

Research on Network Security and Law Enforcement Professional Construction and Personnel Training

Gao Jian

Information technology and network security College, People's Public Security University of China, BeiJing, China
Email address: gaojianbeijing2006[AT]163.com

Abstract— This paper summarizes the development history and current situation of network security and law enforcement professionals, the existing problems are analyzed, and puts forward the reform of the education system, credit reform, reform, reform of personnel selection and assessment focused on training five reform views. Finally, the paper analyzes the framework of the NICE space security personnel team, and takes the network attack and defense direction as an example, and analyzes its work content, skills requirements and training methods.

Keywords— Network security and law enforcement; Training; Reform.

6	2013	Zhejiang Police College	083108TK	Engineering
7	2013	Henan Police College	083108TK	Engineering
8	2013	Hebei Police College	083108TK	Engineering
9	2013	Sicuan Police College	083108TK	Engineering
10	2013	Gansu Police College	083108TK	Engineering
11	2014	Railway police college	083108TK	Engineering
12	2014	Xinjiang Police College	083108TK	Engineering
13	2015	Shandong Police College	083108TK	Engineering
14	2015	Jiangxi Police College	083108TK	Engineering
15	2016	Shanxi Police College	083108TK	Engineering
16	2016	Jilin Police College	083108TK	Engineering
17	2016	Hunan Police College	083108TK	Engineering
18	2016	Guangdong Police College	083108TK	Engineering

I. INTRODUCTION

The Police colleges in china, the construction of network security and law enforcement professionals can be traced back to the computer application specialty of Chinese People's Public Security University in 1978 by the International Institute of politics at the early stage of construction, set up, according to the demand of public security work, the construction of professional curriculum system gradually, in 1998 the new investigation of computer crime investigation, in 2009 the first network security and law enforcement professionals, 2010 national the approval of the Ministry of Education officially enrolled in network security and law enforcement professional students, in 2011 officially owned technology subjects of public security [1], [2].

TABLE I. Subject level of public security technology and sub-discipline.

Code	Sub-discipline name
0838	Public Security Technology
083801	Criminal Science & Technology
083802	Humanbody Examination & Identification Technology
083803	Cyber Security Enforcement Technology

According to the Ministry of Education announced over the years in Colleges and universities of professional settings filing or approval of the results of statistics, as of 2016, a total of 18 schools set up a national network security and law enforcement professional "education of four years, belongs to the category of engineering [3].

TABLE II. School for network security and law enforcement.

Nub	Year	College	Code	Degree
1	2009	People's Public Security University of China	082107S	Engineering
2	2012	Criminal Investigation Police University of China	083108TK	Engineering
3	2012	NanJing Forest Police College	083108TK	Engineering
4	2013	Beijing Police College	083108TK	Engineering
5	2013	Jiangsu Police College	083108TK	Engineering

II. THE PROBLEMS

A. School System is Short, Content is Much

Network security and law enforcement professionals on the practical ability of the students has higher requirements, comprehensive and overlapping characteristics, the needs of students in 4 years of schooling, learning the police physical fitness, shooting and other basic police course; at the same time, the constitution, the people's police law, criminal law, criminal procedure law and other law courses; in addition also, need to master the professional foundation courses and professional skills courses; then deduct the last semester of the freshman military training time, time junior senior year internship, graduation design 4 and half a year after the time to find a job, the final is equivalent to the students in less than 3 years to learn all the lessons.

B. Employment Does Not Investigate Professional Courses

At present, the network security and law enforcement in public security college students employment basically depends on the national civil service examination and public security examination in two way, mainly inspects the civil service exam on line application and testing, and the public security investigation examination legal foundation and public security foundation knowledge. Investigation of only a few provinces network security department recruits will pay attention to professional knowledge [4], [5]. Therefore, under the influence of this great employment orientation, most students think that professional courses can pass and lose the motivation to learn. Only a few interested students pay attention to the study of professional skills.

III. THE REFORM IDEAS

A. School System Reform

Most of the medical undergraduates in our country adopt the 5 year system, and the training methods of network

security and law enforcement can draw on the educational system settings of medical major, so that we can learn more about network security knowledge. But this method has shortcomings are obvious, network security and law enforcement professionals belong to the public security professional, if only the students change the educational system, the students will be more professional than other late graduation situation, which may form the majority of students choose other professional, leading to the difficult situation of professional recruitment. Therefore, the school extension policy should be implemented with other incentives, such as network security and law enforcement professional school system set up for five years, while the students enter the school that is the police.

B. Curriculum Evaluation Reform

At present, students need to follow the school syllabus, learn the required courses each year, and choose the corresponding elective courses to complete their studies. The school according to the professional characteristics, set up a variety of free channels and diversification of the credits, let some talented, loving the students have more free time to the study of new technology. For example: the compulsory course of C language programming, network security and law enforcement professionals in data structure, operating system, computer network, database principle and information security system can carry out the assessment through the computer grade examination, after the exam is eligible to apply for exemption. Computer grade examination three each year, students can choose the course after studying the exam, may choose to take the exam, exam and the students can advance through the proposed exemption application. This way can avoid the students' final highlight teacher ", " exam is not difficult "lucky idea, you can also save teacher, marking the examination papers, examination time organization. This method is no longer a teacher's question, students test, to dispel the students' whether or not to pass the key in the teacher 'illusion. The formation of the computer grade examination committee questions, students, teachers guide the new situation, can pass the exam, the teacher and the school cannot intervention, teachers and students at the same time is facing the exam, the teacher is fighting with the team, coach, student players.

C. Elective Credit Reform

In most schools, students complete graduation requirements by completing a certain number of optional credits. For some students, elective courses are good or bad, whether they choose standards or not. Entirely deviated from the original intention of elective courses to develop students' knowledge and skills. At the same time, the interest group organized by the school teacher can not form a long-term learning mechanism because the students do not have a fixed time. Students can complete elective courses by participating in the interest groups organized by the teachers, and the students in interest groups can be evaluated through competition ranking and curriculum design. In this way, students can choose different interest groups through

individual interests, and teachers can also train and teach students at different levels through interest groups.

D. Special Talents Enrollment

In 2016, the central network security and Informatization Leading Group Office of the Ministry of education and other six departments jointly issued "on the strengthening of network security discipline construction and personnel training advice", proposed to accelerate the construction of network security disciplines and departments. Opinions pointed out that, support institutions of higher learning to open network security related professional "juvenile class", "special class". Encourage universities and research institutions according to the demand and characteristic, expand the network security professional direction, reasonably determine the scale related to professional training, the construction of cross science, engineering, law, management science and other categories of integrated network security training platform. Network security and law enforcement professional as a special feature of Public Security Colleges and universities, in the process of enrollment, you can recruit some special talents of network security through "special talent" way. Education management department can establish relevant system on the network security of exceptional students, such as every year for high school students held high quality network security competition, winning the competition as a way of exceptional admission or bonus. This will not only stimulate the high school students' love for network security, but also provide a green channel for students with network security expertise.

E. Organized Network Security Training Camp

Continuous, centralized education is more suitable for teaching network security. Compared with the traditional curriculum arrangement, the centralized training will receive better teaching results. Schools can train the special skills of network security through the training methods of network training in the summer and winter vacation, such as: attack and defense, forensics, data analysis, etc.. In the past two years, organized students to enroll in the company held by XMAN and CTF training camp held by the Wuhan University information security training camp, students enthusiasm, interest groups in the network security of the school more than 2/3 students, but because of the limited number of places, only a small number of students to participate in training. This shows that the majority of students have the willingness to learn actively, the public security university can face the school or public security colleges and universities network security and law enforcement professional students, through the summer and winter training, to increase communication and enhance skills [6-8].

IV. TRAINING WAY OF THINKING

We want to develop network security and law enforcement professionals in actual combat ability as the goal, in general education to improve the students' awareness of network security, network security training mainly in the stage of interest; professional education to improve the professional

skills of the students practical ability mainly. We can refine the training objectives of network security and law enforcement professional, and train students into knowledge learning, skills training and ability training. Knowledge is an important basis for skills and abilities, and knowledge and skills are the necessary prerequisite for promoting ability. Our ultimate aim is to cultivate students' ability, and not only stay on the books, one can read a lot of books, said he learned a lot of knowledge, but he is not used, cannot solve practical problems, did not put the knowledge into skills and abilities. Take the computer network as an example, students' learning book knowledge, familiar with the TCP/IP protocol, the message content, but when to get an pcap packet analysis, but confused, this knowledge is just stay on the books, does not translate into skills; so we need to make their own capture,

analysis the package in the training stage, with data packets to verify the protocol, so that the students will have the capture and protocol analysis skills, can do some work with related tools; in the future with some skills to the students, can produce some network fault data packets, packet or network attacks to analysis failure or network attack tracing and analysis of network behavior, this stage is to cultivate the students' ability in emergency response network fault or security incidents. The training of knowledge and skills can be basically completed in classroom teaching, and the training of ability needs to be realized on the platform of some second classes. Through the analysis of the direction of network attack and defense, the work tasks, ability requirements, skills requirements and knowledge reserves are analyzed as follows:

TABLE III. Skill analysis of network attack and defense direction.

Job Post	Network Attack and Defense
Typical tasks	<ol style="list-style-type: none"> 1. build penetration test environment, undertake the related tasks such as penetration test; 2. track security trends, reproduce relevant security incidents and write relevant documents; 3. Develop relevant courses and take part in training with penetration test environment and typical safety incidents; 4. sudden safety incidents, such as vulnerability investigation, security. 5. website vulnerability mining, and data analysis
Post competency requirements	<ol style="list-style-type: none"> 1. more than 2 years experience in penetration test or vulnerability mining; 2. familiar with all kinds of penetration testing tools and common security attack and Defense Technology: SQL injection, XSS and other vulnerabilities, skilled use of various security software, hacking tools, and combat experience; 3. the network security structure, system vulnerabilities, intrusion detection and other in-depth theoretical basis and practical experience; 4. Learn about PHP, Java, python, or any other programming language. 5. proficiency in Widnows, Linux and other platform use, attack skills
Skill requirement	<ol style="list-style-type: none"> 1. Internet search engines and advanced search syntax, search skills, Google, database; 2. Metasploit, Nessus, Nmap and other scanning tools and loopholes in the use of methods; 3. Wireshark, Cain, packet analysis tools, network sniffing and deception techniques; 4. Burpsuit, firebug and other tools, familiar with the reform package, packet capture, playback techniques; 5. IDA, Ollydbg, GDB and other binary analysis tools, dynamic debugging and static debugging, overflow 6. Winhex and other binary tools, file header analysis, data recovery 7. John, the, Ripper, Hydra password cracking tools, WiFi password cracking, system password cracking
Knowledge reserve	Computer foundation, C language programming, assembly language, PHP programming, computer networks, network warfare technology, information security technology, malicious code analysis.....

V. AMERICAN TALENT TRAINING FRAMEWORK

In April 2010, the United States launched (National Initiative of Cybersecurity Education, NICE), expected by the state and the overall layout of the action, three aspects of information security knowledge popularization, in normal education, occupation training and certification to carry out standardization, strengthen the work, to raise the overall information security capabilities [9-11].

The "framework" with "group" to summarize the definition of cyberspace security personnel, according to the need of the ability to work or occupation development path, the professional field (Specialty Area) structure functions and personnel safety network space group. At present, including the "framework" draft will be professional in the field of security division of the network space into seven categories: Securely Provision; Operate and Maintain; Protect and Defend; Investigate; Analyze; Oversight and Development; Collect and Operate. Its main responsibilities are related to such fields as information technology, information assurance and computer science. In addition to those key network security professionals can make the space efficient to complete its work support (Support) role, the relevant

procurement, physical security, critical infrastructure, supervision of electrical engineering specialty occupation not included. Therefore, the framework's intention and its career development plan are designed to better understand how to train and equip teams with cyber skills [12].

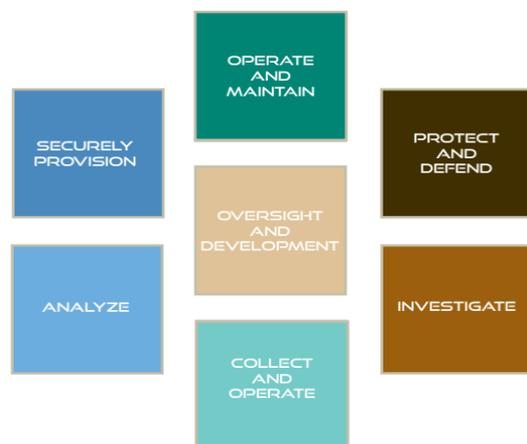


Fig. 1. The domain of cyberspace security is divided into seven broad categories.

VI. CONCLUSION

As the network technology change rapidly, the network crime diversified way, increase the number of cybercrime gradually, network security and law enforcement professionals directly to the public security network security department talents, training is very important. Therefore, we cannot copy the network security personnel training mode of higher education, higher education is also cannot imitate the occupation complete curriculum, we should according to the employment orientation of Public Security Colleges' characteristics and students, and job skill requirements, develop educational system, training program and curriculum content. To strengthen general education to improve the basic quality of students, strengthen the professional education to enhance students' practical skills, you can refer to the set based on the working process of the course "practical teaching methods, professional basic course teaching and examination can be combined with social certification to achieve separation of teaching and testing.

The industry education is mainly in public security colleges, network security and law enforcement professionals is emerging professional, development time is not long, the research on the curriculum system, curriculum setting, personnel training mode, there has been confusion, I hope this will be a few years on the professional summary, hope to reach more the development of network security and law enforcement professional building.

REFERENCES

[1] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, issue 1, pp. 63-72, 2007.

[2] C. Willems and C. Meinel, "Online assessment for hands-on cyber security training in a virtual lab," *IEEE Global Engineering Education Conference (EDUCON)*, pp. 1-10, 2012.

[3] B. D. Cone, M. F. Thompson, C. E. Irvine, and T. D. Nguyen, "Cyber security training and awareness through game play," *Security and Privacy in Dynamic Environments, Proceedings of the IFIP Tc-11, International Information Security Conference*, DBLP, pp. 431-436, 2006.

[4] K. F. McCrohan, K. Engel, and J. W. Harvey, "Influence of awareness and training on cyber security," *Journal of Internet Commerce*, vol. 9, issue 1, pp. 23-41, 2010.

[5] Willingham S., *Network Security Training Needed*, 2000.

[6] Wang H, Huang C, and Wang Z. "Construction of information security staff skills training system," *Network Security Technology & Application*, 2014.

[7] R. Bernard, *Education Training, Security Technology Convergence Insights*, Chapter 4, pp. 49-56, 2015.

[8] D. Shoemaker, A. Kohnke, and K. Sigler, *CyberSecurity: A Guide to the National Initiative for Cybersecurity Education (NICE) Workforce Framework 2.0*, 2016.

[9] C. Haijiana, H. Hexiaob, W. Leic, C. Weipingd, and J. Kunrue, "Research and application of blended learning in distance education and teaching reform," *International Journal of Education & Management Engineering*, vol. 1, issue 3, pp. 67-72, 2011.

[10] D. Li, C. Liu, and B. Liu, "H-RBAC: A hierarchical access control model for SaaS systems," *International Journal of Modern Education & Computer Science*, vol. 3, issue 5, pp. 47-53, 2011.

[11] M. N. A. Khan, M. Khalid, and S. U. Haq "Review of requirements management issues in software development," *International Journal of Modern Education & Computer Science*, vol. 5, issue 1, pp. 21-27, 2013.

[12] G. Jian, "Reform of database course in police colleges based on "working process," *International Journal of Modern Education & Computer Science*, vol. 9, no. 2, pp. 41-46, 2017.



Dr. Gao Jian is a lecturer in information technology and network security college, People's public security University of China. In teaching, he has been focusing on Work Process concepts and Problem Based Learning approaches in Cyber Security Education. In research, his current interests include Botnet, Malware, DDoS.