The Word Frequency Analysis of the Organized Cyber Fraud

Xiaoming Yu[a], Ling Lv[b]

School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400065, China.

[a]S170701023@stu.cqupt.edu.cn, [b]2015211102@stu.cqupt.edu.cn

Abstract

Nowadays, organized and large-scale cyber fraud has been rampant which is carefully planned by organization of loose fraud groups in China. It has seriously affected social harmony and stability. From the perspective of gangs, exploring the behavior mechanism and countermeasures of organized cyber fraud has attached great importance from academics, government departments and industry. It is of great significance to expand the supervision strategy and theoretical research of deepening cyber fraud. Based on this, this thesis first sorts out related documents, policy documents and social reports, and defines the concept of organized cyber fraud which refers that Small-scale criminals form loose fraud gangs. They organize illegally to execute organized and large-scale cyber fraud crime for the illegal possession. In this paper, through case sampling and text mining to verify the model, the key behaviors of the process model of group cyber fraud are studied quantitatively.

Keywords

Organized network fraud; Text mining; Key behaviors.

1. Introduction

With the rapid development of social information technology, the use of communication tools, the Internet and other technical means to implement new types of cyber fraud crime continues to high incidence. The European Commission's executive body for small and medium-sized enterprises estimates that the global economic losses caused by online fraud will be at least 350 billion euros per year, and it is expected to reach 1.89 trillion euros in 2019. In China, the annual growth rate of cyber fraud is 20-30% (Legal network,2017). In 2017 alone, it caused economic losses of 19 billion 940 million yuan (Tencent security,2017; Xinhua news agency,2017;Tencent,2017;Tencent,2018) and showed a continuous upward trend (Legal network,2017). The crazy spread of cyber fraud has become a typical social risk problem in the emerging technology environment (Snyder P2015), which not only causes huge economic losses to the cheated people, but also causes secondary harmful consequences. For example, Xu Yuyu, a freshman admitted to the college entrance examination in Linyi City, Shandong Province, was defrauded of 9900 yuan by a telecommunication scam in the name of granting financial aid by a criminal suspect. Xu Yuyu died of cardiac arrest. "6.08 million cases of 14 people group fraud on the patient group" caused irreparable physical and mental losses to the cheated people. The social impact of cyber fraud cases is extremely bad, which shocked the supreme law, CBRC and other government sectors. Combating cyber fraud has been listed as one of the important tasks of the 19th National Congress of the Communist Party of China to build a social governance pattern of CO governance and sharing (Supreme People's Procuratorate,2017). To this end, the State Council has set up an inter ministerial joint meeting system with the participation of 23 departments and units, to improve the investigation mechanism of telecom related fraud crimes, to deepen cross-border cross regional police cooperation, to establish a mechanism to stop fraud phone calls, and to stop the payment of cheated funds (Supreme People's Procuratorate,2016). However, with great attention and resolute attack, all kinds of new fraud techniques continue to develop, upgrade and spread. On the one hand, it makes the traditional anti fraud knowledge and awareness seem outdated, which causes the public's deep concern about network security (360 online hunting platform,2017); on the other hand, it challenges the excellent values and ethics of the Chinese nation, which seriously affects the healthy and stable development of society (Hu Xiangyang,2010).

Through the investigation and tracking of China's cyber fraud, it is found that cyber fraud usually takes the form of organized and large-scale Gang fraud (Supreme People's Procuratorate,2016). For example, taking high reward as bait, inheriting the family as the reason, through playing the role of rich woman, group texting, withdrawing money, pretending to be a lawyer and other links of division of labor and cooperation, we can cheat others' money by "Jiangxi Yugan heavy money seeking son fraud" "Taobao fraud in Xinluo District, Longyan City, Fujian Province", which cooperates with relatives and friends in the same village to form a group to purchase user information, make phone calls and defraud Taobao buyers' money. Therefore, to combat the organized and large-scale group type cyber fraud should be the top priority in punishing the cyber fraud crime. It is more and more important and imminent to protect the legitimate rights and interests of the masses and maintain social harmony and stability.

As for the serious social harm caused by cyber fraud, network crimes such as cyber fraud have been marginalized by the mainstream criminology in the academic circle for a long time (Diamond B,2015). Until 2008, foreign scholar J Karuppanan, together with some scholars in the fields of Criminology and sociology, has jointly developed the new field of Criminological Research of "cyber crime" (Jaishankar K,2008), reversing the limitations of traditional criminology only focusing on the details of cyber crime technology, and starting to explore from the aspects of attackers, attacks, social networks, etc., which has accumulated a lot in the emergence of cyber fraud, individual behavior process, etc Key research results. Domestic academic circles also followed closely, not only from the field of criminology, but also from the field of management and information science to actively explore the emergence and behavior process of cyber fraud. From the perspective of gangs, the exploration of the behavior mechanism and response mechanism of cyber fraud is becoming an important research direction in the field of information technology and management at home and abroad (Nash R,2013). However, it is regrettable that most of the current studies only focus on individual crime, and there are few theories that can explain the process of cyber fraud from the perspective of gangs, which can not explain and solve the serious social problem of group cyber fraud in China. Based on this, this paper takes the group type cyber fraud as the research object, and theoretically explores the generation, organization and implementation mechanism of cyber fraud from the perspective of the group, so as to provide decision support for innovation of cyber supervision and strengthening the education of cyber fraud prevention.

2. Literature Review

2.1 The concept of cyber fraud

From "guess who I am" to "ask for a son with a lot of money", from "pretending to be a public security law" to "pretending to be a white rich beauty", the crime of cyber fraud has become a social public hazard that seriously affects the legitimate rights and interests of the people and destroys the social harmony and stability. The Supreme People's court, the Supreme People's Procuratorate and the Ministry of public security have unified law enforcement standards to further clarify the legal standards of cyber fraud. In December 2016, in accordance with the provisions of the criminal law and relevant judicial interpretations, the opinions on Several Issues concerning the application of laws in handling criminal cases such as cyber fraud were jointly formulated and promulgated. In the opinions, it was pointed out that cyber fraud is a long-distance non-contact criminal activity implemented by using communication tools, the Internet and other technical means, which seriously infringes upon the safety of people's property and other cooperation Legal interest (Supreme People's Court,2016).

At present, the academic circles generally regard cyber fraud as a new type of fraud by using modern cyber information technology, and its essence is still fraud crime (Zhang Xinbao,2016). Like other fraud, the basic structure of cyber fraud is also: the perpetrator commits fraud - the victim falls into or strengthens the cognitive error - the victim disposes (delivers) the property based on the cognitive error - the perpetrator obtains or causes the third party to obtain the property - the victim suffers losses (Zhang Mingkai,2005). Scholars Hu Xiangyang, Liu Xiangwei, and Peng Wei pointed out that the crime of telecommunication fraud refers to the criminal act of fabricating facts or concealing the truth, sending fraud information by means of modern communication technology, swindling large amount of public and private property, and shouldering criminal legal responsibility (Hu Xiangyang,2010). Zhao Lianqing believes that the cyber fraud refers to the criminal behavior that the illegal elements make up false information, set up a fraud, and implement remote non-contact deception to the victims by means of sending SMS, making phone calls, embedding Trojan horses and other means, so that the victims can make payments or transfers to the crime points (Zhao Lianqing,2017). Jiao Yanpeng, a scholar, from the perspective of technology application, puts forward that the cross use of telecommunication and network technology is involved in the process of cyber fraud. Exploring the concept of cyber fraud should also explain the concept of telecommunication fraud and network fraud (Jiao Yanpeng,2017). She pointed out that telecommunication fraud is a remote non-contact fraud against the victims through the network, SMS and telephone. The network fraud uses the network technology to make up the fact in the network space, and the behavior of non-contact swindling public and private finance. They can't be distinguished simply, but they are both important factors threatening the security of cyber space.

Although the above scholars have different opinions on the concept of cyber fraud, they all emphasize some conceptual characteristics of cyber fraud: first, they all reflect the essence of cyber fraud as a crime of fraud; second, they all reflect that the implementation basis of cyber fraud is modern cyber communication technology. The difference of the above scholars lies in the use of tools and the specific description of tool behavior. Therefore, based on the above academic and criminal views, this paper defines cyber fraud as a new type of fraud crime, which takes illegal possession as the subjective purpose, objectively uses the method of fabricating facts or concealing the truth, uses modern communication network technology to send fraud information and swindles a large amount of public and private property.

2.2 Organized cyber fraud

In recent years, some lawbreakers have formed groups of many people, set up dens, carefully designed scams, and jointly carried out organized cyber fraud crimes with high incidence. Li Ruiyi, vice president of the Supreme People's court, pointed out that the majority of organized cyber fraud cases are joint crimes and gang crimes, with clear division of labor and high degree of specialization. In some areas, there is even a trend of regionalization of cyber fraud (People's daily,2016), such as "Jiangxi heavy money fraud village", "Guangxi Binyang QQ fraud village", etc.

Starting from the most broad sense of organized crime, Chinese academic circles point out that organized crime includes loose criminal groups, criminal groups and criminal organizations with the nature of underworld (Zhao Bingzhi,1999). Based on the conclusion of this study, some scholars put forward that the cyber fraud is a kind of organized and group crime. The internal division of labor within the fraud group is meticulous, and the fraud members are managed in an enterprise way (Zhang Xinbao,2016). Based on the social practice background, many experts put forward that there are two types of cyber fraud: one is the incidental fraud crime with a large number of participants, which is formed by the aggregation of specific groups; the other is the fraud crime with clear division of labor and strict organization (Chen Jialin,2017). Some experts pointed out that the cyber fraud is mainly committed in partnership between the same village or friends, and the organizational form is relatively loose (Tie Yake,2017). It can be seen from the literature review that at present, the organized cyber fraud is mainly divided into two types: one is the group crime with strict organizational form, which generally has a large number of criminal groups, with detailed division of fraud, and has formed strict rules and regulations for the management of members within the group. For example, it is reported by many hot news that "151 people of Taiwan fraud organization cheat the so-called notarial property in the name of suspected illegal articles by posing as Public Security Bureau and Inspection Institute abroad". One is a relatively loose form of organization of gang crime, the members of the gang are not completely fixed, there is no strict discipline. For example, on March 4, 2016, the Supreme People's Court issued a typical case of cyber fraud: "a fraud case in which yangdaji, Danzhou City, Hainan Province, set up a false airline ticket website with many people and arranged a telephone operator to trick the victim into transferring money" (Supreme People's court,2016). Through cooperation with their families, the scam Gang purchases the source code of false websites, constructs scam websites and pretends to be website customer service to commit fraud.

Since the emergence of group cyber fraud, it has been highly valued by the academic and regulatory circles. However, with the rapid development of the gray industry chain, small fraud gangs are rapidly linked, not only directly carrying out the crime of cyber fraud, but also forming upstream and downstream related crimes around cyber fraud, such as illegal use of "pseudo base station", "black broadcast" equipment, illegal acquisition, sale, provision of personal information of citizens, help transfer of fraud proceeds (Supreme People's Court,2016), which has become Key targets of the regulatory authorities. According to the data of cyber fraud in 2016 judicial big data special report released by the Supreme People's court, 88.92% of China's cyber fraud cases are committed by less than 5 people, and 8.6% by 5-10 people. Small scale fraud gangs have become the key subject threatening the security of cyber space (Chu Xuehua,2016).

Based on this, this paper defines the group type cyber fraud as the following: small-scale criminals form fraud groups, take illegal possession as the purpose, cooperate in division of labor, and jointly implement the organized and large-scale cyber fraud.

3. Data Collection

Based on the court judgment in 2014-2016 published on the no litigation website,which has the most complete resource for legal documents,the most convenient and intelligent to query, we selected the judgment with serious plots and huge amounts of fraud to collect randomly, and obtained a total of 2800 court judgments related to organized cyber fraud, as shown in Appendix C.

The steps to obtain the court's judgment of organized cyber fraud are as follows:First, the crime is committed as a crime of fraud, credit card fraud, and the crime of helping information network criminal activities. The form of the crime is a joint crime, For the court's judgment with more serious criminal circumstances, the keyword combination with the ruling time of 2014-2017 is searched on the website of no litigation; then, the collected court judgments were screened.There are three screening principles: one is to eliminate the court judgment that does not conform to the cyber fraud; the other is to select the judgment that describes the fraud process in detail; the third is to select the judgment with more than 2000 words, with a maximum of 10488 words. According to the above principles, the collected judgments were manually screened, and finally 1982 judgments were retained.

4. Word frequency analysis of key nodes

4.1 Word frequency analysis of influencing factors of motivational behavior

Motivation is the core category node, and its corresponding main category node, category node, concept node and label node are shown in Figure 1 below:

Motivation is the inner cause or ideological activity that stimulates and encourages fraudsters to commit criminal acts. It indicates the psychological reasons on which fraudsters commit criminal acts, so the role of motivation is to trigger criminal acts. Motivation can explain the significance of criminal behavior to the fraudster's psychological desire. The previous coding research found that the generation of fraudsters' motives is influenced by many factors. This paper analyzes the coding nodes from three aspects: macro social environment factors, fraudsters' psychological characteristics and fraudsters' demographic characteristics. Since this article is a statistical analysis of label nodes, in the motivation generation stage, this article mainly conducts statistical analysis around the word frequency of its label nodes.

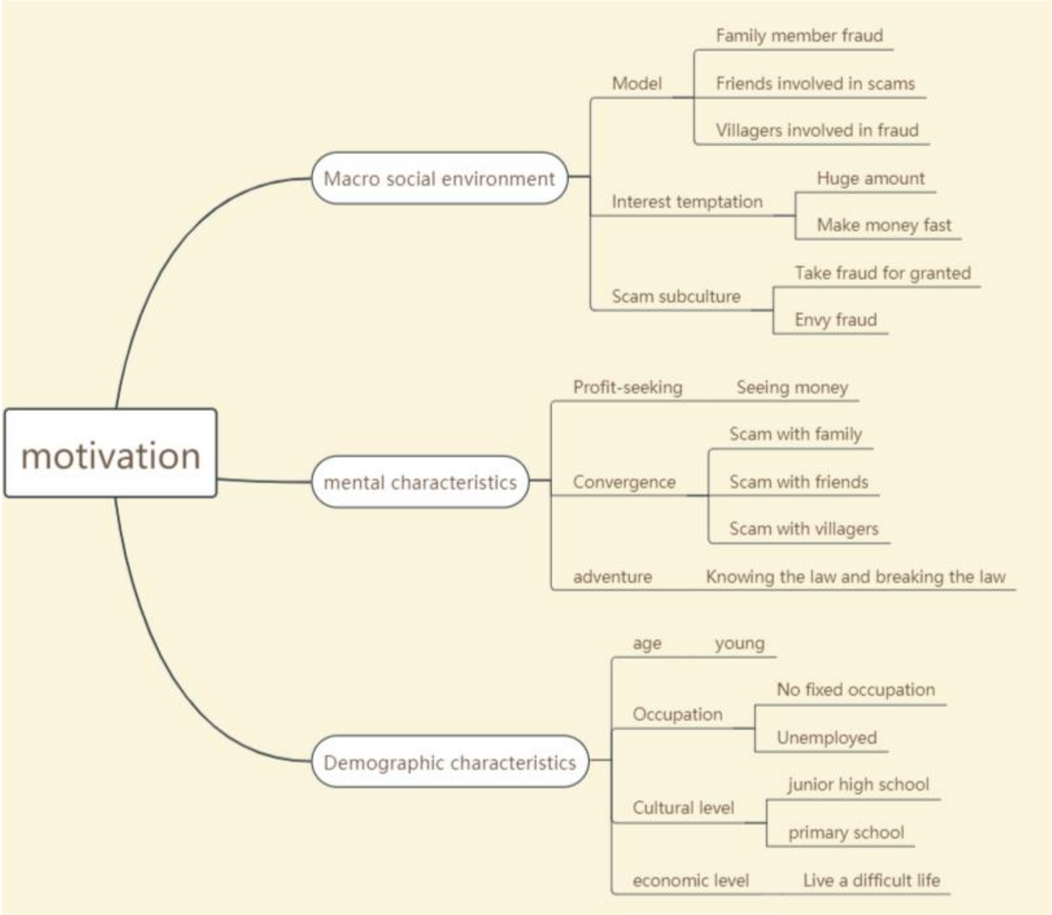

Fig. 1 Diagram of influencing factors at the stage of "Motivation Generation"

4.1.1 Macro social environment

This article makes the following statistical analysis on the label nodes in the macro social environment, as shown in Figure 2.

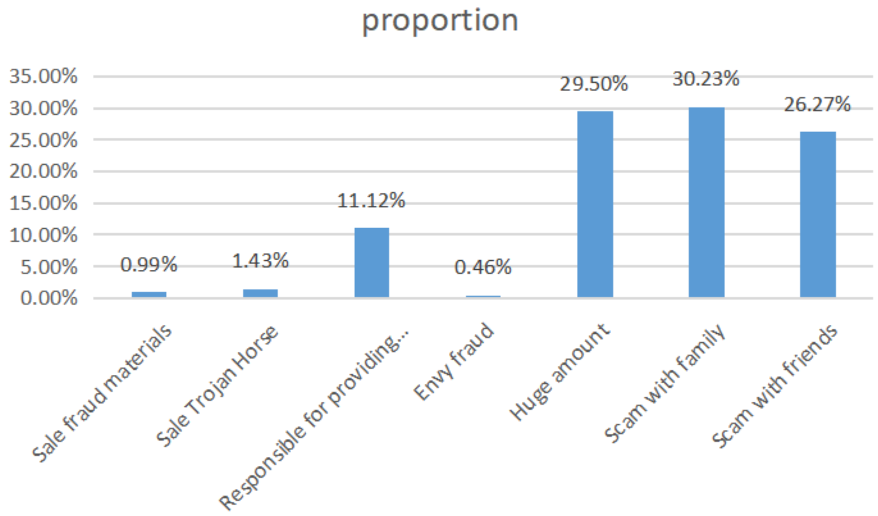

Fig. 2 Distribution of macro social environmental factors

It can be seen from the figure that in the external environment where the fraudsters are located, family members and friends participate in fraud the highest proportion, accounting for 26.66% and 30.68% of the total, respectively. This shows that the fraudsters are mainly affected by the role model information in the external environment and family environment and social environment. In addition, the huge amount of factors in the macro-social environment and other factors affecting interest temptation information reached 29.95%, which has an important impact on fraudsters. The scam subculture has a relatively low proportion of tag nodes, and the two tag nodes that are accustomed to fraud and envious of fraudsters account for 0.79% and 0.46%, respectively. Therefore, this article explains the two most important influencing factors of family member fraud and friend involvement in fraud, and puts forward policy recommendations in a targeted manner.

First, there are fraudsters in the family environment where the fraudsters live, and there are fraudsters among the social objects of the fraudsters. This paper analyzes the actual cases and finds that most fraudsters are motivated by the existence of criminal precedents among family relatives. Living in a family environment with criminal precedents for a long time is more likely to spawn potential offenders. According to the statistics of the Federal Bureau of Investigation, more than 70% of the offenders have at least one relative who has a criminal record.

Second, there are fraudsters among the fraudsters' social objects. Secondly, according to statistics, it is found that the fraudsters engaged in cyber fraud are mainly young people, and some fraudsters have been involved in scam activities since the youth stage. The unfavorable family environment and dating environment have a negative impact in the early stages of the formation of their values, which directly led to The emergence of their criminal personality. With the repeated impact of poor external demonstrations on potential fraudsters, whether it is repeated crimes by fraudsters, the number of fraudsters increased, or only repeated references by surrounding relatives and friends, they will be used as psychological hints to further stimulate the formation of their criminal motives and form malignancy. cycle.

Therefore, in view of the above statistical analysis results, this article puts forward policy recommendations from the following two aspects: one is to strengthen the disclosure of fraud crimes to stimulate the fraudsters to abide by the law and fear law; the second is to purify the social environment and reduce the negative information of the fraud model information Induction.

4.1.2 Personal characteristics of fraudsters

This article makes the following statistical analysis of the fraudsters' psychological characteristics of the tag node, see Figure 3.

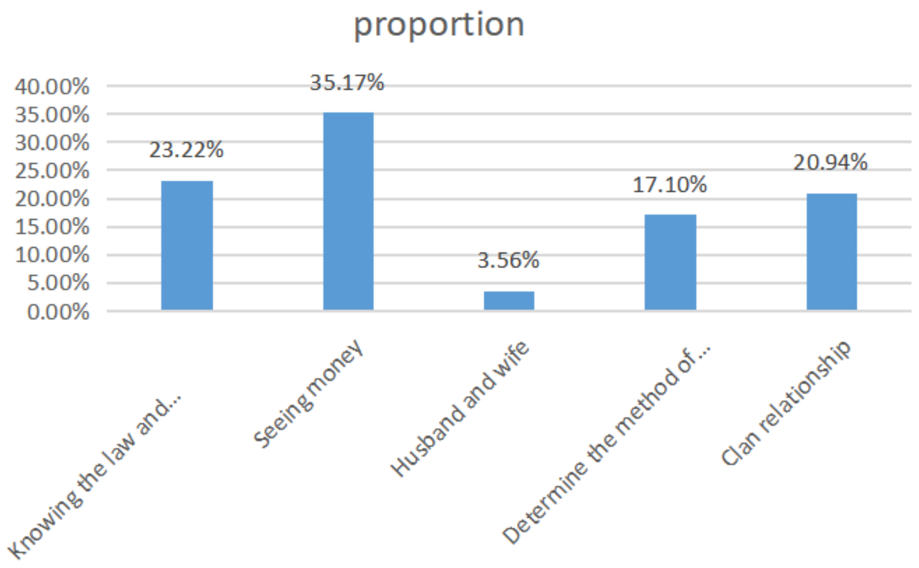

Fig. 3 Distribution of scammers' psychological characteristics

It can be seen from the picture that the fraudsters' profit-seeking intention is to gain profits, to follow others to swindle to converge, and to know the law and commit the law to take risks. Therefore, the regulatory department needs to strengthen the construction of citizens' legal consciousness and create a society that knows and abides by the law Atmosphere.

4.1.3 Demographic characteristics of fraudsters

In this paper, the following statistical analysis is performed on the label nodes of the scam demographic characteristics, as shown in Figure 4.

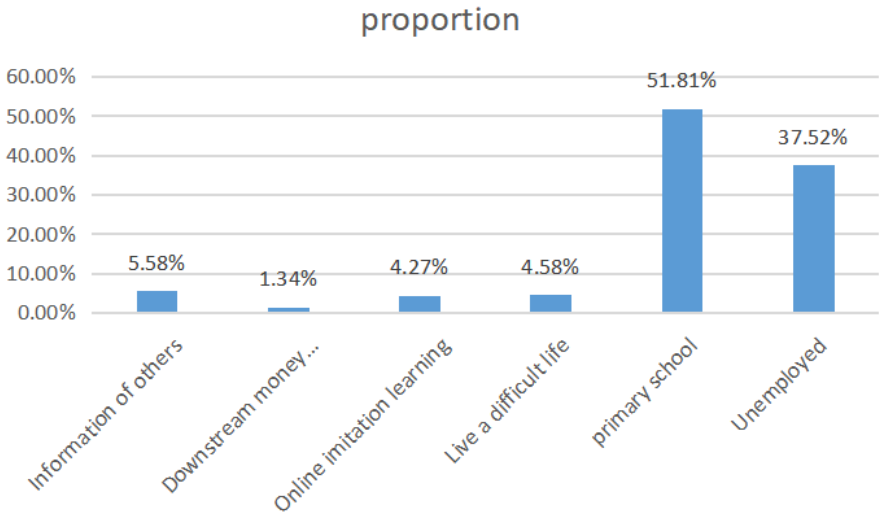

Fig. 4 Distribution of scam demographic characteristics

It can be seen from the figure that the education level of fraudsters is elementary school culture, which is the level of fraudsters' general education, accounting for 51.81%. The fraudster's occupational status is unemployed, accounting for 37.52%. It can be seen from the summary of the cases involved in the judgment that most of the fraudsters in the cyber are elementary or junior high school. The low education level leads to the low competitiveness of this group of people and the difficulty in obtaining job opportunities. Therefore, long-term job hunting and no income are becoming more obvious. Difficulties are more likely to stimulate the emergence of risk-taking psychology, such as "I haven't finished my primary school, I can't find a good job, and I soon started to scam with the same village when I saw the money coming from fraud." American criminologist Cohen proposed that crime subculture and social structure are closely linked. The mainstream value system is a culture suitable for the middle class. Self-satisfaction at the material and spiritual levels can effectively suppress the generation of criminal motives. However, the difficulties in life cause most potential fraudsters to be in the lower social class, lacking the conditions and ways to achieve self-pursuit, leading them to be in a disadvantageous position in the formal social structure, and forming a psychological reaction. This will inevitably conflict with the norms. Therefore, in addition to making individuals more prone to profit-seeking psychology, life difficulties will also exacerbate the directional influence of criminal motivation on individual behavior to a certain extent.

Low education level also makes this kind of people lack legal awareness due to lack of legal knowledge, which reduces their fear of the consequences after crime, resulting in a reduction in their resistance to the temptation of economic and other interests, and the fear of psychological influence is inactive Containment, the influence of the psychology of profit-seeking and the psychology of convergence are amplified, further stimulating the generation of criminal motives. Therefore, this article puts forward the following policy recommendations from the following two aspects: one is to increase the education of various groups of society; the second is to provide social employment opportunities widely.

4.1.4 Statistical analysis of all influencing factors

Finally, in this paper, the statistical analysis and descending order of the proportion of all influencing factors in the motivation generation stage are carried out. The specific information is shown in Figure 5.

It can be seen from Figure 5 that most of the fraudsters are elementary school culture, accounting for 14.56%. There are fraudsters in the fraudsters' households, and 12.45% of the cases are affected by external demonstration information. The temptation information fraud with huge fraud gains is 12.15%. The second is the profit-seeking psychology that arises from seeing the money, the role model demonstration information formed by friends participating in fraud, and the demographic characteristics of unemployed. According to the node hierarchy diagram in Figure 1, this paper summarizes the label nodes corresponding to the category nodes, and finally obtains the macro social environment, the demographic characteristics of the fraudsters and the psychological characteristics of the fraudsters: 40.37%, 28.17% and 31.46%, respectively. It can be seen from this that the macro social environment has the most significant impact on the fraudsters' motives. Therefore, from the macro level, the regulatory department needs to start from purifying the social environment, and actively and clearly start with demonstration and inducement information to avoid the negative impact of adverse temptation information.

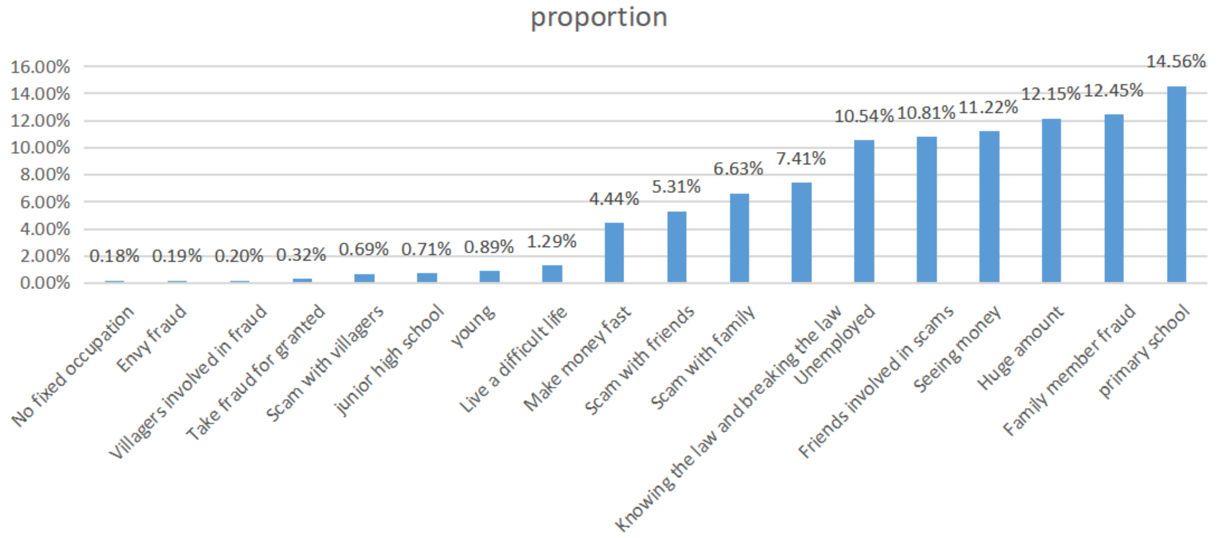

Fig. 5 Distribution of all motivation and Influence factors

4.2 Word Frequency Analysis of Influencing Factors of Gang Organizational Behavior

The gang organization is the core category node of this article. Its core links, influencing factors, and the label nodes corresponding to influencing factors are shown in Figure 6 below:

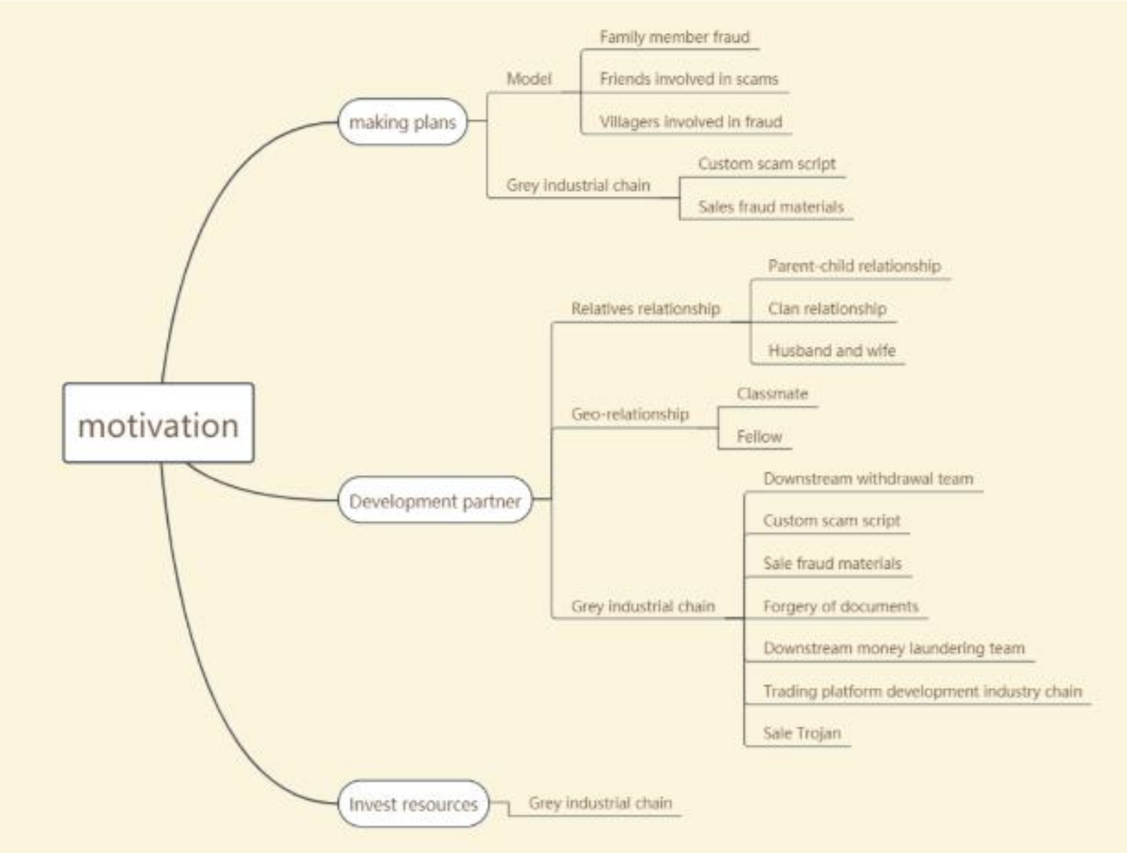

Fig. 6 Diagram of influencing factors in the "gang organization" stage

It can be seen from Figure 6 that there are few influencing factors in the gang organization stage of this article, and they will recur in some links. Therefore, this article takes a statistical analysis of all influencing factors and obtains the following results, see Figure 7.

It can be seen from Figure 7 that the existence of fraudsters in the life environment of fraudsters is the most important influencing factor for the organization of fraudsters. The fraudsters who are mainly in the family can share information such as scam experience exchange and scam skill exchange, which has an important impact on the environment of the framing gang to make plans, which in turn affects the organization behavior of the gang. Second, clan relations are the third influential factor. This influencing factor mainly affects the development of members of fraudulent groups in the organized cyber fraud behavior model constructed above. Therefore, this article proposes that the clan relationship of the fraudsters is the main influencing factor for the fraudsters to construct gangs. Third, the proportion of the downstream withdrawal industry chain is also relatively high at 14.57%, which also reflects that organized cyber fraud entities mainly cooperate with the outside world to establish the task of outsourcing withdrawals.

Therefore, based on the above analysis, this article finds that family-related scams, professional and chained cooperation between gangs are becoming the main form of organized cyber fraud, so the supervisory department can combat and prevent from the following two directions: The construction of patriarchal culture avoids the fraud of gang members; the second is to strengthen the crackdown on fraud-related crimes in cybers and avoid the establishment of professional cooperation among gangs.

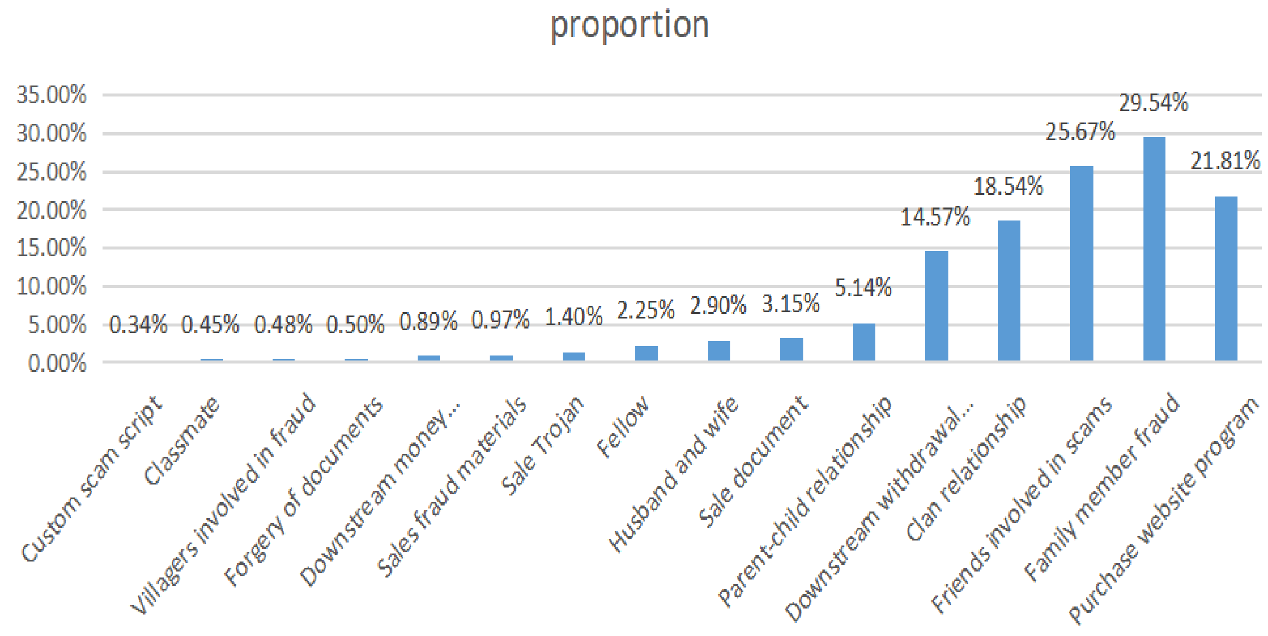

Fig. 7 Distribution of influence factors of gang organizations

4.3 Word Frequency Analysis of Influencing Factors of Gang Organizational Behavior

According to the organized cyber fraud behavior process model constructed above, the organizational behavior elements of organized cyber fraud mainly include planning, development of associates, task division, resource investment and fraud learning, so this article selects some of the nodes for statistical analysis To explore the organizational behavior characteristics of gang-style cyber fraud.

4.3.1 Planning process

In this paper, the relevant label nodes of the plan are studied, and the formula and content distribution are shown in Figure 8.

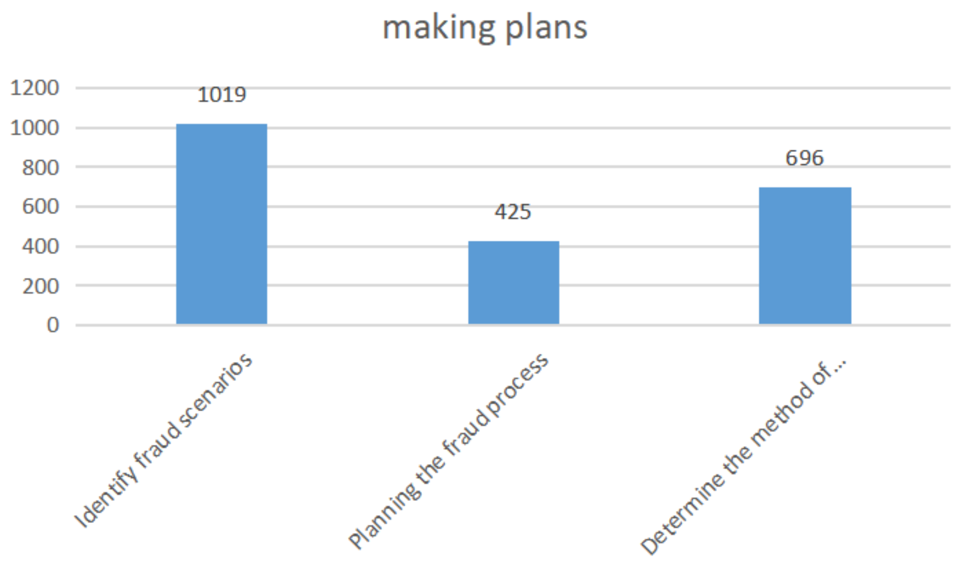

Fig. 8 Planning distribution

From the statistical analysis results (Figure 8) of the plan, we can see that the fraud gangs pay attention to the selection of fraud methods before implementing the fraud, such as fraud through QQ and WeChat. The setting of the fraud scene is mainly to determine the target of the fraud in order to implement more precise fraud. For example, for the marriage network users and lottery network customers, the different fraud scenarios will determine the specific fraud implementation method. It can be seen from this that gang-style frauds are premeditated, non-impulsive crimes. The gang is more concerned about the fraud methods and target scenes, and is more careful about the second plan. The plan for the fraud process is significantly weaker than the above two, because in the current organized telecommunications fraud, there are "scripts" for different fraud scenarios and fraud methods, the implementation process is similar, and the gang itself is more learning about the fraud process Instead of making.

4.3.2 Development partners

According to the behavioral process model constructed in this article, the way of organized cyber fraud to develop associates is mainly to develop individual fraud and establish external cooperation. First, the statistical analysis results related to the development of fraud individuals are shown in Figure 9.

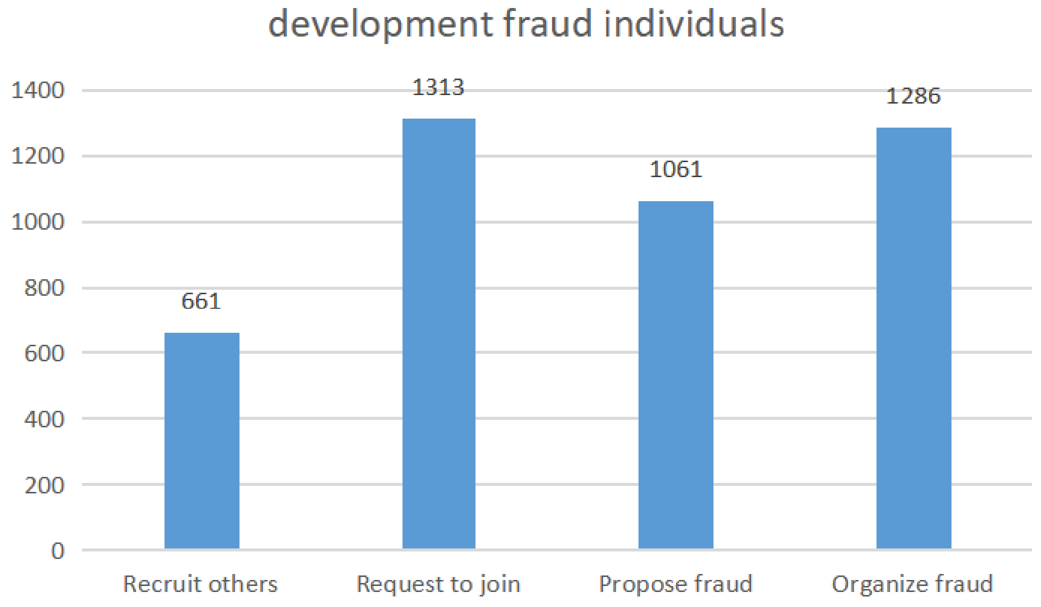

Fig. 9 Distribution of development fraud individuals

It can be seen from Figure 9 that in the development of associates, the number of active joining gangs occurred the most, reaching 1313 times. Through the analysis of the verdict, it is found that there are social relations between members of the gang due to fraud, such as family members, friends, classmates, etc. In the motivation section, the impact of the adverse social environment on fraud motives has been explained. Most of these members are active fraud rather than passive. Therefore, after the organizer appears, more members join the group spontaneously. In the second place, the occurrence of 1286 frauds of other people shows that the construction of fraud gangs first needs to clarify the organizer. The person who undertakes the function of the organization is not necessarily a single individual, but according to the size of the gang and the specific division of labor. Organizers. For example, "I contacted Wang X after deciding to scam, and told him the initial idea, and then the two of us will find someone to join." It can be seen that the organizer of the gang usually refers to the earliest contact, and according to the specific There may be multiple organizers for the difference in fraud, and the organizer has a very important role in determining the specific mode of the entire fraud.

Secondly, when establishing external cooperation, the results of statistical analysis in this paper are shown in Figure 10.

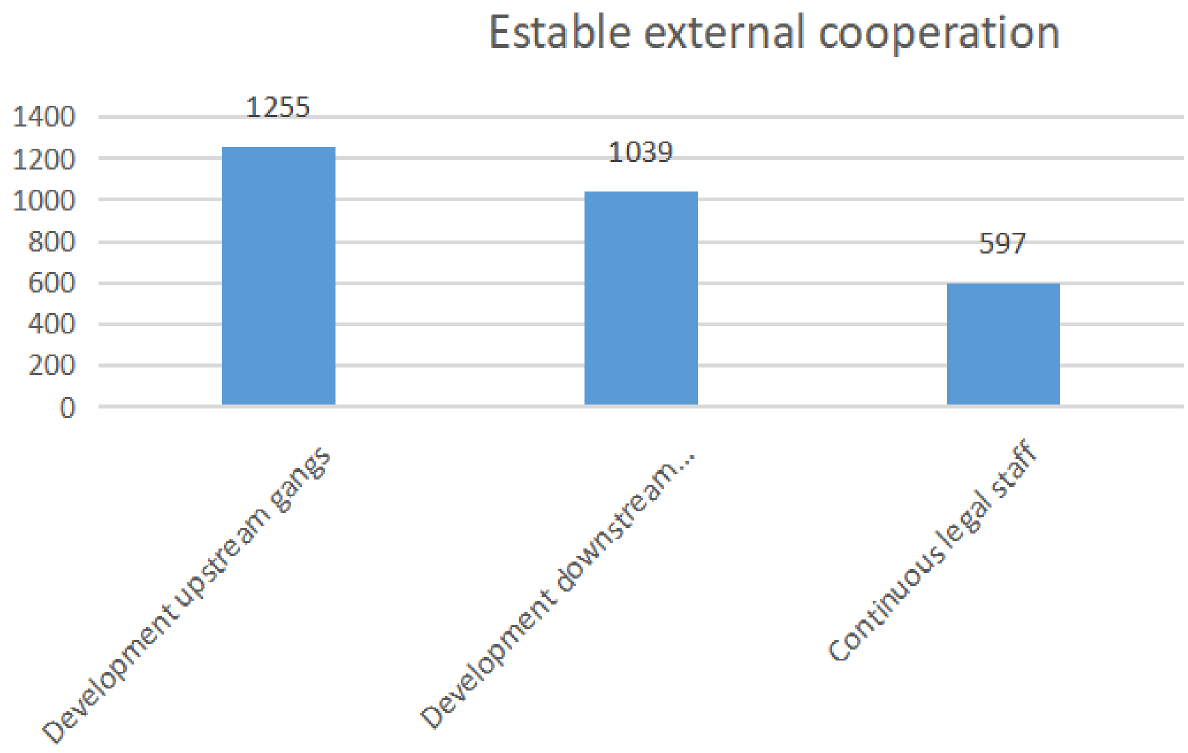

Fig. 10 Establishing external cooperation distribution

Part of the results of establishing external cooperation are shown in Figure 10. In this study, external cooperation refers to the existing gangs and individuals who have undertaken self-constructed fraudulent gangs and cannot assume their functions. Such personnel may be professional offenders or Fraud is an individual who has other jobs as a "sideline". Therefore, this part has three characteristic words; contact upstream gangs, develop downstream gangs, and contact legal staff.

Among them, the development upstream gang appeared the most, 1255 times. In the actual gang construction, due to the influence of technical level and cost, it is difficult for core members of the gang to complete complete resource preparation, such as website construction. Therefore, in order to ensure the smooth implementation of the fraud, most gangs will directly contact the gangs or individuals that provide the required services and outsource this link directly to the gangs and individuals. Forgery of documents, etc.

The development of downstream gangs in this article refers to the fact that some gangs will contact others to withdraw money in order to reduce risk after fraud. The specific functions of legal employees may be in any link depending on the method of fraud and gang, so they are independently proposed. Upstream and downstream gangs and gangs that carry out fraud activities together constitute a gray industrial chain of fraud.

4.3.3 Fraud learning

Fraud learning is the key process for fraudsters to acquire scam skills and adjust their scam psychology and attitudes. Only by learning the fraudsters can they successfully commit fraud crimes. Based on the high-frequency tag nodes identified in the previous article, this article makes a statistical analysis of the method and content of fraud learning. This article mainly conducts statistical analysis from two aspects of learning method and learning content according to the structure of the organized cyber fraud behavior process model. The specific information is shown in Figures 11 and 12.

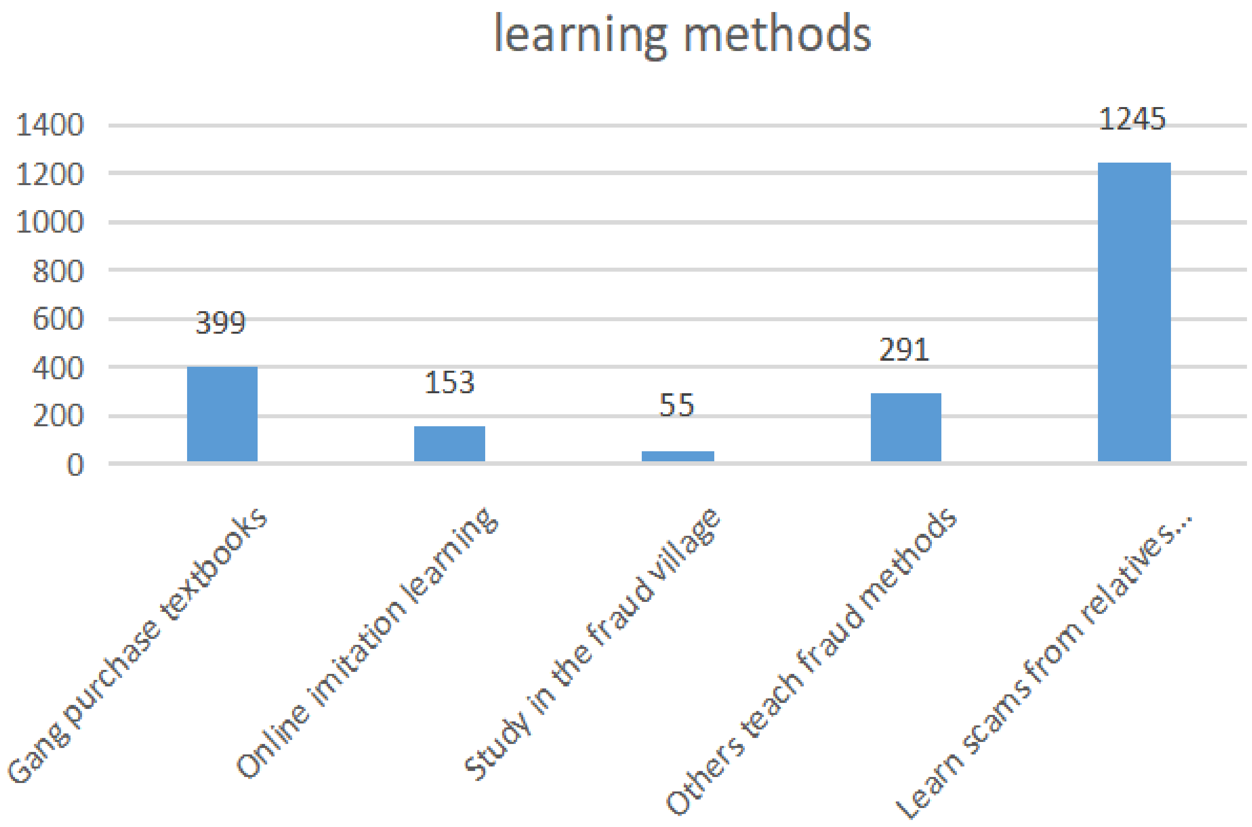

Fig. 11 Distribution of learning methods

In the way of learning about fraud. As shown in Figure 11, the number of fraudulent learning by purchasing textbook training is the largest. At present, many fraud gangs will train or teach fraud associates based on the purchased fraud tutorials, scripts, such as "Wang Moumou did not know where to get a tutorial to guide us how to answer the victim's questions." The second is to learn fraud from relatives and friends, a total of 1245 times. In the development gang, family members are an important part of gang-style cyber fraud, and the resulting mutual fraud learning among loved ones will definitely become a higher number of learning methods. The third is that online imitative learning, self-exploration learning, fraudulent behaviors taught by others, and methods of sharing fraud by others are the lower ones among all learning methods.

On the learning content of fraud. As shown in Figure 12, most of the learning within the fraud gang focuses on stock manipulation knowledge, fraud process learning, website construction knowledge learning and website operation knowledge learning. It can be seen that the content of fraud learning is mainly concentrated on the improvement of fraud skills. The highest proportion of website construction knowledge learning shows that the use of fake website transactions is the focus of current organized cyber fraud. The regulatory authorities should strengthen the examination and ban of illegal and forged websites.

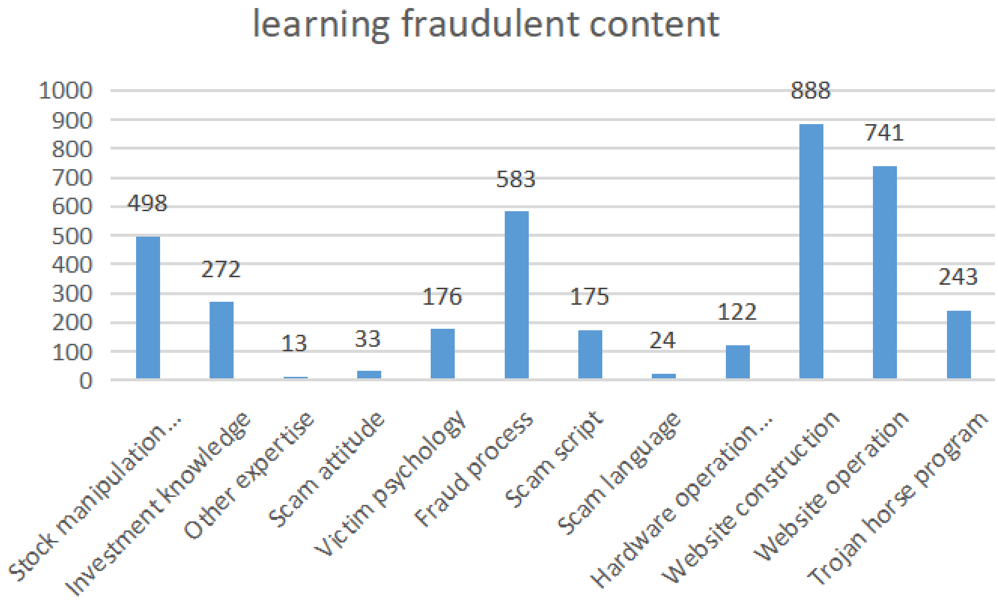

Fig. 12 Distribution of learning fraudulent content

5. Summary

In order to further explore the organized cyber fraud constructed in this paper, this article selects text mining research methods to quantify the core stages of organized cyber fraud: motivation generation and gang organization, and conducts part of the behavior verification analysis. First of all, Wu litigation network randomly collected more than 2000 expected data of court judgments for text mining; secondly, the research team members based on the "motivation" and "gang organization" key stages of the organized cyber fraud behavior model constructed above The coding node extracts the minimum coding constructs of the key links of “motivation generation” and “gang organization”—keywords related to the label nodes, and constructs a keyword library; finally, using PYTHON coding analysis, the frequency of the label nodes is extracted, thereby Perform statistical analysis on key links. The research results show that: Motivation generation links, external factors are the leading factors for fraudsters to generate motives, and they should be focused on; gang building links, gray industrial chain provides important support for fraud gangs to establish cooperation and invest resources; fraud learning links, fraudsters Purchasing teaching materials for gang training is the most important way to improve gang's criminal ability.

References

[1] Legal network. Supreme law: in 2016, cyber fraud increased by 51.47% year on year. (2017-06-24) http://news.china.com.cn/rollnews/news/live/2017-04/13/content_ 38087789.htm.

[2] Tencent security. Big data report on anti cyber fraud in the first quarter of 2017 (2017-05-12) http://www.sohu.com/a/139984223_ three hundred and ninety-four thousand five hundred and seventy-seven

[3] Xinhua news agency. The loss amount of cyber fraud in the second quarter increased by 47.5% month on month (2017-08-04) http://jjckb.xinhuanet.com/2017-08/04/c_ 136499865.htm

[4] Tencent. Tencent's "Guardian plan" released the third quarter big data report on anti cyber fraud (2017-11-13) http://tech.qq.com/a/20171113/018584.htm

[5] Tencent. Tencent Guardian plan: big data report on anti cyber fraud in the fourth quarter of 2017. (2018-02-07) https://baijiahao.baidu.com/s?id=1591707531972698312&amp;wfr= spider&amp; for=pc.

[6] Snyder P, Kanich C. No Please, After You: Detecting Fraud in Affiliate Marketing Networks// Proceedings of the Workshop on the Economics of Information Security (WEIS). 2015.

[7] Supreme People's Procuratorate. Full text of the report of the 19th National Congress (October 18, 2017) http://www.spp.gov.cn/tt/201710/t20171018_ 202773.shtml

[8] The six departments of the Supreme People's Procuratorate of the people's Republic of China jointly issued the notice on preventing and combating the crime of cyber fraud (2016-09-24) http://www.spp.gov.cn/zdgz/201609/t20160924_167801.shtml

[9] 360 online hunting platform. 2016 Research Report on online fraud trend (2017-01-08) http://bbs.360.cn/thread-14788950-1-1.html

[10] Hu Xiangyang, Liu Xiangwei, Peng Wei. Research on prevention and control measures of Telecom fraud. Journal of the people's Public Security University of China (SOCIAL SCIENCES EDITION), 2010,26 (05): 90-98

[11] Diamond B, Bachmann M. Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. International Journal of Cyber Criminology, 2015, 9(1): 24-34.

[12] Jaishankar K. Space transition theory of cyber crimes. Crimes of the Internet, 2008: 283-301.

[13] Nash R, Bouchard M, Malm A. Investing in people: The role of social networks in the diffusion of a large-scale fraud. Social networks, 2013, 35(4): 686-698.

[14] Opinions of the Supreme People's Court on Several Issues concerning the application of law in handling criminal cases such as cyber fraud (2016-12-20) http://www.court.gov.cn/fabu-xiangqing-33361.html.

[15] Zhang Xinbao, Ge Xin. Research on comprehensive governance of Telecom fraud based on personal information protection. Journal of the Party School of the CPC Central Committee, 2016, 20 (5): 42-49.

[16] Zhang Mingkai. On property loss in the crime of fraud. Chinese law, 2005 (5): 118-137.

[17] Hu Xiangyang, Liu Xiangwei, Peng Wei. Research on prevention and control measures of Telecom fraud. Journal of the people's Public Security University of China (SOCIAL SCIENCES EDITION), 2010,26 (05): 9.

[18] Zhao Lianqing. Criminal law protection of citizens' personal information security: from the perspective of frequent cases of cyber fraud. Learning and exploration, 2017 (9): 80-84.

[19] Jiao Yanpeng, Yang Hongmei. An Empirical Study on the criminal justice pattern of online fraud crime -- with 389 effective criminal judgments as the analysis object. Journal of Gansu University of political science and law, 2017 (4): 91-102.

[20] People's daily.com. Why do all kinds of network fraud succeed repeatedly? (2016-03-21) http://tech.china.com.cn/it/20160321/223185.shtml.

[21] Zhao Bingzhi, Yu Zhigang. On the punishment of organized crime in China's new criminal code. Law and business research (Journal of Central South University of political science and law), 1999 (01): 27-33.

[22] Chen Jialin, Wang Xuecheng. The evaluation dilemma and criminal law adjustment of the criminal responsibility of the crime of network fraud -- Based on 100 random cases. Politics and law, 2017 (3): 60-75.

[23] Tie Yake. Comprehensive governance of the rule of law in cyber fraud -- Taking the governance experience of Danzhou City in Hainan Province as an example. People's rule of law, 2017 (3): 68-74.

[24] Supreme People's court. Typical cases of cyber fraud (2016-03-04) http://www.court.gov.cn/zixun-xiangqing-17152.html.

[25] Chu Xuehua. Study on the punishment and prevention of the crime of telecommunication fraud -- Thoughts triggered by "Xu Yuyu incident". Journal of Jishou University: Social Sciences Edition, 2016 (S2): 81-83.