Cyber Security Training in Europe and America and its Enlightenment to China

Weiwei Wang[1,*] and Liang Guo[1]

[1]*Air Force Engineering University, Xi'an, Shaan xi 710000, China*

ABSTRACT
With the rapid development of emerging information technology and the deep popularization of social information, a series of cyber security problems pose a serious threat to national security, economic stability and people's lives. If we want to effectively reduce the risk of cyber security with the characteristics of high-tech confrontation, the key link is to train cyber security talents seriously at all levels. This paper combs the strategy and practice of cyber security personnel training in the United States and Europe, and puts forward some suggestions on the training of cyber security talents in China from the aspects of strategy and supporting policies, continuing education, curriculum system, information security literacy and so on. Through comprehensive analysis, sophisticated cyber security talents cultivation mechanism and mode under the background of big data were proposed, which incorporates the education system, social cultivation system and talent evaluation system, to improve cyber security talents cultivation mechanism and respond to the threat of big data. Finally, the paper puts forward some suggestions and thinking about building more complete cyber security talents cultivation mode.

***Keywords**: cyber security, talents, education, cyber security literacy*

1. THE BACKGROUND OF GLOBAL CYBER SECURITY PERSONAL TRAINING

With the rapid development of cyber technology and the deep popularization of social information, the operation of government departments, transportation, energy, aviation, finance, communications, medical and other systems rely more and more on cyber systems. In the context of the information society, information has evolved into a national strategic resource, which together with material and energy constitute the three basic elements for the survival and development of human society. Due to the inherent defects and human factors of cyber technology, a series of cyber security problems, such as cyber infrastructure damage and network data theft, pose a serious threat to national security, economic stability and people's life. It has aroused great concern in the global society, especially in Europe and the United States, and has become a global hot issue.

If we want to reduce the risk of cyber security with the characteristics of high-tech confrontation, we should develop the information industry vigorously, make up for the loopholes in information technology, and reduce the space in which human factors can be brought into full play. the key link is to train cyber security personnel at all levels. cyber security personnel mainly refer to the personnel engaged in information security or computer network security technology in administrative departments at all levels, enterprises and institutions, information centers, data centers, Internet access units, scientific research institutes, and other institutions. They are generally required to be able to skillfully use basic and specialized skills to complete more complex cyber security work. Be able to independently deal with and maintain the common problems in the work of cyber security [1]. In February 2014, the Central Cyber Security Informatization leading Group was established. General Secretary Xi Jinping stressed that it is necessary to have a team of high-quality cyber security talents, that is, to pool human resources, build a strong team with strong politics, professional expertise and good work style, and train world-class scientists, network science and technology leaders, outstanding engineers and high-level innovation teams. This paper will focus on the analysis of the efforts made by the United States, the European Union, Britain, Russia and other European and American countries in the training of cyber security talents in recent years, in order to provide some reference for our country to better train cyber security talents. In view of the fact that there are many titles in the academic field and government official reports at home and abroad, such as network security, cyber security, cyberspace security, information security and so on, this paper mainly uses cyber security to express it.

2. PROGRESS IN THE TRAINING OF CYBER SECURITY TALENTS IN EUROPE AND THE UNITED STATES

2.1. The overview of the Progress of cyber Security personnel training in Europe and the United States

As a country with the most developed cyber technology and the highest degree of social informatization in the world, the United States has a clear understanding of the great challenges in the field of cyber security. Since the late 1990s, it has begun to study various countermeasures for the training of cyber security personnel, and gradually raised this issue to the height of national strategy with the development and changes of the situation. As early as 2003, the United States incorporated the Cyber Security Awareness and training Program into the National Strategy for Cyberspace Security at the national level for the first time. The European Commission has long paid close attention to the issue of cyber security from a strategic perspective. As early as 2004, the European Network and Information Security Agency (ENISA),) was established and given the role of mandatory intervention in the cyber security strategy of member states, responsible for organizing and coordinating the strategic planning, practice, infrastructure protection and emergency response of cyber security of EU member states. Including the measures that member states should take to improve their national information security literacy. The UK, the first of all G20 countries to be able to resist cyber attacks, launched its first national cyber security strategy in June 2009, pointing out the need to raise awareness of cyber security among governments at all levels. Russia, as the largest network power in Europe, brings information security into the scope of national security management in the Constitution of the Russian Federation, and points out in its programmatic document "National Information Security Theory" that information security is the basis of national security, and efforts should be made to build a talent training system from diploma education to on-the-job education.

2.2. The strategy and practice of training cyber security talents in Europe and the United States

In April 2010, (NIST) of the National Institute of Standards and Technology released the Cyber Security Education Strategic Plan (NICE), and worked with the Department of Homeland Security, the Department of Defense, the Department of Education, the National Science Foundation and the Office of the Director of National Intelligence to promote the implementation of the program. The plan includes four modules: national network security awareness module, formal network security education module, network security talent architecture module, network security personnel training module and career development module. The National Cyber Security Awareness Module, led by the U.S. Department of Homeland Security, aims to increase American public awareness of cyber security threats and raise public awareness of cyber security through stop-think-connect (stop-think-connect) activities. The formal cyber security education module is jointly undertaken by the U.S. Department of Education and the National Science Foundation,which increase the formal cyber security education programs focusing on science, technology, engineering and mathematics, to train the cyber security researchers, cyber security professionals, cyber security skills and citizens with cyber security awareness for the country. We will expand the reserve force of professional and technical personnel in government departments and private enterprises. The network security talent architecture module is still under the unified leadership of the United States Department of Homeland Security, focusing on the evaluation and management of network security professionals. The cyber security personnel training and career development module is jointly led by the Office of the Director of National Intelligence, the Department of Defense, and the Department of Homeland Security, by coordinating local governments, industry, the private sector, and academia, work together to develop the cyber security training and career development process for national cyber security personnel. As a special national cyber security education program, NICE fully expresses the importance that the United States attaches to the training of cyber security talents. In March 2013, the National Network Security personnel Framework divided cyber security professionals into seven categories and 31 specialties, including security provision, operation and maintenance, protection and defense, security investigation, collection operations, security analysis and supervision and development. and the main tasks of each specialty and the professional knowledge, technology and capabilities that should be possessed are defined in detail [2].

The European Commission launched the Digital Europe Plan in August 2010, and specially opened a chapter on "credibility and Security" to explain the importance of raising public awareness and capability of network security prevention and the measures that member States should take, including: (1) requesting the European Network and Information Security Agency to put forward a proposal for the implementation of "Network Security qualifications" in 2013 to improve the professional capacity of personnel in the information technology industry; (2) it is planned to hold cyber security championships in 2014 to encourage college students to participate in cyber security construction; (3) member states are required to hold a "Cyber Security month" every year from 2013 to formulate national cyber security training plans, and from 2014 to provide cyber security training courses in schools, provide special cyber security training for computer major college students and provide basic training for government civil servants. The European Network and Information Security Agency also released the European cyber Security Education Project Roadmap (Roadmap for NIS education programmes in Europe), in October 2014. The key users of the report are educators in the field of cyber security education. Second, there are policy makers in the field of cyber security education, who can decide which courses should enter the field of education. The report recommends that (Europass); a "European pass" in the field of cyber security education, be launched for the public to deploy better continuing education programs for teachers to strengthen their multiple roles. Relevant European organizations and departments should begin to develop a large-scale online open course on cyber security, (MOOCs);. Provide a series of cyber security training courses for health practitioners, lawyers and digital security experts, relevant personnel of small and medium-sized enterprises and continuing professionals in digital forensics [3].

On the other hand, the UK issued the Cyber Security Strategy in November 2011 and decided to allocate 650 million pounds of special funds to support the implementation of cyber security technology and legal action in the next four years. The strategy document details the UK's cyber security prospects and implementation details of the action plan for 2015. The latter includes seven aspects with strong maneuverability, such as policy guidance, law enforcement system, institutional cooperation, technical training, personnel training, market cultivation and international cooperation. In April 2013, the British government decided to set up a global cyber security centre at the University of Cambridge to help countries develop comprehensive plans to deal with cyber threats. In May 2013, the British government decided to allocate 7.5 million pounds to Oxford University and the University of London to jointly develop expertise to combat virtual attacks and train cyber security experts. In October 2013, the newly established Joint Network Reserve Board pointed out that if convicted computer hackers pass security checks, they could be recruited to the agency. Hundreds of people will be recruited from the reserve force to form a computer expert group to work with regular forces. In March 2014, the British government also issued a Guide to the Certification of cyber Security Professionals, which sets out the responsibilities and technical capability requirements of cyber security professionals in the government public sector and its contract manufacturers. clarify the selection, training and management of information security personnel. The framework divides cyber security professionals into seven categories: security assessors, information security auditors, information security architects, security and information risk consultants, IT security officers, communications security officers and penetration testers.

Russia regards seven specialties in the field of cyber security, such as information security, computer security, information security automation system, information security analysis system, information security of television communication system, information defense system method and cryptography, as the priority development direction of national education and science and technology. In March 2013, the Russian Defense Ministry will set up a science and technology company set up by college students to detect foreign cyber attacks and prevent various cyber threats. In July of the same year, two science and technology companies began to serve around Moscow and the Air Force Academy. They have also begun to recruit young programmers graduated from non-military colleges and universities and to develop necessary software products for the military over the next five years [5]. Russia is also actively using the services of "white hackers", that is, network experts who have no criminal record and have rich experience in discovering system vulnerabilities to deal with cyber attacks. These "white hackers" will regularly check the website protection capabilities of government departments and establish a computer attack detection system against external national or enterprise-level computer attacks against Russian information systems [6].

2.3. Strategies to raise awareness of cyber security in Europe and the United States

Since 2002, the United States has designated October as the "National Cyber Security Awareness month", which aims to raise the public's awareness of cyber security and educate the public that they should contribute to ensuring the security of cyberspace. Every year, the National Cyber Security Awareness month has a specific theme, and a specific key theme is set every week of that month. Take the National Cyber Security Awareness month in October 2014 as an example, the theme of the first week is "stop-think-connect", that is, to promote secure Internet activities, with a focus on providing passwords with sufficient strength, and do not share it with anyone; keep computer operating systems, browsers and other key software updated in a timely manner; It is recommended to minimize the provision of personal information on the Internet and to use privacy settings to avoid information disclosure. The theme of the second week is "secure Development of Information Technology products", focusing on educating the public to embed elements of cyber security into the development of computers, tablets, smart-phones and other information technology products.

The theme of the third week is "critical Infrastructure Security and the Internet of things", which focuses on the importance of critical infrastructure security while telling the public to protect all devices. The theme of the fourth week is "Network Security for small and medium-sized Enterprises", which mainly showcases new technologies and business models that can be used to protect small and medium-sized enterprises. The theme of the fifth week is "Cyber Crime and Law Enforcement", which mainly advocates to work with law enforcement agencies and fight cybercrime, while telling the public how to avoid becoming victims of cybercrime [7].

The European Commission launched its first Europe-wide pilot project, the European Cyber Security Month (ECSM), on October 1, 2012. Since 2013, the European Commission has officially designated October every year as the "European Cyber Security month". Its activity time is similar to that of the United States, and it is also October every year. Its goal is to raise public awareness of cyber security, improve their understanding of cyber security threats, and use platforms such as daily television or radio advertisements, social media activities, award-winning guesses, news reports, conference seminars, student exchanges, and so on. Provide the public with the latest network security information. The Department of Education said in a statement in August 2013 that it would set up a new curriculum to ensure that British children begin to receive a series of cyber security education from the age of five on how to protect themselves online, how to respect each other, and how to communicate more safely. In September 2014, a new computer course will enter primary schools in the UK to help pupils learn how to use technology more safely and ensure personal privacy. In October 2014, the British government announced the launch of free online training courses to help British companies improve their ability to prevent cyber attacks. The training targets are mainly lawyers and accounting professions, including how to prevent and deal with common network security threats, how to protect digital information and so on.

3. THE ENLIGHTENMENT TO THE TRAINING OF CYBER SECURITY TALENTS IN OUR COUNTRY

3.1. The promulgation of China's cyber security personnel training strategy and various supporting policies

Although in the "opinions on vigorously promoting the development of informatization and effectively ensuring information security" issued by the State Council in 2012, it is proposed to vigorously support the construction of teachers, professional colleges and departments, discipline systems and key laboratories of information security disciplines. However, compared with the strategic documents such as the Cyber Space Security Education Program of the United States, the National Framework of Cyber Security personnel, and the Roadmap of the European Cyber Security Education Project, the relevant documents or the spirit of the speech in China need to be studied in depth, combined with the background of building a network power in China to launch the Chinese version of the cyber security personnel training strategy. At the same time, it is also necessary to issue a number of matching policies, such as the degree Office of the Ministry of Education, after raising the discipline status of the cyber security major to the level of the first-tier discipline, it should be equipped with resources such as teachers, academic places, enrollment, research and education funds, and additional courses related to cyber security can be added from the primary school stage. The human resources guarantee department will study and introduce a more attractive salary incentive system for cyber security practitioners in the public sector as soon as possible, so that existing employees can feel at ease with their jobs. it can also achieve the return of all kinds of high-tech talents, including "white hat hackers".

3.2. Provide good continuing education opportunities for cyber security educators and improve the level of teachers

Cyber security educators play an important role in the training of cyber security talents. However, at present, there is a great shortage of cyber security educators in all levels and all kinds of schools in our country, and the professional core courses in some colleges are often held by full-time teachers of related majors, which greatly reduces the teaching effect. Secondly, many educators lack the training of hands-on operation ability and actual combat ability, and often only pay attention to teaching theoretical knowledge in the process of teaching. Third, the knowledge points in the field of cyber security are updated quickly, and their knowledge reserves need to be updated regularly. Therefore, it is imperative to provide them with diversified continuing education. First of all, they can be encouraged to engage in postdoctoral research, study for doctoral degrees or participate in short-term workshops in universities and key enterprises at home and abroad; secondly, a number of course videos related to cyber security can be selected from the existing national high-quality courses, so that the majority of educators can observe and study carefully and evaluate their teaching practice in a timely manner. Third, the Ministry of Education can take the lead to select a group of cyber security educators who have not yet been selected into the national high-quality courses, record relevant teaching videos for them, and promote these videos to them in the form of (MOOCs), a large-scale online open course, so as to improve their professional level and teaching level.

3.3. Study and compile the course system of cyber security in China, and organize experts to compile high-quality teaching materials

The major of cyber security is becoming more and more interdisciplinary and multifaceted, involving fields of knowledge that span computer science, mathematics, law, criminology and other disciplines. There are great differences in the perspective of attention of different disciplines, so we should coordinate these differences as much as possible when studying and compiling the curriculum system of cyber security in our country.

The National Cyber Security personnel Framework and the British cyber Security Professional Certification Guide are an effective classification of relevant skills and a good starting point for the construction of cyber security course system, which is worthy of in-depth study. Although there are many teaching materials with the names of "cyber security", "network security" and "information security" in our market, there are still few teaching materials that can be widely accepted by the majority of students and cyber security practitioners. The existing teaching materials put too much emphasis on the operational theory of cyber security prevention, and pay less attention to cyber security management contents such as cyber security laws, norms, standards, and so on. It is necessary to pay more attention to the existing neglected parts, improve the quality of compilation, and make the majority of students and cyber security practitioners more interested in the content of the textbook.

3.4. Increase the content proportion of cyber security in the national computer grade examination, so that cyber security literacy has become a necessary element for job hunting and promotion

Many units and departments which have taken mastering certain computer knowledge and application skills as one of the important bases for post qualifications, cadre recruitment, professional title evaluation, and job promotion. With the increasing investment in information and communication technology and the continuous improvement of the degree of social informatization, all walks of life in our country are more and more likely to suffer from cyber security challenges, which also means that the requirements for potential job seekers in cyber security literacy are getting higher and higher. The Ministry of Education should make new adjustments to the computer basic education curriculum system and the national computer grade examination to adapt to the changes of the times, and timely increase the proportion of the inspection content of knowledge points related to cyber security. In particular, it should increase the operational ability of potential job seekers and the ability to solve practical problems, and further enhance the gold content of the national computer grade examination certificate.

3.5. Give further play to the role of Network Security publicity week to further enhance the public's literacy of cyber security

Although China's first Network Security publicity week ended successfully in 2014 with the strong support of people from all walks of life, Shanghai has also successfully held several Information Security weeks, which has gradually improved the public's cyber security literacy, but compared with foreign network security months, there are still some gaps. For example, foreign network security months are more diverse in the choice of themes, richer in content, and more lively in form. The coverage of the participating groups is wider and specific, and the holding time is longer. In order to carry out cyber security publicity week in the future, we should not only hold more activities at the national level, but also sink these activities to the provincial, municipal, autonomous regional, and even municipal levels. By setting up special training and interactive websites, issuing public publications, issuing guides or manuals, holding public welfare lectures, comparing security knowledge posters, holding security knowledge competitions and network attack and defense drills, broadcasting network videos or television broadcasts, etc. to enable more members of the public to participate, effectively improve their cyber security literacy.

4. CONCLUSION

Cyberspace security is an important part of national security. With the arrival of "Big Data Era", it is of great strategic significance to build a complete training model of cyberspace security talents. Since "Cyberspace Security" was added as a national first-class discipline, the training of related talents has embarked on a high-speed road. As a new discipline, how to cultivate "cyberspace security"

It is still in the exploratory stage to cultivate high-quality cyberspace security talents that meet the requirements of the state and society. In this paper, referring to the relevant literature on cyberspace security and its personnel training in Europe and America, we summarized the situation of cyberspace security personnel in China, and put forward some suggestions for improving the problems existing in the training of cyberspace security personnel under the background of big data in China. Drawing lessons from the existing training models of related disciplines, we integrated three major aspects: education system, social training system and national overall planning, and put forward some thoughts and suggestions on building a relatively complete training model of cyberspace security.

REFERENCES

[1] Liu Jinfang, Feng Wei, Liu Quan. Observation on the current situation of information security personnel training in my country [J]. Information Security and

Communication Confidentiality, 2014(5): 26-28.DOI: https://doi.org/10.1007/3-540-11494-7_22

[2] Zhao Qian, Liu Feng, Lin Dongdai. American Cyberspace Security Education Strategic Plan [J]. China Information Security, 2014(8): 91-94.DOI: https://doi.org/10.1007/978-3-540-30494-4_16

[3]Roadmap for NIS education programmes in Europe[OLS].https://www.enisa.europa.eu/activities/stakeholder-relations/nis-bro-kerage-1/roadmap-for-nis-education-programmes-in-Europe(In Chinese)

[4] Wang Xing. Research on the construction system of British cyber security talent team [J]. China Information Security, 2015 (11). DOI: https://doi.org/10.1007/978-3-642-82453-1_5(In Chinese)

[5] Ma Jianguang, Zhang Naiqian. Net Warfare: Russian Army Aims at the "Sixth Generation War" Layout[OL].http://www.81.cn/rd/201602/26/content_6929347.htm(In Chinese)

[6] The Russian Federal Council intends to use "white hackers" to respond to cyber attacks [OL]. http://www.chinanews.com/gj/2014/01-26/5780781.shtml(In Chinese)

[7] Li Miao. Research on American Information Security Education and Awareness Training [J]. China Information Security, 2012(5): 72-75.DOI: https://doi.org/10.1007/978-3-642-12002-2_3