amounts of illegal proceeds, while E is the region with the smallest increase of amounts of illegal proceeds, which shows that although amounts of illegal proceeds are considered in different regions, the effect of amounts of illegal proceeds is the same. It can be seen that although the amounts of illegal proceeds are considered in different regions, there are also some differences in their effects.

In addition, there are some problems with some of the data in Table 8, such as the negative correlation between recidivism and fine punishment in E and the negative correlation between the number of people helped and fine punishment in SW. If we exclude the possibility that there are problems in the construction of the model and the statistics of the variables in this study, there are some problems in the determination of sentencing circumstances and fine punishment in the above two regions.

Table 8 Statistical table of the differences in sentencing and crime circumstances on the imposition of fine punishment

Region	Model		Non-standardized coefficient		t	Sig.
			B	Standard Error		
N	1	Amount of illegal proceeds	.460	.092	5.024	.000
		Payment settlement amount	.000	.000	15.510	.000
NE	1	Amount of illegal proceeds	.303	.008	36.162	.000
		Plead guilty to a fine	-5475.631	2398.048	-2.283	.030
		Number of people helped	589.948	193.912	3.042	.002
E	1	Payment settlement amount	.000	.000	10.913	.000
		Amount of illegal proceeds	.038	.004	10.601	.000
		Recidivism	-20299.018	9724.932	-2.087	.037
		Payment settlement amount	5.506E-005	.000	2.840	.005
C	1	Amount of illegal proceeds	.103	.012	8.524	.000
		Plead guilty to a fine	-8159.235	2733.387	-2.985	.003
S	1	Recidivism	19822.881	8032.609	2.468	.017
		Number of people helped	-431.772	152.351	-2.834	.006
SW	1	Amount of illegal proceeds	.041	.001	31.641	.000
		Plead guilty to a fine	5556.983	2788.103	1.993	.050
		Actively return stolen goods	10424.422	2179.923	4.782	.000
NW	1	No significant factors				

3. The main problems of geographical differences and suggestions for improvement

The comprehensive data above shows that the geographical differences of this crime are mainly manifested in the following aspects:

Firstly, there are large differences in the judging amount of penalty between regions. In terms of the freedom penalty, the average value of the freedom penalty imposed in all three northern regions is above 10 months. Among them, especially NE and N regions, the average value of imposed freedom penalty is higher than 12 months, which is significantly higher than other regions and is the region with heavier freedom penalties. In terms of specific types of freedom penalty, the percentage of probation imposed in the S region is significantly lower than that of other regions, but the three northern regions are still the regions with the lowest percentage of probation imposed right behind them, with the percentage of all three being below 15%, which differs greatly from C, E, and SW regions. Thus, from the perspective of free sentences, the NW, NE, and N regions, in general, have heavier penalties, and the S region not only has a higher average value of freedom penalty than the N region, but also has the lowest proportion of probation, and is also a region with heavier penalties; while C, E, and SW are less punitive.

And from the perspective of fine punishment, the mean values in N E, and NE are significantly higher than other regions, and the mean value in S is the lowest, but the difference is not significant compared with other regions. In General, the imposition of fine punishment should be influenced by the differences in crime circumstances and economic development, and income levels in each region. However, except for the E region, the N and NE regions have relatively more moderate crime circumstances, but their mean values of fine punishment are still higher.

Secondly, the crime situation varies greatly from region to region; SW has the most severe crime situation, and S has the most severe penalties overall, with a higher number of people helped and a higher payment settlement amount. Although the average proceeds of crime are low, the overall crime situation is second only to SW in terms of severity. N and NW regions are more moderate, not only the number of cases is lower, the overall crime situation is lighter, and the positive offence behavior is mostly fraud, and the type of behavior is mostly payment settlement behavior, and the overall reflects the characteristics of single crime behavior. NE region number of people helped and the payment settlement amount is in the lower position, and the average value of illegal income is in the middle of the water, which shows that the crime situation in this region is generally lighter than in other regions. E and C regions, as the regions with the most concentrated case volume, also have certain characteristics of the crime situation they face: although the number of people helped and the average payment settlement amount in the E region are in the middle stage of each region, its average illegal E has the highest average illegal income. In addition to the higher level of economic development and higher average income in this region, it may also be because the perpetrators in this region tend to show the characteristics of committing crimes in pursuit of economic benefits. At the same time, the region also shows the lowest proportion of fraud among the types of the principal offender, a higher degree of diversification of the types of the principal offender, and a relatively high proportion and the largest absolute number of technological support behaviors, indicating that the criminal behavior in this region is more variable. In C, the average value of payment settlement amount is significantly higher than other regions, and the proportion of payment settlement behavior is also significantly higher than other regions, which indicates that this region is the most serious in terms of the situation of "two-card"[3] type help information network crime.

Thus, the overall crime situation in the northern region, including NW, N NE, is more moderate and less serious; E and C in the central region not only have a large number of cases but also have significant characteristics of the crime situation, which should be considered from the perspective of criminal policy. From the perspective of criminal policy should be targeted to consider; SW, S, two regions of the overall crime situation is more severe and reflects the characteristics of technological support behavior. In general, this crime in practice generally shows the characteristics of the crime from north to south, the crime is gradually serious, the type of criminal behavior is gradually diversified, and the proportion of technological support behavior is gradually increased.

Thirdly, there are some variabilities in the determination of sentencing circumstances and circumstances of the offence from region to region. As mentioned earlier, not only did the proportion of specific sentencing circumstances identified differ somewhat from region to region, but the effect of various sentencing circumstances on the imposition of freedom penalty and fine punishment also differed significantly from region to region. In general, the proportion of surrender was higher in SW, and this circumstance had a significant effect on the determination of freedom penalty in this region, which shows that this region is more lenient in the determination of freedom penalty. In S, not only was the overall sentencing circumstance more severe but also the only sentencing circumstance that had a significant effect on the

[3] The so-called "two-card" type of aiding information network crime refers to the helping behavior of using one's information to handle on behalf of the perpetrator, or selling to him or her the telephone card, bank card, company account, etc. handled by himself or herself or others with real information. See, Huang Cheng and Kong Yao, "Personal Information Infringement and Regulation in the Chain of Telecommunication Network Fraud "Black Industry"--The Helpful Acts of "Two Cards" Crime", in Taiyuan City Vocational College Journal, 2021. *Journal of Taiyuan City Vocational College*, No. 7, 2021

freedom penalty was surrender. In addition, there were only 18 cases of surrender in this region, so it can be considered that this region is more stringent in terms of the leniency of sentencing.

The above geographical difference characteristics are not only the different performance of the crime of aiding information network criminal activities between the various regions but also from the side to reflect current China's network crime in the formation of significant differences between the regions. Its overall presents the Internet fraud crime and related crimes occupy the main position of network crime; the number of cases is concentrated in central E, C region; the crime situation presents the characteristics of lighter in the north and heavier in the south; the means of crime are more single in the north, more complex in the central and southern regions; the overall heavier sentences in the north and central and southern regions as a whole lighter, but S region exception of the significant features. This trend is consistent with the current trend that the development of China's overall network technology and environment in the north are more backward than that in the south, and also reflects the characteristics of the crime situation in the SW and S regions based on the prevalence of cross-border cybercrime, which leads to the crime of aiding information network criminal activities heavier than that in the north. However, this overall trend reflects an important issue: there is a contradiction between the current penalties imposed in each region and the crime situation they face. In general, from the perspective of criminal policy, regions with more severe crime situations should have harsher sentences. N NE, and NW regions face a more moderate crime situation, but their freedom penalties are the heaviest, and the average value of fine punishment in N and NE regions are also at the top, which shows that the above three regions are suspected of having heavier penalties.

The crime situation in E and C has its characteristics, among which the E region reflects the higher average value of fine punishment imposed according to the crime situation of the higher average value of illegal income in the region. It can be said that this is to some extent a combination of punishment and crime situation, while the C region does not show the correlation between its sentence and the crime situation of "two-card crimes" in the region. The SW and S regions, where the crime situation is most severe, show opposite characteristics in terms of sentencing. The SW region has the most lenient sentences overall, while the S region has the most severe sentences.

This problem may arise from the differences in the identification and application of specific sentencing circumstances by the judicial authorities in each region. Although sentencing sentences in each region are generally influenced by the more central element of the number of illegal proceeds in the circumstances of the crime. However, as the aforementioned data show, except for surrender, other leniency sentencing circumstances, especially confession and plead guilty to a fine, which occupy the highest proportion overall, do not have a significant effect on the freedom penalty and fine punishment in practice. In addition, whether or not to actively return the stolen money is also an important factor in examining whether the perpetrator substantially confesses and repents, and should be a discretionary sentencing circumstance that plays an important role in the sentencing process of this crime. The fact that this circumstance only has a significant effect on the sentencing of the freedom penalty in C and fine punishment in SW indicates that there are problems in the application of this circumstance in each region. In addition, the data alone do not reveal the relationship between the sentencing circumstances and offence circumstances that have a significant impact on sentencing in each region and the specific crime situation in that region. For example, in the C region, which is characterized by a high concentration of "two-card" crimes, the payment settlement amount does not have a significant impact on the discretionary sentences; in the SW and S regions, where technological support behaviors are high, the number of people in the region does not have a significant impact on the sentences. In SW and S, where technological support behavior is high, the number of people helped only had an effective impact on the determination of fines in SW. Therefore, to solve this problem, each region must introduce appropriate criminal policies to regulate this crime according to its specific crime situation.

Specifically, this paper puts forward the following recommendations in response to the above issues:

First, the three northern regions should moderately relax the application of probation for this crime. Since the overall number of cases in the three northern regions is relatively small and the crime situation is not severe, but the penalties in the region are significantly heavier, moderately relaxing the application of probation to perpetrators in the region can help achieve balanced sentencing between regions.

Second, C should focus on combating the "two-cards" type of assistance, not only in the sentencing process to consider the payment settlement amount as a sentencing circumstance, but also strengthen the standardized management of bank cards, telephone cards, and other common tools of such crimes, to combat the high incidence of "two cards" crime in the region.

Third, E, SW, and S should focus on preventing and combating the technical support type of help. The number of people helped, which has a strong correlation with technical support behaviors[4]. Therefore, by strictly dealing with technical support behaviors that help a large

[4] Most scholars believe that the harm of technical support is mainly reflected in the characteristic of "one-to-many" help, and the number of helpers is a visual indication of this characteristic. See Hu Yunteng, "Theoretical and

number of positive offenders, it is an effective way to suppress the crime situation in the above-mentioned regions where technical support-type help behaviors account for a high percentage.

Fourth, the SW region should increase the penalties for this crime moderately. As mentioned above, compared with S, where the crime situation is more serious, the penalty in the SW is too light to achieve the effect of preventing this crime utilizing punishment. Therefore, the region should moderately increase the punishment for this crime, such as reducing the proportion of probation and moderately increasing the amount of fine punishment, so that the average value of sentencing in the region is not significantly lighter, which will help to achieve balanced sentencing between regions and also help to control the more serious crime situation in the region.

4. Conclusions

Based on the above study, the crime of aiding information network criminal activities reflects the characteristics of significant regional differences, as well as the trend of progressively severe crime situations from north to south, and progressively diverse types of behavior. At the same time, it also shows the main problems in the application of sentencing circumstances and discretionary penalties in each region, i.e., the existence of incongruity between penalties and regional crime situations, and gives relevant criminal policy recommendations accordingly.

However, it should be noted that this paper is still slightly inadequate in the depth and breadth of data mining, especially in the specific application of sentencing circumstances. The relevance of the data and conclusions, and the rationality of the mathematical model used are worthy of deeper exploration. At the same time, issues such as the main influencing factors of sentencing probation around the world and the effect of the type of principal offender behavior on the penalty still need further research and discussion.

References

China Judicial Big Data Service network (http://data.court.gov.cn)

Huang Cheng and Kong Yao (2021) Personal Information Infringement and Regulation in the Chain of Telecommunication Network Fraud "Black Industry"--The Helpful Acts of "Two Cards" Crime". Journal of Taiyuan City Vocational College, No. 7, pp. 189-192.

Practical Innovations of the Criminal Law Amendment (IX)", in China Trial, No. 20, 2015, p. 27. Yin Jianfeng and Liu Xuedan, "Legal Doctrinal Analysis of the Crime of aiding information network criminal activities," in Criminal Law Series, No. 4, 2016, p. 214.

Hu Yunteng (2015) Theoretical and Practical Innovations of the Criminal Law Amendment (IX)". China Trial, No. 20, p. 27.

Yin Jianfeng – Liu Xuedan (2016) Legal Doctrinal Analysis of the Crime of aiding information network criminal activities. Criminal Law Series, No. 4, p. 214.

Zhang Haimei – Liu Zihao – Fan Jinyuan (2021) Judicial expansion and reduction path of aiding the crime of information network crime -- An Empirical Study Based on 1737 criminal judgment documents [J]. Journal of Xi'an University of Electronic Science and Technology (SOCIAL SCIENCE EDITION), 31 (01): 66-71.

Zhou Ming (2019) "Hot" and "cold": the picture of judicial application of aiding the crime of information network crime -- An Empirical Analysis Based on 72 criminal judgment documents [J]. Application of law, (15): 23-32.

Zhang Lei – Zhang Meng (2021) Research on the judicial application of the crime of helping information network crime -- from the perspective of 131 judgments [J]. Juvenile delinquency, (04): 42-55

News from the word of the Hungarian and international criminal geography

News from the International Criminal Geographical Association Facebook profile

Dear Madam / Sir,

Welcome to the Facebook page of the recently formed International Criminal Geographical Association. The Alliance aims to conduct research and surveys and bring together those interested in the criminal geography around the world.

Please follow our Facebook page, attend our events, and if you would like to join our scientific community, contact us at criminalgeography@gmail.com.

Best regards:
The leadership of the International Criminal Geographical Association

Szabolcs Mátyás (president) (Hungary)
Vince Vári (vice-president) (Hungary)
Máté Sivadó (vice-president) (Hungary)
János Sallai (vice-president) (Hungary)
László Igényes (vice-president) (Slovakia)
Hunor Kádár (vice-president) (Romania)
Dragana Čvorović (vice-president) (Serbia)

Dear Readers,

The organizers are happy to announce that many applications for the essay competition in English and Hungarian have been received by the International Association of Criminal Geography. In the case of the Hungarian essay category the jury has proposed a split ranking for the 3rd place, while in the English essay category, the jury decided to award the 1st place only.

The results of the Hungarian language category are the following:
1st place: **Dominik Iván** (NKE RTK)
2nd place: **Enikő Harman** (DE TTK)
3rd place: **Brigitta Cselleng** (NKE RTK) and **Péter Pásztor** (NKE RTK)

The result of the English language category is the following:
1st place: **Tamás Bence Fazekas** (DE BTK)

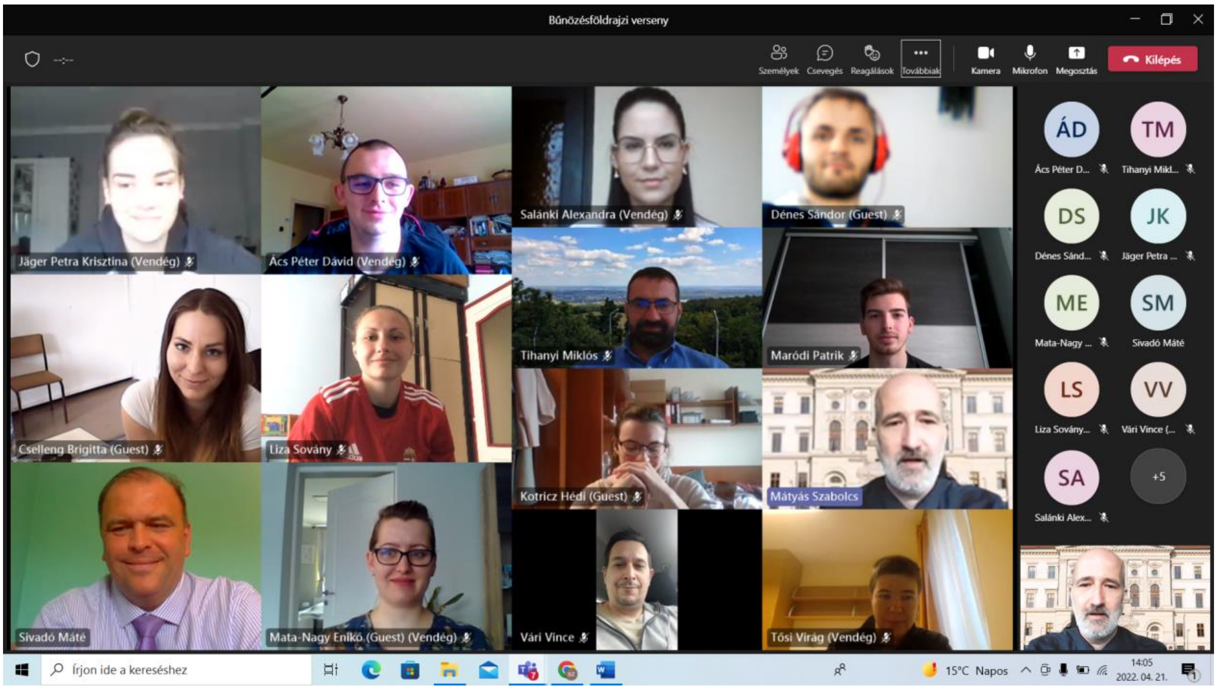
Congratulations to all winners!

Dear Readers,

The I. Béla Földes International Criminal Geography Competition was held today, with the following results:

1st place: Brigitta Cselleng (NKE RTK)
2nd place: Sándor Dénes (DE TTK)
3rd. place: Péter Ács (DE GTK)

Congratulations to all winners!



ICGA
SIN IS
GEOGRAPHICAL

International Criminal Geographical Association

Call for publication proposal

The International Criminal Geographical Association is announcing an essay competition. The essay may cover any sub-topic within the topic of criminal geography, with a maximum of 20,000 keystrokes including spaces, footnotes and bibliography.

The best essays will be published in the scientific Criminal Geographical Journal by the organizers.

The essays should be sent to the organizers to the following email address: criminalgeography@gmail.com.

Deadline for submission: 31 December 2022

Applications will be judged by an international jury.

Evaluation criteria:

- professional standard
- readability

The organisers,

Dr. Szabolcs Mátyás Ph.D.
Dr. Vince Vári Ph.D.
Dr. Máté Sivadó Ph.D.
Dr. Miklós Tihanyi Ph.D.

Conditions of publishing

Length of paper: max. 40 000 characters with spaces
CGR is an English-language journal. Either US or British/Commonwealth English usage is appropriate for manuscripts, but not a mixture of these.

Word processing formats: MS Word (docx, doc)
Page layout size: A4
Font type: Times New Roman, font size: 12 pt.
Abstract: 200-300 words
Keywords: 4-6 maximum
References style in text: 10 pt, footnotes
References: at the end of the paper in alphabetical order (TAYLOR, Tom (2018))
Picture format: JPG
Authors name: main author must be underlined
Citation: APA format

Potential topics might include:

- Crime and GIS
- Crime and analytical work
- Predictive policing
- Geographical features and crime
- Spatial criminalistic methods
- Criminology in spatial aspect

What kind of work do we wait for?

- Original articles
- Critical reviews
- Surveys
- Opinions

The journal is published only in online version.
4 issues per year

Peer review

The CGR operates a single blind review process. All contributions will be initially assessed by the editor for suitability for the journal. Papers deemed suitable are then typically sent to a minimum of two independent expert reviewers to assess the scientific quality of the paper.

Title page information

Title should be informative, please avoid abbreviations.

Author's names: Be kind clearly indicate the given name(s) and family name(s) of each author. Provide the e-mail address, work of place and academic or scientific title.

For example:

Tom Taylor Ph.D. assistant professor
University of London (England)
tom.taylor@gmail.com

We do not accept papers with poor English!

Please do not use highlights in your paper.

Impresszum / Impressum
Kiadó / Publisher: Magyar Rendészettudományi Társaság Bűnözésföldrajzi Tagozat /
Hungarian Association of Police Science Criminal Geographical Section
Cím / Address: 1089 Budapest, Diószegi Sámuel u. 38-42.
A kiadásért és szerkesztésért felelős személy / Responsibles for publishing and editing:
Dr. Mátyás Szabolcs / Dr. Szabolcs Mátyás
Kapcsolat / Contacts: criminalgeography@gmail.com
web: www.rendeszet.hu