Research on the Training of Innovative Talents in Cyber Security and Law Enforcement Specialty under the Background of New Engineering and Technical Discipline

Jinqiang Ma
China People's Police University
Langfang, China

Junjing Tian
China People's Police University
Langfang, China

Yan Bi
China People's Police University
Langfang, China

Abstract—**Cyber security is closely related to the long-term stability of the country, economic development and people's happiness. In order to adapt to the development of information technology, police universities have established a new specialty of cyber security and law enforcement. In the context of new engineering and technical disciplines, this paper analyzes the demands of cyber security and law enforcement professionals guided by the needs of the network police professional position. Combining with the teaching characteristics in police universities and the construction requirements of new engineering and technical disciplines, as well as the needs of network police positions, this paper puts forward a set of perfect talent teaching system and mode which integrates teaching, learning, practice and training, and the mode is suitable for cyber security and law enforcement specialty, which can improve the training mechanism of cyber security talents in China's public security education. The teaching system and mode which is proposed in the paper focuses on the characteristics of public security, emphasizes practicality, adapts to multi-angle and multi-level network security work.**

Keywords—new engineering and technical discipline; cyber security and law enforcement; Innovative Talent; talent cultivation

I. INTRODUCTION

According to the "Statistical Report on the Development of China's Internet Network", the number of Internet users in China reached 829 million, and the Internet penetration rate was 59.6% by December 2018. With the rapid development of the Internet, Cyber security incidents occur frequently, and cybercrime has risen year by year. Xi Jinping emphasized that "without cyber security, there will be no national security." The foundation for building a powerful nation in the network field is human resources. Talent training is a key point in the network space security system under the background of increasingly prominent network security management requirements [1]. The quality and level of cyber security talents are important factors that influence cyber security.

According to the prescribed ratio of 10,000:1 for internet users and network police, China needs more than 80,000 cyber police. However, there are only 20,000 online police in China at present [2]. The network police are relatively scarce, so speeding up the training of talents of network security and law enforcement is extremely urgent.

II. THE DEMAND FOR CYBER SECURITY AND LAW ENFORCEMENT TALENTS

The Higher Education Department of the Ministry of Education proposed the "New Engineering and Technical Disciplines" construction route called "Tianda Action" in April 2017, which clarified the direction of engineering education and the planning of training the diversified and innovative engineering and scientific talents that the country urgently needs. The proposal of this plan is a major innovation in the history of higher education in China. According to the goal of "New Engineering and Technical Disciplines" planning, a new engineering construction model is established by 2020, and can adapt to new technologies, new industries, and new economic situations [3].

Social needs have accelerated specialty development. With the rapid development of "Internet plus" and big data applications, network security has become a necessary condition for maintaining national security, social security and economic security. Cybercrime continues to increase, and the security of the information faces severe pressures and challenges. The public security organization is responsible for the important tasks of network security and cybercrime investigation. How to maintain network security and combat cybercrime is an important task of the public security organization.

The Law of the People's Republic of China on Cyber Security was officially implemented on June 1, 2017, and the cyber security was promoted into a national security strategy in the form of law. The twentieth item in the law specifies that

the nation supports the enterprises and higher education schools, vocational schools and other education and training institutions to carry out network security-related education and training, train network security talents by various methods, and promote communication of the network security professionals. Therefore, the establishment of network security and law enforcement major in public security universities is not only the implementation of the overall national security, but also the needs of maintaining the cyber security. The establishment of the major can implement cyber security law and fulfill the duties of public security colleges. The network security and law enforcement specialty is highly relevant to other disciplines [4]. Therefore, in order to better cultivate talents who meet the requirements of cyber security, the specialty must not only take advantage of other subjects, but also highlight its characteristics in the process of cultivating talents.

At present, the widespread application of new technologies such as big data and artificial intelligence in the public security field has fundamentally changed the traditional case handling procedures, methods and technical means, and promoted the deep reformation of the traditional police mode. The public security department has developed new information systems such as the "Eye in the Sky" system and the DNA Library relying on the Golden Shield project. New applications such as face recognition, trajectory tracking, and real-time monitoring are becoming more and more popular [5]. New types of services such as cybercrime detection, network monitoring, online case handling, online intelligence gathering and analysis, and electronic data acquisition and identification are more widely spread. A new policing model led by information technology and supported by intelligence was established. New technologies, new applications and new models have put forward new requirements for the ability and quality of the public security professionals. Cultivating compound talents who are familiar with network security law enforcement procedures and master network investigation technology has become an urgent need to build a new type of public security team.

III. CHARACTERISTICS OF CYBER SECURITY AND LAW ENFORCEMENT SPECIALTY

The specialty of network security and law enforcement is an emerging major that belongs to public security technology. The Ministry of Education officially approved the establishment of the major of network security and law enforcement in the "Catalogue of Undergraduate Majors in General Colleges and Universities (2012)". The specialty code is 083108TK. The technology of network security law enforcement as a secondary discipline is built under the first-level discipline of the technology of public security. At present, more than ten police academies, such as the People's Public Security University of China, the China People's Police University, Criminal Investigation Police Academy of China, have set up specialties of network security and law enforcement. The major can adapt to the needs of network technology advancement, and study the technical laws of maintaining national security and social order in the information age.

The training of network security and law enforcement professionals has its own characteristics. First of all, the education of network security and law enforcement is not only related to national security, but also to sustainable education which involves national strategic and long-term planning. Secondly, the major of network security and law enforcement covers a wide range of knowledge, such as hardware, software, technology, management, principle and training. Having mastered the knowledge mentioned above, the students of the major can maintain the security of cyber and combat cybercrime. Thirdly, the knowledge about network security and law enforcement updates rapidly. With the emergence of new technologies, new security issues follow. There are many problems that cannot be solved simply by traditional methods, such as how to protect users' personal privacy in big data environment. Fourthly, the education of network security and law enforcement should pay attention to improve the application ability and practical level. Students should not only master the frontier theory, but also be able to solve the network security problems in reality.

IV. TRAINING OBJECTIVES OF CYBER SECURITY AND LAW ENFORCEMENT SPECIALTY

The training objective is the general requirement of designing and implementing teaching activities. The training goal of cyber security and law enforcement specialty is to train a large number of professional talents who can meet the requirements of professionalization and practicality of police work, and who are engaged in technical work in public security organizations and relevant departments. The students should have firm and correct political orientation, strict organizational discipline and good police professional ethics. They should grasp the characteristics of cyberspace technically, be familiar with computer network knowledge, and have excellent legal literacy and law enforcement business ability in professional literacy. The students should achieve the following levels when they graduate:

(1)Understand relevant laws and regulations, master the basic theories of policing work, law science, public security science, and the general requirements and policies of the national information technology and cyber security, and have the basic ability of network security work.

(2)Master the professional theories and business knowledge about network security supervision, cybercrime investigation and evidence collection, electronic data analysis and identification, and have the ability to collect the Internet intelligence information, combating cybercrime activities, and supervising the security of important information system.

(3)Have strong computer operation skills and the ability to understand and analyze new technologies about network security.

The major of cyber security and law enforcement trains students to prevent and combat cyberspace crimes, safeguard and maintain the order of virtual society, and improve the ability of law enforcement agencies to deal with cyberspace enforcement and manage the virtual society. The major of cyber security and law enforcement is a comprehensive subject, which integrates computer science and technology,

law science, sociology, public security science and other subjects. In addition, the students in the major should master the knowledge about network investigation and digital forensics in the discipline of public security, as well as the network intelligence and network supervision. The curriculum system of this major is shown in Fig. 1.
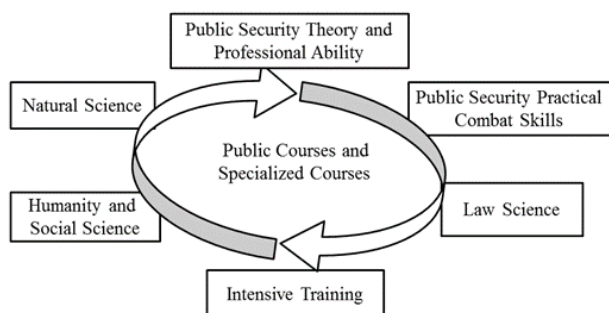

Fig.1. The curriculum system of cyber security and law enforcement

V. THE CONSTRUCTION OF THE TRAINING MODEL OF PROFESSIONAL TALENTS

The task of cyber security and law enforcement specialty is to train network policemen who have the ability to fight, prevent, manage and control all kinds of illegal and criminal activities on the Internet. The teachers should combine practical cases, explain practical knowledge, and pursue higher education efficiency in the teaching process. In order to improve the core competence of the students in their posts in the future, the teachers should follow the mainline of "thinking ability formed by theory teaching- professional skill formed by practice teaching- management ability formed by daily exercise- development ability formed by post exercising", strengthen the mechanism of multidimensional education, and combine the curriculum process, design process, practice and special training. Knowledge imparting, practical strengthening and value shaping are integrated into the teaching process, and an integrated training mode of teaching, learning, training and action is constructed, as shown in Fig. 2.
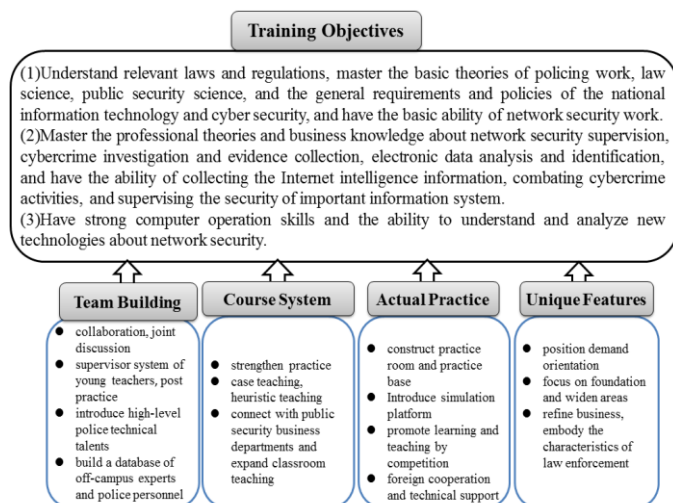

Fig.2. Integrated training mode of Cyber Security and Law Enforcement Specialty

A. Building a faculty with working knowledge and rich practical experience.

The construction of the teaching staff is the primary step in the cultivation of talents. The construction of the teaching staff can embody professional characteristics and show professional strength. According to the training requirements of the major of cyber security and law enforcement, it is necessary to do a good job in the construction of teaching staff from the following aspects in order to cultivate students with strong professional practice ability:

Firstly, according to the requirements of training objectives, we should do a good job in the construction of teacher team. The specialty of cyber security and law enforcement sets up four teaching teams that mainly focus on the basic network technology, network combat and network crime investigation, electronic forensics technology and public opinion control. Team leaders are set up in the teaching team. Team members insist on preparing lessons, attending lessons and evaluating lessons collectively. In addition, Teacher training plans are well planned with the teaching team as the basic unit. Research and teaching seminars are carried out on the hot and difficult points in the work of public security.

Secondly, the teachers are encouraged to go to the front line for practical training. On the one hand, the teachers directly participate in network security monitoring, investigation and case handling through case tracking and dynamic practice, and improve the ability to apply professional skills. On the other hand, the teachers can participate in police practice by electronic forensics, remote network support or remote interactive platform in the university.

Thirdly, the database of experts and police personnel with rich practical experience should be established to make full use of the outside forces. The teachers of the major should strengthen exchanges and cooperation with research institutes, judicial authentication institutions, network security products companies and public security research institutes, invite network security experts, scholars, famous masters and the elite of network security department to give a lecture during the school's academic activities week. In addition, the teachers can take advantage of the project of industry, education and research proposed by the ministry of education to cooperate with each other to develop professional courses, design training topics, and innovative practical teaching systems.

B. Constructing the open and multi-cooperative courses and teaching system for the major of cyber security and law enforcement

In the teaching process of this major, the teachers should promote the reformation of teaching mode, take advantage of the forces of many subjects, set up the new courses which include inter-disciplinary knowledge, strengthen the practical function of the teaching content, and help students grasp theoretical knowledge and practical operation by means of abundant case analysis. By setting up a suitable curriculum system and a core curriculum group to meet the needs of the industry, the teachers carry out rich and colorful practical teaching, which will help to solve the problem of

disconnection between the training of the professionals of cyber security and law enforcement and the needs of the industry.

Professional curriculum setting mode should be career-oriented. According to the relationship between profession and occupation, the teachers should list the knowledge points, skills points and working methods needed by the position, and then summarizes the common points of the position according to the occupational environment and occupational ability. According to the requirement of post competence, the teachers should set up a teaching base for the specialty of cyber security and law enforcement to carry out experiments and training in the network police department, and build a new pattern of "complementary advantages, resource sharing, mutual benefit, and common development". The teachers should take advantage of the off-campus teaching bases to carry out experiments and training. The teachers should work closely with the public security organs in the aspects of the design of training scheme, faculty construction, curriculum construction, teaching method research, teaching activities implementation, practice base construction and the assessment of the students. In order to improve the practical ability of the students, the skill training should be the main form of the teaching mode, and make students truly possess the ability of network security management, master the security skills and computer network crime detection capabilities.

C. Construction of training platform, simulation environment and case base for cyber security and law enforcement specialty

In order to provide perfect teaching resource facilities and environment for the students majoring in cyber security and law enforcement, it is necessary to provide supporting hardware facilities, software facilities, and communication network facilities and so on. Therefore, in order to better serve the discipline construction and professional construction, the university has established network training room, electronic confirmation training room, network attack and defense training room, etc. On the basis of satisfying undergraduate professional teaching and scientific research, these training rooms can also provide technical support for the network security department of public security organs, and provide electronic material evidence identification service for the society.

In addition, the teachers can also strengthen cooperation with the network security department and jointly establish the professional case base. The public security departments can equip the school training room with common tools and facilities to move the actual combat environment into the school, improve the actual combat ability of teachers and students and the quality of personnel training. The university can provide an educational environment for the front-line network security police. The two sides can cooperate with each other in network police training, scientific research cooperation, assistance in handling cases, judicial expertise and other aspects, achieve complementary advantages and resources, and train more cyber security and law enforcement professionals.

D. Constructing a professional team for the students and carry out innovative practical training activities

The second classroom should be established to train professional team of the students. Taking the professional team as the basic unit, the teachers should carry out the training about network security, certificate acquisition, independent practice, subject competition and scientific and technological activities to fully mobilize the initiative of students. In addition, the teachers should encourage student teams to participate in professional competitions such as network security and electronic forensics, establish a team of instructors, and form a training model for instructors and key players to guide new players. The teachers should invite students who are interested in their major to join the team and establish a mutual promotion mechanism. The teachers should make full use of existing laboratory resources, carry out internal technical competitions, and select outstanding elites to participate in competitions by internal competitions, achieve the goal of promoting learning by competitions.

VI. Conclusion

The talent training of the major of cyber security and law enforcement has become an important part of national security strategy. Under the background of new engineering construction, the professional teachers should focus on training the practical personnel that can adapt to network security and law enforcement work, closely achieving the training objectives of the major, adopting the integrated training mode of "teaching, learning, training and warfare". In the process of teaching, the teachers should strengthen the construction of capital team, curriculum system, practice training platform and student team. In addition, the mode of experimental teaching was a benefit for the students to improve ability of practice and inspire innovative consciousness, which can improve the competence of students majoring in cyber security and law enforcement.

References

[1] Zhou Jianhua, Chen Yanyu, Li Huanhuan. Research on Cultivation Goals and Approach of Network Security and Law Enforcement, Journal of Hubei Adult Education Institute, Jan.2018.

[2] LIU San-man, Achieving Way of Cultivating Talents of Network Security and Law Enforcement Directed by Combat, Journal of Shanxi Police College, Jul, 2017.

[3] Li Binyong. Exploration on the Training Mode and Ways of Talents in Cyberspace Security Discipline, Computer Education, Sep. 2016.

[4] Li Yang, Innovative cyber security talent cultivation mechanism of higher education in the new era, Cyber Security, Vol.09, No.2 Feb.2018.

[5] Liu zhijun, Huang Fenglin, Exploration and Thinking on the Talent Training of Network Security and Law Enforcement, Journal of Hubei University of Police, May. 2017.

[6] Yank Lianbin, Zhou Xinli, Liu Sihan, Cyber Security Talents Cultivation Mechanism and Mode in the Big Data Era, Journal of intelligence, Dec. 2016.