Translation

The following white paper, drafted by the Chinese Ministry of Education in concert with several universities, details China's system for cultivating homegrown "live-fire" cybersecurity talent. The authors describe the methods China uses to train cyber talent—including formal education, corporate training, certification courses, competitions, and bug bounties—but warn that in spite of these efforts, the country's supply of cybersecurity professionals remains woefully insufficient. The white paper concludes with policy recommendations designed to ameliorate the mismatch between the skills of newly minted graduates and the actual cybersecurity needs of Chinese companies.

Title

2022 White Paper on the Live-Fire Capabilities of Cybersecurity Talents: Attack and Defense Live-Fire Capability Edition

2022 网络安全人才实战能力白皮书 攻防实战能力篇

Authors

The steering organization (指导单位) for this white paper is the Ministry of Education Steering Committee on Instruction for Higher Education Cybersecurity Majors (教育部高等学校网络空间安全专业教学指导委员会). The director of the white paper's editorial committee is Feng Huamin (封化民).

Source

China Big Data Industry Observer (中国大数据产业观察; 数据观), September 13, 2022. China Big Data Industry Observer is a privately run web portal, think tank, and online news source focused on China's big data industry.

The Chinese source text is available online at:

http://www.cbdio.com/BigData/2022-09/13/content_6170512.htm

An archived version of the Chinese source text is available online at: https://perma.cc/34X6-7FRS

U.S. $1 ≈ 7.2 Chinese Yuan Renminbi (RMB), as of August 22, 2023.

Translation Date	**Translator**	**Editor**
August 22, 2023	Etcetera Language Group, Inc.	Ben Murphy, CSET Translation Manager

2022 White Paper on the Live-Fire Capabilities of Cybersecurity Talents: Attack and Defense Live-Fire Capability Edition

2022 White Paper on the Live-Fire Capabilities of Cybersecurity Talents
Attack and Defense Live-Fire Capability Edition

Drafting Organizations

Steering Organization:

Ministry of Education Steering Committee on Instruction for Higher Education Cybersecurity Majors

Lead Drafting Units:

Beijing University of Aeronautics and Astronautics (Beihang University)

University of Science and Technology of China (USTC)

Integrity Technologies (北京永信至诚科技股份有限公司)

Assistant Drafting Units:

Xidian University

Southeast University (SEU)

Wuhan University (WHU)

Huazhong University of Science and Technology (HUST)

Shanghai Jiao Tong University (SJTU)

Participating Editing Units (参编单位):

Beijing Electronic Science & Technology Institute (BESTI)

Shandong University (SDU)

Sichuan University (SCU)

Beijing University of Posts and Telecommunications (BUPT)

Preface

In the final analysis, cyberspace competition is a talent competition. Cybersecurity talents empower thousands of industries and are the cornerstone of the secure development of the digital economy. In the development of network and information security, the construction of talent teams is key.

While the cyber powerhouse[1] strategy is being further promoted, the huge gap in cybersecurity talents has become one of the main problems facing the cybersecurity industry, especially the serious shortage of live-fire (实战) talents. Data shows that by 2027, China's cybersecurity talent gap will reach 3.27 million, while the scale of talent training in colleges and universities is only 30,000 per year. In China, there is a serious shortage of cybersecurity talents who have live-fire capabilities and understand attack methods and attack pathways. On the one hand, only 8% of the heads of corporate information departments and security departments believe that their teams are "not lacking in any aspect of live-fire attack and defense capabilities". On the other hand, the most tangible problem in the cultivation of talents in Chinese colleges and universities is in "internship and practice." The construction of the live-fire capabilities of cybersecurity talents has become a new proposition of the era that requires an urgent solution.

The *White Paper on the Live-Fire Capabilities of Cybersecurity Talents* (hereinafter referred to as the "White Paper") is the first white paper in the industry to focus on the live-fire capabilities of cybersecurity talents. Based on 420 events, used to sample 85,761 pieces of cybersecurity competition information, as well as 889 survey questionnaires, combined with an investigation of the supply side of live-fire talents and the demand side of employers, this white paper comprehensively presents the current supply and demand situation, training status, evaluation methods, and development suggestions for live-fire talents in China. This *White Paper* was written for Party and government agencies, state-owned enterprises (SOEs), enterprises and public institutions[2], and universities. It is hoped that this effort will provide a detailed

[1] Translator's note: Alternate English translations for the Chinese term wǎngluò qiángguó (网络强国)—here translated as "cyber powerhouse"—include "cyber superpower," "network powerhouse," "network superpower," and so on. For a more thorough discussion in English of the meaning of the term wǎngluò qiángguó, see: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

[2] Translator's note: "Public institutions" (事业单位) are organizations created and led by Chinese government departments that provide social services. Unlike state-owned enterprises (SOEs), public institutions do not create material products and are non-profit. Public institutions are not considered government agencies, and their employees are not civil servants. Most public institutions are fully or

reference for the formulation of talent strategies by various units.

This *White Paper* has the following main features:

(1) The basic concepts are clear and the methodology is clear. First, it defines cybersecurity talent live-fire capabilities and attack and defense live-fire capabilities and proposes the "4+3 Model" of cybersecurity talent live-fire capabilities and "ASK-P Model" of cybersecurity talent training in order to establish standards for the categorization and evaluation of cybersecurity talent live-fire capabilities.

(2) The content is comprehensive and complex topics are explained in a clear and simple way. The white paper provides a comprehensive comparison of the cybersecurity talent development environment in China and abroad, the supply and demand of cybersecurity talent live-fire capabilities, and cybersecurity talent live-fire capabilities in various industries and various regions throughout China in order to reach a large number of conclusions. The authors try to avoid using obscure language to describe abstract theory and technical knowledge, instead conveying this information with the help of a large number of diagrams.

(3) This is the work of experts and represents cutting-edge information. The authors have drawn on their many years of teaching and cybersecurity frontline work in colleges and universities and have accumulated many important accomplishments over their long periods of work. Many of the authors have also won awards such as Outstanding Cybersecurity Teacher Awards, Outstanding Cybersecurity Talent Awards, National Technology Invention First-Prize Awards, and Beijing Science and Technology Invention First-Prize Awards. They have integrated their profound teaching philosophies and practical experience into the *White Paper*.

The *White Paper* is guided by the Ministry of Education Steering Committee on Instruction for Higher Education Cybersecurity Majors. Its lead drafting units are Beijing University of Aeronautics and Astronautics, University of Science and Technology of China, and Integrity Technologies; its assistant drafting units are Xidian University, Southeast University, Wuhan University, Huazhong University of Science and Technology, and Shanghai Jiao Tong University; and its participating editing units are Beijing Electronic Science & Technology Institute, Shandong University, Sichuan University, and Beijing University of Posts and Telecommunications.

This *White Paper* focuses on live-fire attack and defense capabilities. It is one of a series of *White Papers on the Live-Fire Capabilities of Cybersecurity Talents*. In the

partially government-funded, but some fully privately funded (but still government-led) public institutions exist. Public institutions typically provide services in areas such as education, science and technology, culture, health, and sanitation.

future, this series will release three parts: Vulnerability Mining Capabilities, Engineering Development Capabilities, and Combat Effectiveness Evaluation Capabilities. Due to human error on the part of the authors and the limited time in which this paper was produced, there are inevitably omissions and inadequacies. We invite all criticisms and corrections.

Contents

Chapter 1 | Analysis of the Current Status of Talents in the Cybersecurity Industry

With the rapid evolution of new computing technology, network technology, and communications technology, cyberspace has become the fifth domain for sovereignty competition after land, sea, air, and space. Cybersecurity is related to national security, social stability, economic development, the people's lives, and other aspects. For the sake of national stability and prosperity, we must ensure the security of China's cyberspace. We must build a national cybersecurity assurance system to protect the cybersecurity of government, military, enterprises, and other important departments as well as important infrastructure such as finance and energy infrastructure. General Secretary Xi Jinping clearly pointed out that talent is the number-one resource; and competition in cyberspace is, in the final analysis, competition for talent. The core competency of cybersecurity lies in professional talents. Only by cultivating sufficient outstanding network professionals and technical talents can a country ensure it will gain an advantage in future cyberspace conflicts. Therefore, countries all over the world are raising the training of cyberspace talents to the level of national strategy, investing huge amounts of financial and material resources, and building comprehensive training systems for cybersecurity talents.

1.1 Macro Policy Environment

At present, the United States is the most powerful country in cyberspace. Its cybersecurity talent training is superior to other countries in quantity and quality. Its comprehensive talent training system is worthy of study by China. At the same time, the UK, France, Germany, Japan, South Korea, Russia, Israel, and other cyberspace powers rely on their own national conditions to cultivate cybersecurity talents.

At the strategic level, the United States successively released several cybersecurity strategies such as the *Cybersecurity Talent Program* (2002),[3] *National Initiative for Cybersecurity Education* (2010), *National Initiative for Cybersecurity Education Strategic Plan: Building a Digital Nation* (2011), *Federal Cybersecurity Workforce Strategy* (2016), and *Executive Order on America's Cybersecurity Workforce* (2019). These strategies provide detailed specifications for the cultivation of cybersecurity talents at multiple levels, from education in colleges and universities, training by cutting-edge technology enterprises, to the discovery of talents in society and the selection of top high school students, and then to selecting the very best (掐尖)

[3] Translator's note: This mention of a U.S. "Cybersecurity Talent Program" (网络空间人才计划) probably refers to the Cyber Security Research and Development Act of 2002.

cybersecurity talents (that is, attracting global cybersecurity talents by offering generous conditions).

The European Union released its *Cyber Security Strategy* in February 2013, requiring member states to carry out network and information security education. In 2011, the United Kingdom released the *National Cyber Security Strategy*, emphasizing the need to "improve cyber skills and education," Germany released the *Cybersecurity Strategy for Germany*, emphasizing "enhancing the public's awareness of Internet risks and strengthening the training of professionals," and France released *Information systems defense and security, France's strategy*, which proposes to establish a network defense research center, engage in the training of professional talents, and increase the proportion of young information security talents. European countries generally value education at the master's and doctoral degree levels and have established professional evaluation and authorization certifications for highly educated talents in schools. In terms of professional talent certifications, the CCT and CCP professional certification programs were established to determine the grades of cybersecurity talents with professional skills and afford them corresponding treatment.

Since 2011, Japan has spent about 100 million yen [$700,000] per year on the training of cybersecurity talents, including sending talents to foreign universities, enrolling in information security-related institutions for advanced studies, and participating in Japan-U.S. information technology (IT) forums. Japan issued its *National Security Strategy* in June 2013, which proposes a basic route for cultivating and discovering outstanding cybersecurity talents who have a mastery of innovative methods and technologies.

Russia has released several editions of its *Information Security Doctrine* to guide the promotion of information security construction and talent training. Informatics is a core course at the middle-school level in Russia. This course covers information technology, network technology, algorithms, and programming languages. According to statistics, 60,000 middle school students register to take the AP computer science exam every year. This course has allowed Russia to train more than 600,000 computer-related technical talents, including a large number of world-renowned hackers. Russia is vigorously cultivating cybersecurity talents within its military system. In 2015, the Ministry of Defense established an IT technological armament school to train reserve talents for its specialized cyber force.

In addition, the cultivation of cybersecurity talents in the United States, United Kingdom, South Korea, Russia, and Israel also relies on the cooperation between the military and local institutions. The U.S. Navy, Army, and Air Force have allocated a large amount of funds to universities and research institutions for the research and development of cyber attack and defense technologies, and opened the Air Force Research Laboratory to reserve officers and ordinary college students. In 2014, the South Korean Ministry of National Defense and Chung Cheong University established an academic department to cultivate cybersecurity talents for the South Korean cyber force. Japan's 2017 budget allocates 70 million yen [$500,000] to the U.S. military for the training of information system talents. Israel's cyber warfare unit 8200 has the right to take priority in the recruiting of talent at high schools.

1.1.1 International Situation

In 1999, the National Security Agency (NSA) launched the Center of Academic Excellence in Information Assurance Education (CAE-IAE) program. In 1999, the first batch of seven universities was accredited by this program. In 2004, NSA cooperated with the U.S. Department of Homeland Security (DHS) to launch the CAE-IAE certification program. In 2008, the CAE program added the Center of Academic Excellence in Cyber Research (CAE-R) certification. In 2010, the Center of Academic Excellence in Cyber Defense (CAE-CD) program was launched, oriented to research centers, technical schools, and government training institutions. It provides certifications for three programs: four-year bachelor's and master's degree education, two-year preparatory education, and research center program certification.

In April 2010, U.S. President Barack Obama launched the "National Initiative of Cyber security Education" (NICE). The expectation was that, through the overall layout and actions of the country, systematic and standardized strengthening work would be carried out in the popularization of general knowledge about information security, formal academic education, and professional training and certification, so as to comprehensively improve the information security capabilities of the United States.

In 2012, the Center of Academic Excellence in Cyber Operations (CAE-CO) program was launched. As part of the NICE framework, the CAE-CO program is a supplement to CAE-CD, with a special emphasis on network operation expertise. The CAE-CO certification is open to four-year undergraduate and graduate institutions, and participating institutions must have established departments with computer science (CS), electrical engineering (EE), or computer engineering (CE) majors, or departments with majors of equivalent technical level, or departments with collaboration between two or more majors. In 2017, the name of the CAE-IAE was changed to the Center of Academic Excellence in Cyber Defense Education (CAE-CDE). In October 2019, the CAE-CD program was merged into the CAE-CO program. In the same year, the CAE decided to increase the weight of academic achievement output in evaluations and consider other factors at the same time.

As of September 1, 2020, a total of 334 institutions in the United States had obtained CAE certification, and 116 community colleges offer associate degree programs and degrees. 48 institutions had both CAE-CDE and CAE-R certifications; 6 institutions had both CAE-CDE and CAE-CO certifications; 2 institutions had both CAE-R and CAE-CO certifications; 10 institutions had all three certifications.

The NCAE program is supported by many relevant government departments, including but not limited to the Department of Defense (DoD), Department of Education (DoE), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), NICE, United States Cyber Command (U.S.-CYBERCOM), and the National Science Foundation (NSF).

At the end of 2011, when the country's first National Cyber Security Strategy was still in its infancy, the UK Government Communications Headquarters (GCHQ) launched the Academic Centers of Excellence in Cyber Security Research (ACEs-CSR) construction program. At the beginning, 8 universities formed an academic alliance that had grown to 19 universities by 2020 in order to systematize the cybersecurity research of UK universities.

An important initial objective of the program was to identify the UK's leading research institutions in the field of cybersecurity and to identify technical areas where the UK possessed significant research achievements. It also helped to identify research areas that needed to be strengthened. The program's vision is to provide support for government and business. It will help government and enterprises to engage more effectively with academic institutions in order to more deeply understand leading cybersecurity research and use it to the benefit of the UK. The research fields considered by ACEs-CSR mainly include the following eight categories: cryptography, key (密钥) management and related protocols, information risk management, system engineering and security analysis, information assurance methodology, operational assurance technology, technology and product security research, cybersecurity science, and trusted system construction.

The UK Engineering and Physical Sciences Research Council and the National Cyber Security Center have conducted 6 rounds of ACE-CSR certifications. During each round of certifications, there was no limit to the number of institutions that could be certified. The aim of the UK government is to invite all institutions that meet the criteria to join the program. After the 2019 (sixth round) certification process, the deadline for [the next round of] ACEs-CSR certification was June 30, 2022.

In recent years, under the planning of the European Union Agency for Cybersecurity (ENISA), the EU and European Free Trade Association (EFTA) countries have established the Cybersecurity Higher Education Database (CyberHEAD), which strives to serve as a reference for all citizens wishing to advance their knowledge in the field of cybersecurity. This database enables young talents to make more informed choices by giving them a clearer understanding of the possibilities offered by higher education in cybersecurity. At the same time, it helps universities attract students interested in assuring Europe's cybersecurity.

Separately, the CyberSec4Europe research program, funded by the European Union's Horizon 2020 Program, conducted a survey of master's programs in cybersecurity at European universities. One of the program's research goals was to "identify and prioritize cyber skills needed in university education," as well as to survey existing cybersecurity curricula.

1.1.2 Domestic Situation

China also attaches great importance to the cultivation of cybersecurity talents and has issued a series of relevant policies, laws, and regulations to promote cybersecurity talent construction. In 2015, the State Council Academic Degree Committee (国务院学位委员会) and the Ministry of Education jointly issued the *Notice on Establishing Cybersecurity as a First-Level Discipline*, which aimed to comprehensively raise the level of cybersecurity discipline construction. In 2016, the Office of the Central Cyberspace Affairs Commission[4] issued the *Opinions on Curricula Construction and Talent Training for Cybersecurity*, which aimed to strengthen the discipline and major construction and talent training of cybersecurity colleges. In December 2016, China promulgated the *National Cybersecurity Strategy*, the first time cybersecurity was presented in the form of a national security document. This document set forth requirements to "implement the cybersecurity talent project and strengthen the construction of cybersecurity curricula and majors" and "form an ecosystem conducive to talent training, innovation, and entrepreneurship." The *Cybersecurity Law of the People's Republic of China* implemented in 2017 emphasized the training of cybersecurity talents. This elevated cybersecurity curriculum construction and cybersecurity talent training to unprecedented heights.

In the process of conducting cybersecurity-related major education, colleges and universities shall use government policies as supports and focal points to strengthen construction of the discipline and major of cybersecurity and reasonably plan the cybersecurity major and discipline. In China, 34 schools have already established cybersecurity as a first-level discipline (一级学科). In 2017, jointly organized by the Office of the Central Cyberspace Affairs Commission and the Ministry of Education, 7

[4] Translator's note: The Office of the Central Cyberspace Affairs Commission (中央网络安全和信息化委员会办公室; 中央网信办) is effectively the same organization as the Cyberspace Administration of China (CAC; 国家互联网信息办公室; 国家网信办), as they share the same personnel and the same offices.

colleges and universities were identified as the first batch of demonstration projects for the construction of first-class cybersecurity colleges, including Xidian University, Southeast University, Wuhan University, Beijing University of Aeronautics and Astronautics, Sichuan University, University of Science and Technology of China, and People's Liberation Army Strategic Support Force Information Engineering University. In 2019, Huazhong University of Science and Technology, Beijing University of Posts and Telecommunications, Shanghai Jiao Tong University, and Shandong University were added as the second batch of first-class cybersecurity college construction demonstration project universities. As of 2021, a total of 73 Chinese colleges and universities had established master's programs in cybersecurity (083900).

1.2 Talent Development Environment

1.2.1 College Training Environment

China's cybersecurity talent training layout is still in an early stage, but the environment for cybersecurity talent training is still not optimistic. According to statistics from the Ministry of Education Steering Committee on Instruction for Higher Education Cybersecurity Majors, China's cybersecurity talent gap in 2019 was between 700,000 and 1.4 million, while the number of cybersecurity practitioners in China was about 100,000, so the talent gap ratio is as high as 93%. Moreover, the current annual training scale of cybersecurity talents in China is about 30,000, which is far from meeting China's need for security talents. In addition, there are relatively few high-end cybersecurity talents. According to estimates by professional organizations, the number of cybersecurity practitioners needed in China will be 1.55 million in 2020 and 3.27 million in 2027. The number of cybersecurity talents currently trained is far from meeting the demand.

At present, the training of cybersecurity talent in China is mainly focused on undergraduate education, and the training of research-oriented talents (mainly master's and doctoral students) is relatively insufficient. The number of qualified cyberspace teachers is also insufficient. Because it is not long since cybersecurity was made a first-level discipline, most of the cybersecurity teachers come from other majors.

The training of cybersecurity talents in an interdisciplinary process involving a wide range of fields, and traditional knowledge systems can no longer meet the needs of national strategies and rapid industry development. The courses and knowledge systems of related majors are scattered, and students lag behind in terms of knowledge structure and practical abilities. Existing cybersecurity training programs are not completely suited for the development needs of cybersecurity itself. It is necessary to explore cybersecurity talent training models based on relevant professional knowledge and reconstruct the curriculum and knowledge system.

Cybersecurity is also a discipline with strong practicality. The traditional teaching process is weak in the cultivation of practical abilities. There is a lack of practice and innovation platforms to meet new needs, and students do not have strong engineering practice and innovation abilities. All colleges and universities have begun to pay attention to the cultivation of talents' practical abilities and have carried out many explorations in curriculum setup, experimental environments, and school-enterprise cooperation. At present, however, the talents cultivated by colleges and universities lack sufficient training in practical abilities, so it is difficult for them to meet the needs of society. Therefore, it is necessary to strengthen the experimental and practical teaching stages and build a diversified practical education system and platforms bringing together government, industry, education, research, and application.

The evaluation of the capabilities of cybersecurity talents is unique in certain ways. The traditional talent evaluation method focuses on knowledge assessment, and the quality standards for the training of cybersecurity talents have yet to be perfected. General Secretary Xi Jinping pointed out: "For special talents that we sorely lack and urgently need, we can't use the same yardstick to measure everyone." At present, the training and assessment of cyberspace talents in China has not advanced beyond “only considering degrees and publications” (“唯学位”、“唯论文”), so our ability to identify cyberspace talents is too limited.

Therefore, it is necessary to build a new mechanism for the multi-dimensional evaluation and continuous improvement of core cybersecurity capabilities to ensure the quality of cybersecurity talent training.

1.2.2 Employers’ Use of Cybersecurity Talents

In recent years, with the increasing number of cybersecurity incidents around the world, individuals, enterprises, and countries are paying increasing attention to this field, and the demand for cybersecurity talents on the part of governments and enterprises has also exploded. Cybersecurity talents are in short supply, and there is a structural shortage.

In order to cope with increasingly severe cybersecurity threats, China has gradually implemented the *Cybersecurity Law* and a series of supporting policies and regulations, and the demand at the domestic government, business, and institute level for cybersecurity talents has rapidly increased. At present, from a geographical point of view, the supply and demand of cybersecurity talents are highly concentrated. Beijing, Guangdong, Zhejiang, and Shanghai are the regions with the largest demand for cybersecurity talents. The total demand for talents of these four regions accounts for 48% of the total national demand. The demand for talents is largely related to the differences in the level of Internet development in Chinese cities and the geographical distribution of Party and government agencies, large SOEs and corporate headquarters, and cybersecurity companies.

According to survey statistics, of the talents with live-fire cybersecurity capabilities in China's cybersecurity industry today, the "bachelor's degree" group is still the main force in the industry, accounting for 68.0%, followed by the "master's degree" group, accounting for 17.5%, the "junior college and higher vocational school" (“大专/高职”) group accounting for 9.4%, while the total proportion of people with "high school" (“高中”) or "secondary vocational school" (“中专”) education is less than 5%. From the perspective of enterprises, when recruiting, employers pay the most attention to practical cybersecurity capabilities (60%), followed by professional cybersecurity expertise (45%). This shows that, in the field of cybersecurity, academic qualifications are not the most important factor for employers. What enterprises need are security technicians who have practical operational capabilities and can solve practical problems, rather than people who only have academic abilities and lack hands-on skills.

According to statistics, in the field of cybersecurity, the average monthly salary expected by job seekers is about Chinese yuan Renminbi (RMB) 14,013.2, while the average monthly salary provided by government and enterprise institutions for relevant job positions is about RMB 11,554.8. The salary level provided by employers is actually significantly lower than the salary expected by job seekers. At present, however, there are few experienced talents in the cybersecurity market. It is expected that, in the next 3-5 years, security operations and maintenance personnel with practical skills and high-level cybersecurity experts will become the most scarce and sought-after resources in the cybersecurity talent market.

China's current cybersecurity talent supply is lacking in both quantity and quality. In terms of quantity, in order to develop and grow, enterprises must continuously introduce excellent cybersecurity talents from the outside while training internal employees. Compared with traditional developers, the supply of cybersecurity talents is obviously insufficient. Even if the salary is higher than the industry average standard, it is difficult to introduce a sufficient number of talents. In terms of quality, enterprises need practical-type talents. Talents recruited from the outside lack the corresponding hands-on and problem-solving abilities, and enterprises need to provide in-depth practical training in order for them to be competent at their jobs. This will increase the cost of talent recruitment for enterprises, and also goes against the original intention of recruiting talent from the outside.

The thinking behind cybersecurity talent identification work is relatively narrow. During recruitment, the demand side usually emphasizes that the talents they require must have a professional background in cybersecurity. Even some cybersecurity talent certification agencies require a professional background or work experience when conducting talent certification. However, many people in society become cybersecurity talents through independent study, and they possess cybersecurity knowledge and skills sufficient for handling some practical problems. Therefore, if we blindly emphasize professional background and work experience, many excellent cybersecurity talents may be buried. At the same time, some traditional enterprises pay more attention to product production internally, and do not pay much attention to cybersecurity. In this case, cybersecurity personnel have few opportunities for retraining and improvement. There are few opportunities to deepen and broaden their security knowledge while working at their posts, and they have no promotion channel.

1.3 Cybersecurity Talent Practical Capability Categories

Cybersecurity talents are typical hybrid talents (复合型人才), and it is necessary to build a cybersecurity talent capability structure model based on a basic qualifications structure, knowledge structure, skill structure, and professionalism.

1.3.1 Definition of Cybersecurity Talent Live-Fire Capabilities

The live-fire capabilities of cybersecurity talents are an important goal of talent training.

Proceeding from the needs of business scenarios, the live-fire capabilities of cybersecurity talents can be summarized into four types: "attack and defense live-fire capabilities," "vulnerability mining capabilities," "engineering development capabilities," and "combat effectiveness evaluation capabilities."

1. Attack and defense live-fire capabilities refer to the ability to use cybersecurity technologies and tools to carry out security monitoring and analysis, risk assessment, penetration test event research and judgment, security operations and maintenance, and emergency response in real business (业务) environments. The factors that determine the level of these capabilities include the skill level in attack and defense business technologies, understanding of cutting-edge technology and industry dynamics, and degree of mastery of business models and service scenarios.

2. Vulnerability mining capabilities refer to the ability to comprehensively apply various technologies and tools to discover potential vulnerabilities in networks and systems. These capabilities have high requirements for theoretical and practical knowledge, tool application, work experience, and vulnerability information mastery on

the part of security talents.

3. Engineering development capabilities refer to the research and development abilities for cybersecurity products and tools and cybersecurity system integration abilities. The level of these capabilities depends on talents' own understanding of business scenarios, mastery of security knowledge and tool application, and product engineering abilities.

4. Combat effectiveness evaluation capabilities refer to the possession of top-level design and strategic planning abilities for security defense systems, the possession of operational (作战) command and coordination support abilities in response to emergency cybersecurity incidents, and the ability to evaluate the combat effectiveness of cybersecurity weapons and equipment used to complete specified tasks.

In the *Information Security Technology - Basic Requirements for Competence of Cybersecurity Workforce* (draft for comments) proposed by the National Information Security Standardization Technical Committee (SAC/TC260), cybersecurity work is divided into 5 categories: cybersecurity management, cybersecurity construction, cybersecurity operation, cybersecurity auditing and assessment, and cybersecurity research and education, as shown in Table 1-1.

Table 1-1 Job Categories and Job Tasks

No.	Job Category	Job Tasks
1	Cybersecurity management	Cybersecurity need analysis Cybersecurity planning and management Network data security protection Personal information protection Password technology applications Cybersecurity consultation
2	Cybersecurity construction	Cybersecurity need analysis Cybersecurity architecture design Cybersecurity development Supply chain security management Cybersecurity integration implementation Network data security protection Personal information protection Password technology applications

No.	Job Category	Job Tasks
3	Cybersecurity operations (运营)	Cybersecurity operations and maintenance Cybersecurity monitoring and analysis Cybersecurity emergency response management Network data security protection Personal information protection Password technology applications
4	Cybersecurity auditing and assessment	Cybersecurity auditing Cybersecurity testing Cybersecurity assessment Cybersecurity certification Electronic data forensics
5	Cybersecurity research and education	Cybersecurity research Cybersecurity training

The draft for comments lists in detail the general knowledge and general skills that cybersecurity practitioners should possess to complete work tasks and provides the basic professional knowledge and required skills that practitioners who undertake corresponding job categories should possess. Because different organizations divide job roles in different ways, the mapping relationships between job categories, job roles, and national cybersecurity career settings are also given. The live-fire capabilities of cybersecurity talents are relevant to all positions, and different types of positions have different live-fire capability requirements.

Security management positions: Talents must possess the ability to plan security strategies, coordinate security resources, design network systems, plan support systems, manage and forecast risks, design defense systems, and design emergency response systems.

Security construction positions: Talents must possess the ability to design security architecture, configure and deploy security products, perform basic security tests, schedule security support resources, design security testing plans, and identify and evaluate security risks.

Security operations positions: Talents must possess the ability to maintain the operation of network equipment, manage threat intelligence, prepare contingency plans, organize emergency drills, eliminate monitoring agendas (排除监控议程), respond to security emergencies, and trace the source of intrusion.

Testing and evaluation positions: Talents must possess the ability to perform vulnerability penetration testing, assess data risks, prepare cybersecurity audit plans, perform cybersecurity assessments and audits, conduct legal compliance reviews, and perform electronic tracing and evidence collection.

Scientific research and education positions: Talents must possess the ability to research cutting-edge technologies, discover unknown vulnerabilities, develop arsenals, formulate training plans, design training programs, implement training assessments, and evaluate and improve training content.

1.3.2 Model of Cybersecurity Talent Live-Fire Capabilities

Practice is an effective standard for testing live-fire cyberspace capabilities. In recent years, China has made a lot of useful explorations in the modes, systems, and mechanisms of cybersecurity talent examination. From the gradual strengthening of the practical training model, to the introduction of cybersecurity competitions as a mode of skill testing and evaluation, to live-fire drills and crowdtesting activities with wide participation of all different types of people, all these practices use the "technical application scenario" model to test and supervise the progress of personnel, and they have achieved remarkable results.

In conclusion, based on the four types of capabilities and three verification methods of cybersecurity talents, we launched the "4+3 model" of cybersecurity talent live-fire capabilities, as shown in Figure 1-1.

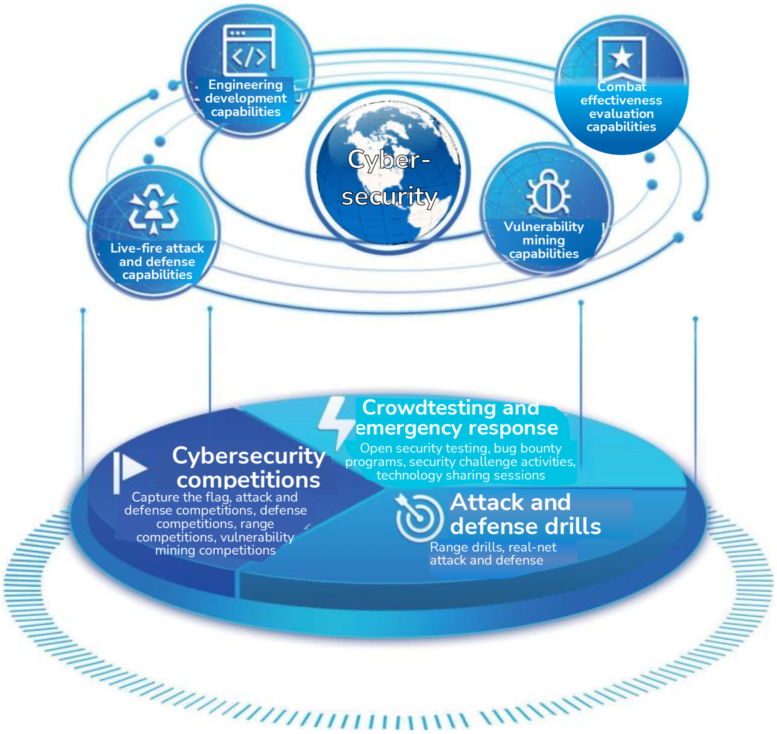

Engineering development capabilities
Combat effectiveness evaluation capabilities
Cyber-security
Live-fire attack and defense capabilities
Vulnerability mining capabilities
Crowdtesting and emergency response
Open security testing, bug bounty programs, security challenge activities, technology sharing sessions
Cybersecurity competitions
Capture the flag, attack and defense competitions, defense competitions, range competitions, vulnerability mining competitions
Attack and defense drills
Range drills, real-net attack and defense

Figure 1-1 4+3 Model of Cybersecurity Talent Live-Fire Capabilities

The subsequent sections of this White Paper will provide a detailed analysis and discussion of the "Live-Fire Attack and Defense Capabilities," which are part of the live-fire capabilities of cybersecurity talents.

Chapter 2 | Analysis of Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

With the acceleration in the process of digitalization, network boundaries are gradually disappearing and the exposure to cyberattacks is expanding without limit, posing a serious threat to cybersecurity and even national security. The pressure on the defenses of various enterprises and public institutions is increasing day by day. As the most direct and front-line important capabilities, live-fire attack and defense capabilities have become one of the cybersecurity talent capabilities that enterprises and public institutions focus on. In the context of a severe cybersecurity talent gap, cybersecurity talents with live-fire attack and defense capabilities have become the focus of attention.

Live-fire attack and defense cybersecurity capabilities refer to the potential and level of actual effectiveness of talents in real-world attack and defense cyber confrontation scenarios in terms of technology application, coordination and cooperation, and emergency response.

Specifically, live-fire attack and defense capabilities require cybersecurity personnel to master practical experience in the implementation of various security standards, be proficient in using cybersecurity technologies and tools, conduct risk assessments for specific businesses, and provide guidance and suggestions for security implementation planning. At the same time, cybersecurity personnel should also have certain investigation and evidence-gathering capabilities. They must be able to collect, process, save, analyze, and present evidence related to cyberattacks after the fact so as to provide assistance for subsequent attack source tracing or case investigation.

Cybersecurity competitions are characterized by a high level of practicality, innovation, and confrontation. After vigorous development in recent years, they have become one of the important ways to comprehensively test and improve live-fire attack and defense capabilities in the discovery, training, and selection of a large number of front-line cybersecurity talents. The concept of "promoting learning with competitions, and conducting training through competitions" has also been fully implemented in various cybersecurity work. Participants in cybersecurity competitions are playing an increasingly important role in a wide range of cybersecurity work.

In this chapter, we will use 85,761 cybersecurity competition data points from the past three years as a sample and focus on presenting a detailed description of the live-fire capabilities of Chinese cybersecurity talents. The sample covers 31 provinces (including autonomous regions and province-level municipalities, and excluding Hong Kong, Macao, and Taiwan) and the Xinjiang Production and Construction Corps nationwide and covers important industries such as communications, transportation, finance, healthcare, political and legal affairs (政法), government affairs, energy, electricity, colleges and universities, and vocational schools, the Internet, and cybersecurity.

2.1 Current Situation of Live-Fire Attack and Defense Cybersecurity Talents

2.1.1 Gender, Age, and Education

Data analysis shows a major disparity in the gender ratio of live-fire attack and defense cybersecurity talents. The overall distribution is "male-dominated," and the female population only accounts for 16% of the total, as shown in Figure 2-1.

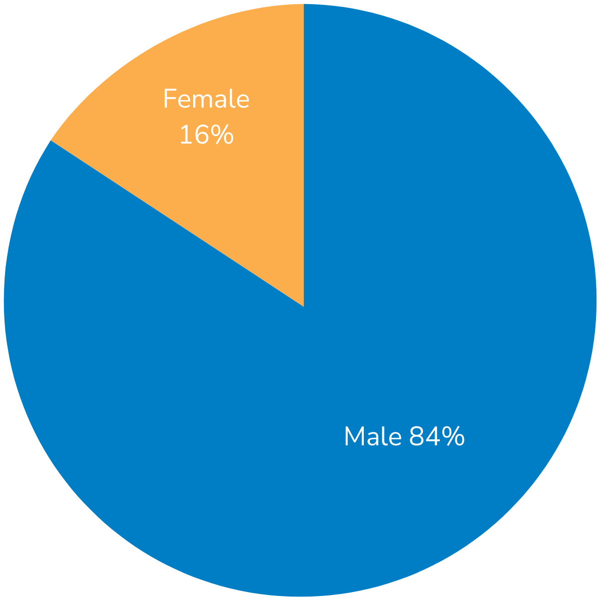


Figure 2-1 Gender Distribution of Live-Fire Attack and Defense Cybersecurity Talents

The data shows that the age of live-fire attack and defense cybersecurity talents is mainly concentrated in the "18-35" age group, among which the "20-25" group accounts for the highest proportion at 40%. The proportions of the "25-30" and "30-35" groups are relatively close, at 22% and 20% respectively, and the "under 20" group account for another 10%, as shown in Figure 2-2.

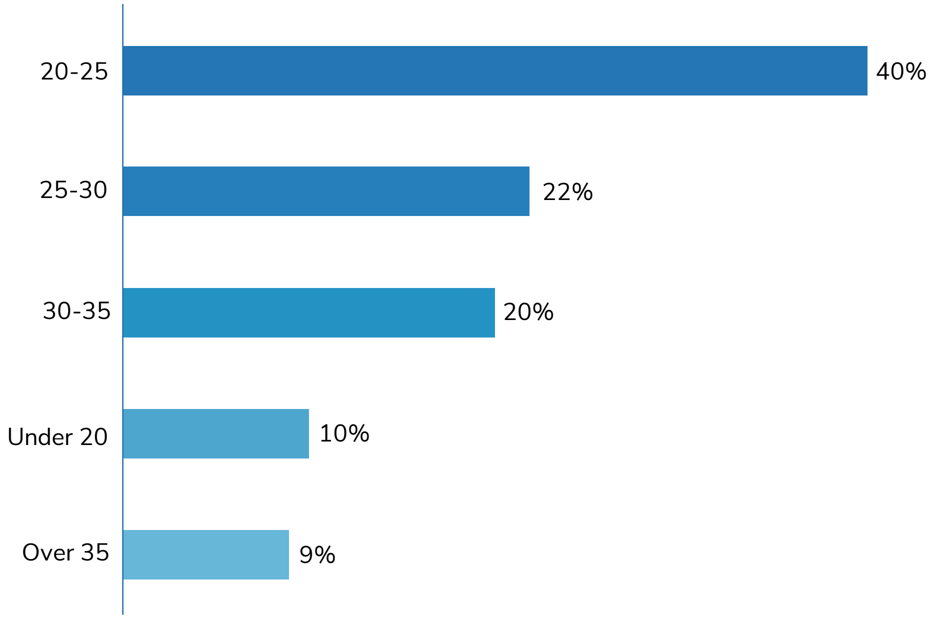


Figure 2-2 Age Distribution of Live-Fire Attack and Defense Cybersecurity Talents

Further analysis of the data shows that the "18-25" group is mostly made up of students, accounting for 95% as shown in Figure 2-3. On the one hand, the growing number of students shows that colleges and related majors are now paying more and more attention to live-fire offense and defense and there is a wide range of channels open. On the other hand, it also shows that the future reserve force of the cybersecurity industry is gradually expanding. The proportion of "students" and "practitioners" in the "25-35" age group is completely different. This age range is basically dominated by practitioners, accounting for 94%, as shown in Figure 2-3.

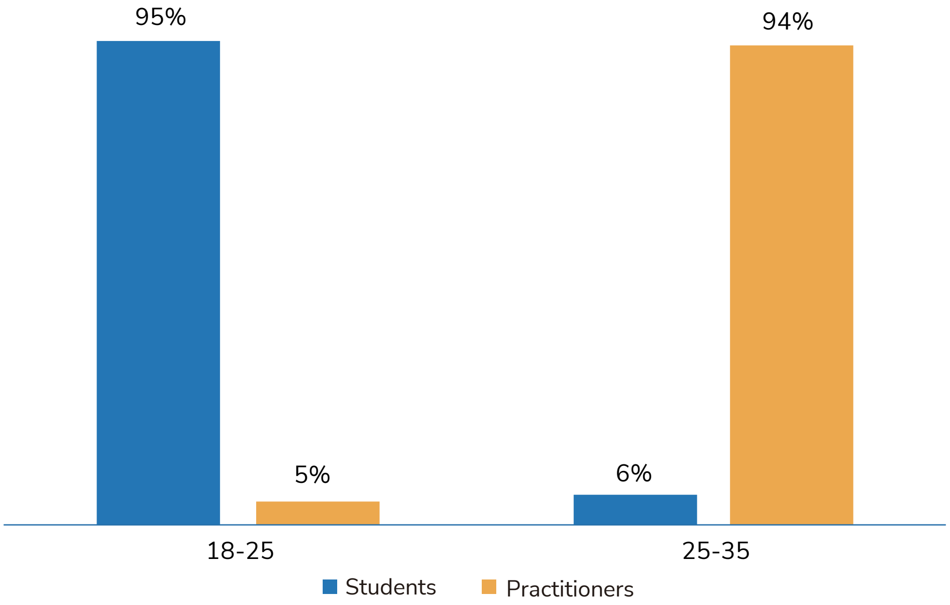


Figure 2-3 Attribute Distribution for Different Age Groups

Analyzing the education status of live-fire attack and defense cybersecurity talents shows that the "bachelor's degree" group is still the main force in the industry, accounting for 68%, followed by the "master's degree" group, accounting for 18%, the "junior college and higher vocational school" group accounting for 10%, while the total proportion of people with "high school" or "secondary vocational school" education is less than 5%, as shown in Figure 2-4.

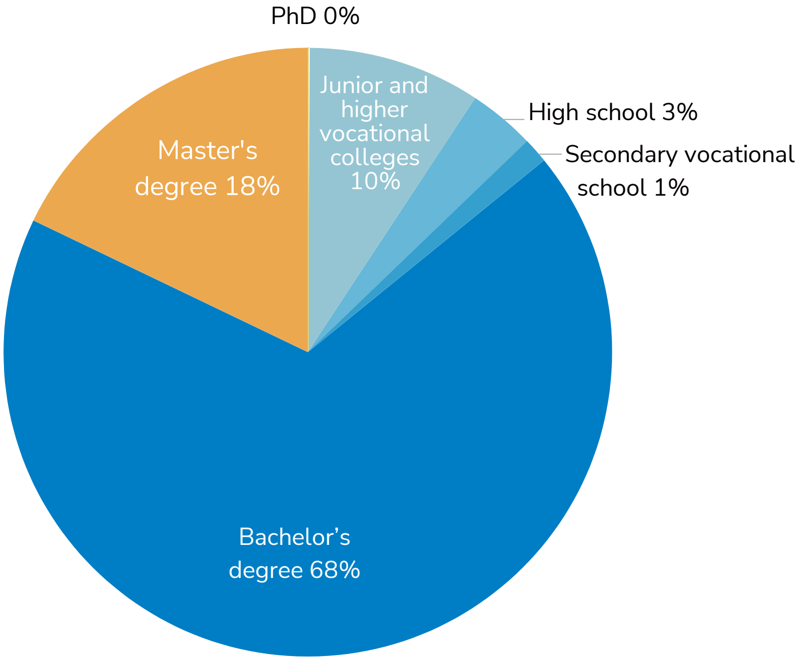


Figure 2-4 Educational Level of Live-Fire Attack and Defense Cybersecurity Talents

2.1.2 Geographical and Industry Situation

If we divide talents by geographical region, we find that live-fire attack and defense cybersecurity talents are distributed in 31 provinces (including autonomous regions and province-level municipalities, and excluding Hong Kong, Macao, and Taiwan) and the Xinjiang Production and Construction Corps throughout the country. Among these regions, "Beijing" ranked first in the proportion of live-fire attack and defense cybersecurity talents, with a total of 12.1%. Next came "Guangdong" at 10.3%, and then "Zhejiang" at 5.9%, as shown in Figure 2-5.

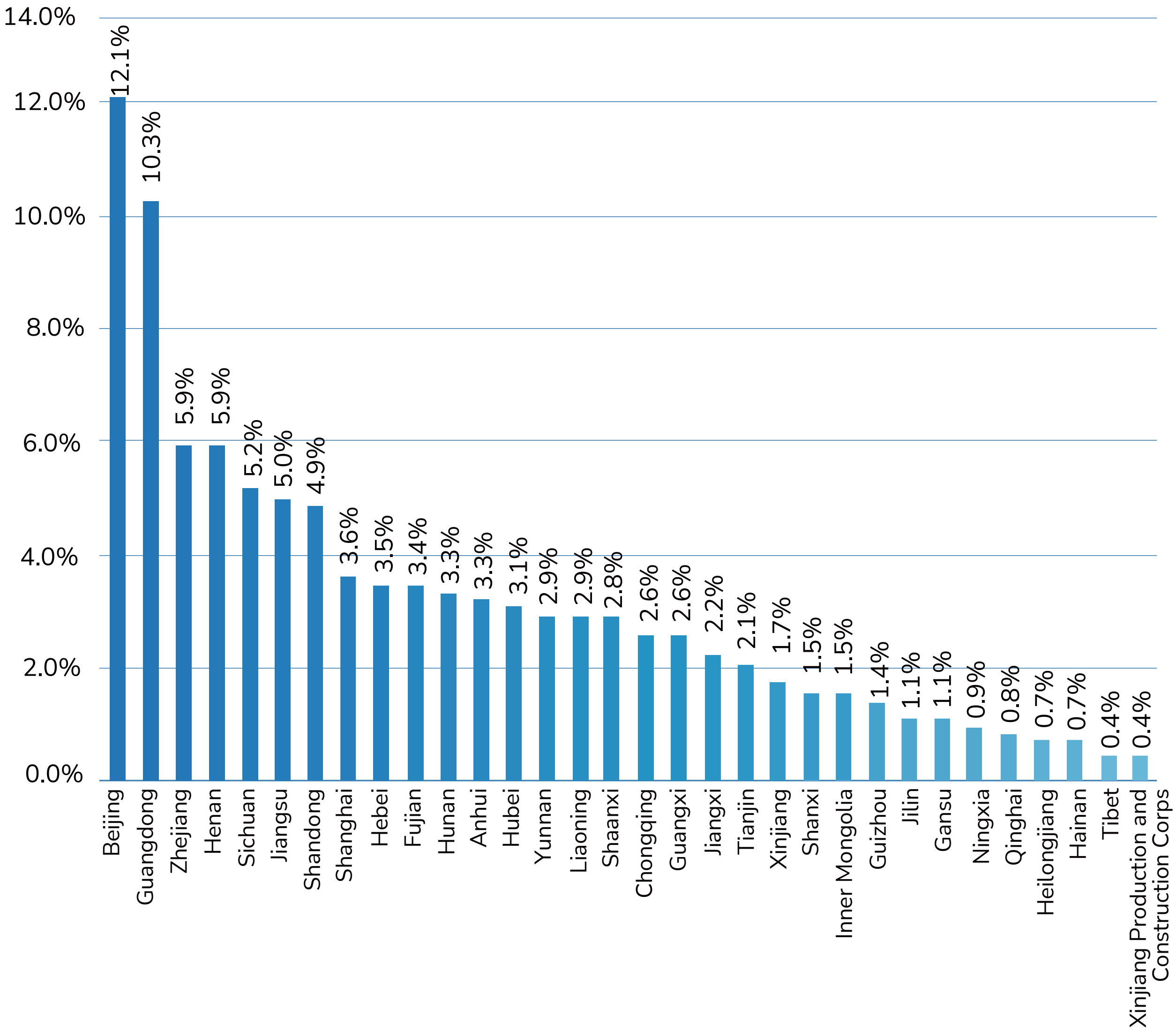


Figure 2-5 Geographical Distribution of Live-Fire Attack and Defense Cybersecurity Talents

On the whole, it can be seen that "East China" has the highest proportion of live-fire attack and defense cybersecurity talents, accounting for 28.3%, "North China" accounts for 20.7%, and the overall difference between "South China," "Southwest China," and "Central China" is relatively small, as they account for 13.6%, 12.5%, and 12.3% of talents respectively, as shown in Figure 2-6.

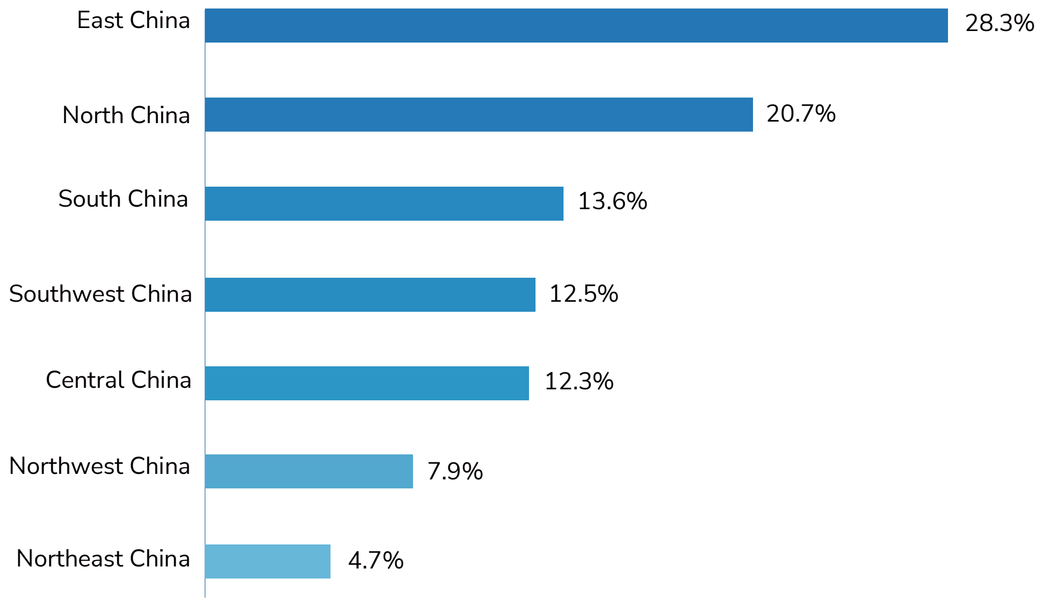


Figure 2-6 Regional Distribution of Live-Fire Attack and Defense Cybersecurity Talents

After further analyzing the industry data of live-fire attack and defense cybersecurity talents, we find that the proportion of cybersecurity talents from "institutions of higher learning" is much higher than the shares of other industries, accounting for 28% of all talents. This shows that students have a high level of participation and enthusiasm for improving their practical cybersecurity capabilities.

After "institutions of higher education", critical information infrastructure industries represented by "finance," "communications," "energy," and "transportation" account for relatively similar shares of talents, with "finance" at 11%, "communications" at 10%, "energy" at 9%, and "transportation" at 9%. In addition, "Internet enterprises" accounted for 7% of talents, and "cybersecurity companies" accounted for 4%, as shown in Figure 2-7. To a certain extent, the proportion of talents in various industries also reflects the demand of these industries for live-fire attack and defense cybersecurity talents.

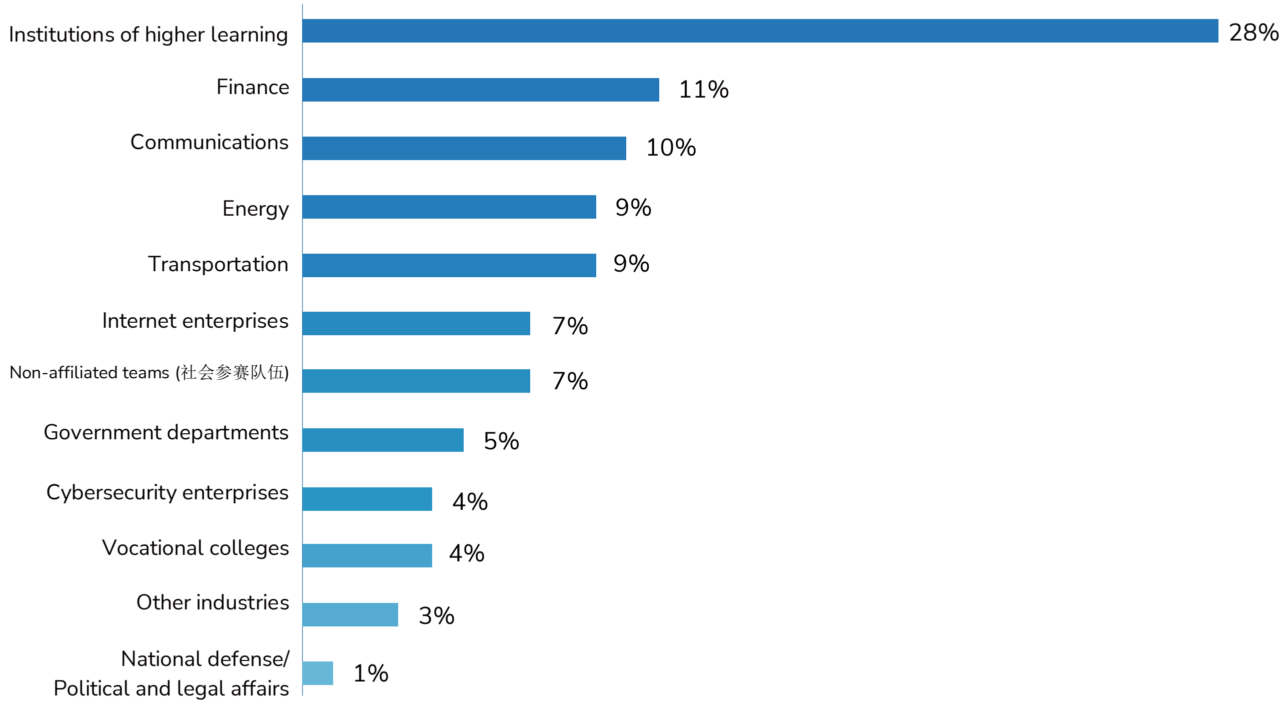


Figure 2-7 Industry Distribution of Live-Fire Attack and Defense Cybersecurity Talents

2.2 Current Situation of Live-Fire Attack and Defense Cybersecurity Capabilities

2.2.1 Technical Aspects of Live-Fire Attack and Defense Cybersecurity Capabilities

In order to more intuitively test the live-fire attack and defense capabilities of cybersecurity talents, these capabilities are generally divided into five technical directions, "web security," "binary vulnerability mining and exploitation," "reverse engineering," "cryptography research," and "other categories" (also called "miscellaneous").

The web security technical direction mainly involves intelligence collection, traceability, asset sorting, security management, risk assessment and discovery, emergency response, security operations and maintenance, security development, middleware security, database security, static code auditing, and other live-fire attack and defense technical capabilities.

The cryptography research technical direction mainly involves trusted computing, blockchain, research on encryption and decryption algorithms, implementation of cryptographic algorithms, and other live-fire attack and defense technical capabilities.

The reverse engineering technical direction mainly involves reverse analysis, defense reinforcement, security development, operating system security, virus and trojan analysis, mobile security, automated reverse analysis, and other live-fire attack and defense technical capabilities.

The binary vulnerability mining and exploitation technical direction mainly involves vulnerability discovery and exploitation, security development, operating system security, Internet of Things (IoT) security, defense reinforcement, automated vulnerability mining, and other live-fire attack and defense technical capabilities.

The other categories (also called miscellaneous) technical direction mainly involves intelligence collection, traceability, asset sorting, electronic forensics, traffic analysis, protocol analysis, 5G security applications, AI security applications, and other live-fire attack and defense technical capabilities.

2.2.2 Situation of Live-Fire Attack and Defense Cybersecurity Capabilities

The data shows that cybersecurity talents present different distributions when divided according to technical direction and expertise.

Among cybersecurity talents with live-fire attack and defense capabilities, those who are adept at web security accounted for the largest proportion at 29%, followed by reverse engineering at 22%, miscellaneous at 20%, and cryptography at 19%. However, only 10% of talents had expertise in binary vulnerability mining and exploitation, as shown in Figure 2-8.

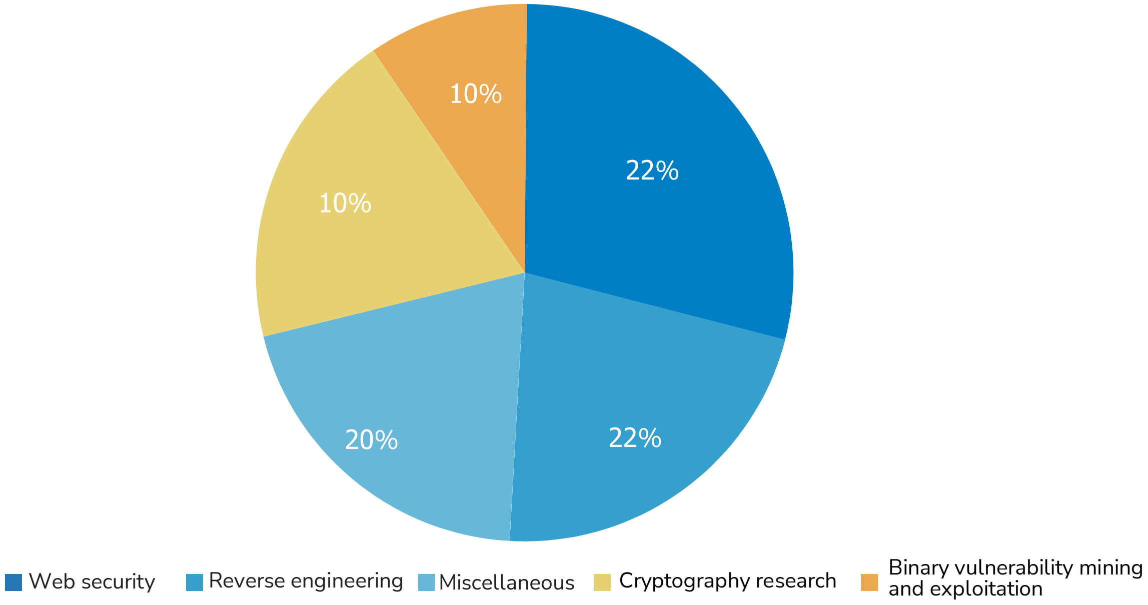


Figure 2-8 Distribution of Talents by Capability Expertise

Looking at the capability expertise of talents, 70% of talents with live-fire attack and defense capabilities have a single specialty, 15% of talents have two specialties, generalists with 3 specialties account for 10%, only 4% of talents have 4 specialties, and talents with all 5 specialties are even rarer at 1%, as shown in Figure 2-9.

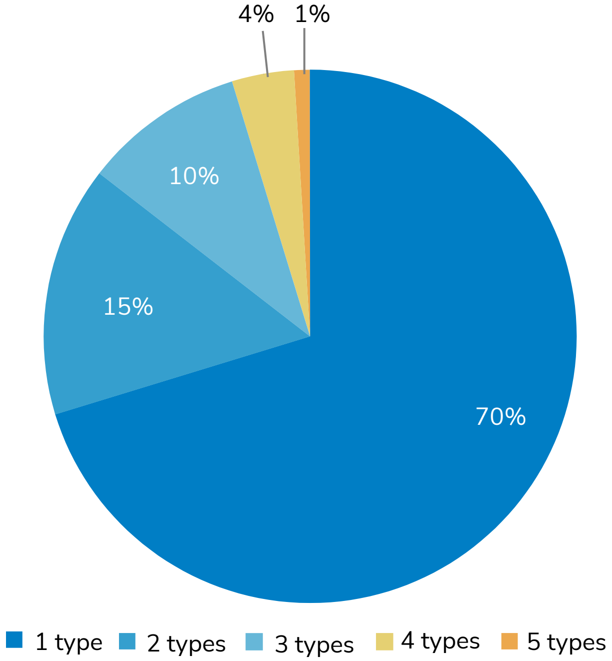
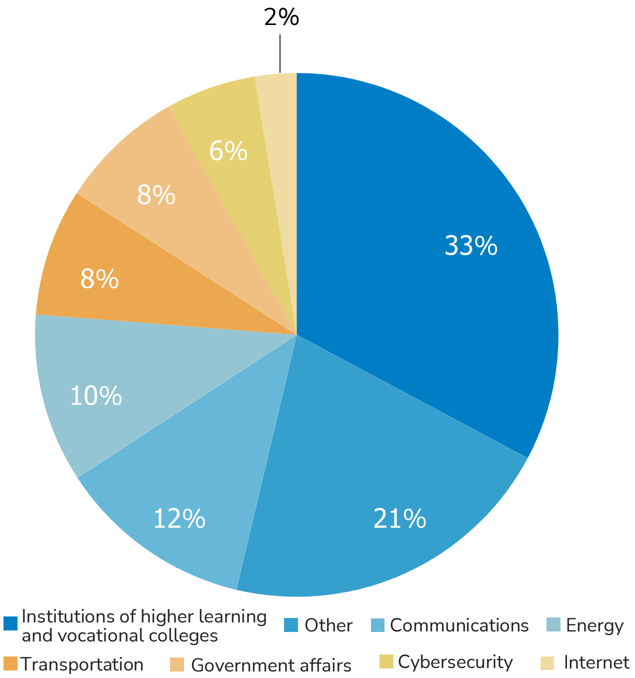


Figure 2-9 Capability Specialty Coverage of Live-Fire Attack and Defense Talents

According to the data, a statistical analysis of the dimensions of various industries shows that the live-fire attack and defense capabilities of cybersecurity talents are distributed as follows: (1) In the industry distributions of web security talents and cryptographic research talents, institutions of higher learning and vocational colleges represent the plurality, accounting for 33% and 38% respectively, and the proportions represented by the communications industry and the energy industry exceed 10% in both distributions, as shown in Figures 2-10 and 2-11.



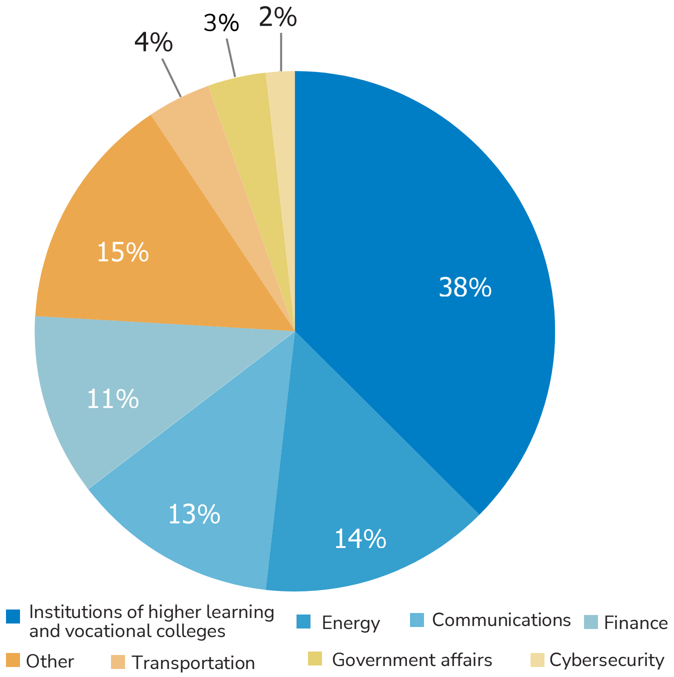


Figure 2-10 Industry Distribution of Web Security Talents

Figure 2-11 Industry Distribution of Cryptographic Research Talents

(2) In the industry distribution of miscellaneous talents, the communication industry represents a plurality, accounting for 28%, followed by the energy industry, accounting for 18%, and then the financial industry, accounting for 12%, as shown in Figure 2-12.

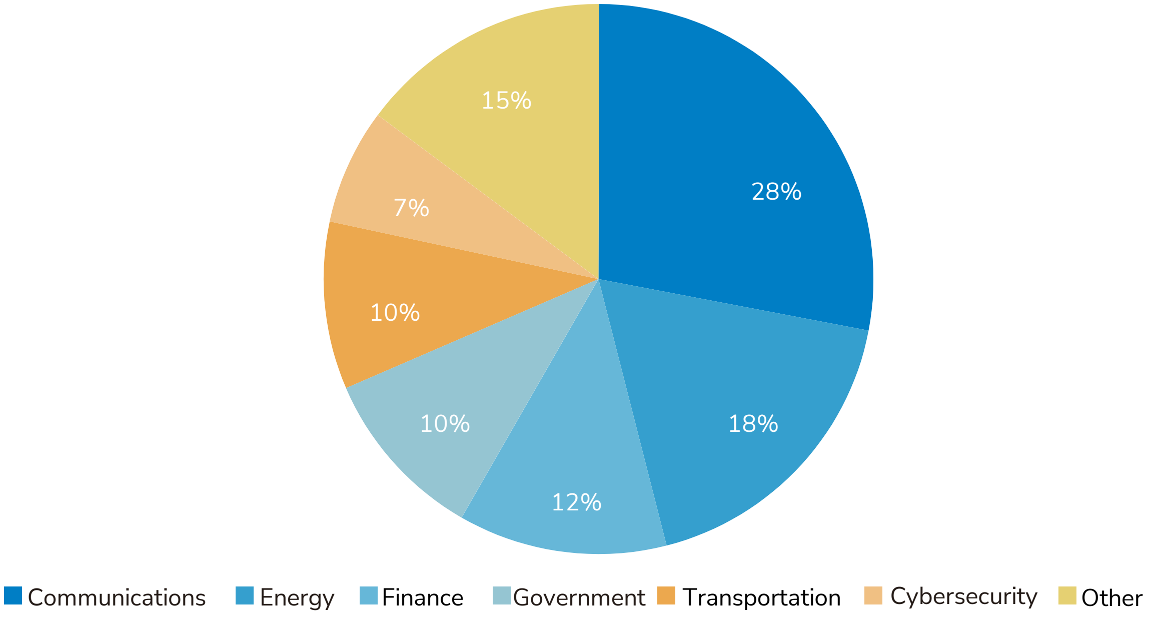


Figure 2-12 Industry Distribution of Miscellaneous Talents

(3) A plurality of binary vulnerability analysis and exploitation talents can be found in institutions of higher learning and vocational colleges, accounting for 31%, followed by the energy industry, accounting for 15%, and then the financial industry, accounting for 9%, as shown in Figure 2 -13.

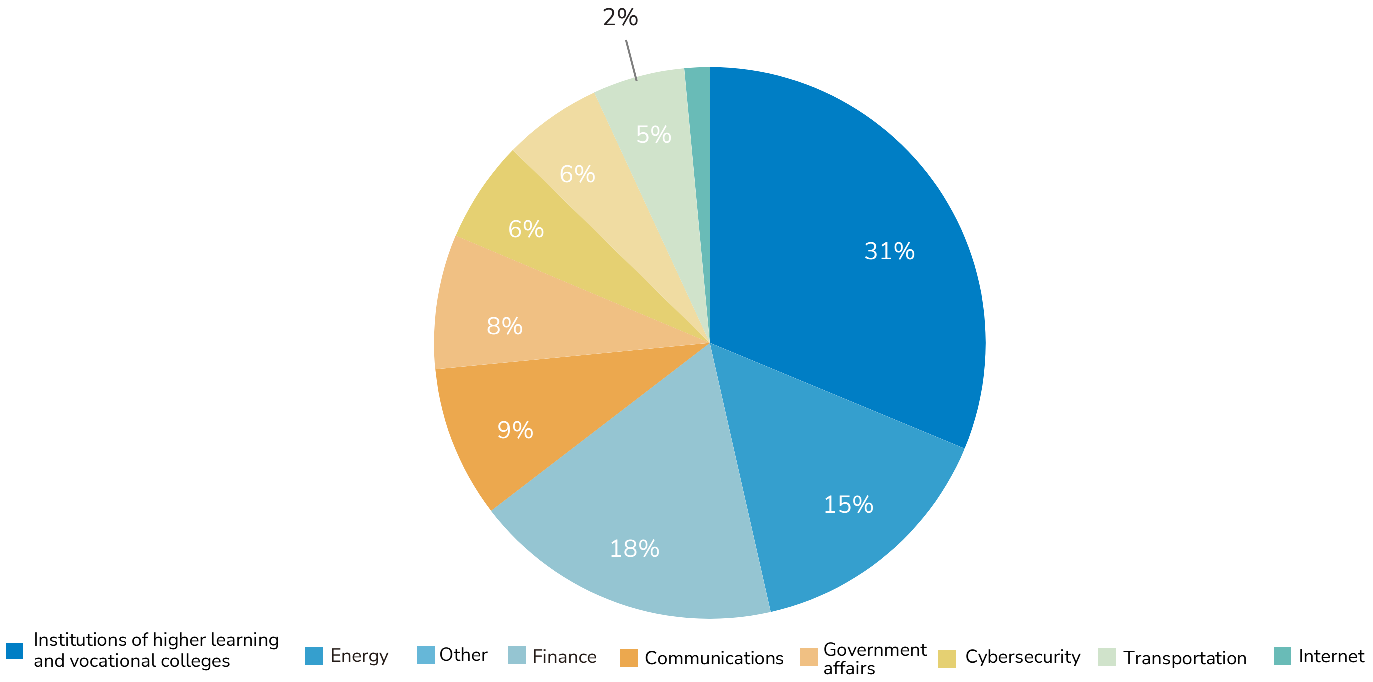


Figure 2-13 Industry Distribution of Binary Vulnerability Mining and Exploitation Talents

(4) In the industry distribution of reverse engineering talents, institutions of higher learning and vocational colleges represent a plurality, accounting for 46%, followed by the communications industry, accounting for 9%, and then the government affairs industry, accounting for 6%, as shown in Figure 2-14.

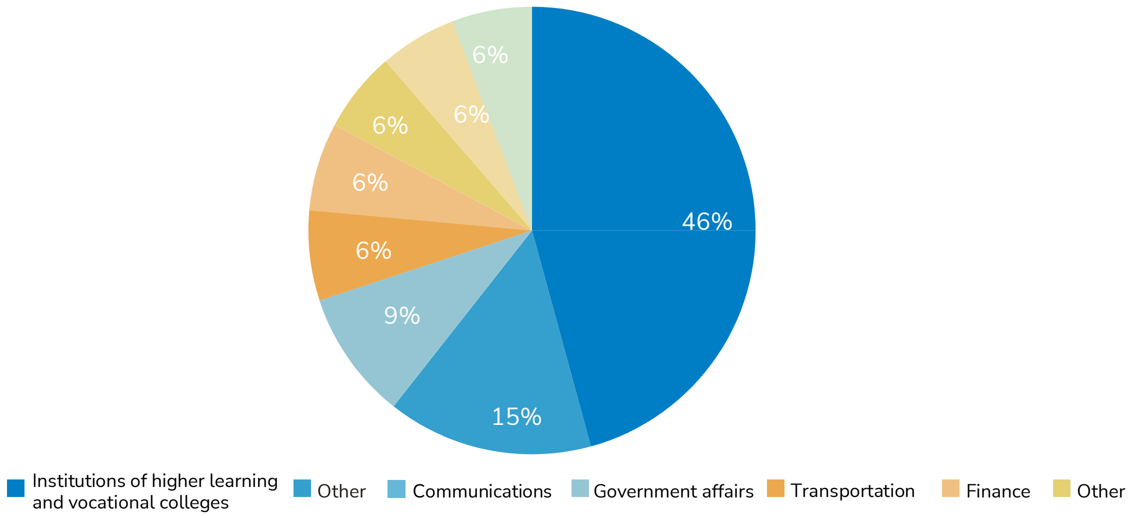


Figure 2-14 Industry Distribution of Reverse Engineering Talents

It is clear that institutions of higher learning and vocational colleges prioritize the improvement of students' live-fire capabilities. Talents from these institutions are involved in and widely participate in practical competitions of various dimensions. The communications, energy, and other industries have accumulated many talents in the web security, cryptography research, reverse engineering, and miscellaneous fields. The energy industry and the financial industry pay more attention to the technical direction of binary vulnerability exploitation and mining, and the government affairs industry pays more attention to the reverse engineering and miscellaneous technical directions.

2.3 Analysis of the Live-Fire Attack and Defense Experience of Cybersecurity Talents

2.3.1 Status of Participants in Cybersecurity Competitions

Based on a statistical analysis of cybersecurity competition data, we found that:

Among the people who participated more than 2 times in the past three years, 4% participated more than 10 times, which is a very small percentage. 11% of the participants participated 5-10 times, 16% participated 3-5 times, and 49% participated 2 times, as shown in Figure 2-15.

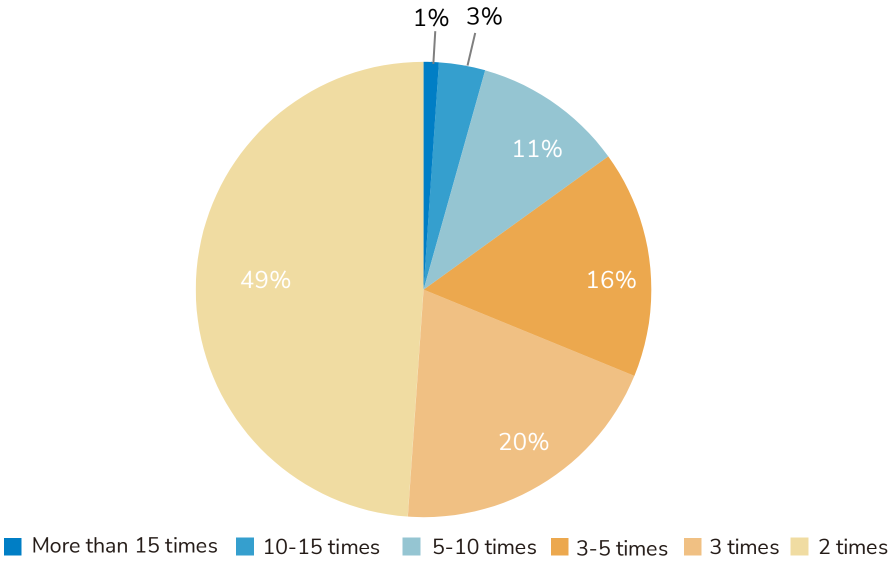


Figure 2-15 Number of Contests Participated in

Among all those who participated twice or more, more than half were from schools (58%), as shown in Figure 2-16.

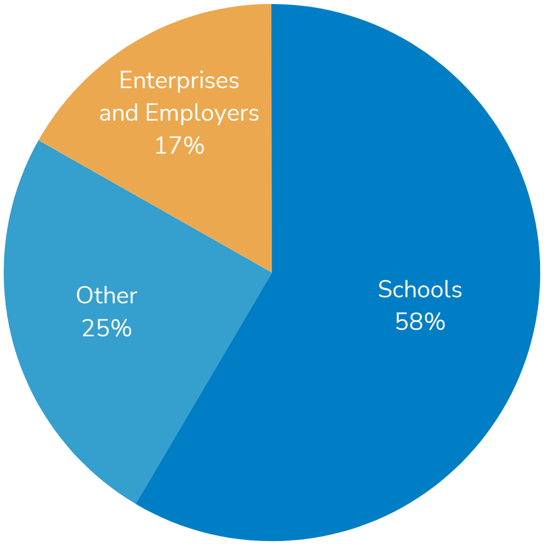


Figure 2-16 Contestants' Affiliations (min. 2 contests)

Those who participated more than 5 times still mostly come from schools, accounting for 73%, with people from enterprises and employers (企业/单位) accounting for 13%. Of people who participated 2-5 times, 17% are employees of large enterprises and employers, as shown in Figure 2-17. It can be seen that, compared with employees of enterprises and public institutions, the student group has a higher degree of participation and enthusiasm in all major competitions.

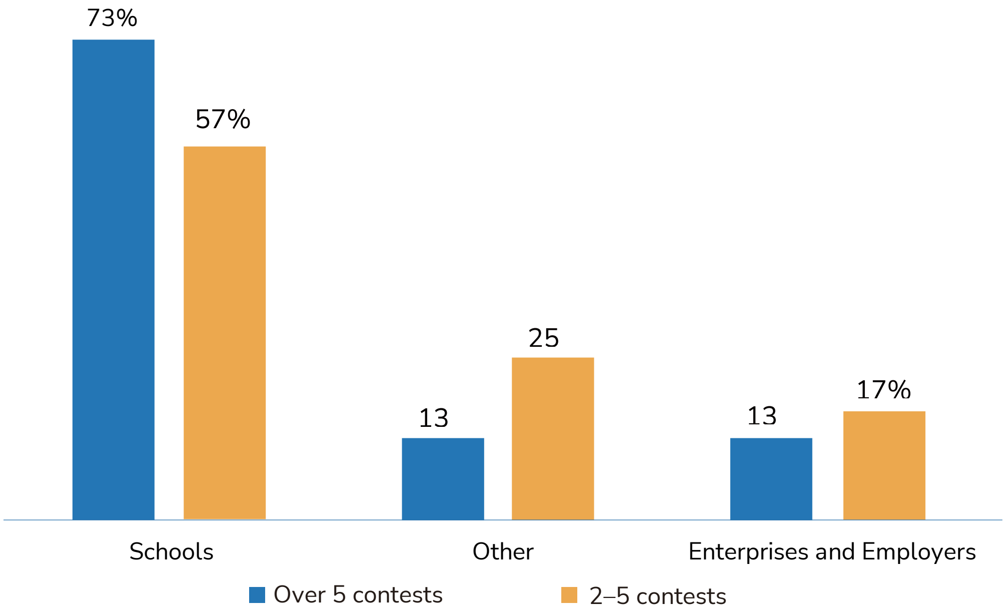


Figure 2-17 Contestants' Affiliations (2–5 and 5+ contests)

2.3.2 Cybersecurity Competition Experience and Achievements

After more than 30 years of development, cybersecurity competitions have become popular all over the world and have developed vigorously in China.

Internationally renowned competitions include capture-the-flag (CTF) competitions represented by DEF CON and cracking competitions represented by Pwn2Own. Many well-known Chinese teams participate in these competitions. In our country, various ministries, commissions, industries, and regions have held many cybersecurity competitions, providing a stage for the selection, evaluation, and improvement of the live-fire capabilities of cybersecurity personnel. For example, the "Wangding Cup" (“网鼎杯”), the world's largest national-level competition, the "Strong Net Cup" (“强网杯”), a national-level cybersecurity competition under the guidance of the Office of the Central Cyberspace Affairs Commission, and other national-level comprehensive competitions; the "Network Protection Cup" (“护网杯”), the largest domestic industrial internet cybersecurity training event, the "Health Industry Cybersecurity Skills Competition" (“卫生健康行业网络安全技能大赛”) sponsored by the National Health Commission and focusing on the healthcare industry, the "National Data Security Competition" (“全国数据安全大赛”), a national-level competition that focuses on the field of data security, the "University Students Information Security Competition - Innovative Ability Practice Competition" (“大学生信息安全竞赛创新能力实践赛”), a highly selective competition for colleges and universities nationwide, the "Blue Hat Cup" (“蓝帽杯”), a high-level cybersecurity competition for police academy students nationwide, and other industry brand competitions; the "Longjian Cup" (“陇剑杯”), China's first "defense-oriented" national-level cybersecurity competition, "Peak Geek" (“巅峰极客”), China's first city-level [cyber] range drill, the "Red Hat Cup" (“红帽杯”) in South China, the "Xiangyun Cup" (“祥云杯”) in Northeast China, the "Great Wall Cup" (“长城杯”) in the Beijing-Tianjin-Hebei region, and other regional brand competitions.

From technical exchanges to skills training, cybersecurity competitions are entering various industries and coming to provinces and cities across the country, where they continue to improve the live-fire attack and defense capabilities of cybersecurity talents. China can use this method to select talents, the organizations affiliated with the various teams can also communicate with each other through technical exchanges, and the contestants can also learn many new skills and master new technologies through the competitions, which play a positive role in personal development.

However, through an analysis of the participant data, we also found some potential problems:

First, most of the contestants come from schools. Although enterprises and organizations have a relatively large personnel base, they do not represent a high number of participants or instances of participation. Their degree of participation needs to be strengthened. In fact, this is closely related to the talent training goals of relevant majors in schools, as well as the intensity and coverage of propaganda. Many colleges and universities link some competitions with students' personal assessment and evaluation indicators, so the mentors and teachers at schools also encourage students to participate in competitions and other activities.

Second, most of the top-ranked teams are from schools. In the past three years, of the teams that ranked in the top 10 twice, schools accounted for 59%, followed by joint teams, accounting for 29%, and then cybersecurity enterprise teams, accounting for 12%, as shown in Figure 2-18.

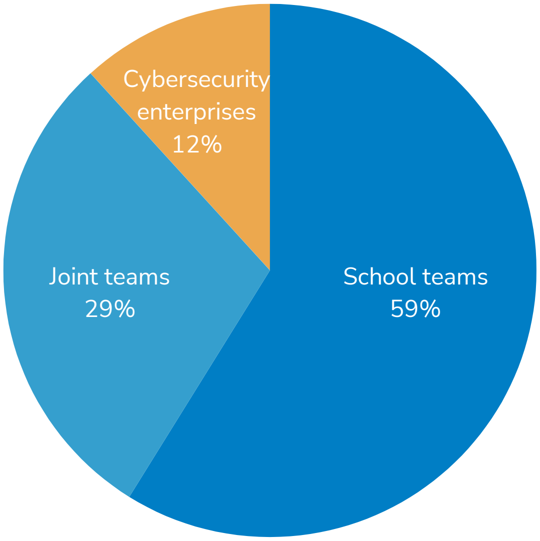


Figure 2-18 Industries of Teams Placing in the Top Ten Twice

Third, based on the statistics of people who participated more than 2 times, we found that the turnover of contestants in cybersecurity competitions is relatively high. There are few "veteran players" who have participated in multiple competitions, and most of them are college and university students. Through the questionnaire, we found that this is related to the high technical thresholds of the cybersecurity competitions and the fact that they are not sufficiently beginner-friendly.

Fourth, from the industry perspective, the distribution of high-level live-fire attack and defense cybersecurity talents is relatively concentrated:

Through composite statistical analysis of the top 100 talents for various technical specialties, we found that the cybersecurity industry accounted for the highest proportion of talents at 20%, followed by institutions of higher learning and vocational colleges with 15%. Communications comes in third, with a proportion of 13%, and energy, government affairs, transportation, and Internet account for 11%, 11%, 7%, and 5%, respectively. From an analysis of individuals, we can see that groups of high-level talents have emerged in the cybersecurity industry, institutions of higher learning and vocational colleges, and the communications industry, as shown in Figure 2-19.

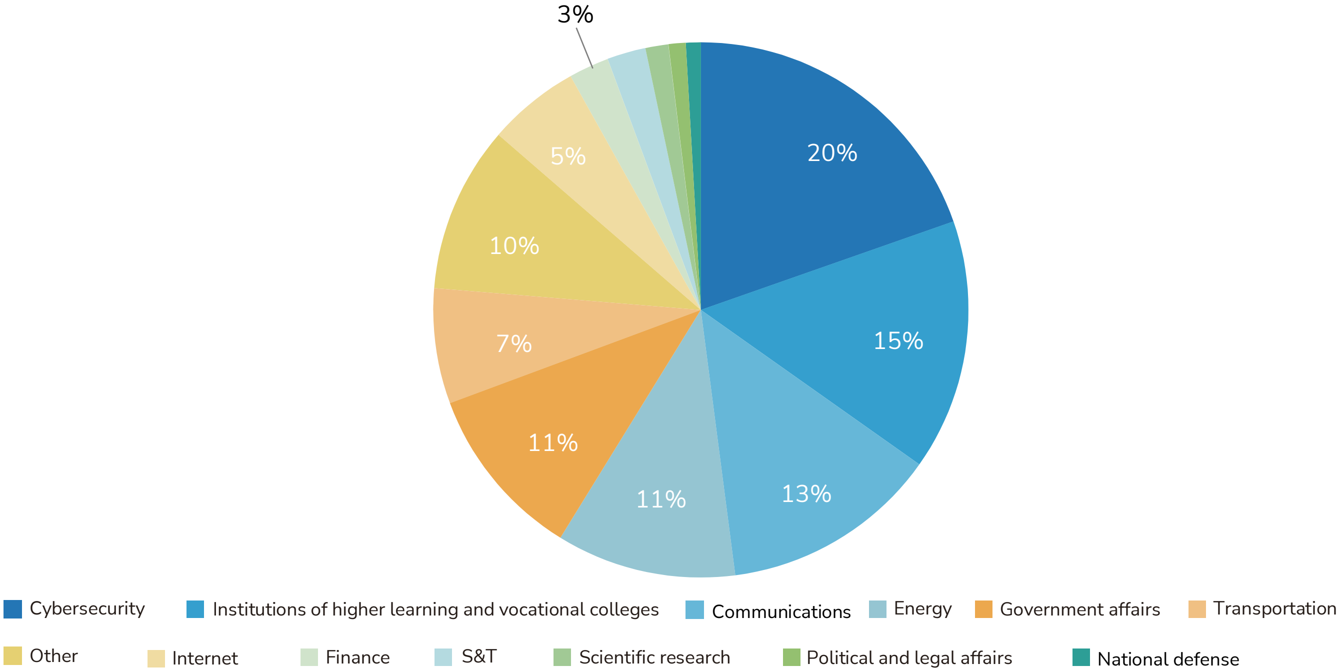


Figure 2-19 Industry Distribution of Top 100 Talents

The analysis of the top 100 talents specializing in each technical direction reveals the following industry distribution status quo:

In the web security technical direction, 26% of the top talents are distributed in institutions of higher learning and vocational colleges, followed by the energy industry with 21%, and then cybersecurity with a proportion of 12%, as shown in Figure 2-20.

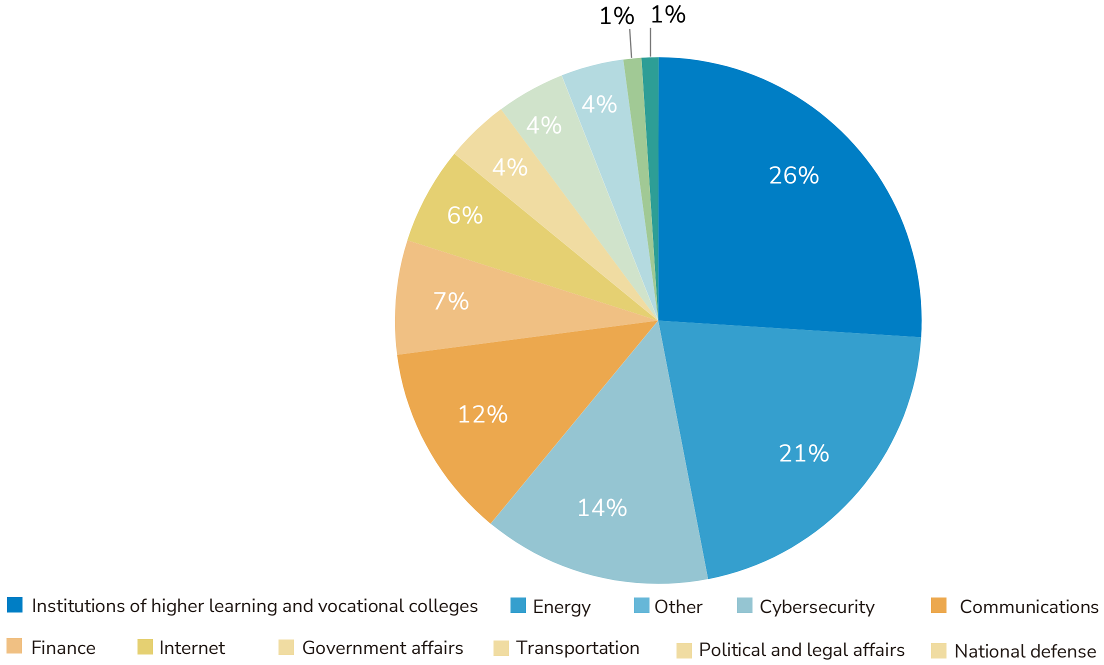


Figure 2-20 Industry Distribution of Top 100 Web Security Talents

In the miscellaneous technical direction, 34% of the top talents are distributed in the cybersecurity industry, followed by institutions of higher learning and vocational colleges with 19%, and then the Internet industry with a proportion of 12%, as shown in Figure 2-21.

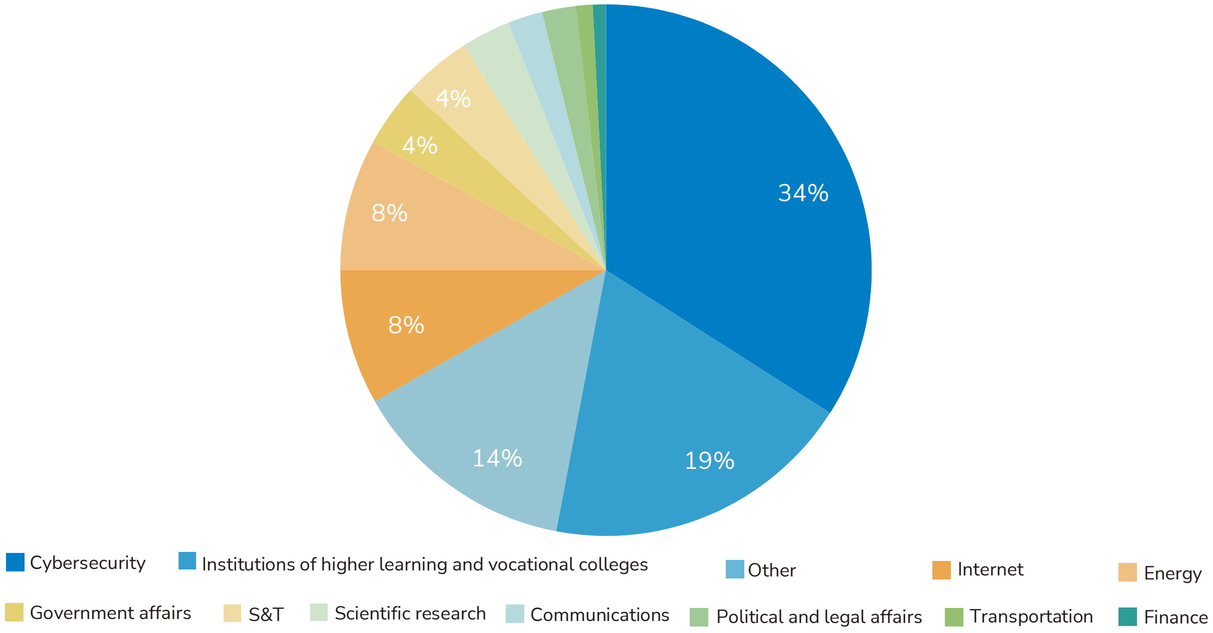


Figure 2-21 Industry Distribution of Top 100 Miscellaneous Talents

In the cryptography research technical direction, 19% of the top talents are distributed in the security industry, followed by the communications industry with

18%, and then institutions of higher learning and vocational colleges with a proportion of 16%, as shown in Figure 2-23.

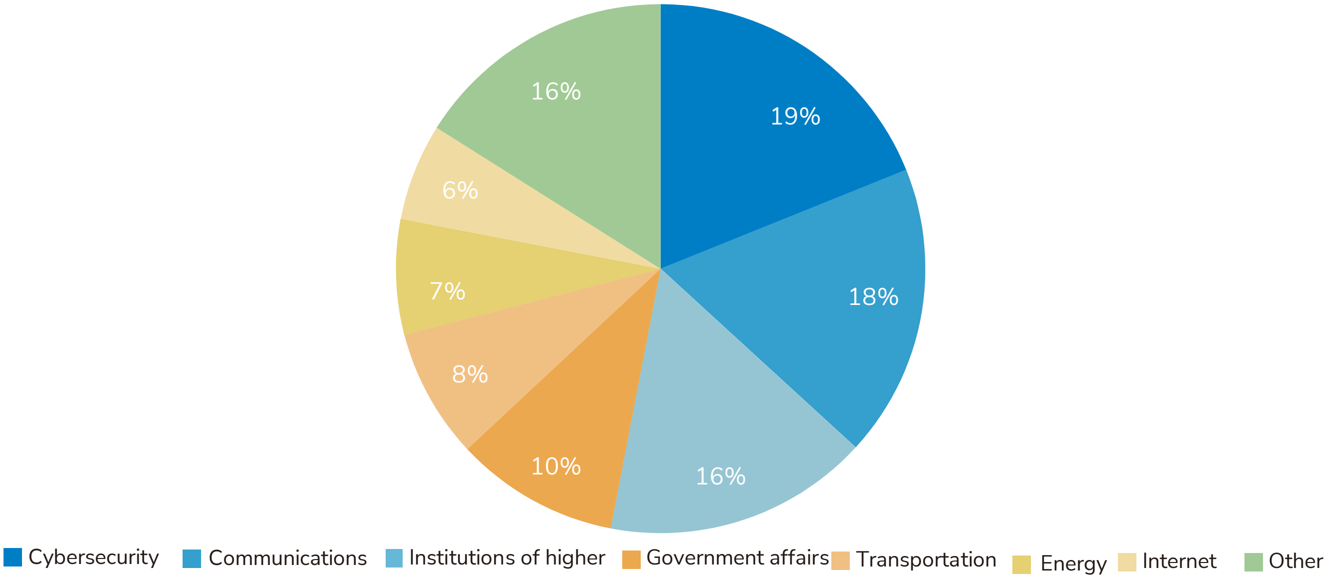


Figure 2-22 Industry Distribution of Top 100 Cryptographic Research Talents

In the binary vulnerability mining and exploitation technical direction, 28% of the top talents are distributed in the cybersecurity industry, followed by the communications industry with 19%, and then institutions of higher learning and vocational colleges with a proportion of 15%, as shown in Figure 2-23.

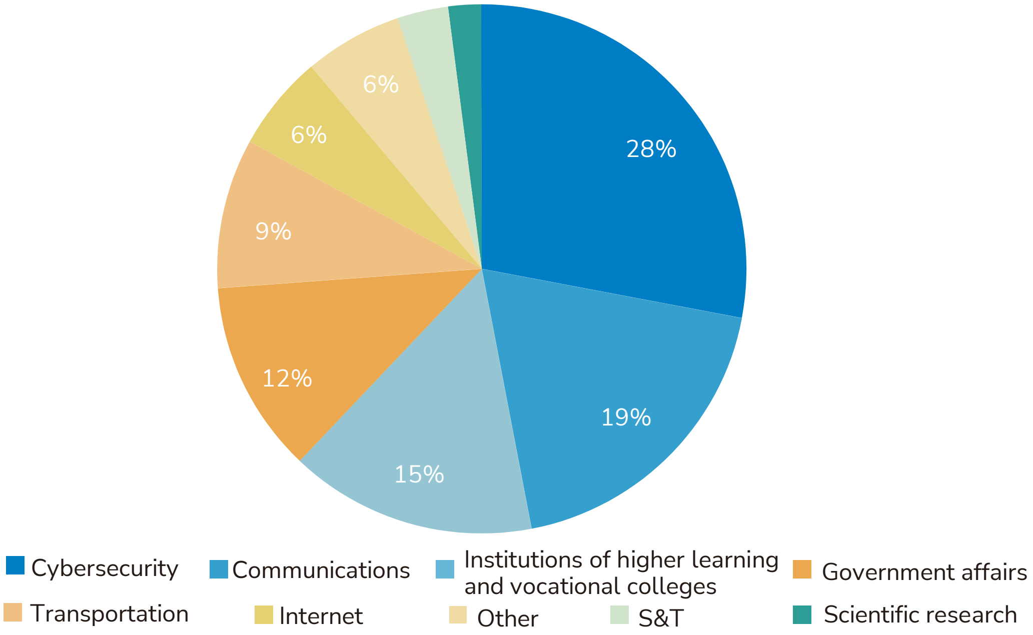


Figure 2-23 Industry Distribution of Top 100 Binary Vulnerability Mining and Exploitation Talents

In the reverse engineering technical direction, the government affairs industry and the communications industry have the most top talents, accounting for 20% each, followed by the energy industry, accounting for 18%, as shown in Figure 2-24.

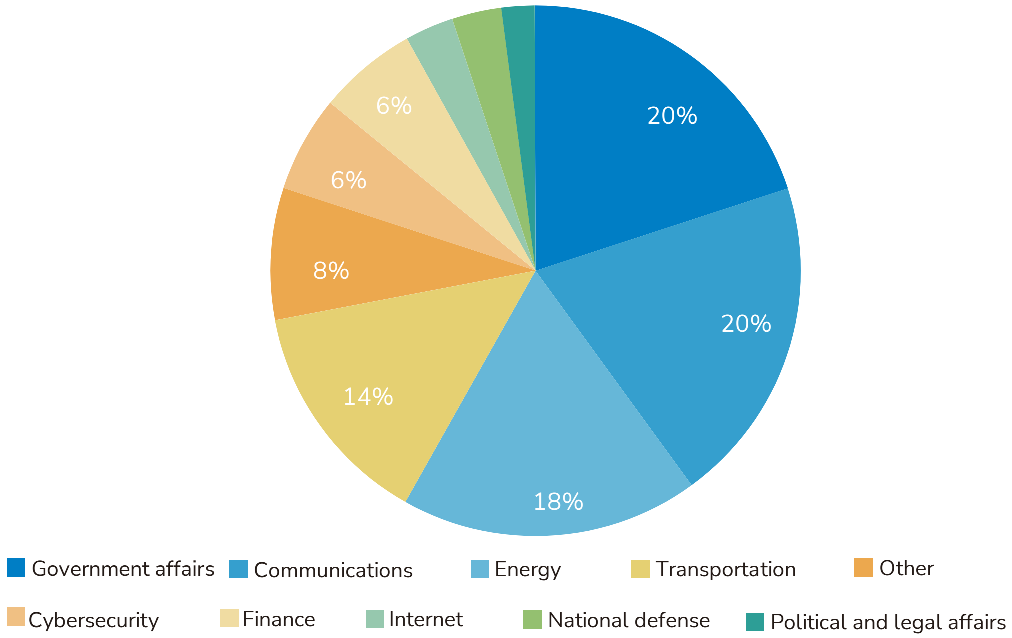


Figure 2-24 Industry Distribution of Top 100 Reverse Engineering Talents

Through statistical analysis, it is not difficult to obtain the basic characteristics of the live-fire attack and defense capabilities of talents:

First, it describes the current situation of the distribution of cybersecurity live-fire talents with reference to three dimensions: basic information, live-fire skills, and needs of the field. From an analysis of the basic information dimension, we found that young people make up the main body of cybersecurity talents, and the majority of them are students who are continuing to grow. This is closely tied to the education investment of schools and other scientific research institutions, as well as the professional choices of students themselves. Second, the gender ratio of cybersecurity talents has a significant imbalance, with the entire talent population dominated by men. In the future, we can consider how to attract more female groups to join the cybersecurity-related workforce. In addition, in terms of geographical distribution, cybersecurity talents are widely distributed across the country, with Beijing and Guangdong topping the list. In terms of regional distribution, cybersecurity talents show a marked preference for East China and North China, which is obviously due to their technological advancement and economic superiority.

From the perspective of live-fire skills, the proportions of personnel who are adept at web security and reverse engineering are the largest. In the future, we should strengthen the cultivation of talents in the other three directions, and especially in binary vulnerability exploitation and mining. There are some differences in the distribution of talents who specialize in different directions. Generally speaking, the plurality of talents in each direction come from institutions of higher learning and vocational colleges. To a certain extent, this reflects that these institutions attach great importance to the improvement of students' live-fire capabilities. Students are involved and extensively participate in practical competitions that focus on various dimensions, and most social industries focus on specific fields.

From the perspective of the needs of the field, there is an overall shortage of live-fire attack and defense cybersecurity talents. This shortage is obvious for high-level talents, and most of such talents are distributed in the cybersecurity industry and institutions of higher learning and vocational colleges. For different live-fire directions, the concentration and distribution of top talents show marked differences. It is worth noting that most live-fire attack and defense cybersecurity talents only have a single specialty, and there is a shortage of well-rounded talents. This tells us that, in the future, we should strengthen the cultivation of multi-dimensional high-level talents and pay attention to the comprehensive development of live-fire cybersecurity talents.

General Secretary Xi Jinping has repeatedly emphasized that, without cybersecurity, there is no national security. As another line of defense outside of the national people’s army (国家人民军队), the importance of the live-fire capabilities of cybersecurity talents goes without saying. In today's rapidly developing society, the formation and strengthening of practical cybersecurity capabilities are becoming increasingly important. Paths form from people treading upon them, and steel comes from iron forged in flame. Likewise, to achieve excellence in live-fire capabilities, skills must be honed gradually through the joint efforts of all different types of people. Only with the courage to reform and innovate and the determination to forge ahead, can we stand at the forefront and remain invincible in this era of fierce competition.

Chapter 3 | Analysis of Employer Needs for Live-Fire Attack and Defense Cybersecurity Talents

At present, as the development of the digital economy accelerates, digital technology is being applied more deeply to all aspects of enterprise production and operations, giving rise to more complex and hidden cybersecurity risks. Therefore, new scenarios and new technologies in various industries present new requirements for cybersecurity defense. China has issued the *Cybersecurity Law*, *Regulation on Protecting the Security of Critical Information Infrastructure*, *Data Security Law*, and many other laws and regulations. As an important component of national security, cybersecurity has been elevated to the height of national strategy. "Competition in cyberspace is, in the final analysis, competition for talent." It has become the consensus of all industries and units that people are the core of security. Especially for government and enterprise units that are in the critical period of digital transformation, the lack of talents has become a problem that must urgently be solved, especially the shortage of live-fire talents. This is becoming a major bottleneck that hinders the improvement of government and enterprise cybersecurity capabilities and levels.

The *Regulation on Protecting the Security of Critical Information Infrastructure* requires that we "encourage cybersecurity professionals to engage in critical information infrastructure security protection; and include operator security management personnel and security technical personnel training in the national continuing education system."

The *Notice on Further Strengthening the Cybersecurity Work of Central Enterprises* ([2017] No. 33) (关于进一步加强中央企业网络安全工作的通知) requires that: we must "increase the intensity of personnel training, improve personnel training mechanisms, strengthen the skills training and assessment of work personnel, carry out qualification certification for personnel in key cybersecurity positions, and improve the capacity to allocate cybersecurity personnel."

The 14th Five-Year Plan emphasizes that, "the state shall provide support to enterprises, institutions of higher learning, vocational schools, and other educational and training institutions to conduct cybersecurity-related education and training, adopt multiple approaches to cultivate cybersecurity talents, and promote exchanges among cybersecurity talents."

Under the guidance of relevant national laws and regulations, various industries have conducted many beneficial explorations in the modes and systems for training cybersecurity talents. The training of cybersecurity talents has been accelerated, and cybersecurity talent training mechanisms are being actively established. From the gradual strengthening of the practical training model, to the introduction of cybersecurity competitions as a mode of skill testing and evaluation, to the practical drills and crowdtesting activities widely participated in by all types of people, all these developments have played an important role in promoting the improvement of the live-fire attack and defense capabilities of cybersecurity talents and have achieved remarkable results.

However, we still face a serious shortage of cybersecurity talent. From the perspective of employers (用人单位), the number of professional cybersecurity positions and personnel at many employers is far from sufficient, and such positions are still considered "part-time" at most employers with many cybersecurity job responsibilities concurrently performed by personnel at other informatization (信息化)-related positions. The fact that allocations of resources, staffing, and training do not match security business development has also become a factor that restricts the recruitment of cybersecurity talents by employers. In addition, the improvement of the overall live-fire attack and defense capabilities of employers depends on the high quality of professional technical personnel and is also closely related to the level of security capabilities of personnel in related positions such as operation and maintenance and research and development. Therefore, finding ways to effectively establish a sound talent system and form scientific and reasonable talent training and evaluation mechanisms would provide important support for promoting the continuous and stable production and operation of enterprises. At the same time, the talent application mechanisms of employers restrict the emergence of experts and geniuses in the field of cybersecurity to a certain extent. This is also a difficulty for employers who need live-fire talents.

In view of the background and current situation presented above, employers have begun to actively marshal their forces to cultivate live-fire cybersecurity talents based on their own business characteristics. Next, this chapter will present organized statistics and analysis concerning the nature and characteristics of employers, job requirements, and other dimensions. Here, we are striving to objectively present the real situations of employers in terms of their needs for cybersecurity talents with live-fire attack and defense capabilities.

3.1 Analysis of Employer Characteristics and Talent Demand

3.1.1 Analysis by Geographical Dimension

We analyzed the characteristics and situation of cybersecurity talents of employers in different regions. The statistics on the talent needs of employers in various provinces (including autonomous regions and province-level municipalities) and the Xinjiang Production and Construction Corps are shown in Figure 3-1.

In terms of geographical distribution, the current demand for cybersecurity talents is highly concentrated in first-tier provinces and municipalities, such as Beijing, Shanghai, and Guangdong. Among them, the demand for cybersecurity talents in Beijing accounts for 18% of the national demand, Guangdong follows closely behind at 15.2%, and then comes Zhejiang at 10.2%. Comparatively, Shanghai's demand for cybersecurity talents has decreased, and it now ranks fourth. Beijing, Shanghai, Guangdong, and Zhejiang's combined demand for cybersecurity talents amounts to nearly half of nationwide demand. This is also related to the fact that these areas have high concentrations of large government and enterprise organizations. Likewise, most cybersecurity companies are headquartered in first-tier provinces and cities.

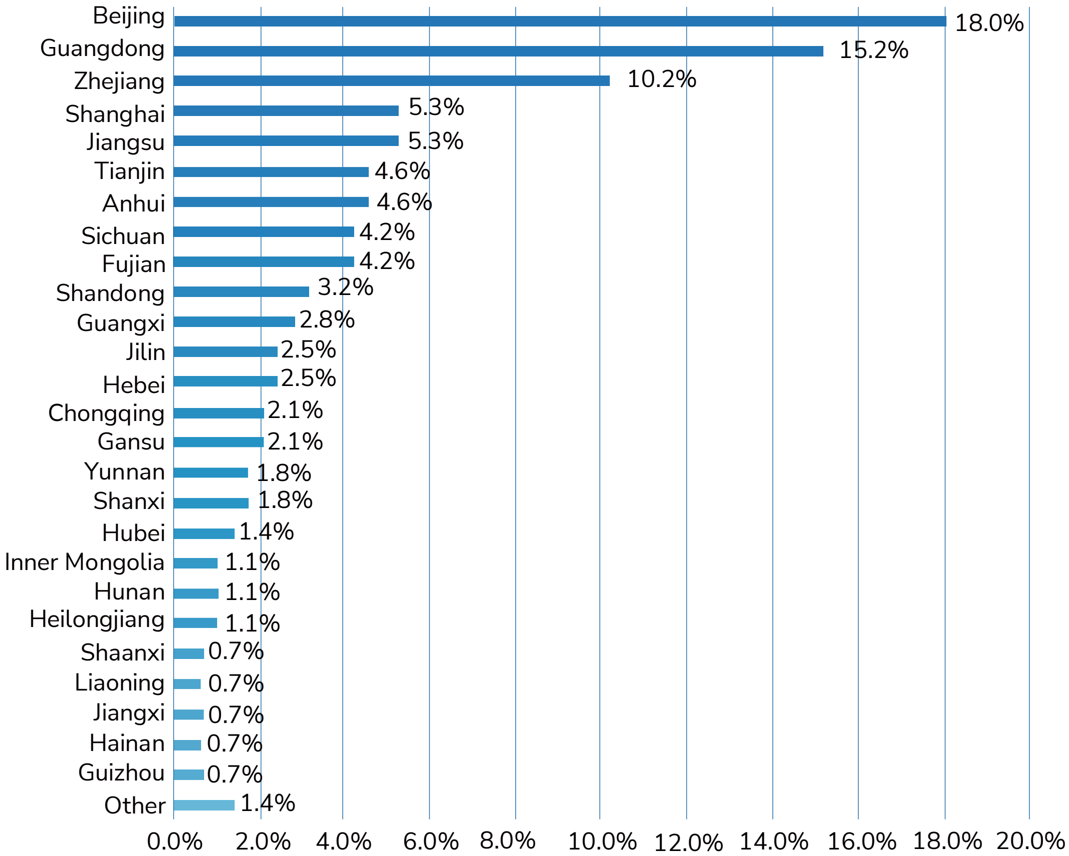


Figure 3-1 Regional Distribution Statistics of Employers

According to an analysis of the technical capabilities employers need from cybersecurity talents in the Beijing, Shanghai, Guangdong, and Zhejiang regions, we found that the demand for talent in the penetration testing direction is the most significant, accounting for 36%.[5] This is followed by the reverse analysis direction and

[5] Translator's note: When presenting data on survey responses, some of the percentages reported

vulnerability discovery and exploitation direction, which account for 32% and 26% respectively. At the same time, we found that in recent years, as various industries have paid more attention to practical cybersecurity attack and defense capabilities, security operations and maintenance has become an independent position. This position is being separated from network operation and maintenance engineers, and its influence is growing. This is shown in Figure 3-2.

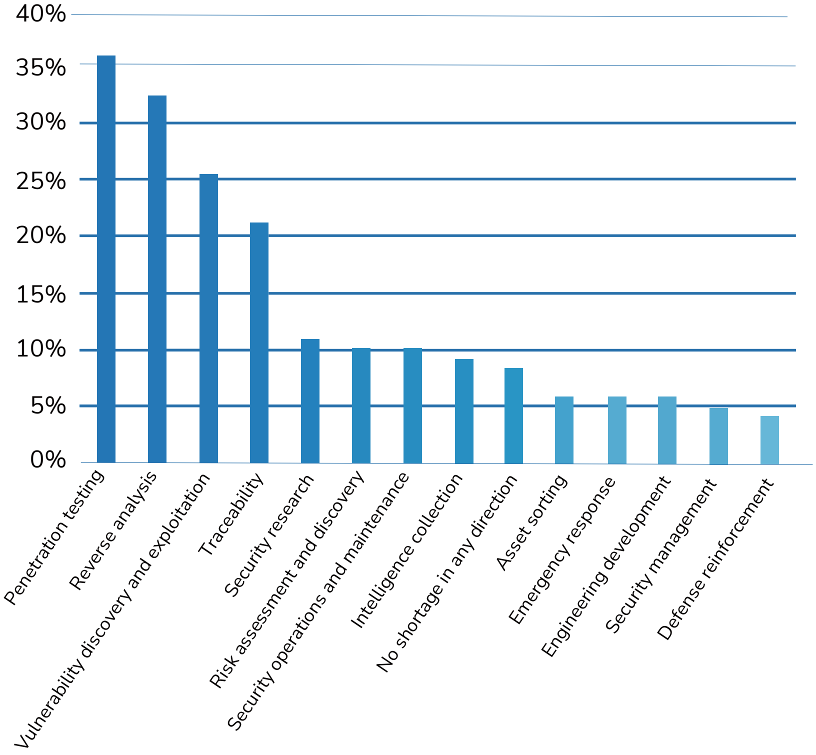


Figure 3-2 Talent Direction Needs in Beijing, Shanghai, Guangdong, and Zhejiang

On the whole, first-tier regions such as the Yangtze River Delta, Pearl River Delta, and Beijing-Tianjin-Hebei have commonalities in their demand for talents, but also have their own unique characteristics. As shown in Figure 3-3 below, all regions have high demand for cybersecurity talents in penetration testing, vulnerability mining, analysis, and exploitation, and reverse analysis, followed by virus and trojan analysis and web security. Beijing-Tianjin-Hebei has high demand for talents in the field of web security. Compared with other regions, the Pearl River Delta needs talents with traceability capabilities and capabilities in emerging security fields such as cloud, 5G,

appear to represent the percentage of respondents reporting a certain situation. For example, the 36% above means that 36% of the employers surveyed reported a need for talents with penetration testing capabilities, rather than meaning that the demand for penetration testing talents accounted for 36% of total demand for talents. The exact meaning of the statistics is often left ambiguous in the source text.

AI, and blockchain.

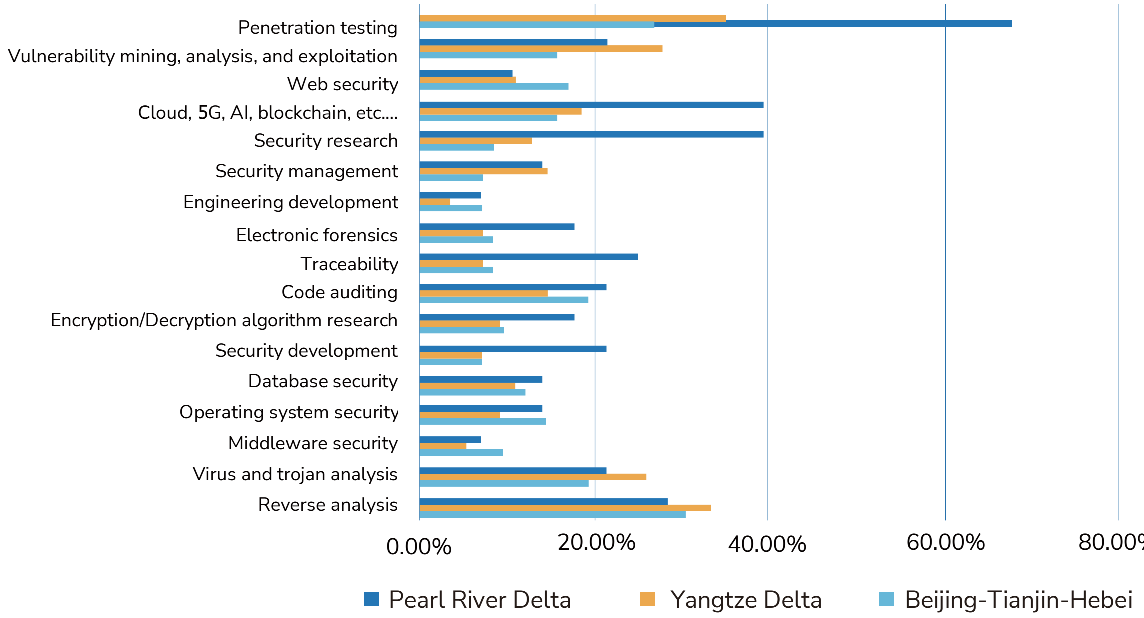


Figure 3-3 Talent Capability Needs in Three Major Regions

3.1.2 Analysis by Industry Dimension

Whether it is in the macro context, the state's guidelines for various policies on cybersecurity, or the micro context, the increase in the potential security awareness of each individual citizen reflects the importance and necessity of cybersecurity to a large extent. In terms of enterprises, the actual demand for cybersecurity talents also varies depending on the industry of the enterprise, the nature of the organization, and the scale of its staff.

After analyzing the demand for cybersecurity talents in various industries based on existing data, we found that the demand in the energy industry ranks first, accounting for 21% of demand broken down by industry, followed by communications, political and legal affairs, finance, and transportation, which account for 16%, 14%, 9%, and 7% of cybersecurity talent demand.

It is worth noting that the share of talent demand represented by cybersecurity enterprises and healthcare also ranks in the top 10, at 6% each. However, after screening for and analyzing cybersecurity practitioners in the education industry (not including students), the data shows that the demand of the education industry for cybersecurity talents still accounts for 2%. This is shown in Figure 3-4.

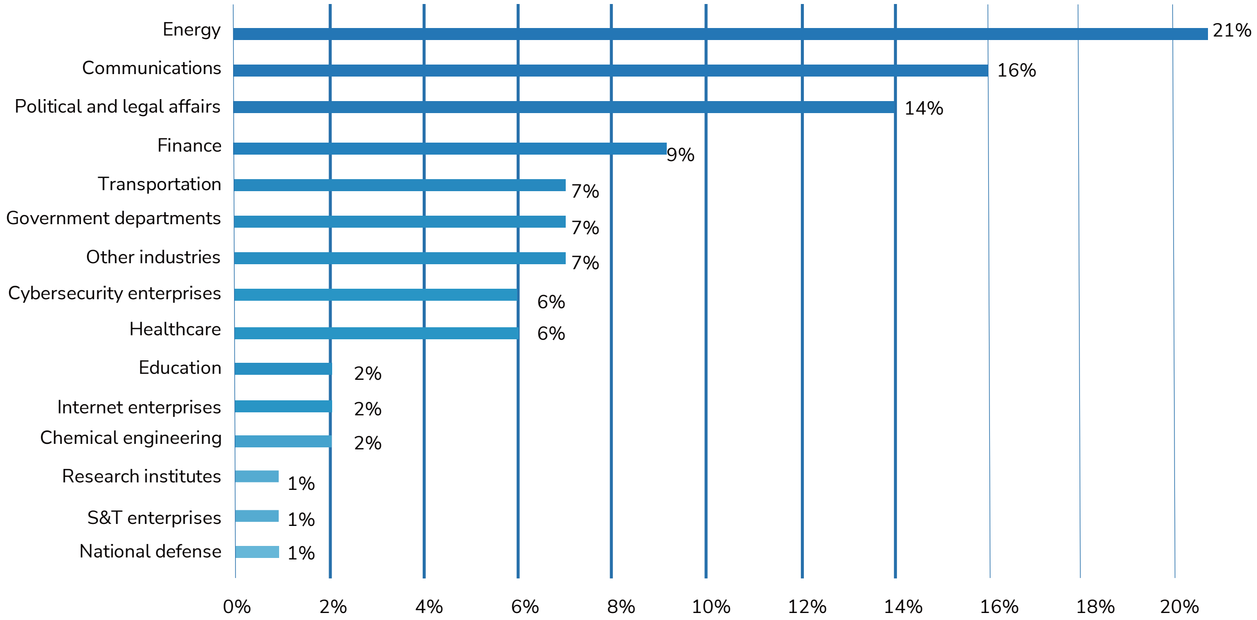


Figure 3-4 Distribution of Talent Demand by Industry

As key information infrastructure, the finance, energy, electricity, communications, transportation, and healthcare industries are the nerve centers of economic and social operations and the top priority of cybersecurity. At the same time, as industries with high economic strength and high requirements for business continuity, they began to build a tiered system of cybersecurity talents many years ago. While meeting employers' own security work needs, systemic and large-scale participation in security competitions, attack and defense drills, risk assessments, and other work stimulate and drive the cultivation of industry security talents.

Taking the five industries of finance, communications, healthcare, education, and the Internet as examples, we analyze their talent capability requirements below.

(1) Financial industry talent requirements

According to an analysis of survey data, the most obvious demand of the financial industry is for cybersecurity capabilities in the directions of penetration testing and reverse analysis, accounting for 30% each.[6] This industry also has a high demand for cybersecurity capabilities in the directions of web security, code auditing, and vulnerability mining, analysis, and exploitation, as shown in Figure 3-5.

[6] Translator's note: Although this is not clear from the text, these statistics seem to refer to the proportion of organizations in the industry that have the relevant need.

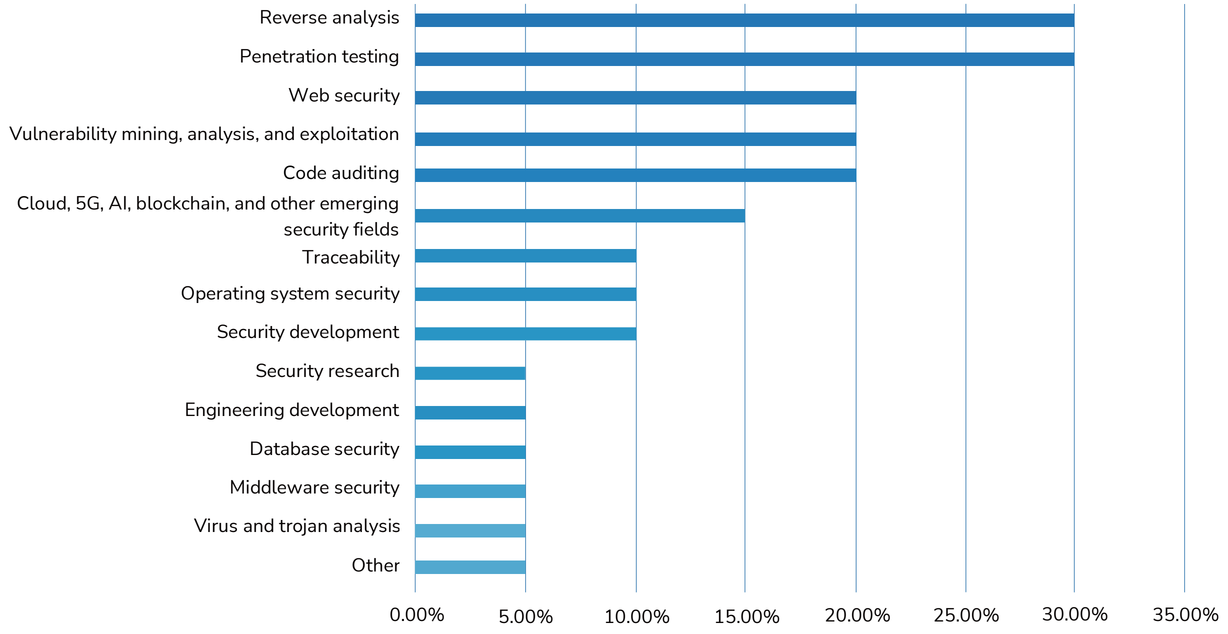


Figure 3-3 Talent Capability Needs of the Financial Industry

(2) Communications industry talent requirements

According to an analysis of survey data, the most obvious demand of the communications industry is for reverse analysis capabilities, accounting for 32%. Its demand for code auditing and virus and trojan analysis capabilities accounted for more than 25%. At the same time, it has a high demand for cybersecurity capabilities in cloud, 5G, AI, blockchain, and other emerging security fields. This is shown in Figure 3-6.

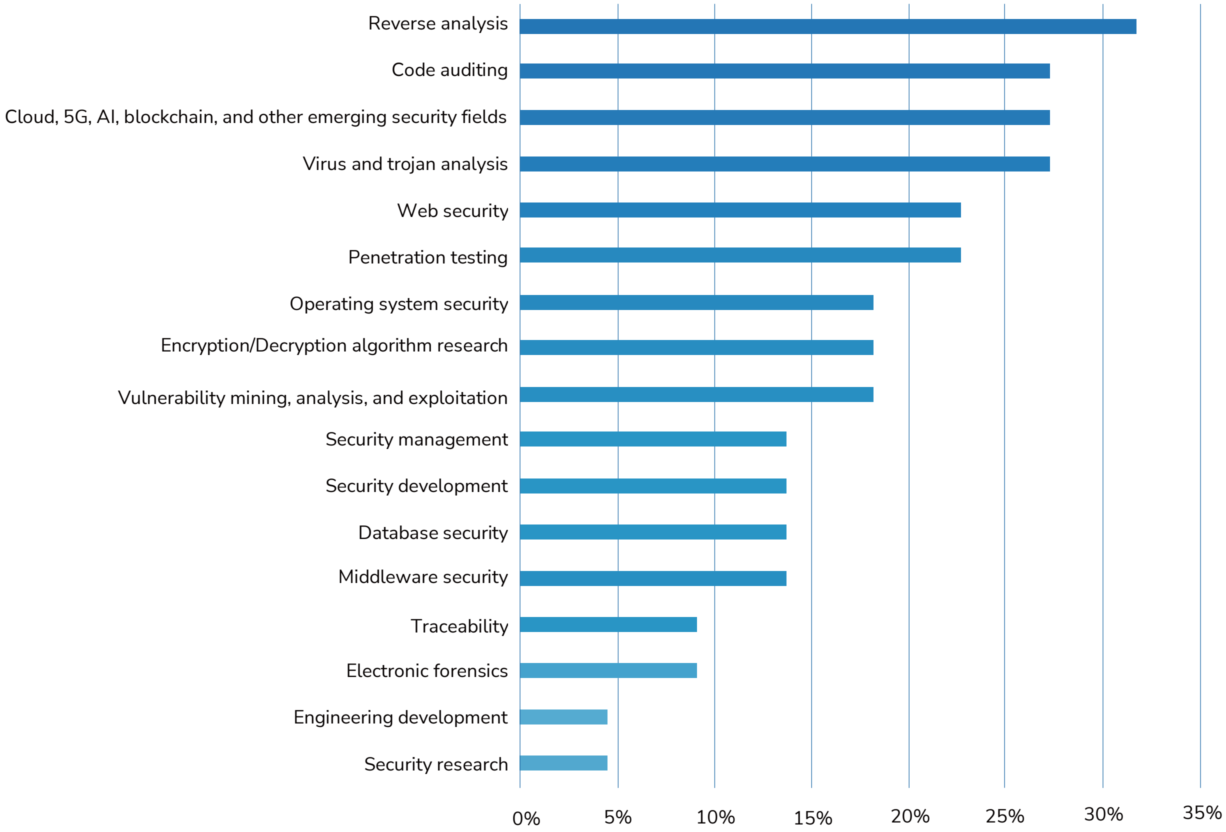


Figure 3-3 Talent Capability Needs of the Communications Industry

(3) Healthcare industry talent requirements

According to an analysis of survey data, 57% of units in the healthcare industry have a demand for cybersecurity capabilities in the direction of penetration testing, making it the most obvious demand. This industry also has high demand for cybersecurity capabilities in the directions of reverse analysis, web security, and database security, as shown in Figure 3-7.

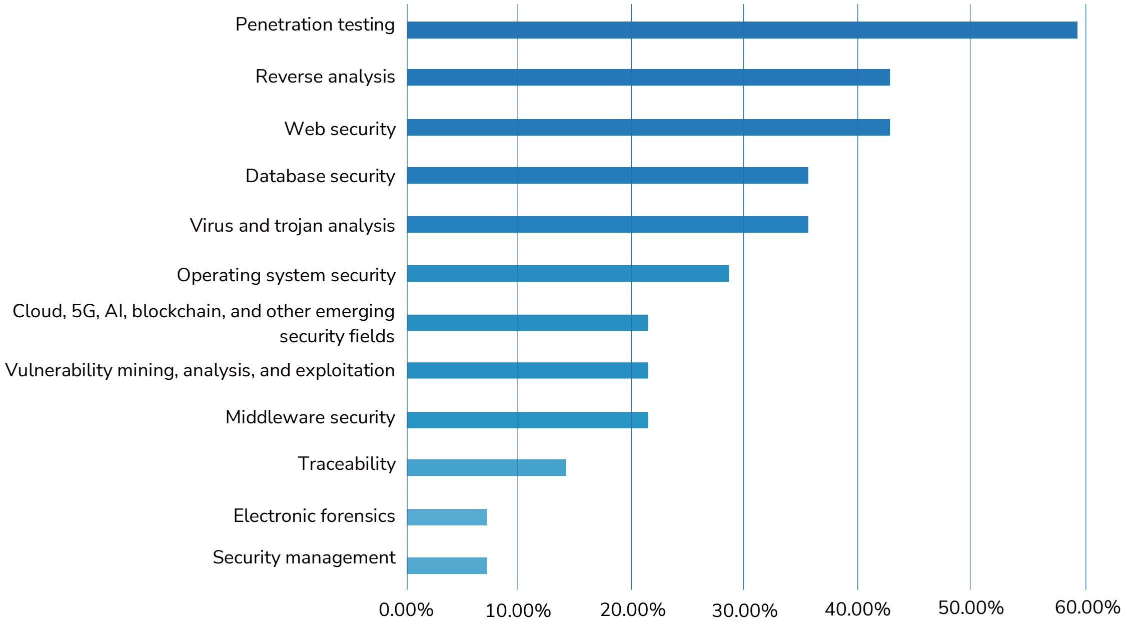


Figure 3-3 Talent Capability Needs of the Healthcare Industry

(4) Education industry talent requirements

According to an analysis of survey data, the most obvious demands of the education industry are for cybersecurity capabilities in virus and trojan analysis and penetration testing, both accounting for 38%. The industry also has high demand for cybersecurity capabilities in the directions of vulnerability mining, analysis, and exploitation, reverse analysis, and web security, all of which account for over 30%, as shown in Figure 3-8.

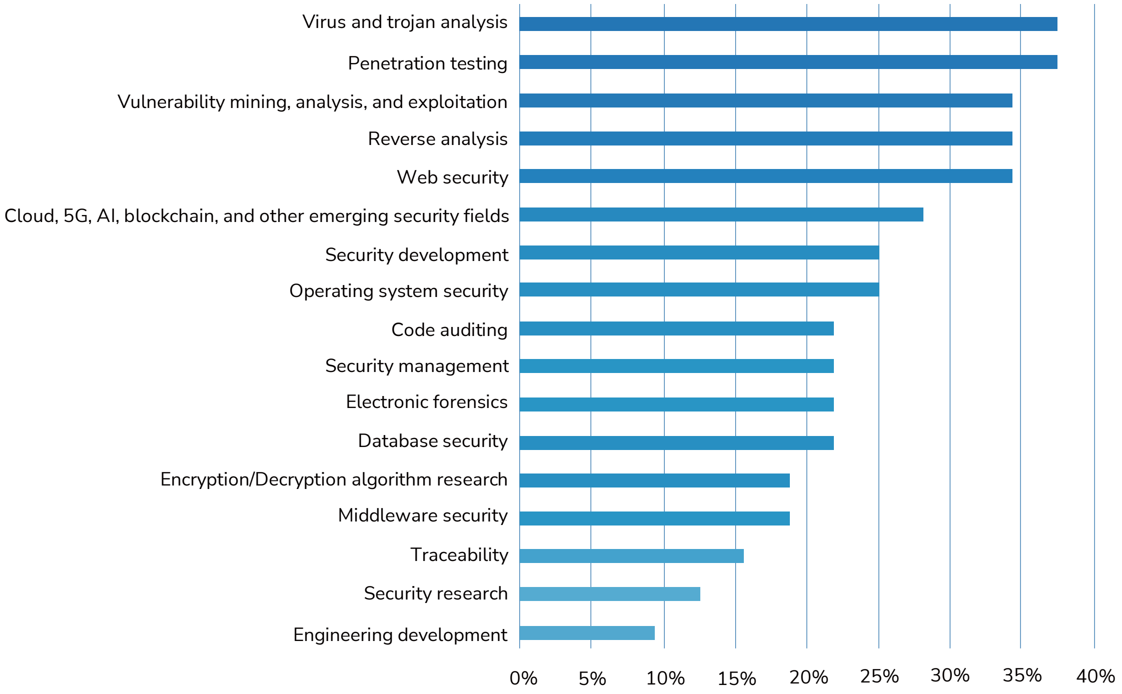


Figure 3-3 Talent Capability Needs of the Education Industry

(5) Internet industry talent requirements

According to an analysis of survey data, 36% of the units in the Internet industry have a demand for cybersecurity capabilities in the direction of reverse analysis, making it the most obvious demand in the industry. It is followed by penetration testing, which accounts for 33%, as shown in Figure 3-9.

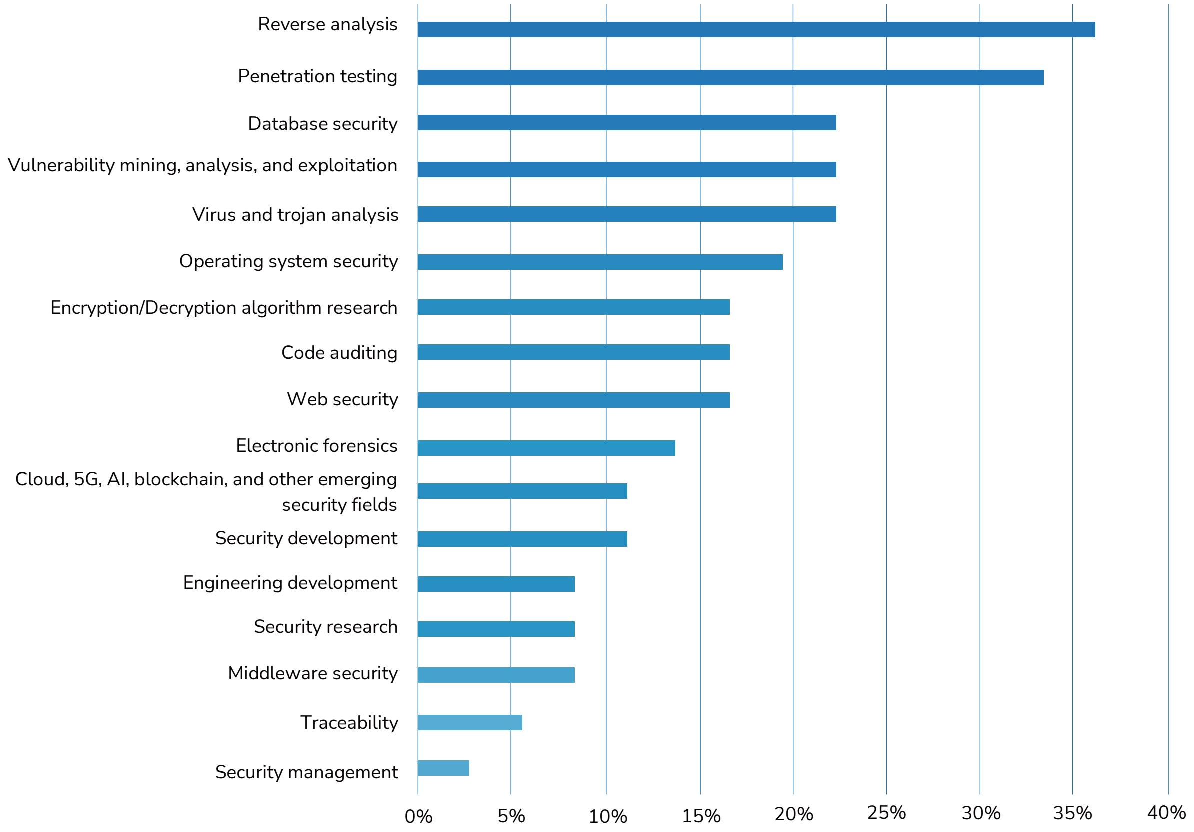


Figure 3-9 Talent Capability Needs of the Internet Industry

According to the survey data, we can see that industries such as finance, healthcare, and education all have obvious needs in the direction of cybersecurity penetration testing, as well as high demands for web security capabilities and reverse analysis capabilities. This is also related to the fact that advanced persistent threat (APT) attacks currently continue to increase, and these industries have become the hardest hit by data leaks. The needs for practical cybersecurity capabilities in the communications industry and the Internet industry are mainly in the direction of reverse analysis. These requirements are related to security challenges such as cyber confrontation, information leaks, data integrity destruction, unauthorized use, and repudiation faced by communication networks and the Internet. In addition, compared with other industries, the communication industry has higher demands for capabilities in the directions of code auditing, cloud, 5G, AI, blockchain, and other emerging security fields, and viruses and trojan analysis.

3.1.3 Analysis by Enterprise Nature and Scale Dimension

In terms of enterprise nature, it is easy to see that "private enterprises" (“民营企业”) have the highest demand for cybersecurity talents, accounting for 45% of demand. "Central enterprises and SOEs" (“中企/国有企业”) account for 18%, followed by "national administrative institutions" (“国家行政机关”), "public institutions," and "universities and scientific research institutes," which each account for about 9%, as shown in Figure 3-10.

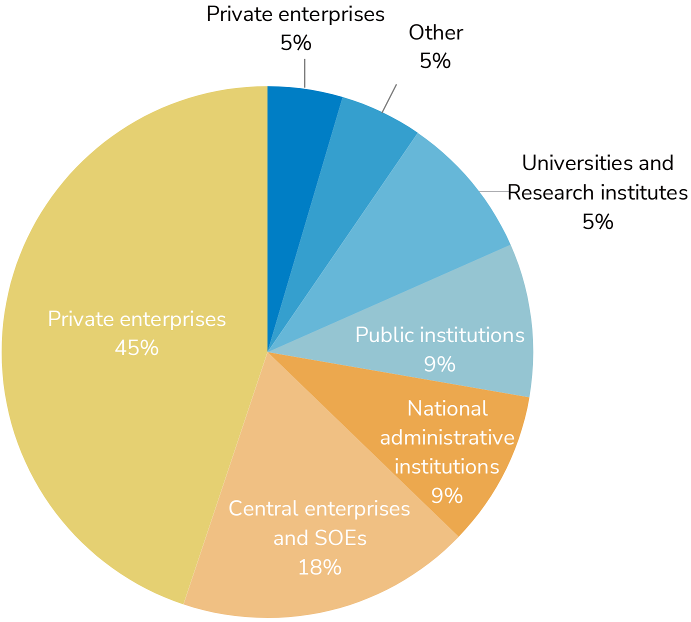


Figure 3-10 Enterprise Nature Statistics[7]

At the same time, when further analyzing the change in demand for cybersecurity talents by the scale of enterprise staff, we found that enterprises with a staff scale of "over 1,000 people" represent the greatest demand for cybersecurity talents, accounting for 29%, followed by small and medium-size enterprises (SMEs) with "101-300 people", accounting for 18%. There was not much difference in the demand for cybersecurity talents between enterprises with "301-500 people" and "501-1000 people," which account for 13% and 12% respectively, as shown in Figure 3-11.

[7] Translator’s note: In the Chinese source text, in Figure 3-10, the dark blue 5% slice at the top and the yellow 45% slice on the left are both labeled “private enterprises” (民营企业).

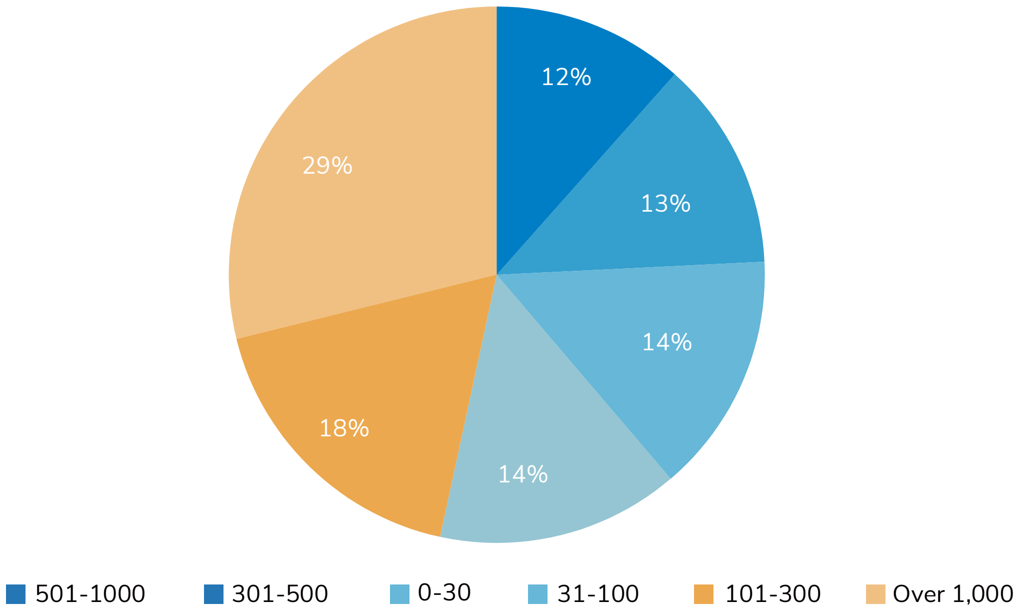


Figure 3-11 Enterprise Scale Statistics

3.2 Position Needs

3.2.1 Basic Position Requirements

Looking at the demand distribution of live-fire attack and defense cybersecurity talents by age, the demand for personnel of age 35 and under accounted for 84% of total demand, indicating that the personnel engaged in live-fire attack and defense cybersecurity work are predominantly young. Statistical analysis shows that people in the 28-35 age group have a greater willingness to seek out challenges, stronger resistance to pressure, and stronger learning abilities, making them more favored by employers. It also shows that China has cultivated more new cybersecurity forces. This is shown in Figure 3-12.

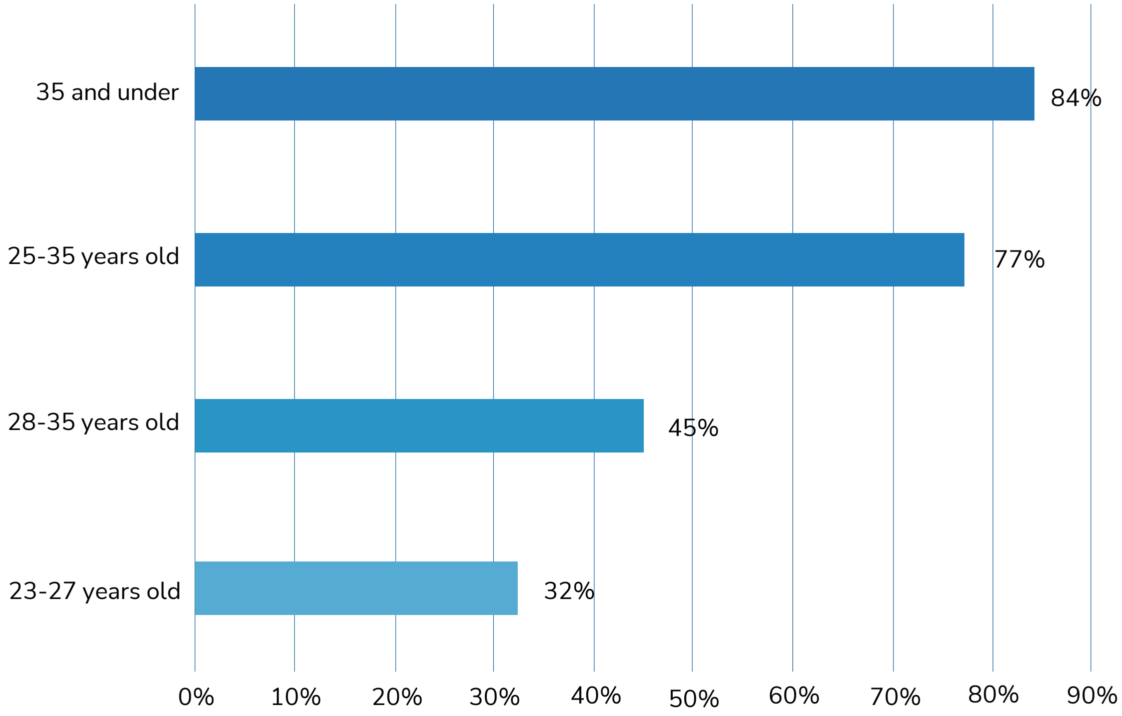


Figure 3-12 Age Distribution of Cybersecurity Talents

Judging from the distribution of educational level requirements for live-fire attack and defense cybersecurity talents, undergraduates accounted for 64.5% of demand. This shows that an undergraduate degree is a basic requirement for most employers that recruit live-fire attack and defense personnel at this stage, and more attention is paid to the application of attack and defense tools and methods by live-fire attack and defense personnel. Employers will put forward higher requirements for the cybersecurity capabilities of live-fire attack and defense personnel. In the future, the demand for personnel with confrontational game theory and strategic and tactical research capabilities will increase. Subsequently, cybersecurity education will be further deepened to provide employers with more highly educated talents. This is shown in Figure 3-13.

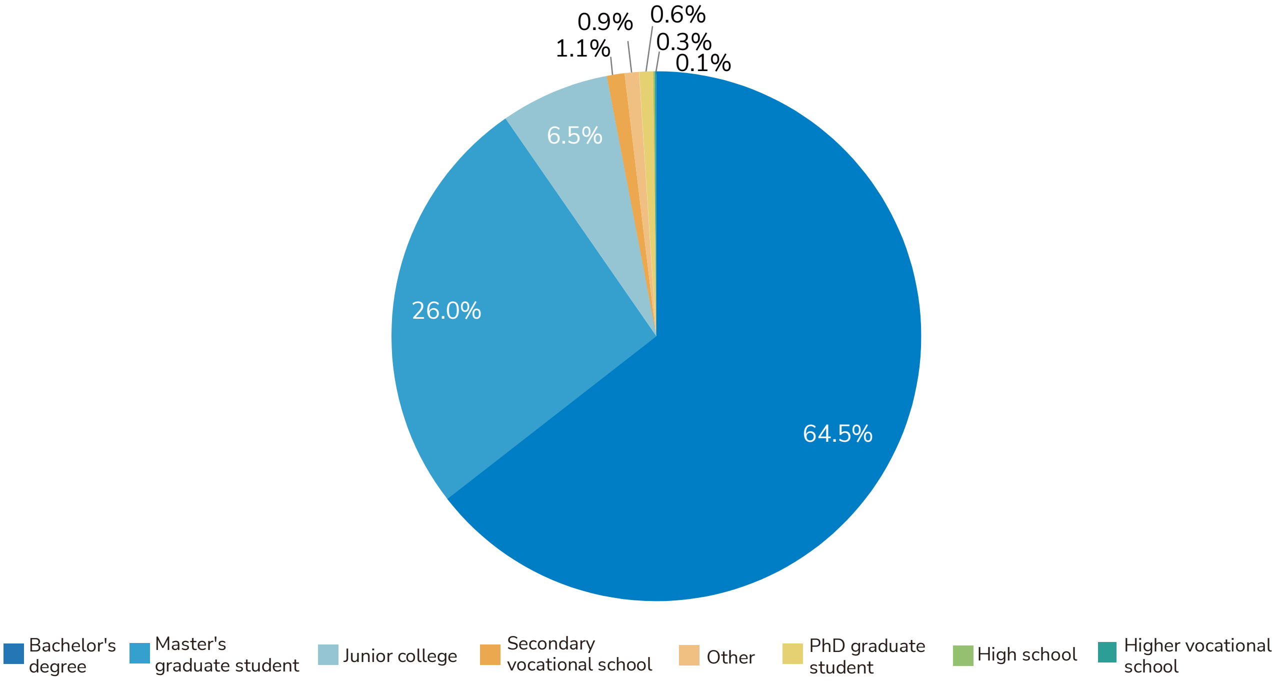


Figure 3-13 Educational Level of Cybersecurity Talents

Judging from the distribution of years of work experience requirements for live-fire attack and defense cybersecurity talents, talents with 5-10 years of experience are the most needed, accounting for 25% of demand. After them come talents with 1-3 years and 3-5 years of work experience, accounting for 20% each. Demand for talents with over 10 years of work experience accounts for 18%. Demand for talents with less than 1 year of work experience accounts for 17%. The above data shows that employers prefer talents with 5-10 years of live-fire experience. Personnel who have been engaged in attack and defense cybersecurity work for 5-10 years have a deep understanding of cybersecurity and have a wealth of experience in live-fire attack and defense operations. They are proficient in using penetration testing tools, cryptographic algorithms, and reverse analysis tools and can better meet the needs of employers. This is shown in Figure 3-14.

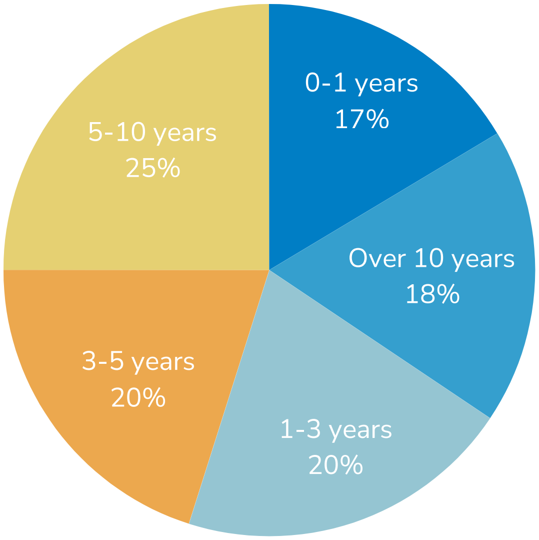


Figure 3-14 Work Experience of Cybersecurity Talents

Judging from the distribution of skill requirements for live-fire attack and defense cybersecurity talents, skills and capabilities in the direction of penetration testing are more favored by employers. This is closely related to the fact that penetration testing capabilities can more comprehensively reflect the overall live-fire capabilities of talents. Such talents not only can play a role in major event assurance, major project technology advancement, attack and defense drills, and emergency response, but also in daily security testing. They can play a role in improving all aspects of overall security protection.

In addition, authoritative certifications in the field of cybersecurity serve to certify the capabilities of live-fire attack and defense cybersecurity talents, proving that talents have systematic information security knowledge and certain live-fire capabilities. 24% of employers will use this as one of their criteria when selecting outstanding talents. Personnel who have obtained authoritative certifications in the field of cybersecurity have a better chance to stand out from other candidates. At the same time, this shows that employers have higher requirements for the learning ability, comprehensive application, and live-fire capabilities of security personnel, as shown in Figure 3-15.

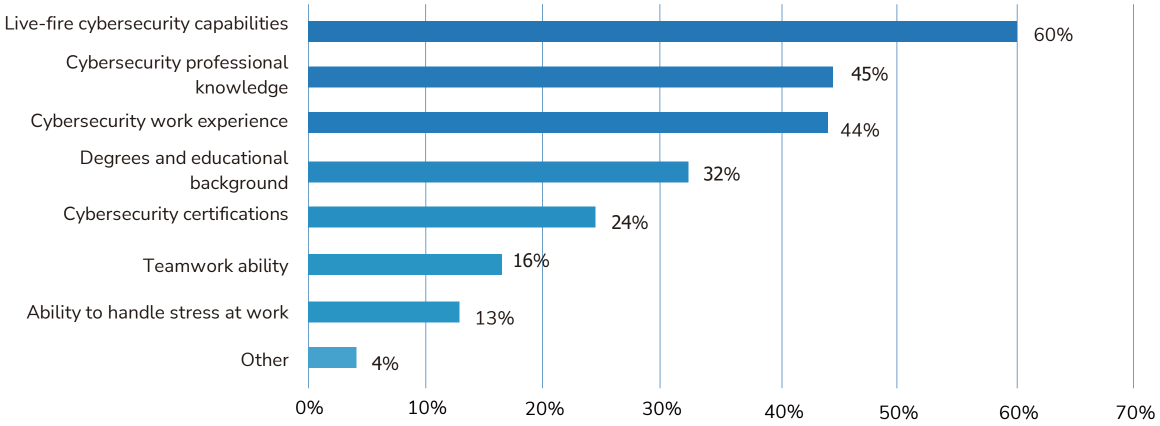


Figure 3-15 Aspects Employers Value when Recruiting Cybersecurity Personnel

3.2.2 Basic Position Needs

According to an analysis of the cybersecurity staffing situation of employers, 82% of employers have set up full-time cybersecurity positions. Only looking at these employers, only 32% of them have established formal staff positions (岗位编制) in line with the actual situation and the actual responsibilities of employees. Most of the units still cannot meet their needs with existing personnel. Among them, 15% have formal staff position arrangements but face difficulties in recruiting personnel, 25% have insufficient formal staff positions and some people must fill multiple roles, and 11% have serious formal staff position shortages so that most people must fill multiple roles.

An analysis of the above data shows that under the security protection requirements of critical infrastructure protection and the Multi-Layer Protection Scheme (MLPS) 2.0 (等保 2.0), employers pay more attention to the security construction and maintenance of information systems, and more employers tend to establish full-time security positions to be responsible for business system security assurance. At the same time, in the post-pandemic period, in order to continuously accumulate individual capabilities, cybersecurity talents show a greater preference for long-term and stable full-time positions, as shown in Figure 3-16.

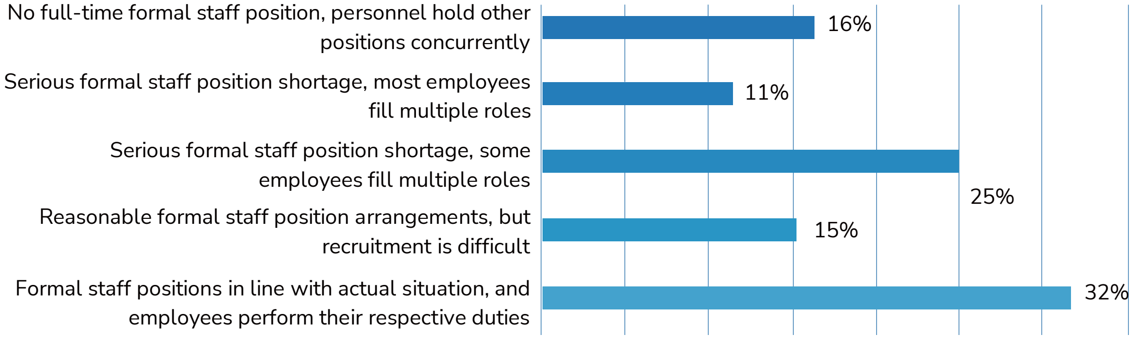


Figure 3-16 Formal Staff Position Situation

Looking at the scale of full-time personnel teams in critical information infrastructure units, 70% of critical information infrastructure units have a cybersecurity team of fewer than 10 people. Among these, 27% of the units have no full-time staff, 29% have 1-5 people, and 15% have 6-10 people, as shown in Figure 3-17.

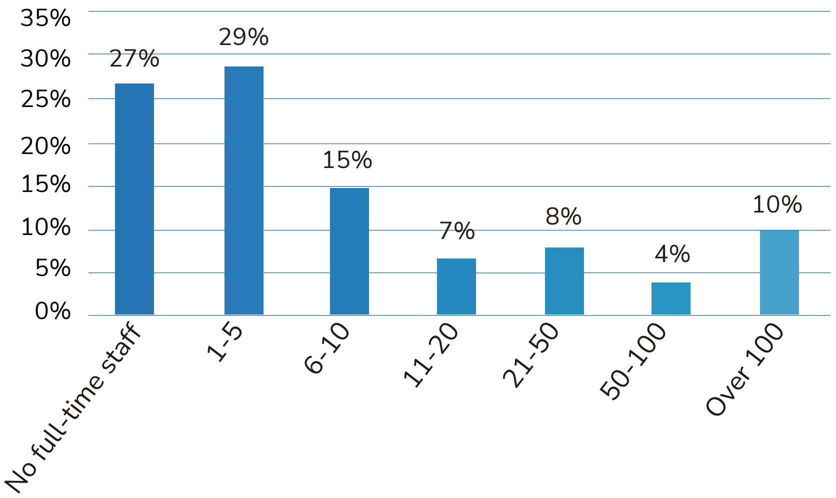


Figure 3-17 Security Team Scale of Critical Information Infrastructure Units

From the perspective of the overall scale of full-time personnel of employers, the sizes of security teams are clearly divided into two levels. The proportion of teams with 1 to 5 people is the highest, at 23%, and the proportion of teams with more than 100 people is also high at 18%. The proportion of mid-size teams is lower at around 10%, as shown in Figure 3-18.

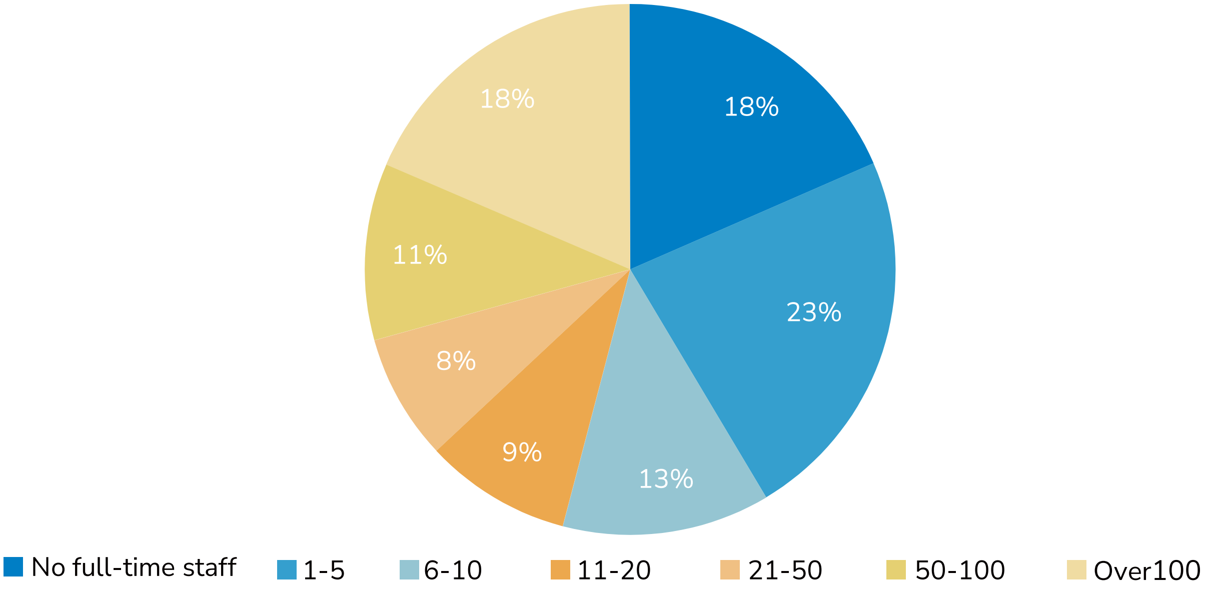


Figure 3-18 Scale of Cybersecurity Professional Teams

From a survey of employers concerning the live-fire attack and defense cybersecurity personnel who are most in short supply, we found large shortfalls in penetration testing, vulnerability discovery and exploitation, and reverse analysis skills, which were reported by 40%, 33%, and 32% of employers respectively, as shown in Figure 3-19. Talents with the above skills are highly sought after by employers. This is because personnel with rich experience in penetration testing are adept at comprehensively inspecting information systems and discovering their vulnerabilities; personnel with rich experience in reverse analysis can analyze the execution logic of programs through decompilation and discover logical defects in applications; and personnel with rich experience in vulnerability discovery and exploitation can comprehensively assess the security risks faced by information systems as well as the consequences and costs of attacks.

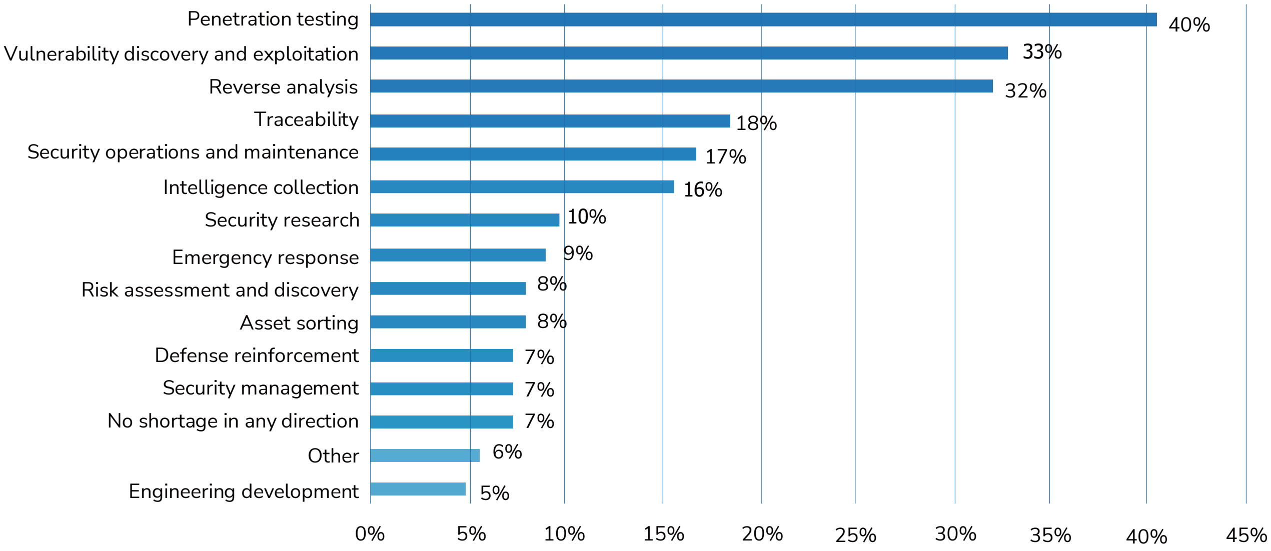


Figure 3-19 Skill Directions of Live-Fire Personnel in Short Supply According to Employers

There is still a big gap between China's cybersecurity development and the speed of live-fire attack and defense talent training. At the same time, there is an obvious specialization tendency in the development of attack and defense talents. In the long run, hybrid talents will account for a larger proportion, and hybrid attack and defense talents will be an important direction for future talent training.

3.3 Analysis of Position and Capability Matching

3.3.1 Distribution of Positions of Talents

Looking at statistical data, the categories of cybersecurity positions can be divided into five main types: security management positions, security construction positions, security operation positions, testing and evaluation positions, and scientific research and education positions. Most of the cybersecurity talents with live-fire attack and defense capabilities hold security operation positions and testing and evaluation positions, while the other three types account for a relatively small number of talents, as shown in Figure 3-20.

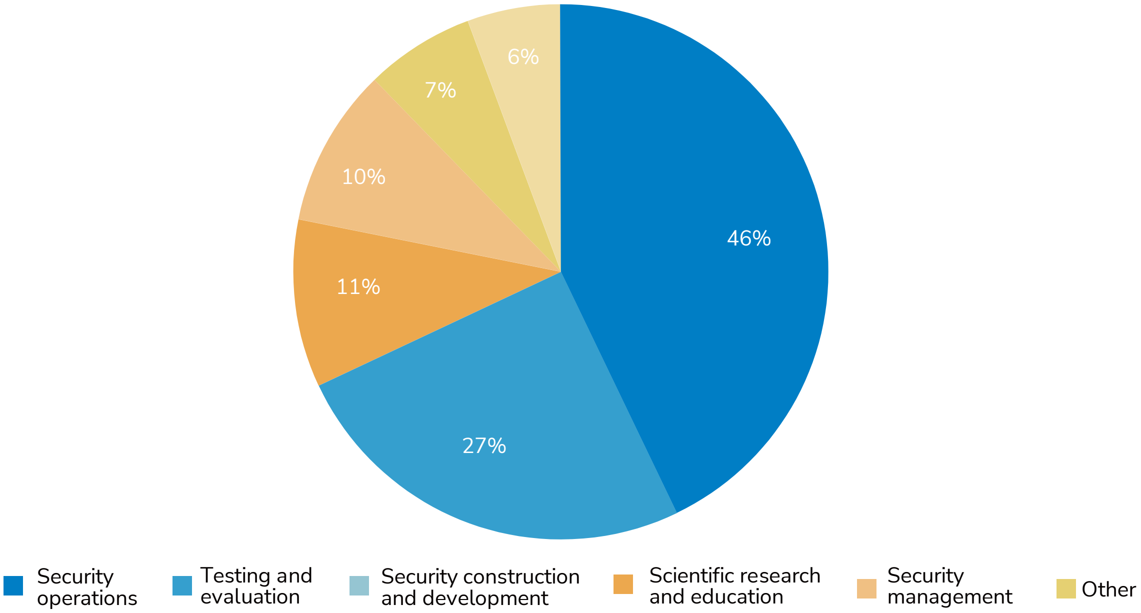


Figure 3-20 Distribution of Position Types[8]

The statistical data show that there are many job titles in the cybersecurity industry, and various employers use different nomenclature according to their own situations. If we summarize the situation, positions that require live-fire attack and defense capabilities are mainly concentrated under the job titles of operation and maintenance engineer, security service engineer, security operations engineer, and penetration testing engineer. Among these, operation and maintenance engineers account for the largest percentage at 26%, followed by security service engineers, and then security operations engineers, as shown in Figure 3-21.

[8] Translator's note: In Figure 3-20, there is a mismatch in the Chinese source text between the colors of the pie chart slices (two of which are shades of blue, and four of which are shades of orange and yellow) and the labels below (three of which are shades of blue, and three of which are shades of orange and yellow). It is highly probable that the 46% slice refers to "security operations and maintenance" and the 27% slice refers to "testing and evaluation." It is unclear how the remaining four labels map up to the four other slices of the pie chart.

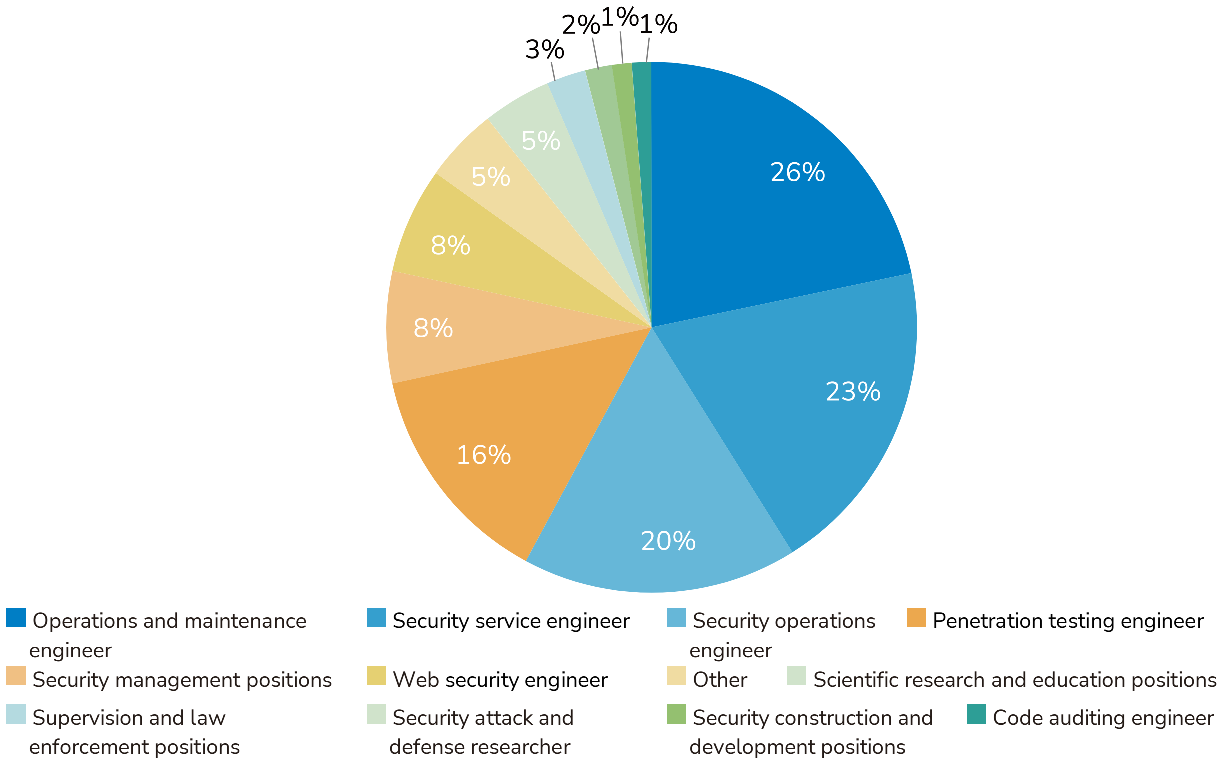


Figure 3-21 Position Distribution

3.3.2 Position Capability Requirements

According to an analysis of survey data, the main practical security capabilities of employees on the job are in the following directions: penetration testing, vulnerability discovery and exploitation, security operations and maintenance, emergency response, risk assessment and discovery, asset sorting, traceability, intelligence collection, security research, defense reinforcement, and reverse analysis, as shown in Figure 3-22.

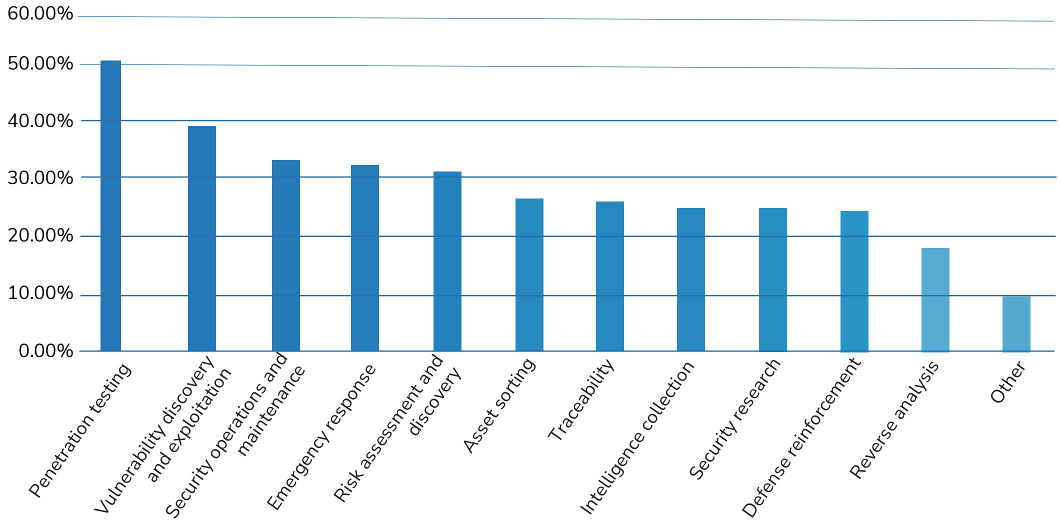


Figure 3-22 Main Practical Directions

Among these, web security engineers pay more attention to cybersecurity capabilities in the penetration testing direction, followed by reverse analysis capabilities and web security capabilities. Among the cybersecurity capabilities in need of urgent improvement for web security engineer positions, penetration testing capabilities account for 65% [of survey responses], reverse analysis capabilities account for 48%, and web security capabilities account for 39%, as shown in Figure 3-22.[9]

Penetration testing engineers pay more attention to cybersecurity capabilities in the direction of penetration testing, followed by code auditing and reverse analysis. They also have high requirements for cybersecurity capabilities in cloud, 5G, artificial intelligence (AI), blockchain, and other emerging security fields. Among the cybersecurity capabilities in need of urgent improvement for penetration testing engineer positions, penetration testing capabilities account for 58%, code auditing capabilities account for 50%, reverse analysis capabilities account for 42%, and capabilities in cloud, 5G, AI, blockchain, and other emerging security fields account for 38%, as shown in Figure 3-22.

The most obvious requirements for operation and maintenance engineers are cybersecurity capabilities in penetration testing, web security, and security management. Among the cybersecurity capabilities in need of urgent improvement for operation and maintenance engineer positions, penetration testing capabilities account for 54%, web security capabilities account for 42%, and security management capabilities account for 38%, as shown in Figure 3-22.

The most obvious requirement for security service engineer positions is for cybersecurity capabilities in the direction of penetration testing. There are also high requirements for cybersecurity capabilities in the directions of vulnerability mining, analysis, and exploitation, virus and trojan analysis, and web security. Among the cybersecurity capabilities in need of urgent improvement for security service engineer positions, penetration testing capabilities account for 59%, and vulnerability mining, analysis, and exploitation, virus and trojan analysis, and web security capabilities all account for 38%, as shown in Figure 3-22.

The most obvious requirement for security operations and maintenance engineer positions is for cybersecurity capabilities in the direction of vulnerability mining, analysis, and exploitation. There are also high requirements for cybersecurity capabilities in penetration testing and cloud, 5G, AI, blockchain, and other emerging security fields. Among the cybersecurity capabilities in need of urgent improvement for

[9] Translator's note: References to Figure 3-22 in this and the following nine paragraphs are actually references to Figure 3-23.

security operations and maintenance engineer positions, vulnerability mining, analysis, and exploitation capabilities and penetration testing capabilities both account for 58%; and cloud, 5G, AI, blockchain, and other emerging security fields account for 53%, as shown in Figure 3-22.

The most obvious requirement for security operations engineers is cybersecurity capabilities in the penetration testing direction. Among the cybersecurity capabilities in need of urgent improvement for security operations engineer positions, penetration testing capabilities account for 44%. The most obvious requirement for security attack and defense researcher positions is for cybersecurity capabilities in the direction of vulnerability mining, analysis, and exploitation. There are also high requirements for cybersecurity capabilities in the directions of virus and trojan analysis and middleware security, as shown in Figure 3-22.

Among the cybersecurity capabilities in need of urgent improvement for security attack and defense researcher positions, vulnerability mining, analysis, and exploitation capabilities account for 73%, virus and trojan analysis capabilities account for 47%, and middleware security capabilities account for 40%, as shown in Figure 3-22.

The most obvious requirement for security management positions is for cybersecurity capabilities in the direction of security management. There are also high requirements for cybersecurity capabilities in the direction of penetration testing and security research. Among the cybersecurity capabilities in need of urgent improvement for security management position talents, security management capabilities account for 61%, penetration testing capabilities account for 57%, and security research capabilities account for 35%.

The most obvious requirement for supervision and law enforcement positions is for cybersecurity capabilities in the direction of reverse analysis. There are also high requirements for cybersecurity capabilities in the directions of penetration testing, virus and trojan analysis, and security research, as shown in Figure 3-22.

Among the cybersecurity capabilities in need of urgent improvement for supervision and law enforcement position talents, reverse analysis capabilities account for 78% and penetration testing capabilities and virus and trojan analysis capabilities both account for 67%, as shown in Figure 3-22.

The most obvious requirements for scientific research and education positions are for cybersecurity capabilities in reverse analysis, operating system security, database security, and cloud, 5G, AI, blockchain, and other emerging security fields. Among the cybersecurity capabilities in need of urgent improvement for scientific research and education position talents, reverse analysis, operating system security, database security, and cloud, 5G, AI, blockchain, and other emerging security fields all account for 43%, as shown in Figure 3-23.

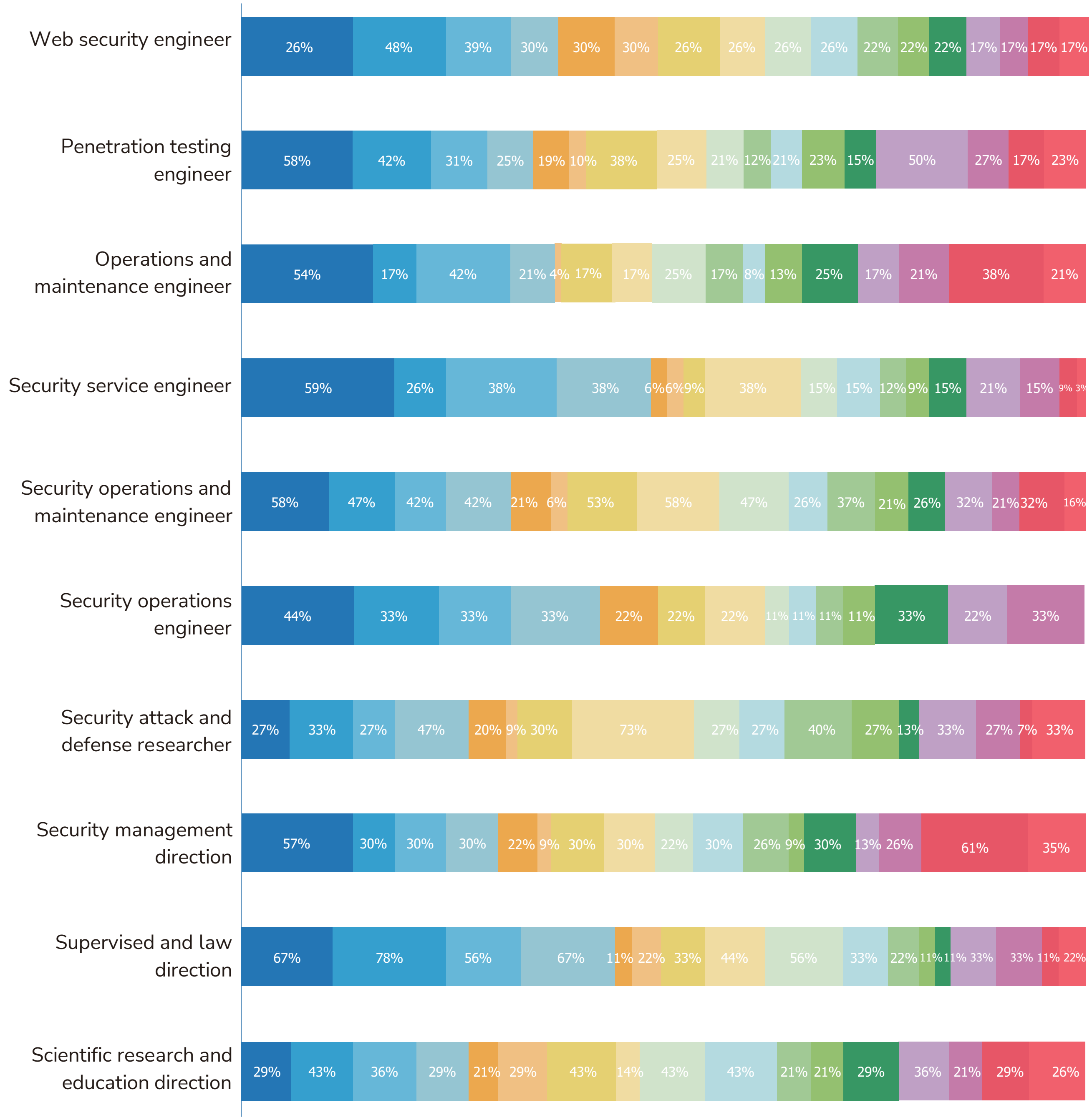


Figure 3-23 Specialized Capability Requirements by Position

Based on the survey data, we can see that the most obvious requirement for web security engineers, security service engineers, security operations engineers, and penetration testing engineers is for cybersecurity capabilities in the direction of penetration testing; the most obvious requirement for security attack and defense researchers and security operations and maintenance engineers is for capabilities in the direction of vulnerability mining, analysis, and exploitation; the most obvious requirement for security management positions and operations and maintenance engineers is for cybersecurity capabilities in the direction of security management; and the most obvious requirement for supervision and law enforcement positions and scientific research and education positions is for cybersecurity capabilities in the direction of reverse analysis.

In addition, web security engineers and penetration testing positions have high requirements for reverse analysis; security management positions, security operations and maintenance engineers, and supervision and law enforcement positions have high requirements for cybersecurity capabilities in the direction of penetration testing; web security engineers, security service engineers, and operations and maintenance engineers have high requirements for cybersecurity capabilities in the direction of web security; security service engineers, security attack and defense researchers, and supervision and law enforcement positions have high requirements for cybersecurity capabilities in the direction of virus and trojan analysis; and security operations and maintenance engineers, scientific research and education positions, and penetration testing positions have high requirements for cybersecurity capabilities in cloud, 5G, AI, blockchain, and other emerging security fields.

Compared with other positions, security attack and defense researcher positions have higher requirements for cybersecurity capabilities in the direction of middleware security; security management positions have higher requirements for cybersecurity capabilities in the direction of security research; scientific research and education positions have higher requirements for cybersecurity capabilities in the directions of operating system security and database security; and penetration testing positions have higher requirements for cybersecurity capabilities in the direction of code auditing.

3.3.3 Requirements for Capability Improvement

According to an analysis of the survey data, only 8% of enterprises believe that the cybersecurity personnel team within the group is relatively perfect overall, that personnel capabilities are relatively complete and comprehensive, and that there is currently no room for improvement. Among the business capabilities generally reported to be lacking by most employers, reverse analysis capabilities account for

35% [of responses], followed by penetration testing capabilities, vulnerability mining, analysis, and exploitation capabilities, and virus and trojan analysis capabilities, at 33%, 27%, and 26% respectively, as shown in Figure 3-24.

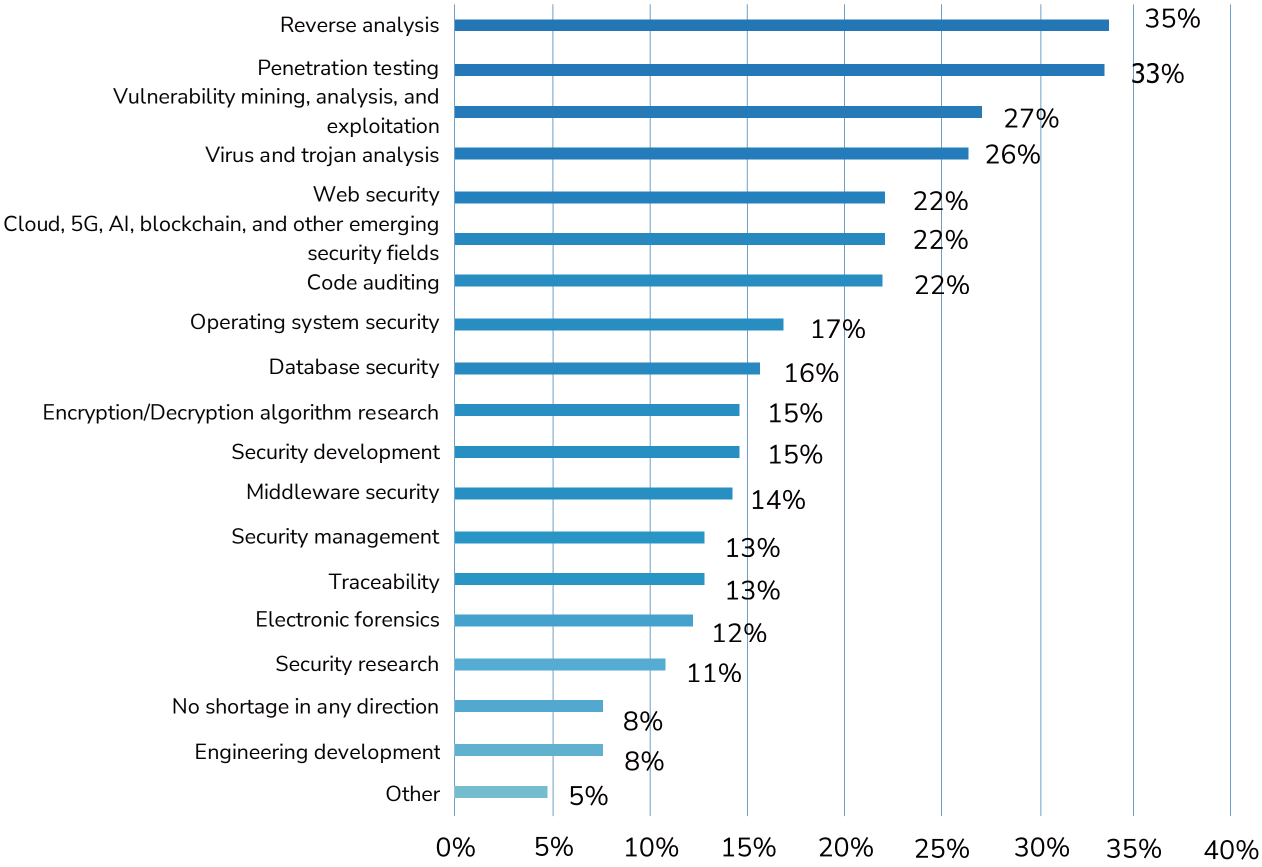


Figure 3-24 Business Capabilities Generally Lacked by Employers

At the same time, cybersecurity talents in various industries are obviously aware of their own shortcomings at work. Taking the five industries of finance, communications, healthcare, education, and the Internet as examples, we analyze the need for talent capability improvement below.

(1) Financial industry needs for talent capability improvement

According to an analysis of survey data, among the specialized cybersecurity capabilities that talents in the financial industry believe are in need of urgent improvement, penetration testing capabilities account for 60%, web security capabilities account for 40%, and reverse analysis capabilities account for 35%, as shown in Figure 3-25.

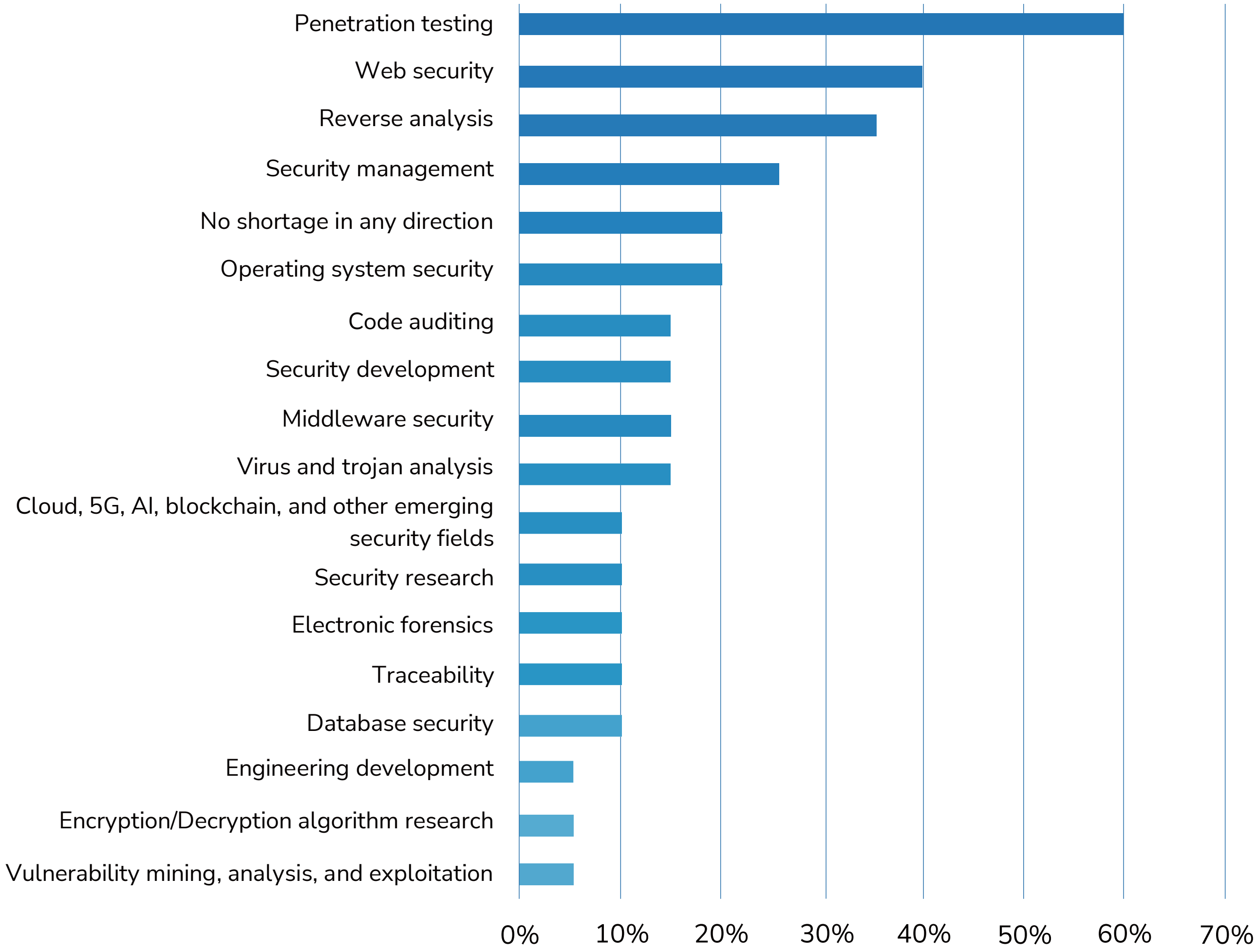


Figure 3-25 Talent Capability Improvement Needs in the Financial Industry

(2) Communications industry needs for talent capability improvement

According to an analysis of survey data, among the specialized cybersecurity capabilities that talents in the communications industry believe are in need of urgent improvement, vulnerability mining, analysis, and exploitation capabilities account for 68%, reverse analysis capabilities and virus and trojan analysis capabilities both account for 59%, and cloud, 5G, AI, blockchain, and other emerging security fields capabilities and penetration testing capabilities both account for 55%, as shown in Figure 3-26.

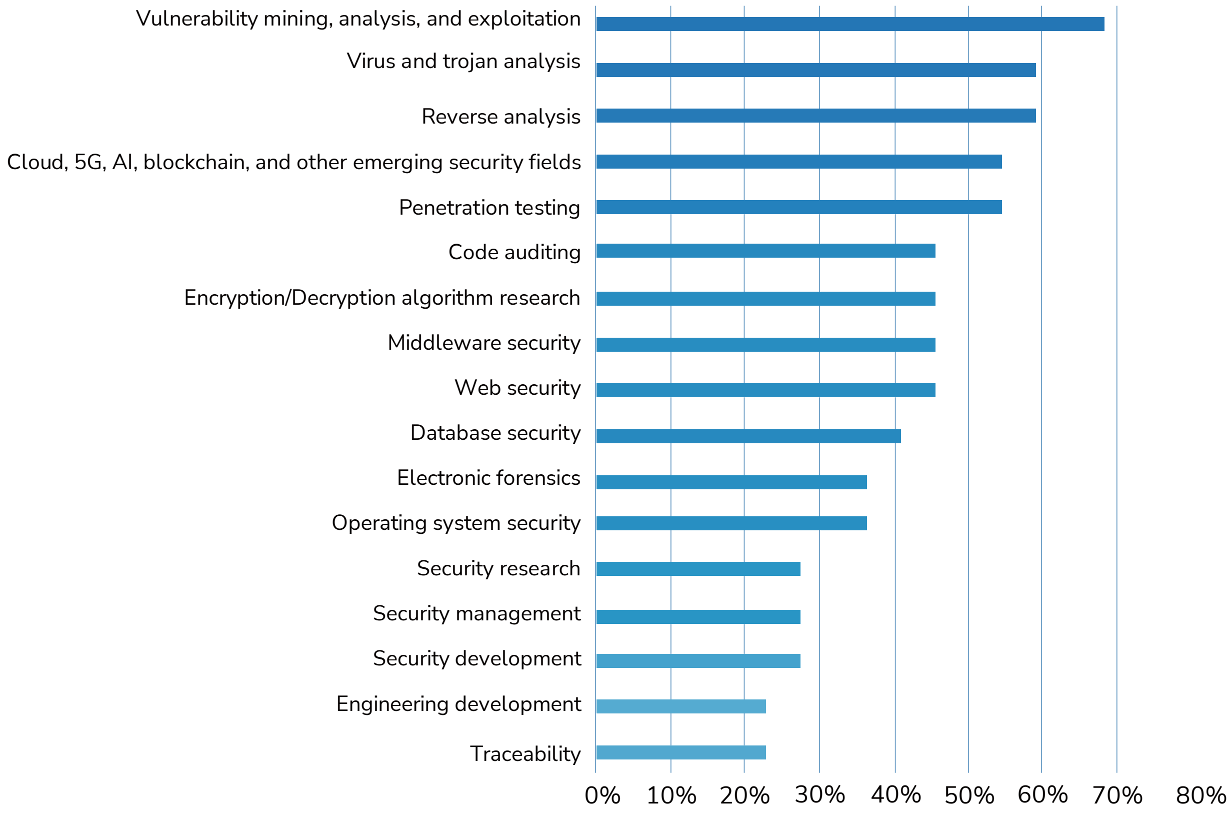


Figure 3-26 Talent Capability Improvement Needs in the Communications Industry

(3) Healthcare industry needs for talent capability improvement

According to an analysis of survey data, among the specialized cybersecurity capabilities that talents in the healthcare industry believe are in need of urgent improvement, penetration testing capabilities account for 50% and reverse analysis capabilities and database security capabilities both account for 35%, as shown in Figure 3-27.

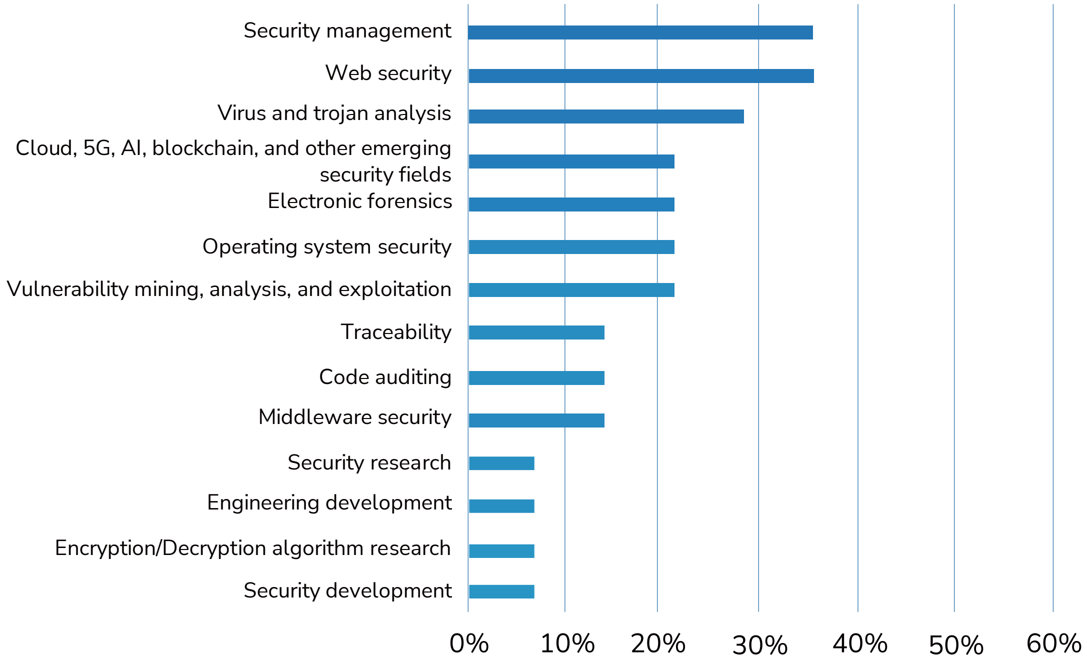


Figure 3-3 Talent Capability Improvement Needs in the Healthcare Industry

(4) Education industry needs for talent capability improvement

According to an analysis of survey data, among the specialized cybersecurity capabilities that talents in the education industry believe are in need of urgent improvement, penetration testing capabilities account for 38% and web security capabilities and operating system security capabilities both account for 34%, as shown in Figure 3-28.

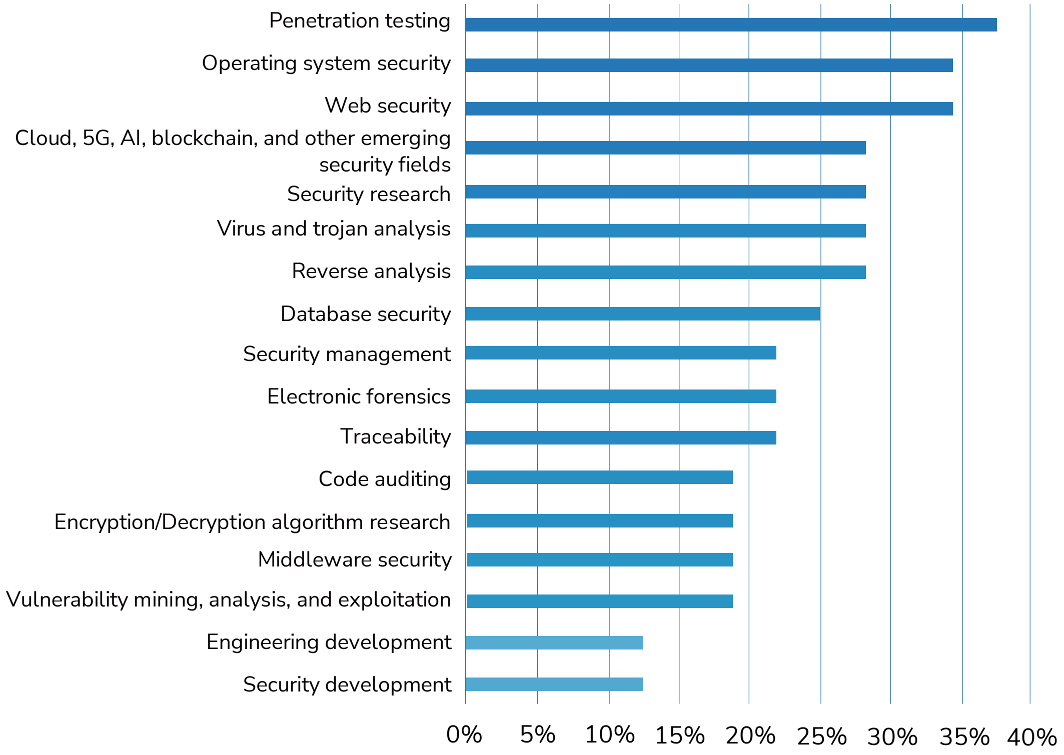


Figure 3-28 Talent Capability Improvement Needs in the Education Industry

(5) Internet industry needs for talent capability improvement

According to an analysis of survey data, among the specialized cybersecurity capabilities that talents in the Internet industry believe are in need of urgent improvement, penetration testing capabilities account for 67%, web security capabilities account for 50%, and reverse analysis capabilities account for 42%, as shown in Figure 3-29.

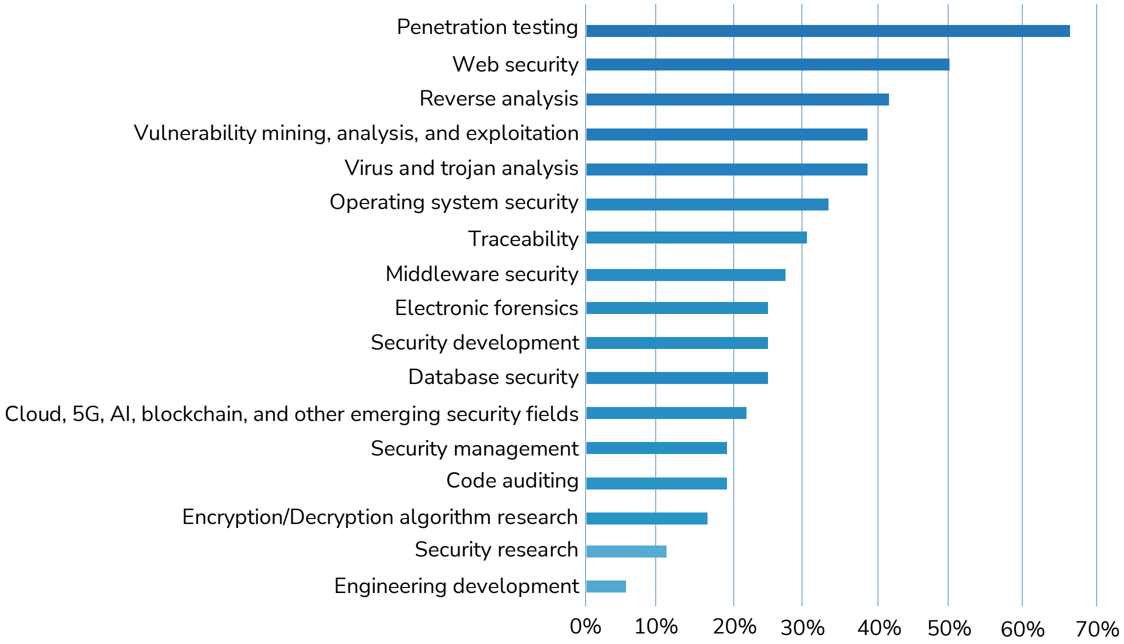


Figure 3-29 Talent Capability Improvement Needs in the Internet Industry

Cybersecurity work is a systematic project. According to a statistical analysis of the data, which is shown in Figure 3-30 below, the most important and effective way for employers to improve their overall security protection level is to build a perfected cybersecurity talent team, followed by sufficient cybersecurity equipment and staff-wide cybersecurity awareness, and then systematic cybersecurity personnel training so that all aspects of the overall layout can better provide effective security defense.

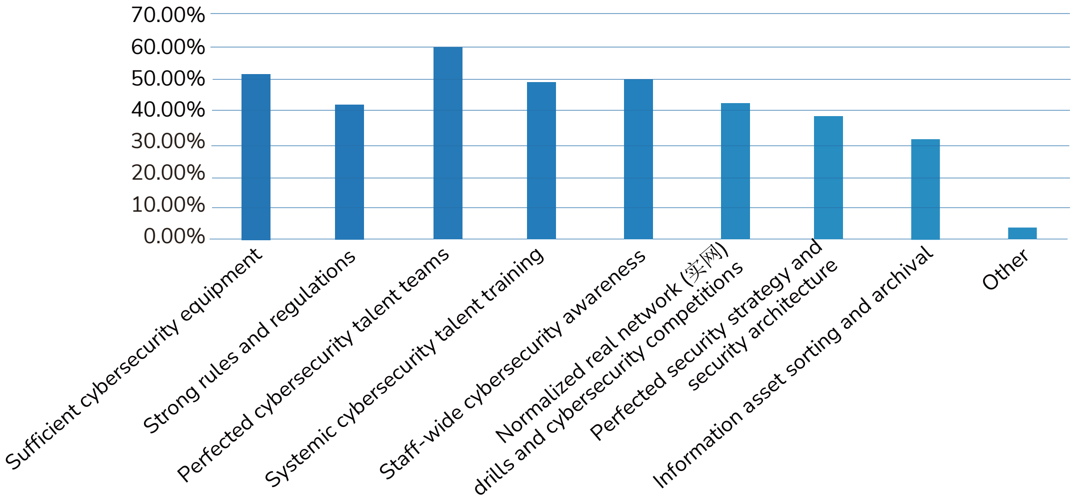


Figure 3-30 Measures Taken by Employers to Improve Their Overall Protection Levels

3.4 Analysis of Personnel Sources

More than 60% of employers highly value live-fire cybersecurity capabilities when recruiting cybersecurity personnel, and more than 40% of employers highly value cybersecurity work experience and cybersecurity professional knowledge. Second to these attributes, employers also value degrees and educational background, cybersecurity certifications, teamwork ability, and ability to handle stress at work, as shown in Figure 3-31.

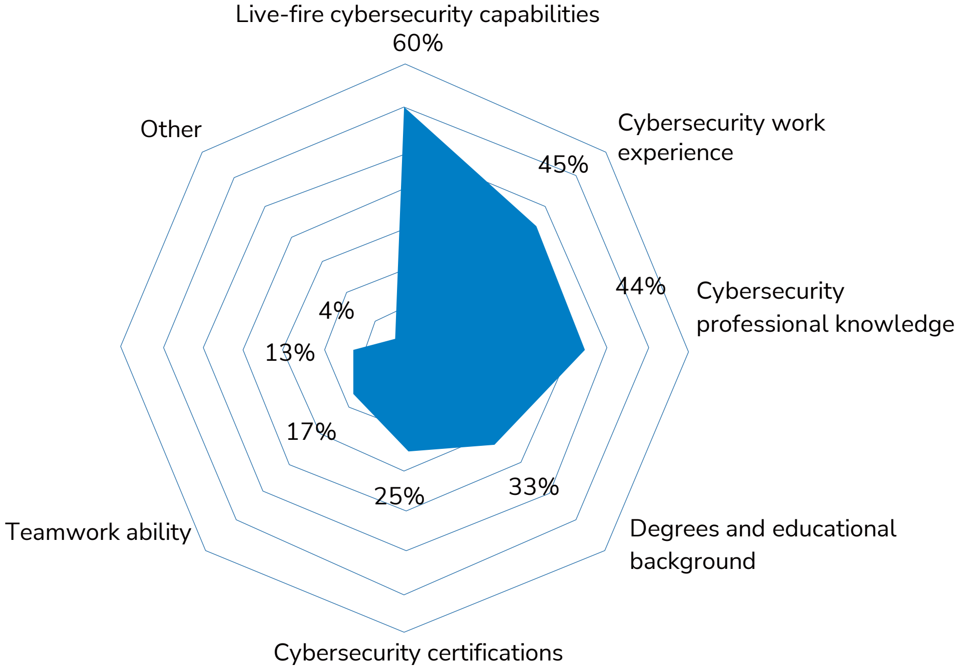


Figure 3-31 Capabilities Most Important to Employers when Recruiting Cybersecurity Personnel

The talent channels that most employers rely on are recruitment websites and campus recruitment. 58% of employers recruit personnel through recruitment websites, and 45% of employers recruit personnel through campus recruitment. After these channels, enterprise internal recommendations, industry acquaintance recommendations, and headhunting recommendations are also common recruitment channels, as shown in Figure 3-32.

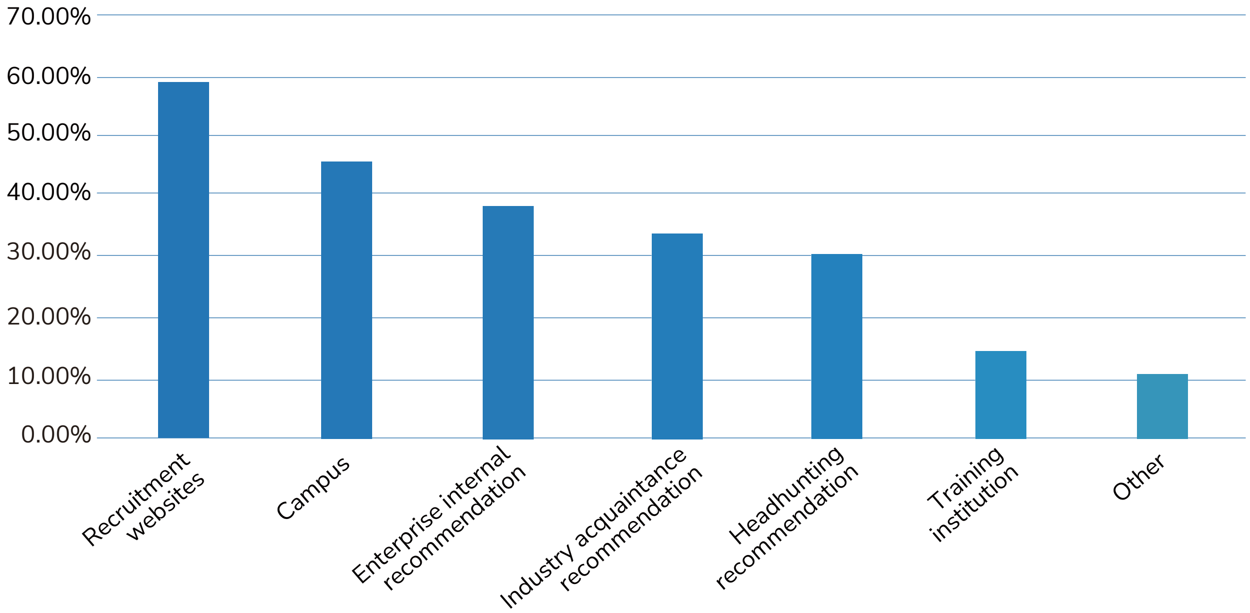


Figure 3-32 Recruitment Channels Used by Employers

The top two recruitment channels considered by employers to be the most reliable are enterprise internal recommendations and industry acquaintance recommendations; followed by campus recruitment, recruitment websites, and headhunting agencies, as shown in Figure 3-33. Among employers, super-large organizations with more than 1,000 employees are more likely to use enterprise internal recommendations and industry acquaintance recommendations; large organizations with 500-1,000 employees and mid-sized enterprises with 300-500 employees believe that recruitment websites and enterprise internal recommendations are more effective.

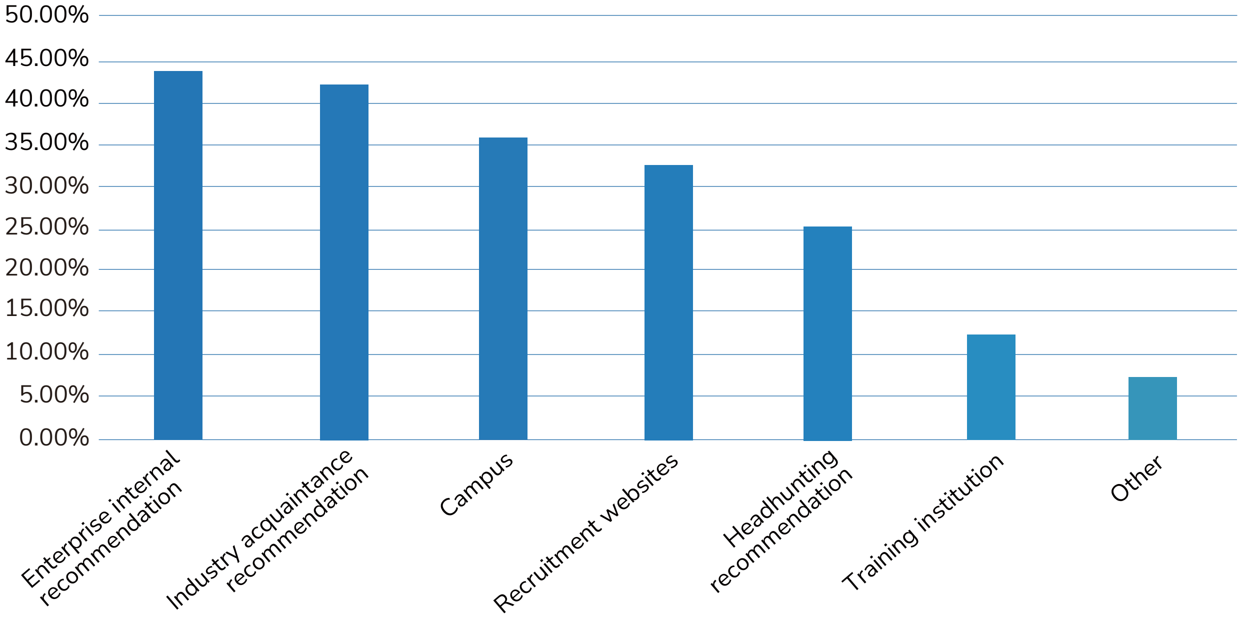


Figure 3-33 Recruitment Channels Employers View as Most Reliable

Chapter 4 | Analysis of Improvements in Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

4.1 Current Situation of Live-Fire Attack and Defense Cybersecurity Talent Training

4.1.1 Establishment of Cybersecurity-related Majors in Schools

Since the advent of the informatization era, the popularity and scope of network applications have constantly increased. As a result, there are more and more cybersecurity problems and they present themselves in increasingly complex, diverse, and unpredictable forms. This poses new requirements for cybersecurity talent construction in China. Generally speaking, there is a large shortfall in the quantity of cybersecurity talents in China, their capabilities and quality are low, and the structure is unreasonable. It is necessary to improve and optimize the path of cybersecurity course construction and strengthen the construction of cybersecurity talents.

Looking at the attributes of the academic discipline, cybersecurity is a comprehensive emerging discipline with a strong interdisciplinary nature, which makes the cultivation of professional talents a relatively difficult and long-term task. In addition to dedicated cybersecurity-related majors, many schools have also established some [more loosely] cybersecurity-related majors. The focus of training in each specialized discipline is different, and they can be regarded as second-level specialized disciplines or interdisciplinary disciplines under cybersecurity. In view of the features and development enthusiasm of specialized directions in the field of cybersecurity, there is an increasing trend of subdivision and specialization in the market, which also affects the training directions of schools. According to our research, the cybersecurity-related majors currently offered by Chinese colleges and universities can be divided into six main categories: cybersecurity, information security, confidentiality technology (保密技术), cryptography science and technology, blockchain engineering, and cybersecurity and law enforcement, as shown in Figure 4-1.

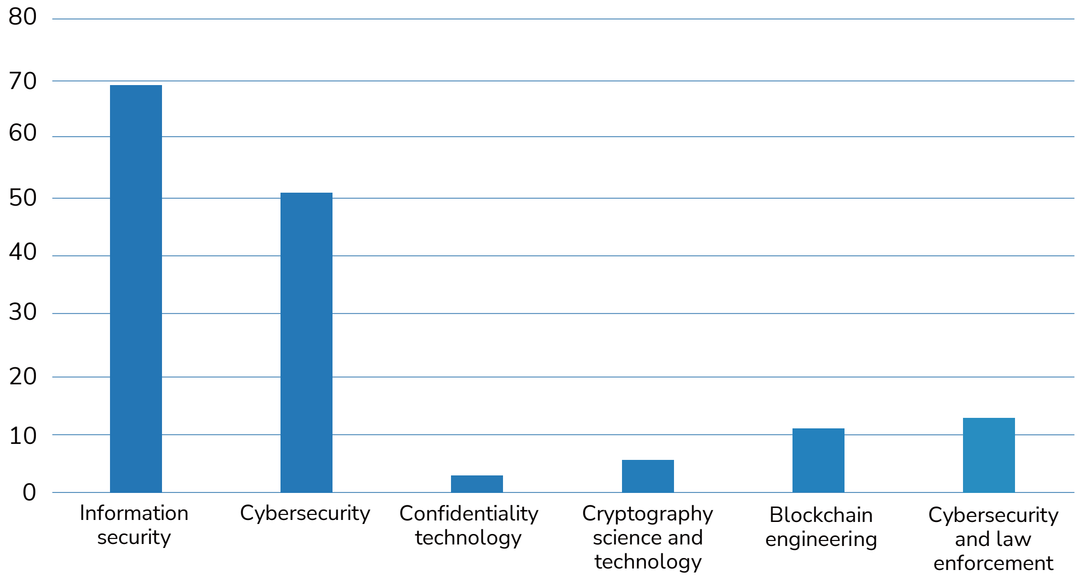


Figure 4-1 Cybersecurity-related Courses

Of all cybersecurity-related courses, information security is the major offered by the most colleges and universities, with 69 schools including the University of Science and Technology of China, Zhejiang University, and Shanghai Jiao Tong University offering this major. It is followed by cybersecurity, with 51 universities including the University of Electronic Science and Technology of China, Huazhong University of Science and Technology, and Beijing University of Posts and Telecommunications. The fewest schools offer majors in security technology, with this major only offered at Fudan University, Beijing Jiaotong University, and Hunan University. Six schools offer majors in cryptography science and technology, all of which are 985, 211, and double world-class[10] institutions, including Huazhong University of Science and Technology, Southeast University, and Beijing University of Posts and Telecommunications. Blockchain engineering is only offered as a major at 11 schools (none of which are 985, 211, or double world-class institutions), such as Taiyuan University of Technology and Qilu University of Technology. Cybersecurity and law enforcement is only offered as a major at 13 public security schools, including the People's Public Security University of

[10] Translator's note: The 211 Project (211工程), launched in November 1995, aimed to build a group of 100-plus Chinese universities into the core source of talent for China's economic and scientific development in the 21st century. The 985 Project (985工程), launched in May 1998, aimed to transform the top 39 of the “211” universities into world-class institutions so as to support China's modernization. Both of these projects have been largely subsumed into the "world-class universities and world-class curricula" (世界一流大学和一流学科) initiative, abbreviated "double world-class" or "double first-class" (“双一流”), launched by the Chinese government in 2017 with the aim of increasing the number of Chinese universities that rank among the world's best. As of September 2022, the government had bestowed the "double world-class" label on 147 universities in China.

China, Zhejiang Police College, and Criminal Investigation Police University of China.

According to statistics, among all colleges and universities offering cybersecurity-related majors, double world-class schools account for about 57.14%, as shown in Figure 4-2. Project 985 schools account for about 24.37%, as shown in Figure 4-3.

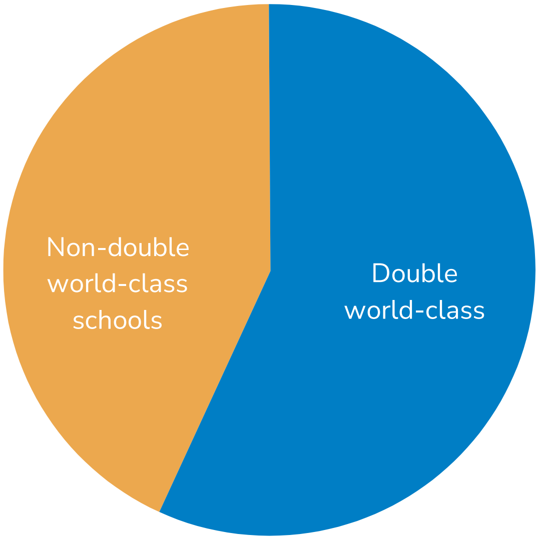


Figure 4-2 Proportion of Double World-Class Schools

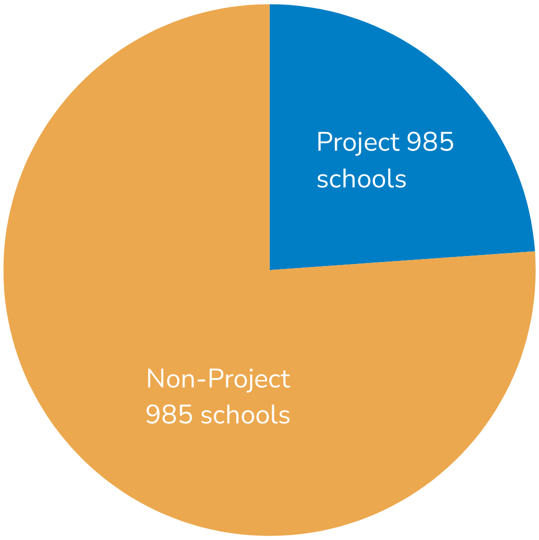


Figure 4-3 Proportion of Project 985 Schools

Statistical results show that Project 211 schools account for about 51.25%, as shown in Figure 4-4.

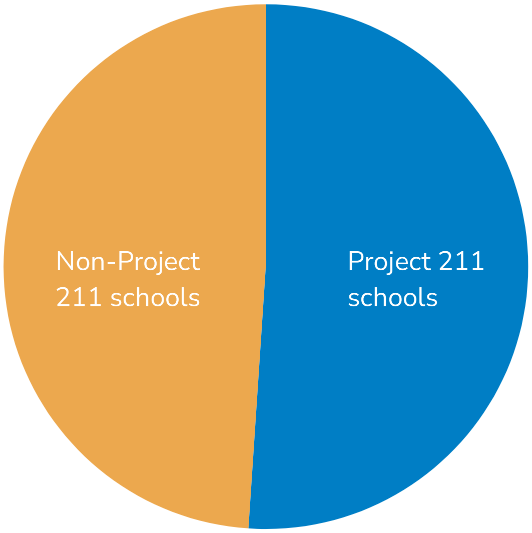


Figure 4-4 Proportion of Project 211 Schools

Among the schools, public security schools account for about 10.01%, as shown in Figure 4-5.

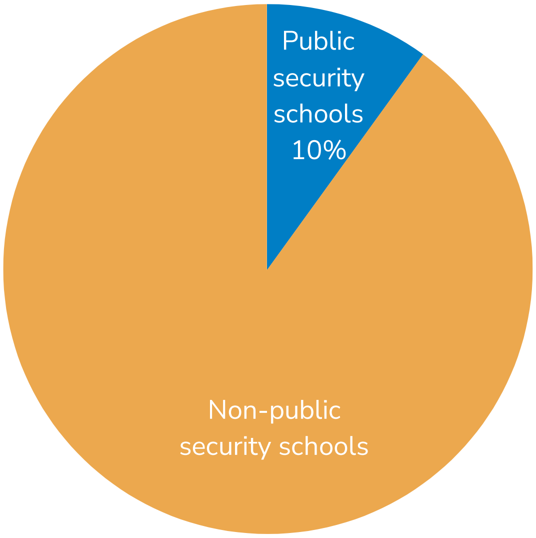


Figure 4-5 Proportion of Public Security Schools

However, in total, there are 2,756 ordinary colleges and universities in China (1,270 bachelor's degree institutions and 1,486 junior colleges [专科]), and the proportion of colleges and universities offering cybersecurity-related majors is only 9% for bachelor's degree institutions and only 4% when junior colleges are also included. From the above data, we can conclude that the total number of colleges and universities offering courses related to cybersecurity in China is still relatively low, and cybersecurity education must be further emphasized, as shown in Figures 4-6, 4-7, and 4-8.

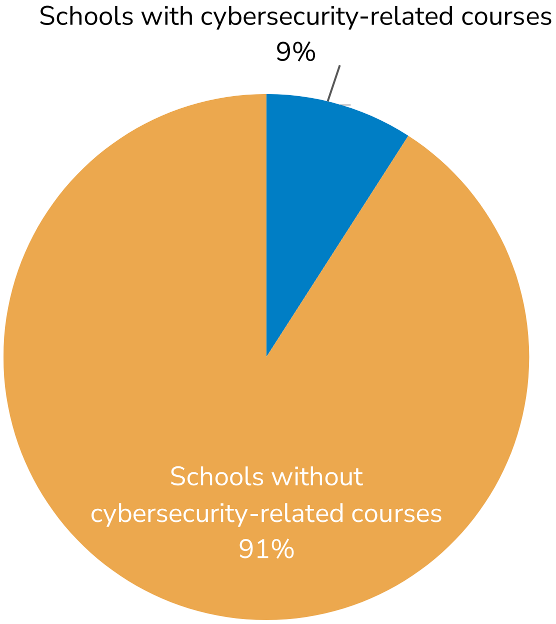


Figure 4-6 Proportion of Colleges and Universities Nationwide (Excluding Junior Colleges)

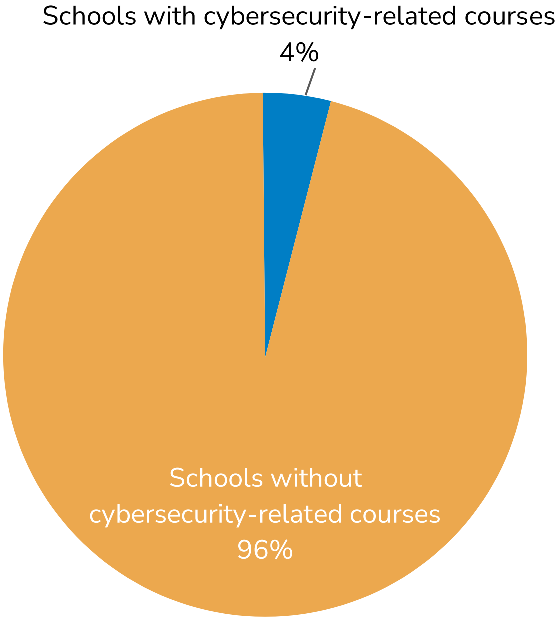


Figure 4-7 Proportion of Colleges and Universities Nationwide (Including Junior Colleges)

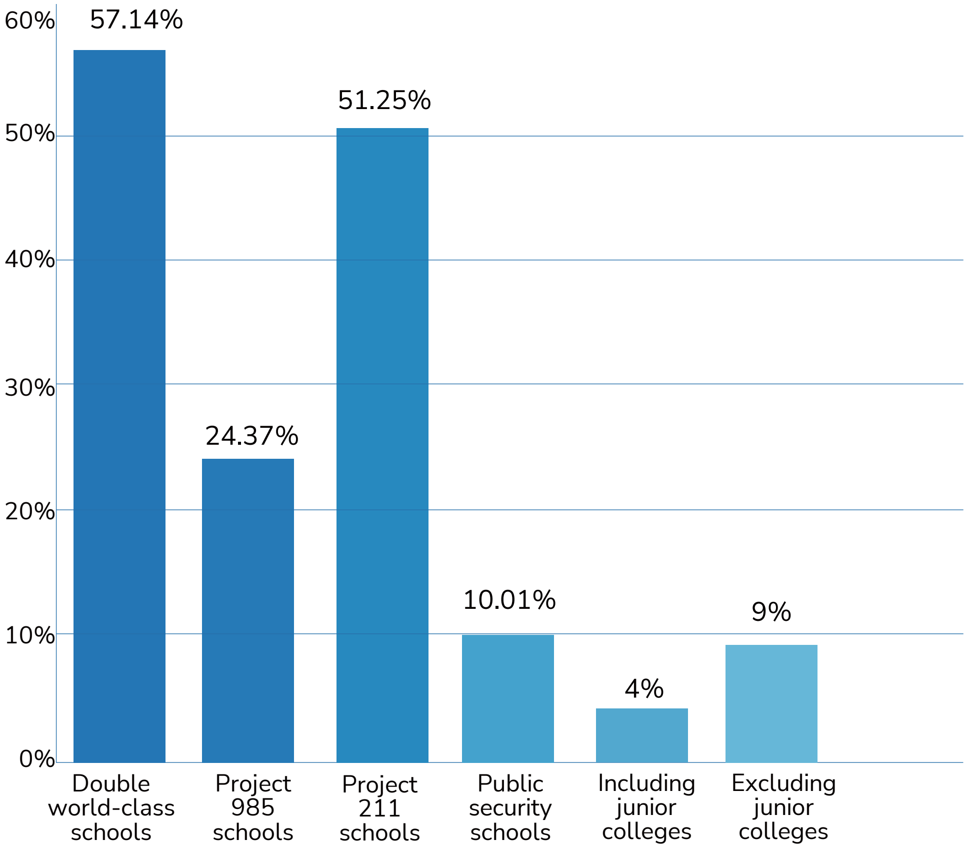


Figure 4-8 Proportions of School Types

Looking at the attributes of schools, education in school focuses more on laying a solid theoretical foundation, building a knowledge system, broadening horizons, providing resource platforms, and cultivating cybersecurity talents of different levels for the country. In the past, when the discipline was first established, it lacked sufficient resources to support the cultivation of students' live-fire attack and defense capabilities, so this relied more on the independent study of students. This can be regarded as one of the shortcomings of capability construction by cybersecurity-related majors in colleges and universities. As training systems have been perfected, network facilities have improved, learning resources have been popularized, various competitions have increased in number, and school-enterprise integration projects have developed, students have more and more practical opportunities. Some schools have established dedicated attack and defense courses to impart practical experience; some schools have upgraded their cybersecurity laboratories to cybersecurity teaching ranges to provide simulated live-fire environments; some schools open up network resources, form CTF teams, and provide extracurricular skills training; and some schools hold cybersecurity-related competitions internally and encourage students to participate in major off-campus competitions to hone their live-fire skills. Various lectures, project practice activities, summer internships, and other activities jointly organized by schools and enterprises have also greatly improved students' live-fire skills.

4.1.2 Development Status of Social Training Institutions

In May 2019, the State Administration for Market Regulation promulgated three major standards: *Information Security Technology—Baseline for Cybersecurity Stratified Protection*, *Information Security Technology—Evaluation Requirement for Stratified Protection of Cybersecurity*, and *Information Security Technology—Technical Requirements of Security Design for Stratified Protection of Cybersecurity*. Since then, for many government and enterprise work units, cybersecurity has changed from something optional to something required or even imposed on them. This has further stimulated the rapid development of the cybersecurity field in China. One after another, various government and enterprise work units have set up independent cybersecurity departments to provide protection for their own data and services.

According to the *2022 Analysis of the Competitiveness of China's Cybersecurity Market and Enterprises* report released by the China Cybersecurity Industry Alliance (CCIA), the scale of China's cybersecurity market will reach about RMB 61.4 billion in 2021, with a year-on-year growth rate of 15.4%. The market is expected to maintain a growth rate of 15%+ over the next three years, with the market size expected to exceed RMB 100 billion by 2024.

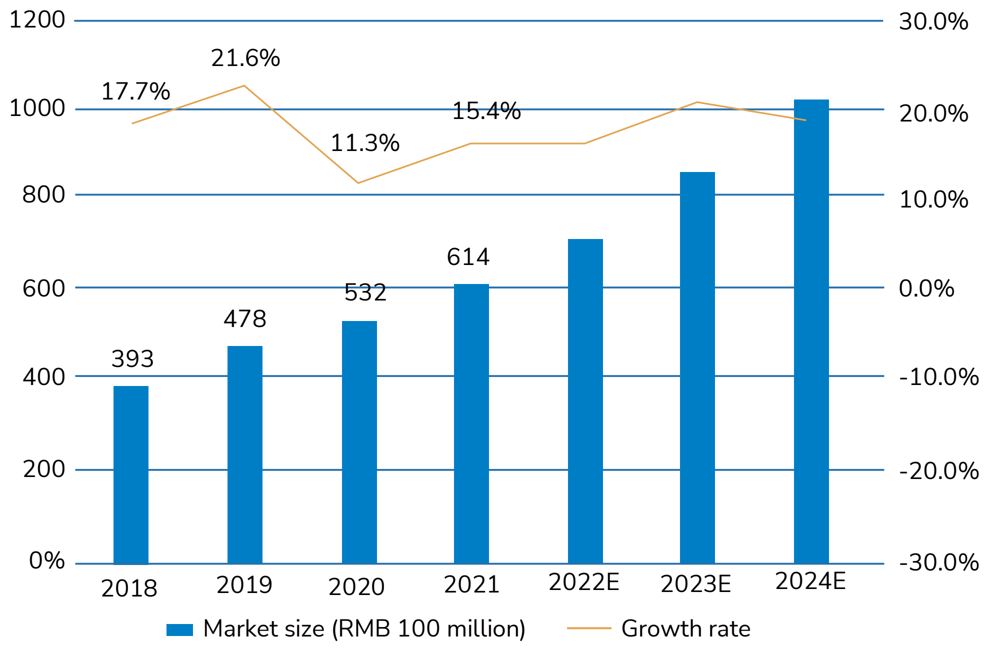


Figure 4-9 Scale and Growth Rate of the Chinese Cybersecurity Market in 2021

With the resumption of work and production in the post-pandemic era, the Chinese economy is recovering at a high speed, and the demand of enterprises for cybersecurity talents continues to increase. Coupled with the promulgation of laws and regulations such as the *Cybersecurity Law*, *Data Security Law*, *Personal Information Protection Law*, and *Regulation on Protecting the Security of Critical Information Infrastructure*, employers' demand for talents has surged, and the shortfall of cybersecurity-related professional talents in China continues to grow. On the other hand, however, few of the students trained by colleges and universities can directly meet the actual needs of employers. Due to this situation, coupled with the continuous increase in employment pressure over many years, many personnel will choose to go to professional social training institutions[11] to improve their abilities in order to find employment or secure a promotion.

According to the results of the survey questionnaire, most of the groups participating in social training do so for the goals of position-based employment, systematic learning of professional knowledge, and enhancement of practical skills, which account for 22%, 21%, and 21% respectively. Another 13% of people do this for the main goal of obtaining certifications, and some people have other goals such as for a hobby, promotion and salary increase, or to participate in security competitions. Generally speaking, basically everyone [who takes cybersecurity social training

[11] Translator’s note: The word “social” (社会) in the term “social training institutions” (社会培训机构) means “not run by the government or the Communist Party,” i.e., private.

courses] is engaged in the field of cybersecurity. They hope that this training will allow them to consolidate their theoretical foundation, enhance their practical operations capabilities, and obtain better employment opportunities.

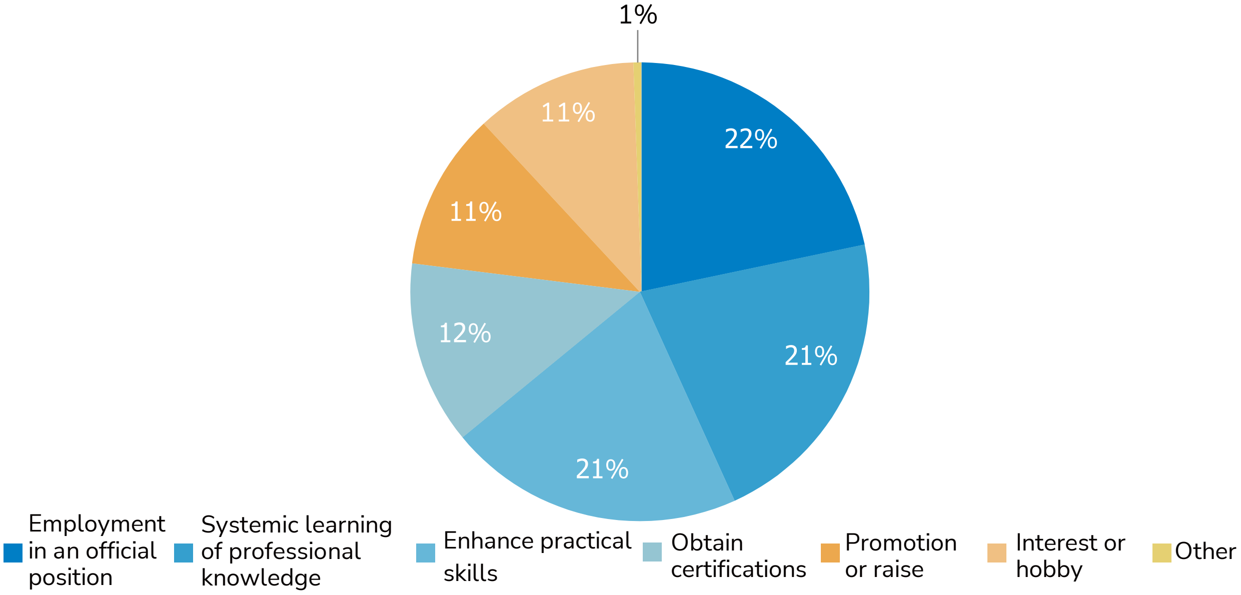


Figure 4-10 Goals of Participating in Training

Influenced by various factors, social training institutions in the cybersecurity industry have developed rapidly. A number of professional training institutions have emerged, including targeted training courses focusing on employment and full-time training courses focusing on research. There are also comprehensive institutions that combine multiple dimensions such as employment, research, and capability improvement. Many people jump into the field of cybersecurity after short-term or medium-term training.

Compared with college and university education, social training institutions pay more attention to cultivating students' live-fire capabilities. They not only designate a large number of course hours for practical training based on real-world scenarios, but also provide simulation laboratories to provide a realistic simulation environment for various vulnerabilities. They also incorporate practice-based activities that lead students to engage in live-fire training such as cybersecurity competitions, security response center (SRC) crowdtesting services, penetration testing, and attack and defense exercises so that students can quickly complete the high-level transformation from theory to practice. Of course, the quality of institutional training also determines the goals and effects that can be achieved.

Social training institutions establish classes of different durations according to the training goals and budget of the personnel, so as to ensure that set goals can be achieved within a limited time. The questionnaire data show that, when cybersecurity personnel choose to participate in training courses, 4-month offline training courses are more popular, with 55% of people choosing to participate; 16% of personnel choose training courses that last 6 months, and 25% of the personnel choose one month or less. Due to work considerations, currently employed personnel are more likely to choose online training with no time limit.

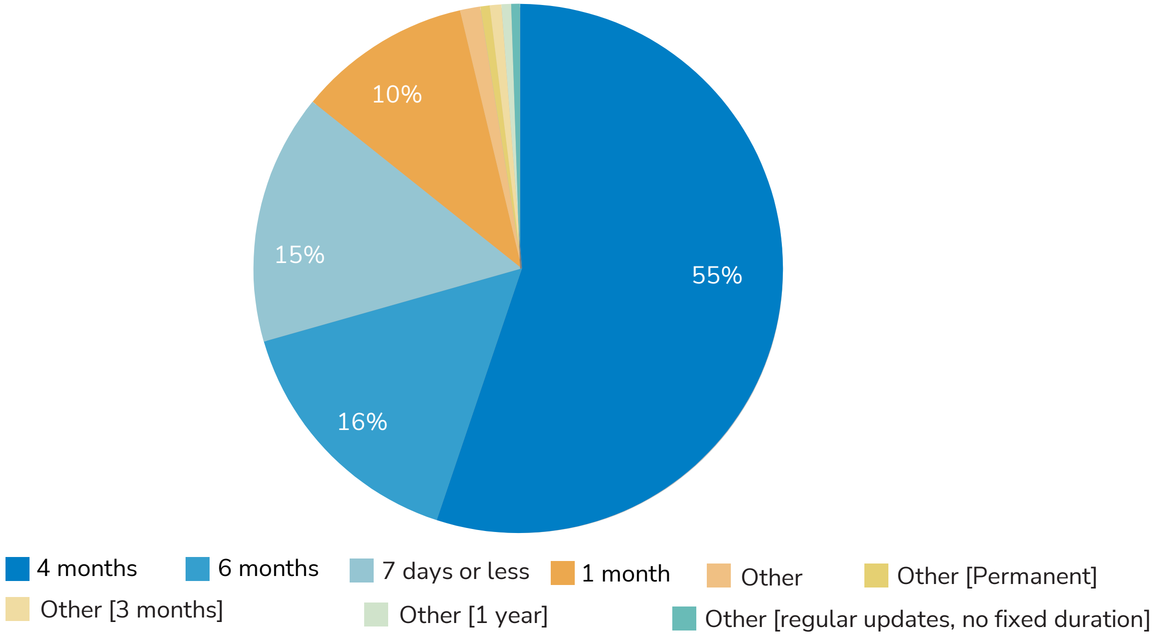


Figure 4-11 Duration of Training Courses Participated in by Cybersecurity Practitioners

From the perspective of market demand, among the courses offered by social training institutions, the demand is higher for web security, penetration testing, and security operations and maintenance courses. On the one hand, there is a large shortfall of existing cybersecurity talents, enterprises are urgently recruiting for the positions corresponding to such courses, and it is easier for trainees to find jobs. On the other hand, the systematic design of such courses is relatively complete, which makes it easier for trainees to systemically master the corresponding knowledge, and the improvement in trainees' comprehensive capabilities will be more obvious.

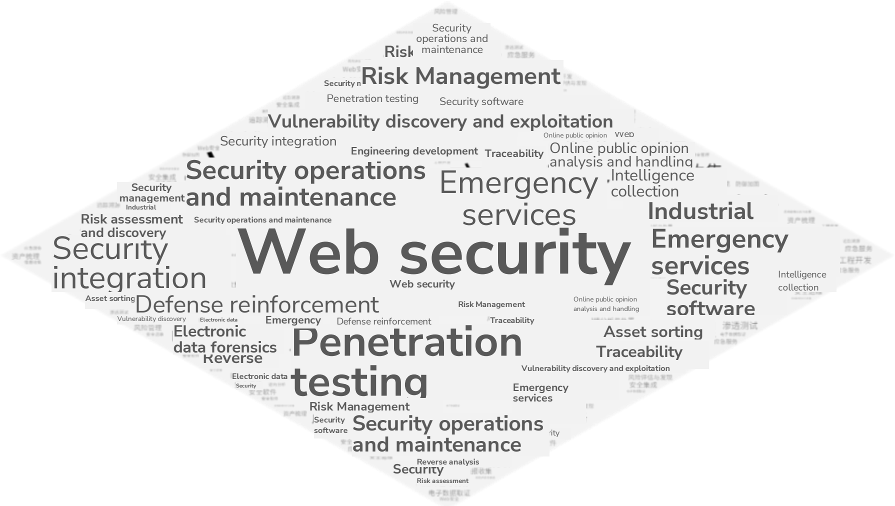


Figure 4-12 Word Cloud of Cybersecurity Course Items

At the same time, with the rapid development of the cybersecurity field, information security professional certifications have gradually become a way for various industries to identify information security talents. It has become a general trend that practitioners in the cybersecurity field must hold certifications in order to hold certain positions. According to International Data Corporation’s (IDC's) *2021 China IT Security Service Market Tracking Report*, in the Chinese security education and training market, security education certification training (including certification training, certification exams, etc.) accounted for half of the market share at 54.2%.

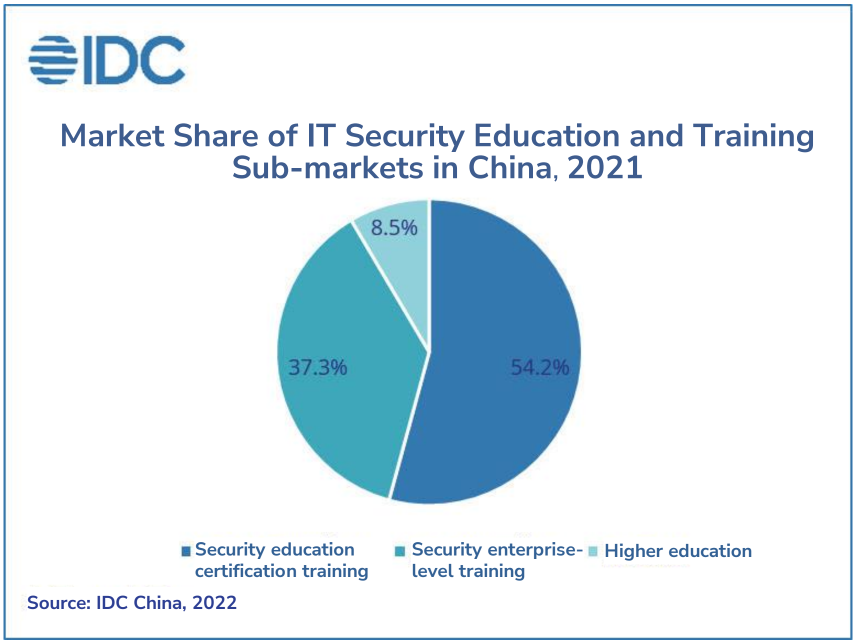


Figure 4 2021 Market Share of IT Security Education and Training Sub-Markets in China

A large number of cybersecurity practitioners believe that obtaining information security certifications can help improve their employment chances and professional capabilities. This is mainly because the process of obtaining a certification is also a process of comprehensively learning and mastering cutting-edge knowledge and technologies in a specific security field, which helps to enhance the competitiveness of individuals in specific security fields so they can steadily improve their careers. According to the *Research Report on the Current Status of Information Security Practitioners in China* released by the China Information Technology Security Evaluation Center, in terms of the types of information security certifications that cybersecurity practitioners have obtained, Certified Information Security Professional (CISP) was the most commonly held certification at 71.8%, followed by Certified Information Systems Security Professional (CISSP) and International Certified Information Systems Auditor (CISA) at over 5% each. In comparison, few people held other types of certifications. This is mainly influenced by factors such as the authoritativeness, degree of recognition, and audience scope of different certifications.

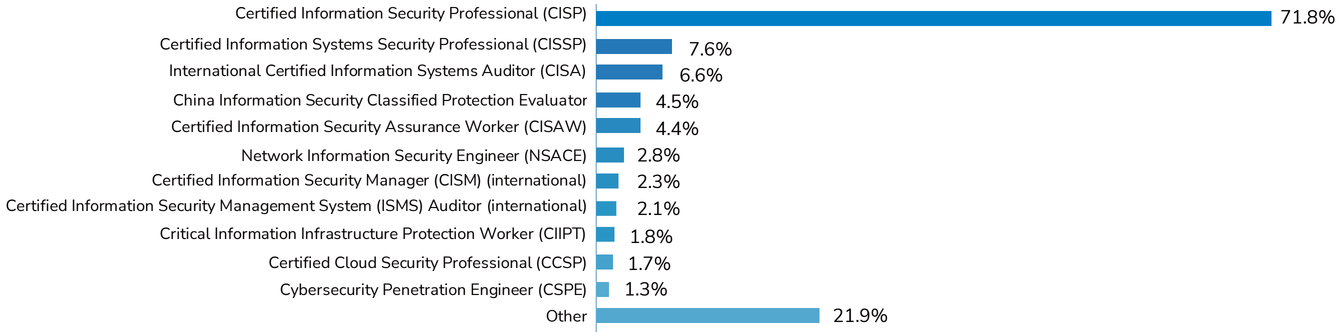


Figure 4-14 Credential Types Held by Cybersecurity Practitioners

4.1.3 Current Status of Employee Training Within Enterprises

With the rapid development of information technology and the gradual blurring of network boundaries, critical information infrastructure, important data, and personal privacy face new threats and risks. The increasing prominence of cybersecurity issues has also sharply increased the demand for diversified, varied, and high-quality cybersecurity talents, especially live-fire and practical talents with a mastery of core technologies. Many companies have already taken internal measures to set up corresponding cybersecurity positions and provide training for security practitioners.

After surveying dozens of enterprises in industries such as cybersecurity, Internet, finance, transportation, chemicals, electric power, political and legal affairs, and healthcare, we found that with the "penetration" of the Internet into various industries, enterprises are also paying more and more attention to cybersecurity issues and have established many security positions and hired professionals to provide protection. Currently, security positions in enterprises mainly include web security engineers, security service engineers, security attack and defense researchers, security management positions, security construction and development positions, and security operations positions, as shown in Table 4-1.

Table 4-1 List of Positions of Corporate Security Practitioners

No.	Position
1	Web security engineer
2	Security service engineer
3	Security management positions
4	Security construction and development positions
5	Security operations and maintenance engineer
6	Security operations engineer

7	Code auditing engineer
8	Supervision and law enforcement positions
9	Scientific research and education positions
10	Penetration testing engineer
11	Operations and maintenance engineer

For the lifecycle of cyberspace software and hardware, security practitioners at different positions need to undertake security responsibilities at different stages. In terms of live-fire security, the main responsibilities of security positions include asset sorting, security research, engineering development, defense reinforcement, penetration testing, security management, security operations and maintenance, intelligence collection, vulnerability discovery and exploitation, risk assessment and discovery, emergency response, traceability, reverse analysis, as shown in Figure 4-15. Among these, penetration testing, vulnerability discovery and exploitation, security operations and maintenance, emergency response, risk assessment and discovery, and security management are particularly valued by enterprises, and most enterprises set up relatively more positions in these directions.

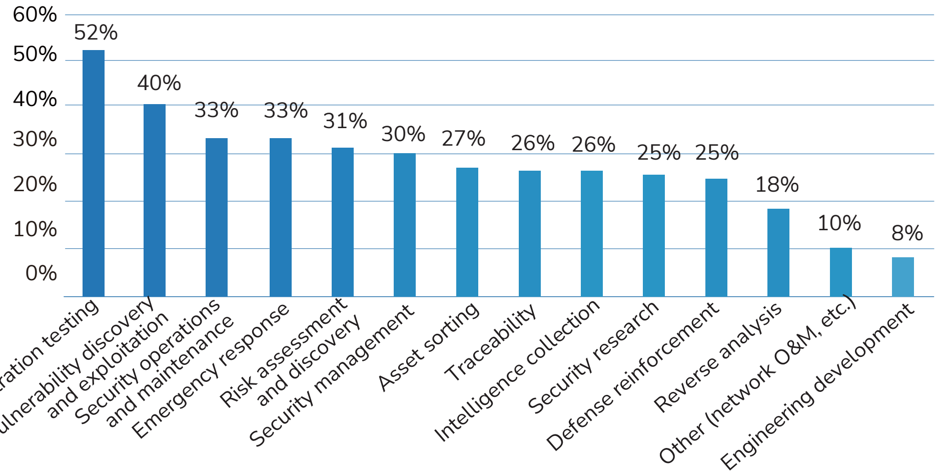


Figure 4-15 Practical Security Responsibilities for Positions Held by Practitioners

However, with the confrontation and mutual promotion of cyber attack and defense and in the face of increasingly complex and diverse cyberattacks, practitioners who can proficiently master and apply professional capabilities such as penetration testing, reverse analysis, web security, and vulnerability mining are very scarce. There is an urgent need for practitioners to improve their capabilities in these areas. At the same time, due to the shortage of professional practitioners and the lack of systematic security management experience in some enterprises, a considerable proportion of enterprises have an unreasonable formal staff position structure that leads to employees holding multiple jobs, or else they have a reasonable formal staff position structure but face difficulties in recruitment, with some having serious deficits of full-time staff of up to 50 people. It can be seen that all of the above situations cause serious cybersecurity risks for most enterprises. This is shown in Figures 4-16, 4-17, and 4-18.

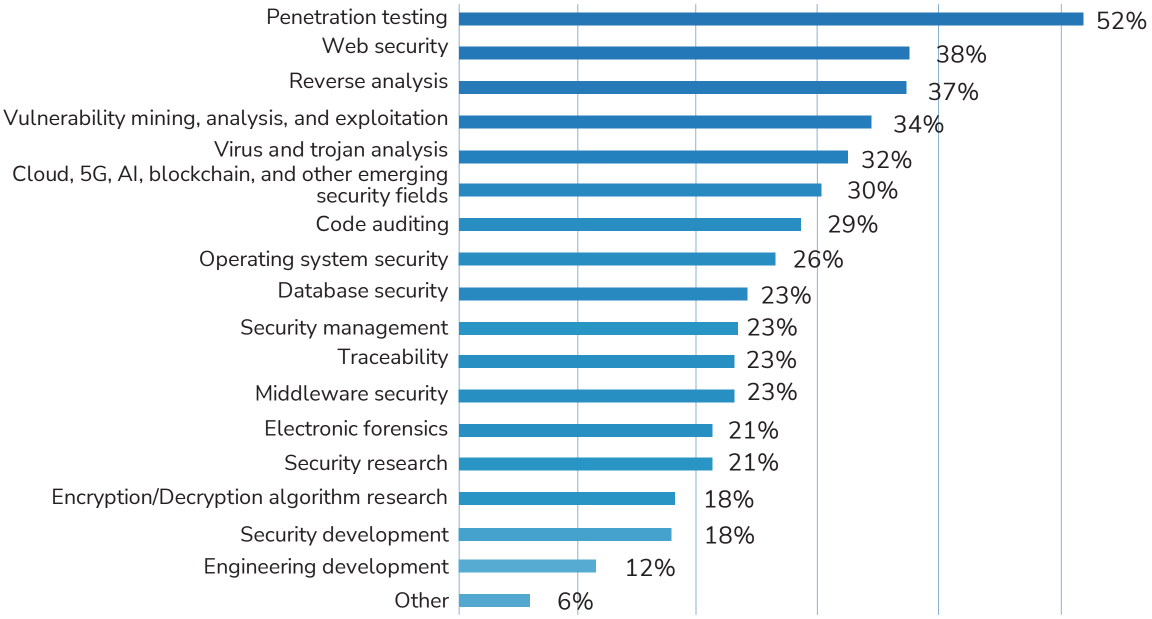


Figure 4-16 Professional Cybersecurity Capabilities that Practitioners Urgently Need to Improve

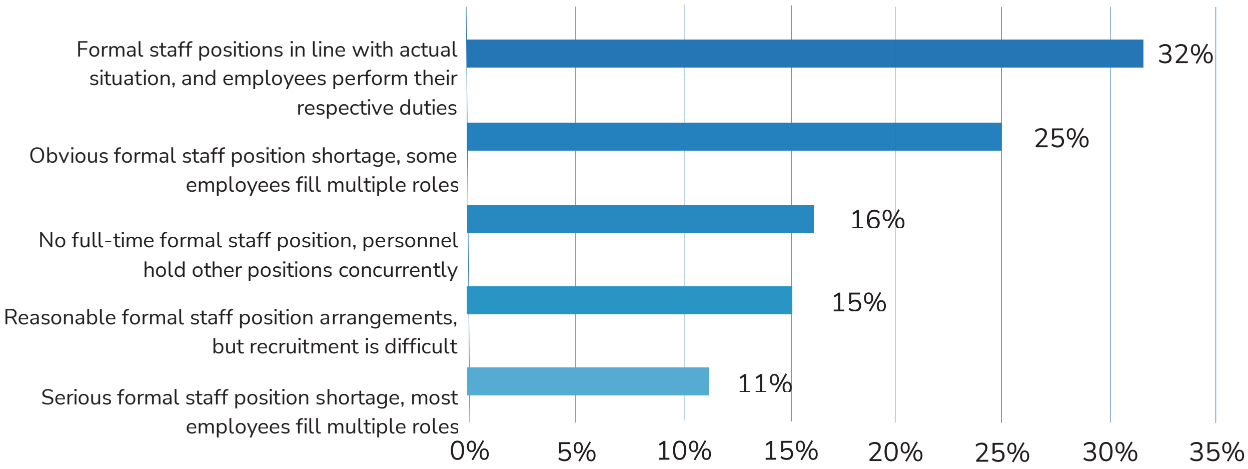


Figure 4-17 Ability of Internal Cybersecurity Professionals to Meet Business Needs

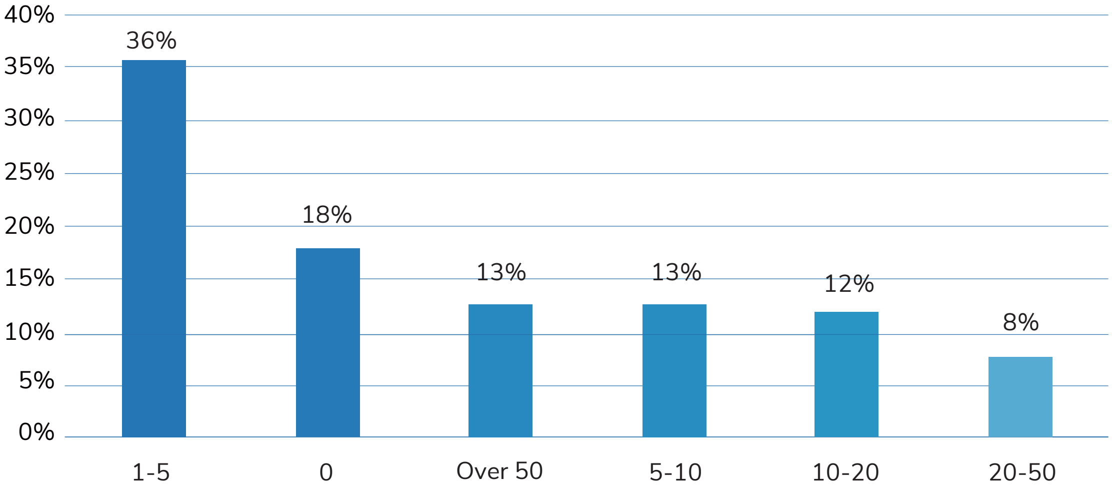


Figure 4-18 Employers' Cybersecurity Personnel Shortfall

4.2 Analysis of Talent Training Methods

4.2.1 Analysis of College and University Training Methods

According to statistics, among the 51 colleges and universities offering cybersecurity courses, 37 have teams or experimental classes. Among them, Xidian University and Southeast University are the two that have received the most competition awards. Xidian University has won more than 290 awards including the grand prize at the National Cryptographic Technology Competition and the first prize at the National University Student Information Security Competition. Students from Southeast University have won more than 30 awards in various cybersecurity competitions.

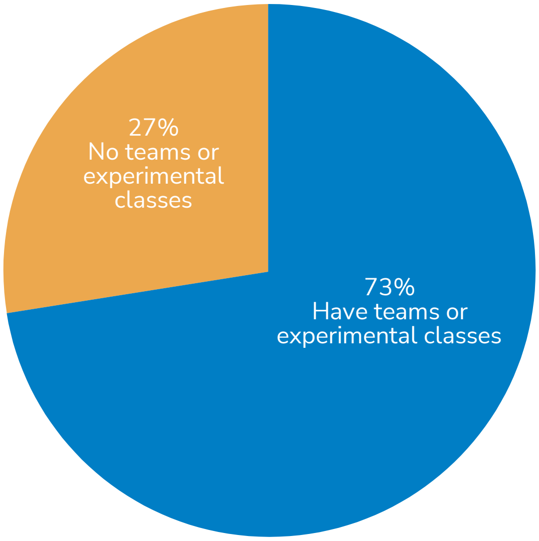


Figure 4-19 Proportion of Schools with Teams or Experimental Classes

Among all the colleges and universities that offer practical courses related to cybersecurity, the statistics on the training programs at each college show that practical courses are mainly distributed in the 3rd to 7th semesters, as shown in Figure 4-20.

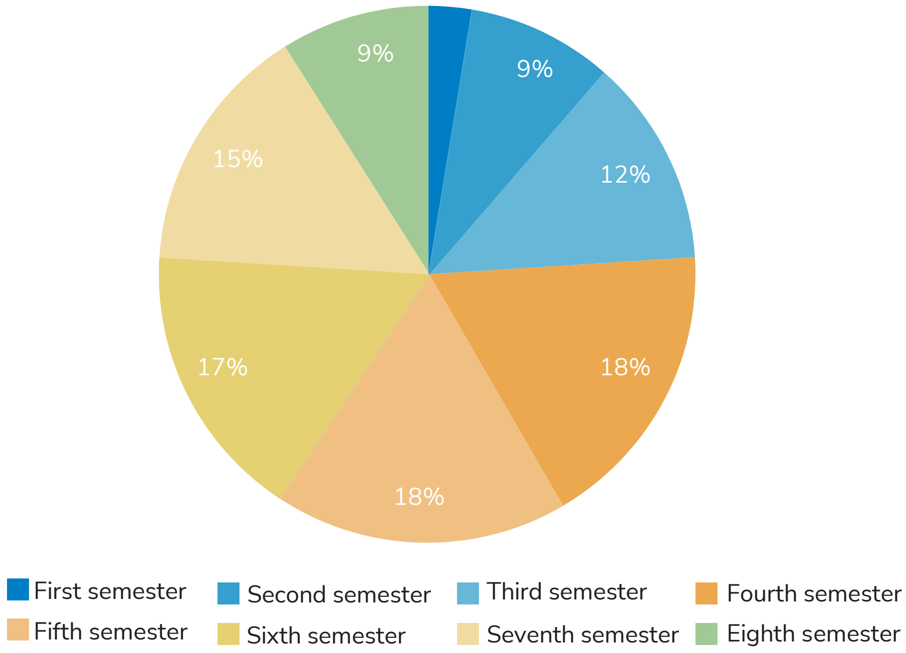


Figure 4-20 Time Distribution of Practical Courses

Little information is available on school-enterprise cooperation courses. The survey only shows that Heilongjiang University has 5 courses, Guilin University of Electronic Technology has 2 courses, and Jilin University has 1 course. In terms of school-enterprise cooperation, 16 schools cooperate with enterprises, 7 schools do not cooperate with enterprises, and cooperation information could not be obtained for 28 schools. Different schools also cooperate with different numbers of enterprises. Nanchang University, for example, cooperates with far more enterprises than other schools, cooperating with as many as 38 enterprises, as shown in Figure 4-21.

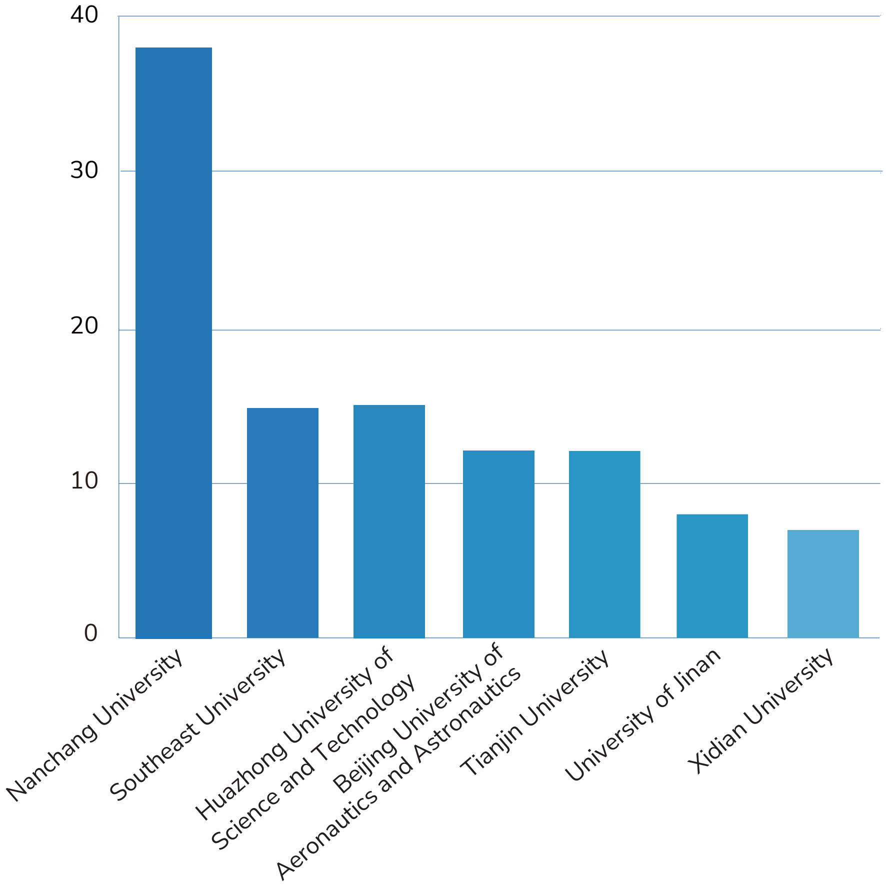


Figure 4-21 Number of Enterprises Cooperated with

According to the relevant course statistics of 51 colleges and universities offering cybersecurity courses, we can see that computer networks, discrete mathematics, data structures, and operating systems are the four courses offered at the most schools. This is shown in the word cloud in Figure 4-22.

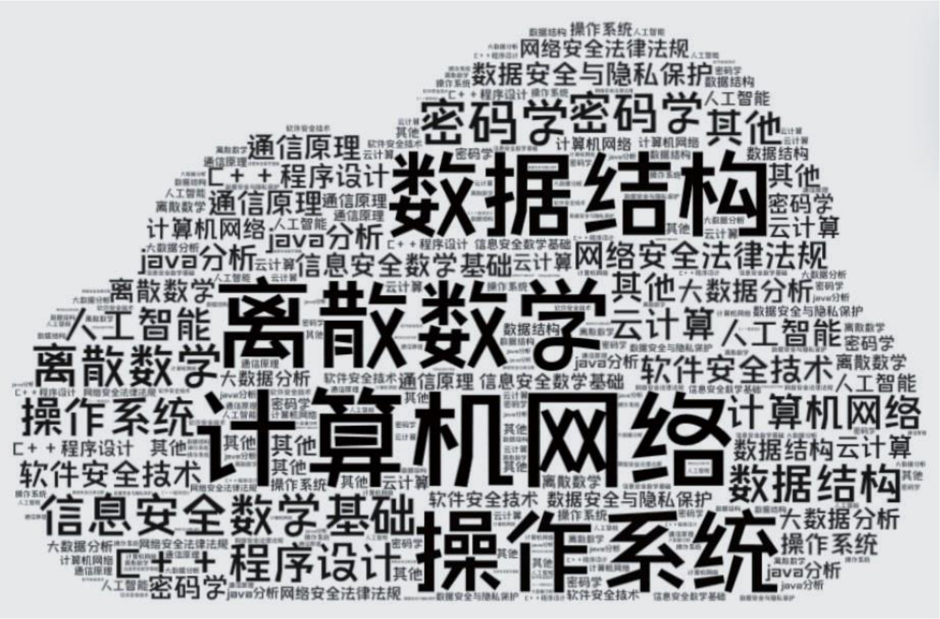


Figure 4-22 Word Cloud of Courses[12]

According to the above data, we can see that most of the colleges and universities with teams or experimental classes and many competition awards are double world-class, Project 985, and Project 211 schools. The various schools pay great attention to the setup of practical courses and the major courses offered are in line with talent training needs, but there are very few schools offering school-enterprise cooperation courses. In the future, more courses of this kind may be offered to allow societal knowledge and technology to enter students' classrooms and better cultivate the individual capabilities of students.

On the whole, schools adhere to a practical capability development system that combines in-class and extracurricular learning, online and offline learning, and on-campus and off-campus learning. This system cultivates students' capabilities through theoretical teaching, case study investigation, experimental operations, simulated confrontation, competitions and contests, projects, research topics, internships, and other means. In addition to the above-mentioned curriculum offerings, competition awards, and school-enterprise cooperation, schools have also widely adopted methods such as lecture training, summer camps, clubs, and social activities to enrich student training methods. They have built attack and defense ranges, provided learning materials and implementation tools, and encouraged participation in attack and defense drills and in practical projects to increase the practical training channels open

[12] Translator's note: The four terms written in the largest font in the Figure 4-22 word cloud are, in descending order of font size, "computer networks" (计算机网络), "discrete mathematics" (离散数学), "data structures" (数据结构), and "operating systems" (操作系统).

to students. These activities generally offer generous prizes and bonuses, along with academic credits, various honors, and even job recommendations, to encourage more students to actively participate and hone the live-fire capabilities of individuals and teams.

4.2.2 Analysis of Social Training Institution Training Methods

The training methods of social training institutions can be divided into three main formats: online courses, offline in-person teaching, and a combination of online and offline. Under the influence of the COVID-19 pandemic, many offline courses have been converted to online in recent years. According to statistics, 56% of trainees would choose to learn through offline in-person teaching, and only 14% of the trainees prefer online classes. If they do not consider the impact of the pandemic, most personnel prefer offline in-person training methods, probably because offline training and teaching can build a good learning environment, and face-to-face exchanges also make communication smoother and facilitate the timely resolution of various problems and questions when learning. Online courses are more popular with people who are busy with studies and work, as it allows them to use their scattered free time to participate in training, and it is also an option for improving their theoretical knowledge and practical operation level, as shown in Figure 4-23.

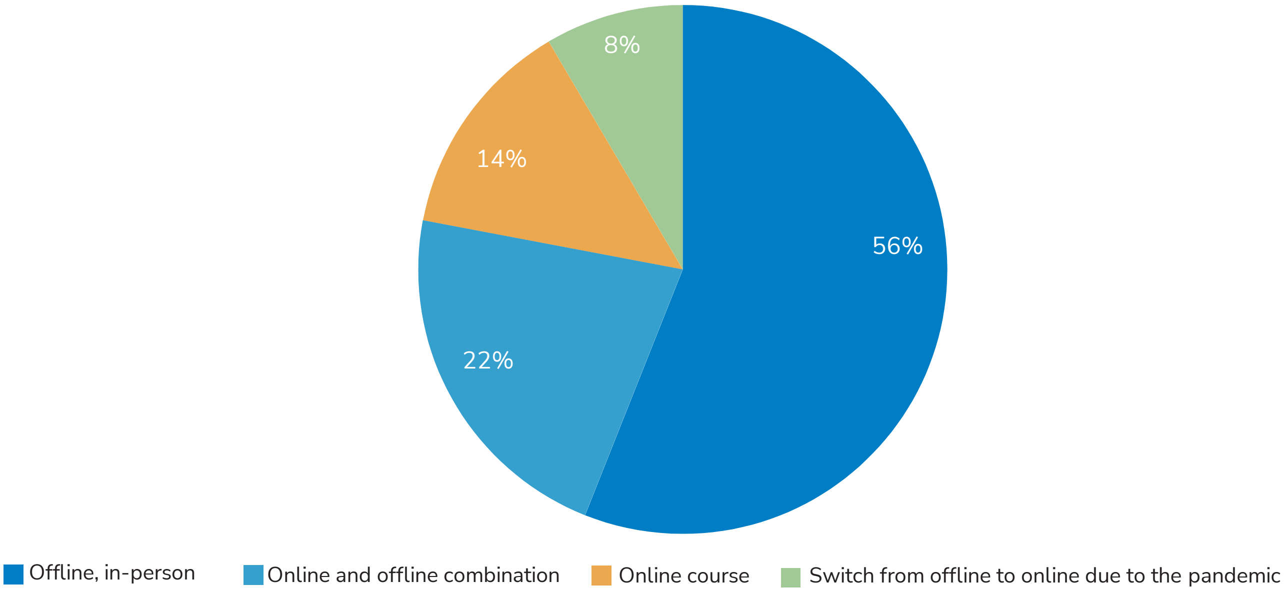


Figure 4-23 Format of Training Courses Participated in by Cybersecurity Trainees

How to effectively improve the live-fire attack and defense level of personnel and cultivate security talents who can deal with real cybersecurity threats and solve practical security problems is critical. In order to improve the construction of cybersecurity talents, Chinese cybersecurity training institutions actively formulate their own talent selection and training programs, incorporate theoretical learning and practical training in multiple dimensions, build high-quality live-fire attack and defense training ranges and overall training systems for support, and establish and improve their selection and training systems for cybersecurity talents.

In terms of curriculum setup, social training institutions with relatively complete services that include five modules, "theoretical courses, practical exercises, assessment and evaluation, real-world practice (社会实践), and interview coaching," and implement a closed-loop process for personnel from training to practice to employment management account for 30%. Institutions with four modules account for 19%, institutions with only three account for 32%, and some institutions are only focused on theoretical courses + practical training. 50% of institutions provide interview coaching to help students better complete employment interviews and find the job of their dreams. At the same time, more than 35% of the institutions have advantages in societal practice resources and can provide special practice modules that offer students comprehensive improvement services from theory to practice, as shown in Figure 4-24.

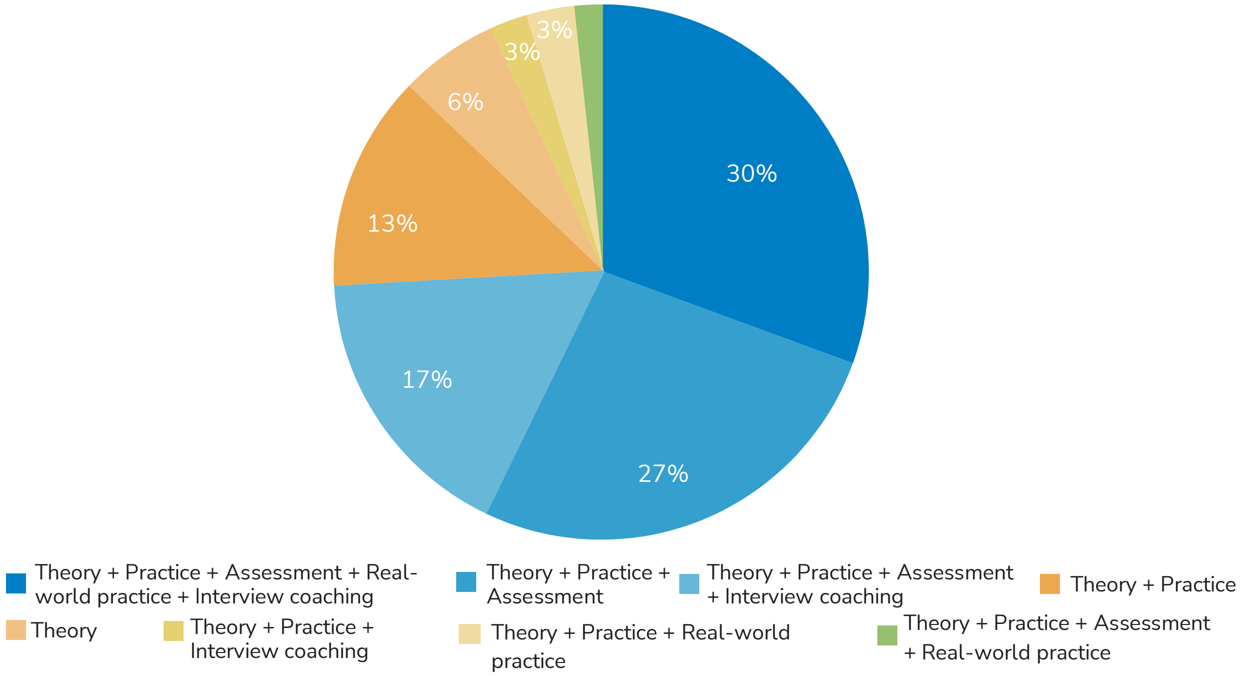


Figure 4-24 Proportions of Social Training Institutions Offering Different Modules

According to the survey results, the courses of training institutions usually cover multiple specific directions in the security field, such as security software, security operations and maintenance, security integration, industrial control cybersecurity, emergency services, penetration testing, electronic data forensics, online public opinion analysis and handling, and risk management. Among these, web security and penetration testing are the most common courses, as they are required courses for almost every trainee. These courses are followed by emergency services, security operations and maintenance, and security integration. For the other directions, training institutions make arrangements according to the specific needs of trainees, as shown in Figure 4-25.

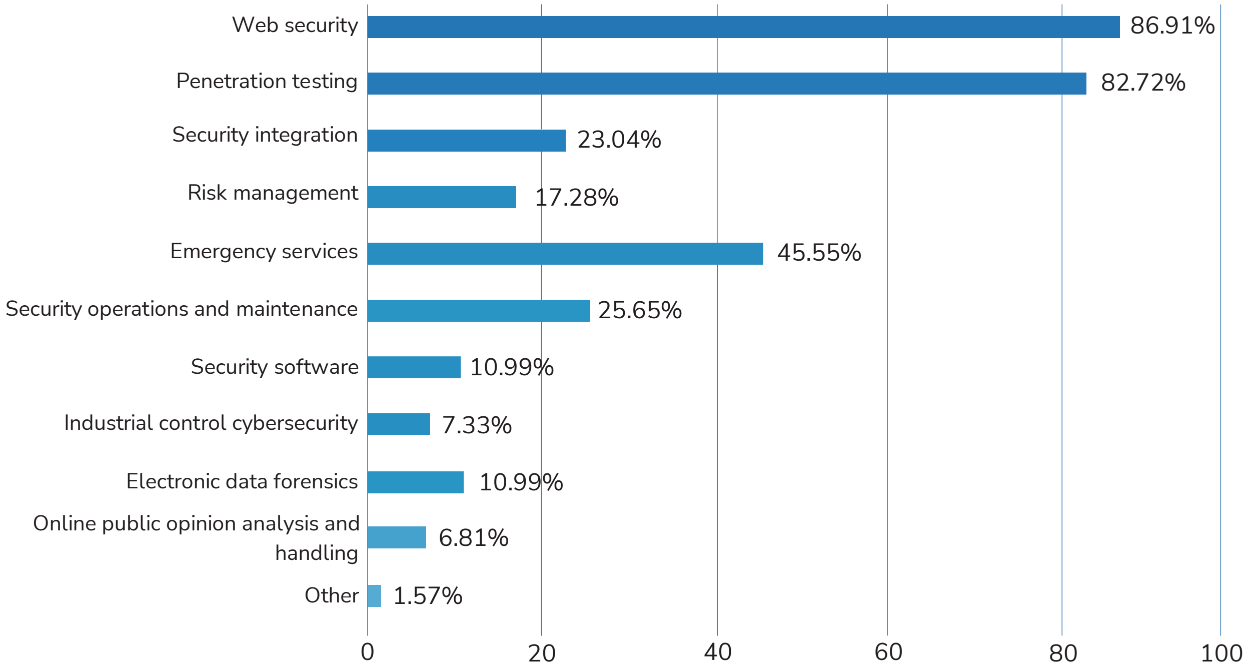


Figure 4-25　Directions of Cybersecurity Training Course Design

Based on the talent training programs of well-known cybersecurity training institutions in the industry such as iSpring and Autumn (i 春秋), Nanjing Cyberpeace (赛宁网安), Hetian Zhihui (合天智汇), GooAnn (谷安天下), Yilinbo (易霖博), and Hunan Cyber Security Base (湖南网安基地), training institutions usually adopt training methods that combine multiple dimensions such as learning, competition, performance, evaluation, attack, and defense when selecting and training security talents. For example, institutions carry out professional theoretical knowledge teaching in the form of inviting domain experts to teach offline in-person or online open classes; build high-quality live-fire attack and defense training ranges and provide offline internship and training venues; organize and participate in various cybersecurity competitions to cultivate live-fire operations capabilities; appoint special mentors to arrange and guide daily learning tasks, explain the industry development situation, and give career planning guidance; and customize training programs for specific needs, such as standardized employment (标准化就业), school-enterprise cooperation, or certification assessment training, as shown in Figure 4-26.

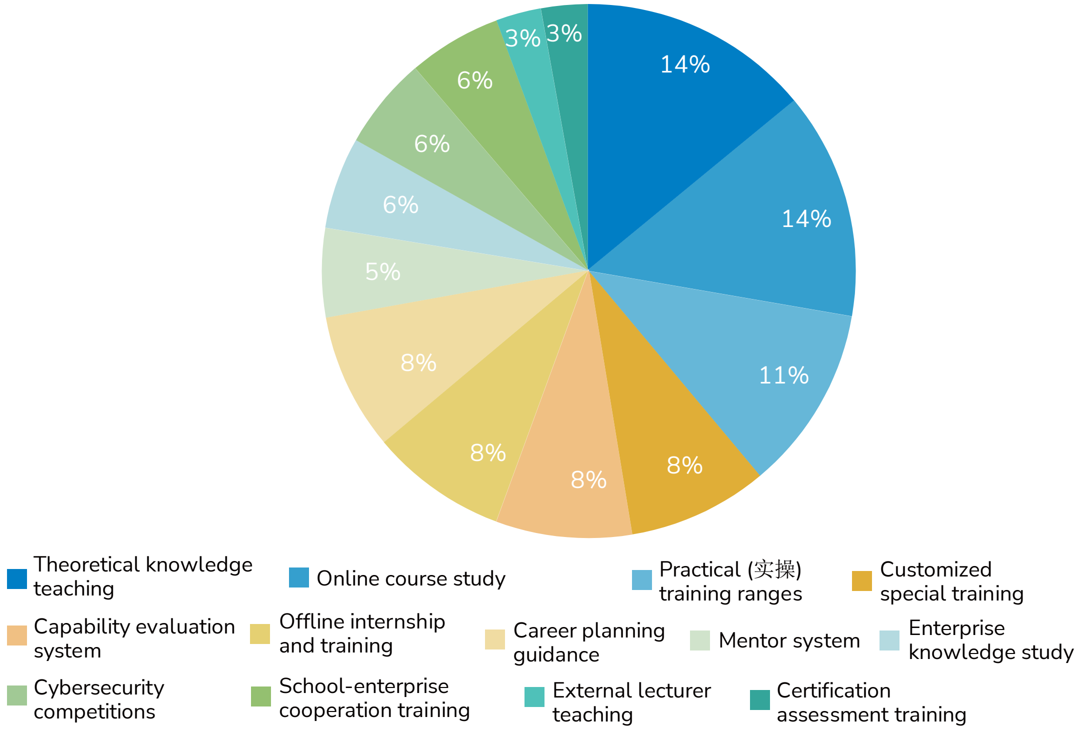


Figure 4-26 Common Training Methods of Mainstream Training Institutions

Major training institutions combine theoretical teaching, hands-on practice, mentor guidance, and customized training, adhere to the guiding idea of "people are the core of security," actively develop comprehensive, professional, and perfected cybersecurity talent training methods, and are committed to improving the professional skills of cybersecurity talents and selecting and training more cybersecurity talents.

4.2.3 Analysis of Enterprise Internal Training Methods

In order to alleviate and effectively solve the problems of insufficient cybersecurity talents and insufficient cybersecurity business capabilities, more and more enterprises are realizing that it is necessary to train employees so that they become security talents.

According to statistics, among all enterprise units, practical cyber personnel in the directions of penetration testing, vulnerability discovery and exploitation, and reverse analysis are the scarcest, followed by the directions of security operations and maintenance, intelligence collection, and traceability. Figure 4-27 shows the practical cybersecurity personnel that work units have the hardest time finding.

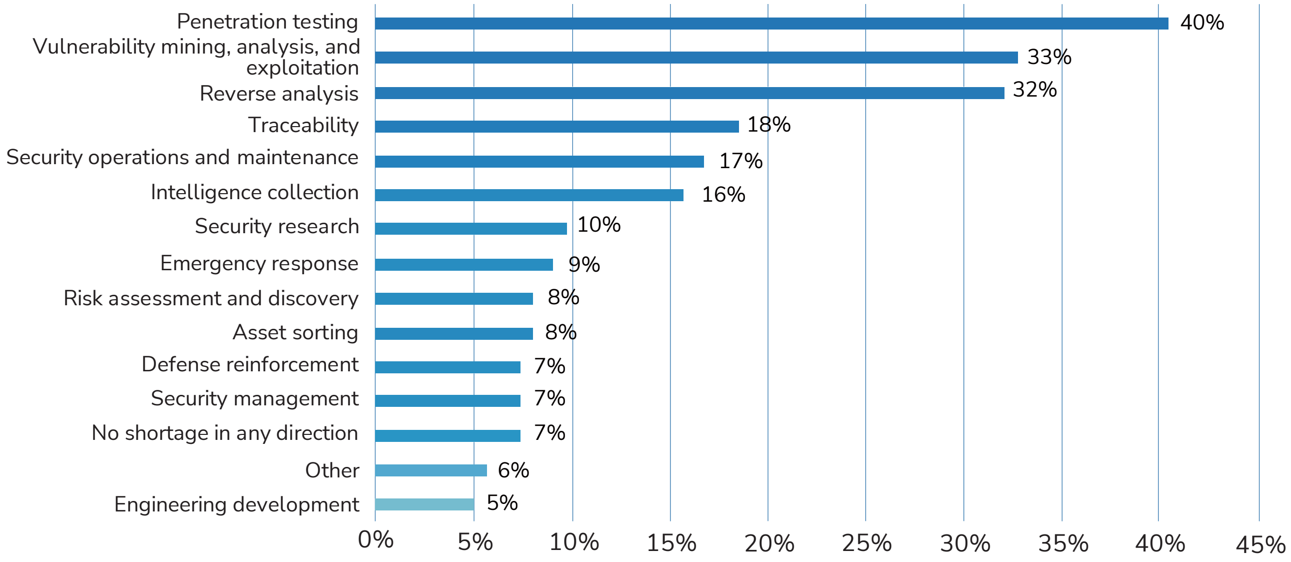


Figure 4-27 Practical Cybersecurity Personnel Work Units Most Lack

In terms of specific cybersecurity business capabilities, due to the short supply of personnel with a mastery of core security technologies, enterprises generally lack corresponding business capabilities such as reverse analysis, penetration testing, vulnerability mining, and trojan and virus analysis. At the same time, with the innovative development of emerging technologies and the accelerated deployment of new infrastructure industries, there are also large shortfalls in security business capabilities in cloud, 5G, AI, blockchain, and other emerging fields. Figure 4-28 shows the cybersecurity business capabilities that units generally lack.

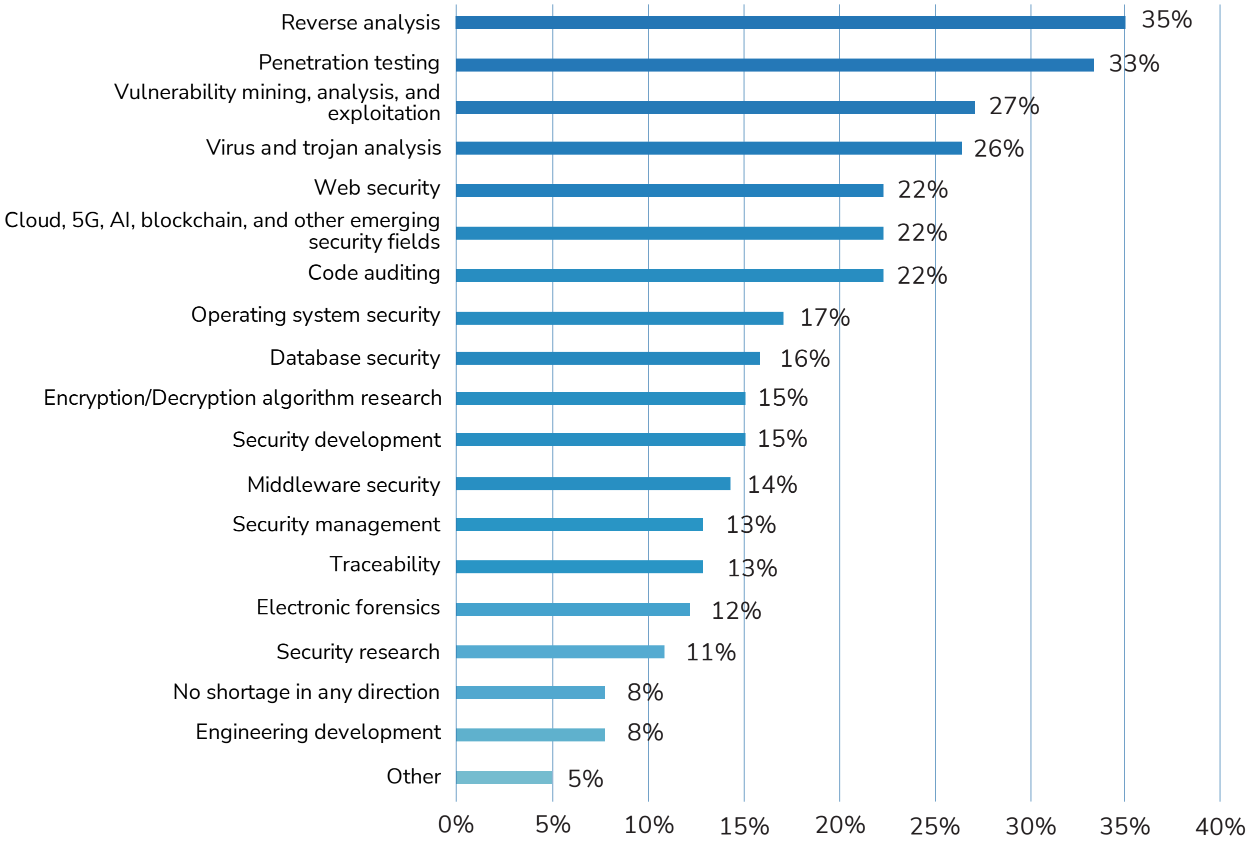


Figure 4-28 Cybersecurity Business Capabilities Generally Lacked by Work Units

Enterprises generally adopt a variety of methods to train security practitioners, for example, establishing a mentor system where experienced people train new people, invite experts to give lectures, customize live-fire attack and defense platforms, regularly organize attack and defense drills, hold internal cybersecurity competitions, and encourage employees to participate in external cybersecurity competitions. Most group-type cybersecurity corporations and giant companies (顶级企业) have established cybersecurity laboratories or teams and organized their participation in some national-level cybersecurity competitions. On the one hand, they use competitions to train employees and hone their skills. On the other hand, these competitions advertise the strength of the enterprise and enhance its reputation. For example, Tencent's “eee” team was crowned champion in the first "Wangding Cup" cybersecurity competition in 2018 and won the grand prize in the 2021 "Strong Net Cup" cybersecurity challenge. Qi An Xin Group's (奇安信集团) Tiger Tally (虎符) team won the championship in the 2nd "Wangding Cup" cybersecurity competition in 2020, and China Mobile's “Guarding Hengshan” (守望者衡山) Team, Information & Data Security Solutions’ (上海观安) Wuxiang Laboratory (无相实验室), and State Grid Corporation of China’s Network Protection Vanguard (护网先锋) Team and Crimson Night (赤霄) Team have all won second prizes. In the first defense-oriented cybersecurity competition, the "Longjian Cup," in 2021, multiple teams under China Southern Power Grid, China Mobile, and other group corporations performed well and won multiple awards. The team formed by Beijing Chaitin Future Technology Co. (长亭) won first prize at the 2019 "Strong Net Cup" cybersecurity challenge, second prize at the 2018 "Wangding Cup" cybersecurity competition, and first prize at the 2016 China Cybersecurity Technology Confrontation Competition. This shows us that, in China's important key industries and large Internet enterprises, it is the norm to form elite teams with live-fire experience. This also reflects the fact that large enterprises are attaching more and more importance to the overall live-fire attack and defense capabilities of cybersecurity professionals.

In addition to competitions, due to the frequent occurrence of data leaks, viruses, ransomware, and other cyberattacks that result in serious losses to enterprises, organizing cyber attack and defense drills has also become an important way for many enterprises to cultivate employees' cybersecurity awareness and attack and defense capabilities. Through such activities, enterprises can detect their own weak points and vulnerabilities, improve the security capabilities of networks, systems, and equipment, and cultivate employees' practical attack and defense capabilities.

Generally speaking, for the cultivation of employee abilities, the mentoring system, in which experienced personnel guide new personnel, is the most common approach. But there are still some units that have not adopted any measures to train practitioners. The improvement measures taken by various units are shown in Figure 4-29.

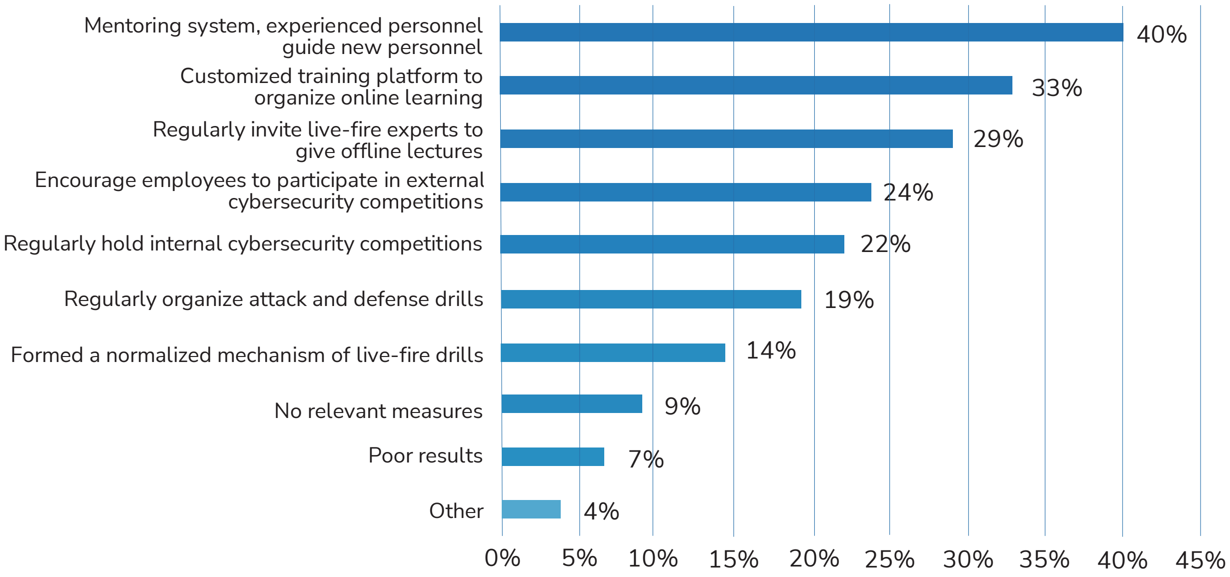


Figure 4-29 Measures Adopted by Employers to Improve the Live-Fire Capabilities of Employees

4.3 Analysis of Talent Training Results

4.3.1 Analysis of College and University Training Results

Among the colleges and universities offering cybersecurity majors, available official data shows that the employment rate [of graduates] exceeds 90%. Some schools have made outstanding training achievements, such as Northwestern Polytechnical University, which trains 54 people every year and achieved a 100% employment rate for its 2021 graduates; the employment rate of the 123 bachelor's degrees graduates from Beijing University of Posts and Telecommunications in 2021 was 96.75%, and its 190 master's degree graduates had an employment rate of 100%.

Our research suggests most of the students with relevant majors trained by colleges and universities believe that they can fully grasp the course content and learn with ease or without much difficulty, as shown in Figure 4-30.

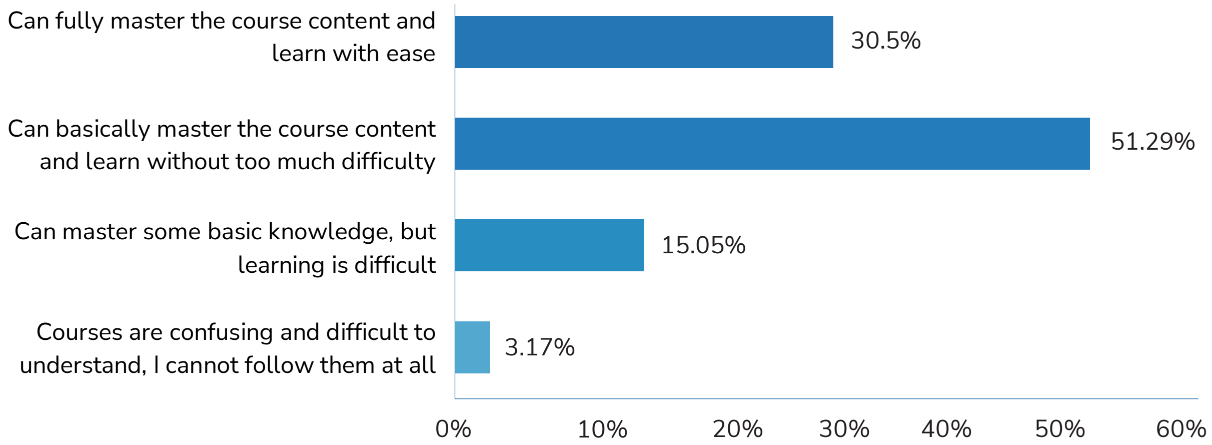


Figure 4-30 Students' Mastery of Knowledge

Although the current employment rate and student comprehension at colleges and universities are good, some problems still exist in the training process. Some students at schools think that teachers' teaching methods are not varied, they emphasize theory over practice, the school's training program is out of touch with the needs of society, and the positioning of training goals is not accurate. These problems require attention. Schools should gradually overcome them in future education and teaching, improve teaching methods, and cultivate new cybersecurity talents who can better meet the needs of society and combine theory and practice.

4.3.2 Analysis of Training Institution Training Results

According to the survey statistics, in terms of control of the difficulty of training courses and students’ absorption of the coursework, most of the students can understand and master the knowledge in the courses, but some students still say that the current course settings are relatively difficult, at least for them. As we can see from

Figure 4-31, the overall absorption of courses by students is relatively good, and the difficulty setting is reasonable and moderate.

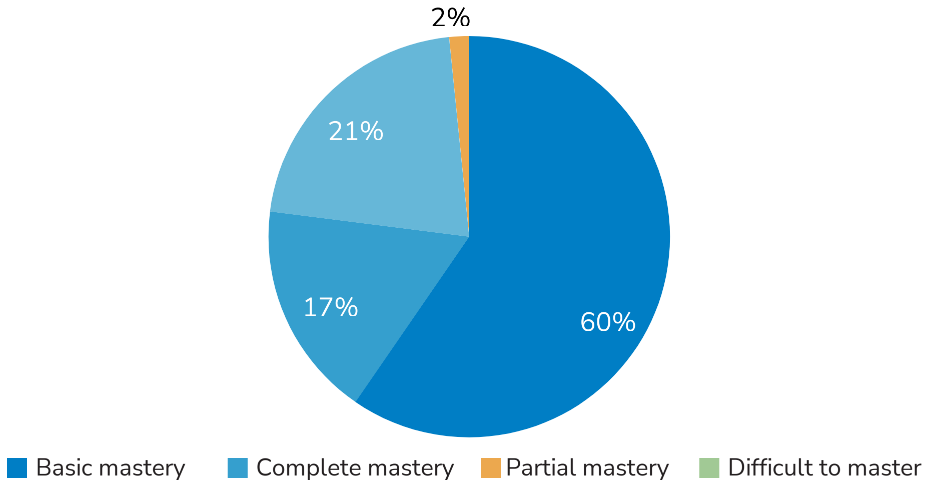


Figure 4-31 Course Mastery of Cybersecurity Training Institution Trainees[13]

Looking at student evaluations of the practicality of training institution courses, about two-thirds of the respondents said that the training courses have a complete system, pay attention to practicing real operations, and have strong practicality. A quarter of the respondents said that the course system was relatively complete but the course did not focus on real operations. As we can see from Figure 4-32, the courses of most training institutions are generally very practical, but there are still some training courses with unreasonable system designs and a lack of training in hands-on capabilities.

[13] Translator's note: In the original Chinese text of the white paper, in Figures 4-31 and 4-32, there is a mismatch between the colors of the pie chart slices (three shades of blue and one orange) and the colors of the pie chart labels (two shades of blue, one orange, and one green).

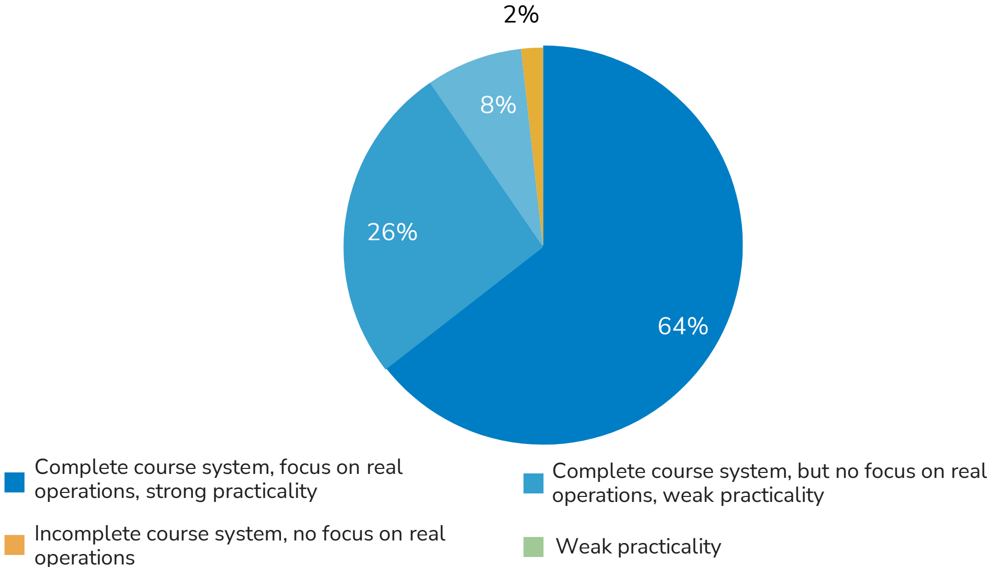


Figure 4-32　Course Practicality Evaluation by Cybersecurity Training Institution Trainees

In terms of the employment situation of graduates, students from different training institutions show different results. A small number of training institutions are highly recognized by some companies for their reputation in training students and want to reserve students at the very start of the course. At most training institutions, some students accept job offers before the end of training, and basically all students are employed by the end of training. However, there are still a small number of surveyed personnel who said that after the training, most of the trainees still had no prospective job offers (意向单位). Overall, trainees have good employment prospects.

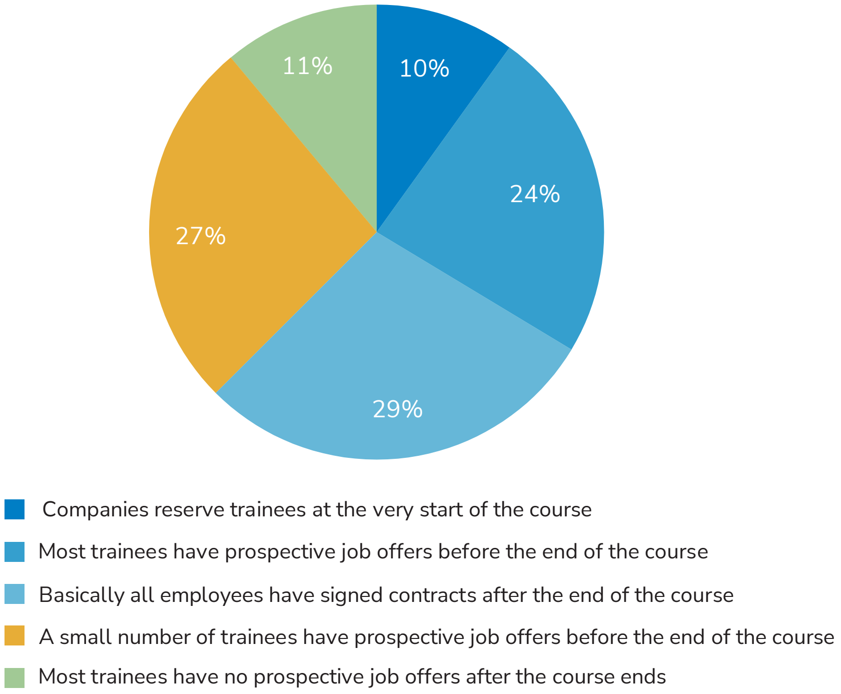


Figure 4-33 Employment Status of Cybersecurity Training Institute Trainees

In terms of the capabilities trainees hope to improve in the future, the mainstream opinion is that they should further improve learning in the directions of penetration testing, vulnerability mining, analysis, and exploitation, reverse analysis, web security, and virus and trojan analysis. In addition, some new cybersecurity directions that have emerged in recent years, such as cloud, 5G, AI, blockchain, and other security fields, have also become directions in which trainees plan to improve in the future.

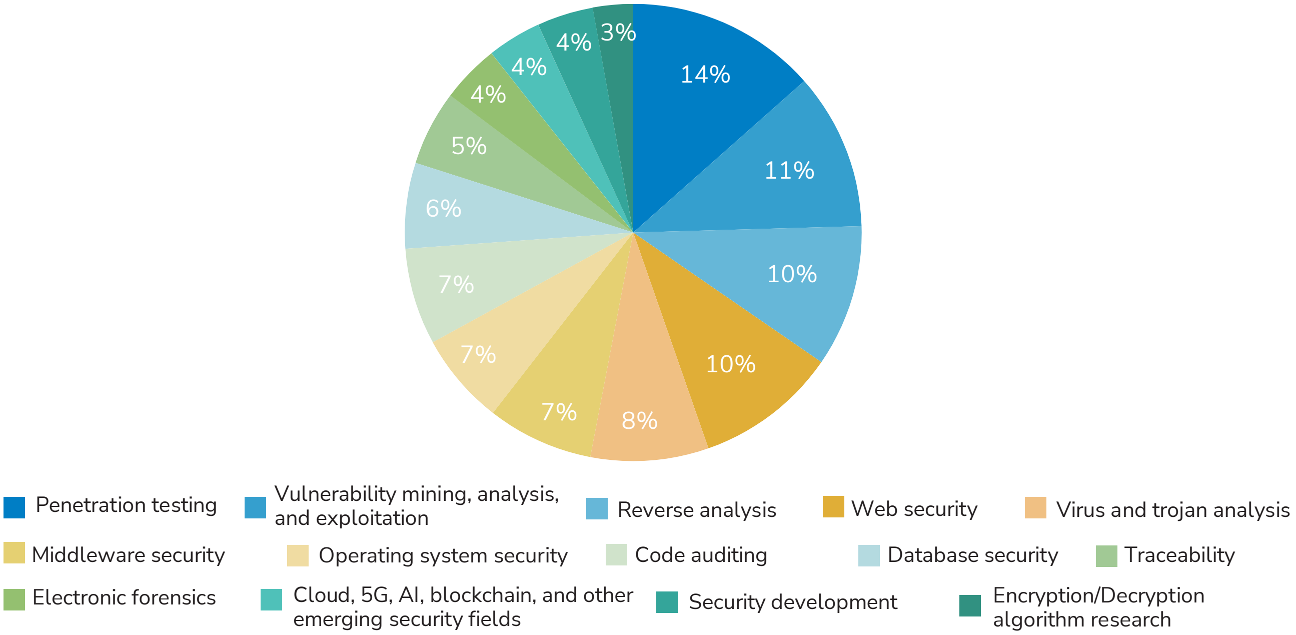


Figure 4-34 Capabilities Cybersecurity Training Institution Trainees Hope to Improve in the Future

4.3.3 Analysis of Corporate Training Results

Enterprises that adopt different training measures see corresponding differences in their training results. Among the measures, mentoring systems with experienced personnel guiding new personnel often produce the best training effect because mentors with rich work experience guide learning and teach knowledge. In addition, measures such as organizing online learning through customized training platforms, regularly inviting practical experts to give offline lectures, and participating in security competitions also have relatively good effects. Practitioners' beliefs concerning the most effective training measures for improving live-fire capabilities are shown in Figure 4-35.

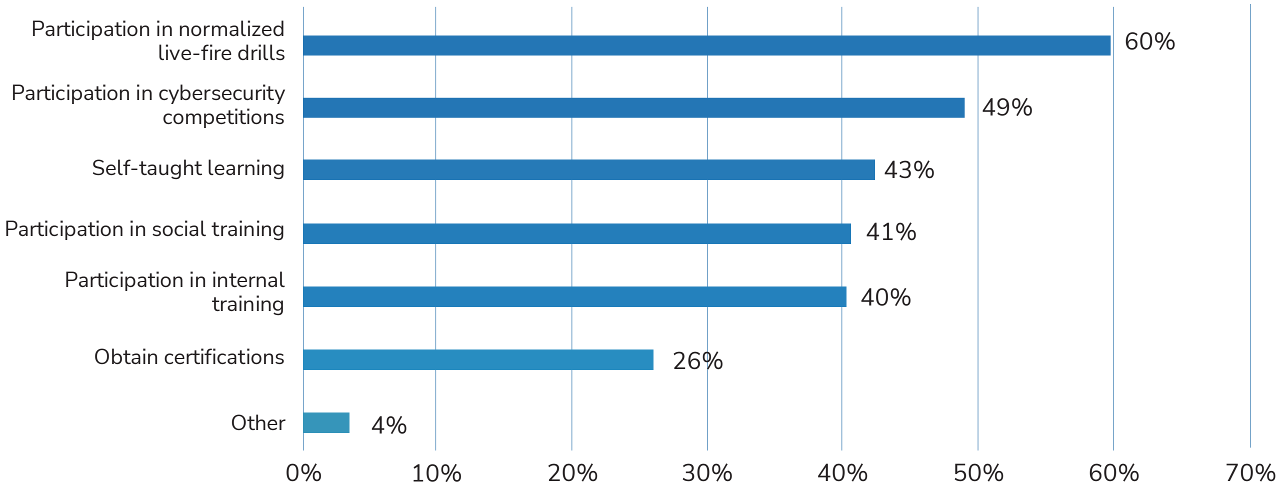


Figure 4-35 Most Effective Measures by Units to Improve Live-Fire capabilities

Chapter 5 | Analysis of the Evaluation of the Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

5.1 Current Situation of the Evaluation of the Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

The purpose of cybersecurity live-fire attack and defense capability evaluation is to judge whether practitioners meet the knowledge, technical, and capability requirements of cybersecurity professional technicians who independently engage in certain cybersecurity professional technical work.

5.1.1 Mainstream Evaluation Methods

At present, the main evaluation methods in China and abroad include job and occupation certifications, skill level (等级) certifications, (enterprise) product training certifications, and skill level points. The main cybersecurity-related skill certifications are provided by governments, universities (research institutions), industry associations, and major companies.

1. Position and Professional Certifications

These include the International Information System Security Certification Consortium (ISC2) Certified Information System Security Professional (CISSP) certification and Certified Cloud Security Professional (CCSP) certification; the Information Systems Audit and Control Association (ISACA) Certified Information Systems Auditor (CISA) certification; the China Information Technology Security Evaluation Center Certified Information Security Professional (CISP) certification; and the professional title evaluations for network information security engineering and technical personnel organized by local cyberspace administration offices and human resources and social security departments.

2. Skill Level Certifications

These include the Ministry of Public Security's Cybersecurity Skill Level Evaluator Certification (网络安全等级测评师认证), and the EC-Council's Certified Ethical Hacker (C|EH) certification and Certified Penetration Testing Professional (C|PENT) certification.

3. (Corporate) Product Training Certifications

Some typical certifications of this type are Cisco's Cisco Certified Network series of security certifications, the Information Security Certification Center of China (ISCCC) Certified Information Security Assurance Worker (CISAW) certification, Huawei's HCIE-Security certification, and H3C's H3CSE-Security certification.

4. Skill Level Evaluation

This is common in various security competitions and the white hat certifications of corporate security response centers (SRC).

In various security competitions, teams are often ranked and evaluated, generally being divided into first, second, and third prize or first, second, and third place. For example, the National College Student Information Security Contest and Innovation and Practical Ability Competition held by the Ministry of Education Steering Committee on Instruction for Higher Education Cybersecurity Majors selects the first, second, and third prizes based on the scores of the participating teams in the offline competitions. In the "Strong Net Cup" national cybersecurity challenge directed by the Office of the Central Cyberspace Affairs Commission, the top 32 teams in the online and offline competitions are awarded first, second, and third prizes. In the Wangding Cup cybersecurity competition held under the guidance of the Ministry of Public Security, first, second, and third prizes are selected based on the performance of the participating teams. In addition, the Golden Tripod, Silver Tripod, and Bronze Tripod are awarded to units based on the total points of their teams, and "Outstanding Cybersecurity Talent", "High-End Cybersecurity Talent", and other certifications are awarded to individuals.

Corporate SRCs generally perform level evaluations based on individual abilities. The Alibaba Security Response Center divides the white hats on the SRC platform into three levels: Young Hero (江湖少侠), Master (武林高手), and Grandmaster (一代宗师) according to the value contributed by "white hats" who submit valid vulnerabilities within a certain period of time (720 days). Platforms such as iSpring and Autumn and

Vulbox (漏洞盒子) rank white hats from low to high as follows: bronze, silver, gold, platinum, and diamond. In its *White Paper on China's Live-Fire White Hat Talent Capabilities* released in June 2021, Qi An Xin stated that its investigation showed 55.8% of white hats occupy job positions that do not require certifications (无证上岗).

5.1.2 Effective Evaluation Methods

The evaluation of live-fire attack and defense cyber capabilities is divided into two aspects: offense and defense. Generally speaking, offensive capabilities tend to be practical, while defensive talents tend to be primarily academic. Therefore, an effective evaluation method should reflect the combination of the academic and the practical. At present, in several national-level live-fire attack and defense combat competitions and typical attack and defense capability certifications in China, both academic and practical capabilities are considered.

For example, in the National College Student Information Security Contest and Innovation and Practical Ability Competition, the preliminary round adopts the form of online Q&A, including a knowledge Q&A stage and an on-site practice stage. The questions cover a variety of innovation and practical ability basic skills. The quarterfinals and semifinals adopt an AWD or AWD+attack and defense competition mode. The final adopts the format of an attack and defense competition based on a semi-open proposition. It has two stages: Build (innovative security application development) and Break & Fix (confrontation combining attack and defense). The Build stage has a weight of 15% and the Break & Fix stage has a weight of 85%. This format ensures a more comprehensive evaluation. The Strong Net Cup online competition adopts the online Q&A (Jeopardy) mode, and the offline competition adopts the attack-defense confrontation (KOH) + practical problem-solving (Realworld) mode. The Wangding Cup adopts a combination of capture the flag (CTF), attack and defense competition (AWD PLUS), cyber range competition (ISW), real-world defense (RDG), AI vulnerability mining (RHG), and other modes.

The National College Student Information Security Contest and Innovation and Practical Ability Competition held by the National Cybersecurity Teaching Steering Committee select the first, second, and third prizes based on the scores of the participating teams in the offline competitions. In the Wangding Cup cybersecurity competition held under the guidance of the Ministry of Public Security, the contestants are evaluated based on the capabilities of cybersecurity personnel according to their individual scores in the Wangding Cup and divided into three levels: beginner, intermediate, and advanced.

A typical attack and defense capabilities certification, the Certified Ethical Hacker (C|EH) certification of the EC-Council, evaluates an individual’s capabilities and is divided into two levels: C|EH certification and C|EH Master certification. The C|EH certification is a knowledge evaluation, and participants must take a 4-hour exam and complete a total of 125 multiple-choice questions. In addition to the C|EH certification requirements, the C|EH Master certification requires participants to complete a 3-hour practical challenge and solve 20 practical challenges similar to real-world scenarios in the iLabs cyber range.

5.1.3 Existing Problems

However, there are still some problems in the use of the attack and defense competitions and attack and defense certifications described above for evaluating the live-fire capabilities of cybersecurity talents.

On the one hand, neither has formed a standardized and generalizable evaluation system. On the other hand, each has its shortcomings in terms of grading and evaluation.

The common problem of attack and defense capability evaluations in various attack and defense security competitions is that the competitions provide relative evaluations. The evaluation is carried out by means of mutual comparison among evaluated individuals or teams, i.e., the level of participants determines the real worth of the competition results. In addition, most competitions only conduct team evaluations; few conduct individual evaluations.

We found that, in recent years, relevant departments have paid more attention to personal evaluation. For example, the "Wangding Cup" competition grants awards specifically for individuals.

In terms of attack and defense certification programs, the Certified Ethical Hacker (C|EH) certification assesses theoretical and practical skills completely independently, and cannot separately evaluate live-fire attack and defense capabilities. Other corporate certifications will combine assessments of theory and practice, but the inspection points generally focus on the company's products, developing functions for them, and product dependencies.

5.2 Evaluation Grading for Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

Based on an understanding and analysis of the live-fire attack and defense capabilities of cybersecurity talents and considering the long-term development needs of attack and defense cybersecurity talents, we propose a group evaluation system for the live-fire attack and defense capabilities of cybersecurity talents that combines knowledge evaluation and skill evaluation.

5.2.1 Capability Grading Description

The evaluation of the live-fire attack and defense capabilities of cybersecurity talents can divide talents into three levels, beginner, intermediate, and advanced, forming a tiered growth path from low to high.

Beginner personnel: Familiar with the basic concepts and processes of live-fire attack and defense cyber capabilities and able to apply them under the guidance of others, possess some independent work ability and practical experience, and are able to conduct security assessment and protection in routine and structured situations.

Intermediate personnel: Have a full understanding of the basic concepts and processes of live-fire attack and defense cyber capabilities, are able to independently complete more complex live-fire attack and defense tasks, possess the ability to guide the work of others, have some practical experience, and are able to conduct safety assessments and give conclusions and handling recommendations in unconventional and complex situations.

Advanced personnel: Have an in-depth understanding of advanced concepts and processes related to live-fire attack and defense capabilities and are able to apply them independently, are proficient in key specialized cyber attack and defense skills, are able to conduct security assessments for and successfully deal with unstructured and complex situations, have a wealth of practical experience, and can provide guidance and advice to others.

5.2.2 Capability Evaluation Content

The evaluation of the live-fire attack and defense capabilities of cybersecurity talents includes the aspects of knowledge and skills. The specific composition of the evaluation content for these two aspects is shown in the figure below.

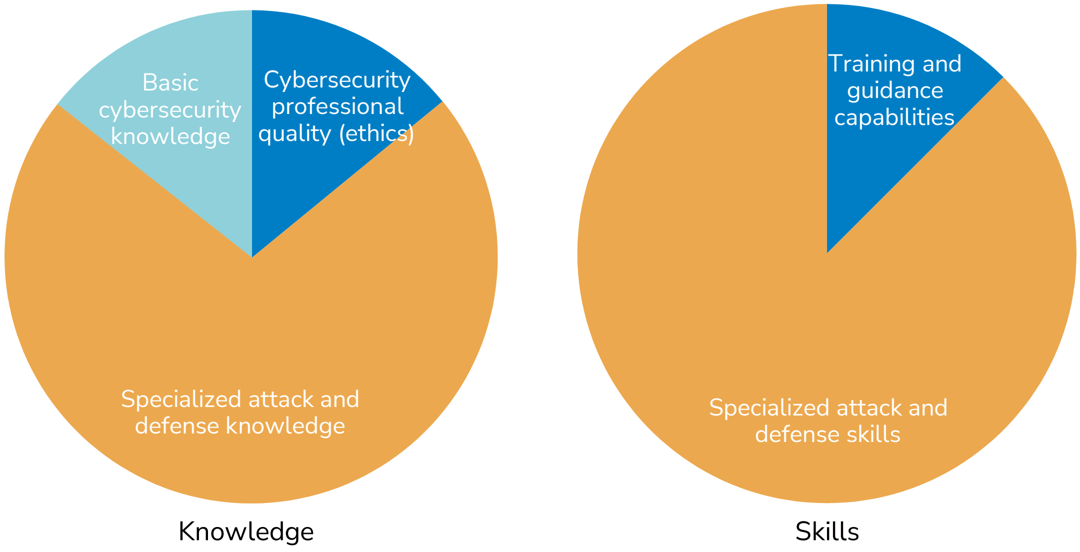


Figure 5-1 Composition of Live-Fire Attack and Defense Capability Evaluation Content

Knowledge evaluation involves three aspects: cybersecurity professional quality (ethics), basic cybersecurity knowledge, and specialized attack and defense knowledge. When evaluating the live-fire attack and defense capabilities of talents, we must pay attention to their professional quality. This is because cybersecurity talents have the responsibility to protect and create a good network ecosystem and promote the healthy development of the Internet industry. As live-fire attack and defense talents have certain destructive skills, they should consciously regulate their professional behavior, strengthen professional ethics, and strengthen legal awareness. The evaluation of knowledge is mainly conducted through written examinations or oral defense.

Skill evaluation involves two aspects: specialized attack and defense skills and training and guidance skills. The evaluation of skills is mainly conducted through live-fire practice, drills, or is based on corresponding certificates.

The core content of live-fire attack and defense capability evaluation is specialized attack and defense knowledge and skills, including the investigation of six aspects. Of these, cybersecurity monitoring and analysis and emergency response examine emergency response capabilities; vulnerability discovery and analysis and penetration testing examine cyberattack capabilities; and attack event research and evaluation and attack sampling and intelligence analysis investigate cyber defense capabilities.

1. Cybersecurity monitoring and analysis

Monitor and analyze security data such as device logs and network traffic as well as the security situation, detect threats, and issue alarms and responses.

2. Emergency response

Analyze information, information systems, information infrastructure, and networks, formulate emergency response plans for security incidents, analyze and handle sudden security incidents, and complete rapid emergency response.

3. Vulnerability discovery and analysis

Analyze information, information systems, information infrastructure, and networks, discover unknown vulnerabilities, evaluate existing vulnerabilities and security threats, assess risk levels, and formulate or recommend appropriate reinforcement measures.

4. Penetration testing

Conduct simulated penetration attacks on target information, information systems, information infrastructure, and networks to verify and test their security.

5. Attack event research and evaluation

During daily operations and attack and defense drills, research, evaluate, and analyze security events of various system applications, quickly and accurately confirm and determine the severity of events, locate problems, perform tracing analysis, and provide reliable containment and recovery solutions.

6. Attack sampling and intelligence analysis

Perform reverse analysis on attack samples and discover malicious attack programs and behaviors by analyzing program codes and process decompilation; collect cybersecurity threat intelligence, categorize and analyze the acquired intelligence data, and promptly discover network threats.

5.2.3 Evaluation Standards

Different requirements for knowledge and skills apply to cybersecurity talents at different levels. Beginner requirements focus more on knowledge understanding, while advanced requirements focus more on the application of skills. The weight table for the knowledge and skill evaluations for each level is shown in Table 5-1.

Table 5-1 Evaluation Weight

Level	Knowledge	Skills
Beginner	60%	40%
Intermediate	50%	50%
Advanced	30%	70%

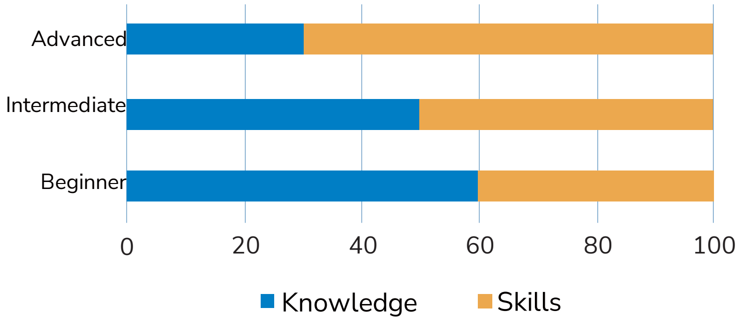


Figure 5-2 Evaluation Weighting for Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

Talents at different levels are required to have different levels of mastery of different knowledge and skills items.

In terms of knowledge evaluation, as the level of talents increases from low to high, the requirements for professional quality (ethics) are consistent, while the proportion of specialized knowledge requirements increases. Specifically, the weight of mastery of operational knowledge decreases and requirements for the mastery of analytical knowledge such as attack research and evaluation and sample analysis gradually increase, as shown in Table 5-2.

Table 5-2 Knowledge Requirement Weight Table

Item		Beginner	Intermediate	Advanced
Cybersecurity professional quality (ethics)		5	5	5
Basic cybersecurity knowledge		20	10	5
Specialized attack and defense knowledge	Cybersecurity monitoring and analysis	30	20	5
	Emergency response	15	15	20
	Vulnerability discovery and analysis		10	15
	Penetration testing	20	15	10
	Attack event research and evaluation	10	15	20
	Attack sampling and intelligence analysis		10	20
Total		100	100	100

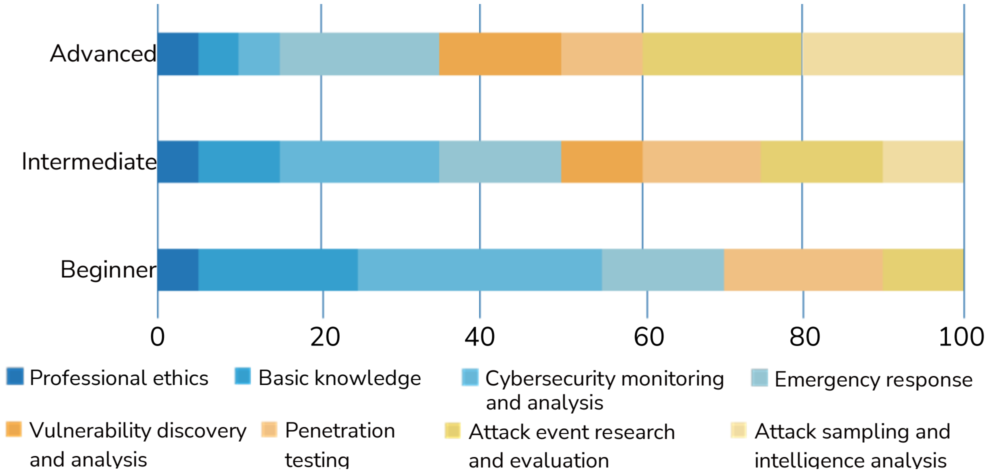


Figure 5-3 Knowledge Requirement Weight Diagram

In terms of skill evaluation, as the level of talents increases from low to high, in addition to the gradual increase in requirements for advanced live-fire attack and defense skills such as vulnerability analysis, attack research and evaluation, and sampling and intelligence analysis, intermediate and advanced personnel should also have corresponding abilities to train and guide others to carry out live-fire attack and defense operations, as shown in Table 5-3.

Table 5-3 Skills Requirement Weight Table

Item		Beginner	Intermediate	Advanced
Specialized attack and defense skills	Cybersecurity monitoring and analysis	40	20	10
	Emergency response	20	20	20
	Vulnerability discovery and analysis		10	16
	Penetration testing	25	20	8
	Attack research and evaluation	15	15	20
	Sampling and intelligence analysis		10	16
Training and guidance capabilities			5	10
Total		100	100	100

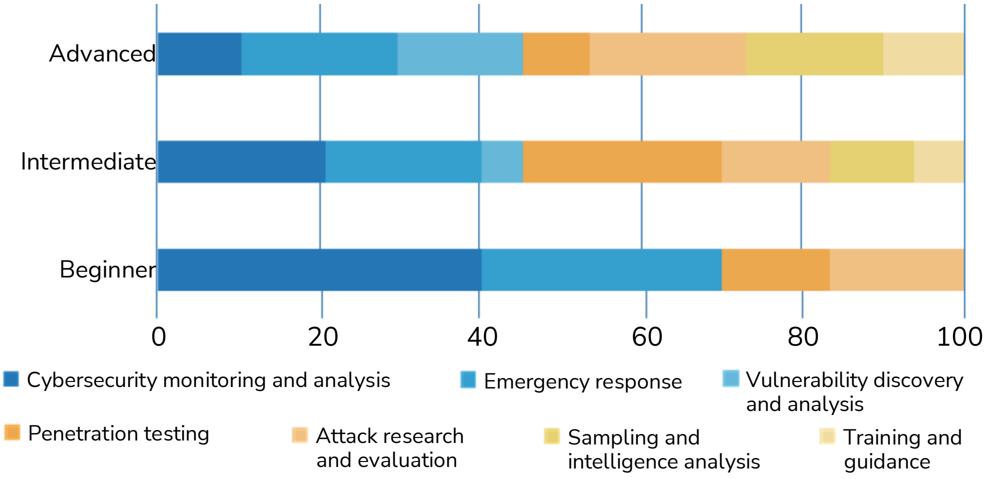


Figure 5-4 Skills Requirement Weight Diagram

5.3 Improvement and Evaluation Methods for the Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

Effective ways to improve the attack and defense capabilities of cybersecurity talents include: security competitions, professional training and certification, security conferences, crowdtesting projects, and attack and defense drills.

5.3.1 Cybersecurity Competitions

Security competitions are an important way to test and improve the live-fire capabilities of personnel. The original intentions of cybersecurity competitions are to "promote teaching, learning, and training through competition," discover one's own shortcomings in a real confrontation environment, mutually learn from each other's skills, and improve talents' attack and defense technical levels and teamwork capabilities.

Cybersecurity competitions originated with the bulletin board system (BBS) hacking competitions initiated by Jeff Moss, the founder of DEF CON, in 1993. Since then, with the extensive participation of all walks of life, various cybersecurity competitions have flourished. Currently, the main categories of cybersecurity competitions include: capture the flag (CTF) competitions, attack and defense competitions, cyber range competitions, vulnerability mining competitions, operations and maintenance competitions, forensic competitions, and policy competitions. At present, there are a large number of Chinese security competitions, which are suited for the initial learning and improvement of comprehensive security knowledge.

After about 20 years of development, there are now nearly a hundred high-level international security competitions each year. The security competitions organized by countries such as the United States, Germany, Russia, South Korea, and Japan have received global attention due to the high-level problems participants are asked to solve. Students who are interested in computers and cybersecurity and practitioners in the security industry enthusiastically participate in and praise them, and batches of security talents have matured in their fierce competition. As an effective way to discover and cultivate talents, various Chinese cybersecurity competitions have also flourished in recent years. There are also dozens of high-level national competitions every year. All major ministries and commissions have launched official competitions. Just in 2022, among the national-level competitions that have been held or will be held in various localities, there is the 6th Strong Net Cup national cybersecurity Challenge under the guidance of the Office of the Central Cyberspace Affairs Commission, the 3rd "Wangding Cup" cybersecurity competitions under the direct guidance of the Ministry of Public Security, the National University Student Information Security Competition and Innovation and Practical Ability Competition held by the Ministry of Education Steering Committee on Instruction for Higher Education Cybersecurity Majors, and other renowned event brands. These have all attracted the attention and participation of groups from all walks of life who are interested in or engaged in cybersecurity-related work. Through the large number of competition-based training events on campuses, many university students have greatly improved their practical skills related to cybersecurity and information security, such as website security penetration testing, binary vulnerability mining and exploitation, and cryptography.

The characteristics of a cybersecurity competition are: First, it simulates real scenarios, which can effectively improve the technical, communication, leadership, and coordination skills of the participants; second, the environment is secure and controllable and will not cause actual damage or loss.

Cybersecurity competitions have positive effects for everyone involved:

----For the government, cybersecurity competitions are a means to improve its ability to defend the country, industry, and citizens;

— For industry accreditation institutions, cybersecurity competitions are increasingly seen as relevant work experience required for accreditation maintenance;

— For professionals, cybersecurity competitions are a way to exercise and demonstrate professional skills, evaluate personnel capabilities, improve awareness and morale, and thereby improve productivity;

— For students, secondary schools and universities carry out competitions of various levels and use hands-on training courses to supplement teaching, which can enrich the ways in which students can learn;

— For the cybersecurity field as a whole, conducting cybersecurity competitions is conducive to promoting both attack and defense innovation at the technical and tactical levels and promoting the sharing of knowledge, technology, skills, and practices.

Cybersecurity competitions can also improve the skills of those who are not able to place (不能层次): students who have no foundation in cybersecurity and information security gain an understanding of the concepts of security attack and defense through competitions; students who have a preliminary foundation improve their live-fire capabilities through trying to solve high-quality competition problems; and students who have already learned a lot broaden their horizons through international competitions and competing against strong international teams.

In the long run, the specialized cybersecurity competitions will not only be of great help to the improvement of the attack and defense capabilities of cybersecurity talents, but also create a reserve of talents for cutting-edge research and promote the development of the security industry.

5.3.2 Security Conferences

Actively participating in various security conferences is also an effective way for cybersecurity talents to improve their live-fire attack and defense capabilities. When a cybersecurity conference is held, not only are the latest research results released, but technical exchanges with peers can take place, and some conferences also organize technical training related to the latest technology.

The Black Hat and DEF CON conferences held in Las Vegas every summer are grand events in the minds of professional researchers who do work related to cybersecurity. It is the dream of many security research teams to be able to attend the Black Hat conference or DEF CON conference as a speaker and present their latest research results in the field of cyber attack and defense. In recent years, Chinese security research teams from Shanghai Jiao Tong University, 360, Tencent, PanGu, etc. presented their findings from the podium of the Black Hat conference. In addition to inviting researchers to publish security vulnerability cracking and security technology research results, conferences also provide a venue to exchange and discuss attack and defense technologies and strategies and provide professional security training for participants. They are an excellent opportunity for cybersecurity talents to understand the trends in attack and defense technologies and improve their attack and defense capabilities.

5.3.3 Training Certifications

The training and certification activities offered by governments, universities and research institutions, professional organizations, and commercial institutions for the attack and defense capabilities of cybersecurity talents include: providing professional certifications for training courses, conferences, and product technology.

At present, highly authoritative and widely recognized international training and certifications related to cybersecurity attack and defense capabilities include:

1. National Centers of Academic Excellence in Cybersecurity (NCAE-C)

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) was launched by the U.S. National Security Agency (NSA) in conjunction with the U.S. Cybersecurity & Infrastructure Security Agency (CISA). This program aims to guide U.S. community colleges, colleges, universities, and other academic institutions to establish cybersecurity curricula and standards of academic excellence, organize cybersecurity practice activities, improve national cybersecurity education, and cultivate the next generation of cybersecurity experts.

This program is a certification of educational institutions' ability to cultivate cybersecurity talents, and it is divided into three certification types:

- CAE-CD, National Centers of Academic Excellence in Cyber Defense
- CAE-R, National Centers of Academic Excellence in Cyber Research
- CAE-CO, National Centers of Academic Excellence in Cyber Operations

At present, more than 300 colleges and universities in the United States have passed CAE-CD certification, 79 colleges and universities have passed CAE-R certification, and 22 colleges and universities have passed CAE-CO certification.

2. International Information System Security Certification Consortium (ISC2)

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)

3. Information Systems Audit and Control Association (ISACA)

- CISA (Certified Information Systems Auditor)

4. International Council of E-Commerce Consultants (EC-Council)

- Certified Ethical Hacker (C|EH)
- Certified Penetration Testing Professional (C|PENT)

5. Computing Technology Industry Association (CompTIA)

- CompTIA Security+

6. Cisco

- Cisco Certified Internetwork Expert (CCIE) – Security

Widely recognized Chinese training certifications related to cybersecurity attack and defense capabilities include:

1. China Information Technology Security Evaluation Center certifications

- Certified Information Security Professional (CISP)
- Certified Information Security Engineer (CISE)

2. Ministry of Public Security's Cybersecurity Skill Level Evaluator Certification
3. Huawei professional technical certifications for security engineers

- HCIA-Security (Engineer)
- HCIP-Security (Senior Engineer)
- HCIE-Security (Expert)

4. H3C's H3CSE-Security (Senior Security Technology Engineer) certification

5.3.4 Security Crowdtesting

Security crowdtesting is an emerging cybersecurity testing method, which relies on online workers to help complete testing tasks. It features low costs, good results, and fast speed. Cybersecurity crowdtesting is a new security service model that brings together security talents to conduct security testing on specific target systems through an Internet platform. It is a kind of directed, open, and authorized penetration testing. As a thriving application in the cybersecurity industry, cybersecurity crowdtesting is in high demand in many important industries and fields such as finance, communications, and industry.

In a cybersecurity crowdtesting task, the manufacturer or platform will test target assets and the corresponding rules (such as prohibiting DDoS attacks, prohibiting data modification, or prohibiting high-intensity scanning activity). For specific personnel and a specific time frame, they announce and set up corresponding awards and bonuses and openly recruit security personnel to conduct security testing on the targets and provide feedback on security vulnerability information. Incentives are given to security personnel based on the actual test results. This open security testing mode can effectively break through the limitations of limited testers and tools for security testing in a closed environment, significantly increasing the number and efficiency of testers. This allows organizations to maximize the effect of security testing given limited funds and time. Cybersecurity public testing follows the principles of openness, fairness, and impartiality. It is mainly applicable to the security testing of information systems that are open to public networks. It adopts preset testing objectives and rewards. The first participant to submit a vulnerability is rewarded, and the higher the vulnerability level, the higher the reward. The process of security testing to find vulnerabilities is also a competition that tests the speed and capabilities of the security personnel who undertake the test task.

In March 2016, the U.S. Department of Defense (DoD) announced that it invited 1,400 white hats to participate in the bug bounty program "Hack the Pentagon." This reflects the openness of the top U.S. defense agency to cybersecurity crowdtesting. In just one month from April 18, 2016 to May 12, 2016, a total of about 250 security personnel reported the vulnerabilities and risks of the Pentagon. In the end, 138 people were determined to be eligible for rewards and received prizes ranging from U.S. $100 to U.S. $15,000. According to statistics, the program paid as much as U.S. $75,000 in rewards. In this bug bounty program, the youngest reward recipient was just 14 years old. This shows that crowdtesting projects are an excellent opportunity for young cybersecurity enthusiasts to exercise their skills and make a name for themselves.

In China, crowdtesting platforms such as iSpring and Autumn, Butian (补天), and Vulbox as well as enterprise SRCs and other platforms have used online and offline activities such as contribution level tables, leaderboards, point rewards, various challenge activities, and technology sharing sessions to attract many young white hats. They have become platforms where cybersecurity talents can develop their talents and mature. In the white hat growth system of iSpring and Autumn, the white hats are divided into different levels, including (from low to high) bronze, silver, gold, platinum, diamond, and star.

5.3.5 Attack and Defense Drills

Cybersecurity attack and defense drills have the goal of obtaining administrator privileges for the specified target system. The attack team is composed of red team experts with a wealth of experience in the attack and defense field. Provided they do not compromise the stable operation of the business system, they can adopt attack methods employing any suitable attack paths and techniques in order to form an organized cyberattack operation. Attack and defense drills are generally controllable and auditable actual attacks on the target system of participating units in a real network environment. The drill is intended to test the security protection and emergency response capabilities of participating units and improve the comprehensive prevention and control capabilities of cybersecurity.

"Cyber Storm" is a national-level cybersecurity event held by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). It is the most extensive cybersecurity confrontation drill in the United States. Started in 2006, it is held every two years in the United States. The "Cyber Storm" drill brings together the government (federal and state governments), industry agencies, international partners, and private enterprises (such as critical infrastructure enterprises and high-tech enterprises). It is generally based on real events and simulates the response to a cyber crisis affecting the country's critical infrastructure. It strengthens U.S. cybersecurity readiness and emergency response capabilities in response to cyberattacks affecting multiple industries by conducting drills of the latest emergency response policies, processes, and procedures.

"Cyber Europe" is a Europe-wide cybersecurity attack and defense drill hosted by the European Union Agency for Cybersecurity (ENISA). Its participants are EU countries and various European Free Trade Agreement (EFTA) and EU agencies and departments. It is held every two years to test and cultivate the capacity of member states to work together to resolve cross-border cyber incidents. The just-concluded Cyber Europe 2022 involved a simulated attack on European healthcare infrastructure. Over 800 cybersecurity experts from 29 EU countries and European Free Trade Agreement (EFTA) and EU institutions participated in the drill.

Starting in 2016, China has emphasized cyber attack and defense drills and put actual operations on the agenda. In recent years, this has become normalized. Non-governmental organizations and major enterprises have also tried to carry out daily attack and defense drills, and the emergence and application of cyber range products have further promoted the development of attack drills.

The Network Protection Operation (护网行动) is a national cybersecurity attack and defense drill organized by the Ministry of Public Security held once a year. It is a live-ammunition (实枪式) attack and defense drill aimed at government agencies, enterprises, and public institutions in the cybersecurity field that is used to evaluate the cybersecurity activities of enterprises and public institutions. The main targets of the attack and defense drill include the key information infrastructure of important industries in the country, and its coverage of industries, work units, and systems is gradually expanding year by year. The Ministry of Public Security has the attacker launch a cyberattack on the defender within a specified period of time (usually a 2-week period) in order to detect the security vulnerabilities of the defender (drill target).

Through attack and defense drills in real network environments, it is possible to comprehensively evaluate the overall security protection capabilities of the network where the target is located, test the effectiveness of the defender's security monitoring, protection, and emergency response mechanisms and measures, and train the emergency response team to improve their ability to handle security incidents. Even more, drills exercise and quickly improve the attack and defense capabilities of cybersecurity personnel and help form a well-trained and experienced emergency response team.

5.4 Channels for the Improvement of Live-Fire Attack and Defense Capabilities of Cybersecurity Talents

Personnel training channels include college and university training, corporate training, institutional training, and individual independent study. How can we reasonably combine or connect these several methods to form an effective pathway for improving the live-fire attack and defense capabilities of cybersecurity talents and promote the continuous emergence of talents?

We recommend that we first establish a unified live-fire attack and defense cybersecurity capability framework to form a guide for talent training and further conduct certification and accreditation for courses and training related to live-fire attack and defense cybersecurity capabilities. At the same time, through the method of "competition-based selection, categorized improvement, and career guidance," the combination of competitions, crowdtesting, attack and defense drills, technology sharing, and other methods will form a normalized growth channel for attack and defense talents.

5.4.1 Unified Framework of Live-Fire Attack and Defense Cybersecurity Capabilities

We recommend referring to the "National Initiative of Cybersecurity Education (NICE)" in the United States. First, led by relevant national agencies, we should establish a unified and open "cybersecurity talent team framework" or "live-fire attack and defense cyberspace capability framework" (hereinafter referred to as the "capability framework"), which clarifies specific requirements for the live-fire attack and defense capabilities of cybersecurity talents. Under the guidance of this capability framework, all institutions, enterprises, and individual learners can find content suited to them that allows them to build or find a suitable orientation and development direction.

The National Initiative for Cybersecurity Education (NICE) is led by the National Institute of Standards and Technology (NIST) and under the joint leadership of the Department of Homeland Security (DHS), Department of Defense (DoD), Department of Education, National Science Foundation (NSF), Office of the Director of National Intelligence (ODNI), U.S. Office of Personnel Management (OPM), and other departments. The plan was launched in 2010, and the NICE Workforce Framework for Cybersecurity (NIST SP 800-181) (hereinafter referred to as the "NICE Framework") was officially released in 2017. The document proposes a categorization of cybersecurity talent roles and a framework of knowledge and competencies that can be used to assess the level of professionalization of the workforce, recommend best practices for anticipated future cybersecurity needs, and develop a national strategy for recruiting and retaining talent.

The NICE Framework analyzes the job descriptions of various organizations in the industry (including data from public sources and DoD and federal government internal data) and systemically organizes the work types, specialty areas, work roles, knowledge, skills, capabilities, and tasks in the security industry based on extensive and sufficient discussions within the industry. The framework uses Categories, Specialty Areas, and Work Roles to describe cybersecurity work. Each Work Role consists of a large number of independent Tasks and the corresponding knowledge, skills, and abilities (KSA), as shown in Figure 5-4.

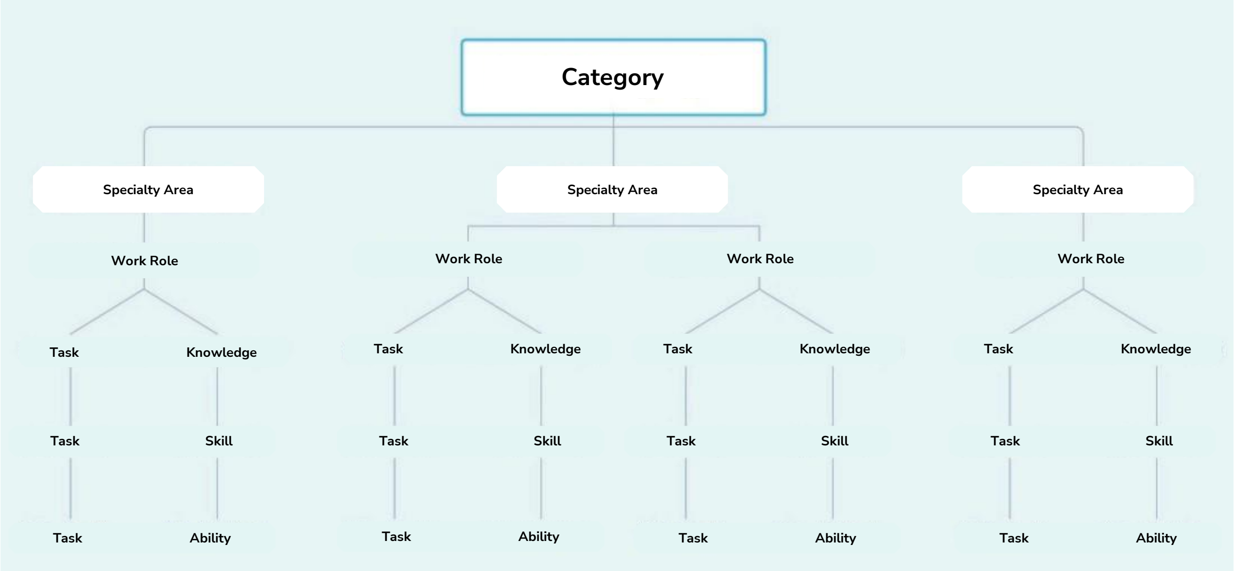


Figure 5-4 NICE Framework

It is undeniable that, as cybersecurity is a highly practical discipline, the evaluation of the live-fire attack and defense capabilities of personnel cannot be evaluated without the assessment of their basic knowledge, basic skills, and ability levels. In the face of an increasingly complex network environment, if we want to more effectively avoid various cybersecurity risks, in addition to the necessary protection based on knowledge and skills, personnel security awareness is the most fundamental requirement, but it is precisely the most likely to be ignored. It is also the thing most likely to reduce security risks at low cost.

When testing the "Abilities" of a Work Role in the NICE Framework, it is necessary to measure specific practices. At the same time, practices are also the best way to improve and test knowledge and skills, and they can directly measure the results of training. The prerequisite for learning knowledge and possessing skills is awareness. Awareness determines behavior. Only with proper awareness can we actively learn knowledge, actively improve skills, have the ability and willingness to participate in practice, and have greater motivation to understand industry norms and required capabilities. Here, the cybersecurity talent training model is divided into four dimensions: awareness, skills, knowledge, and practice. The sub-modules corresponding to each dimension are schematically shown in Figure 5-5.

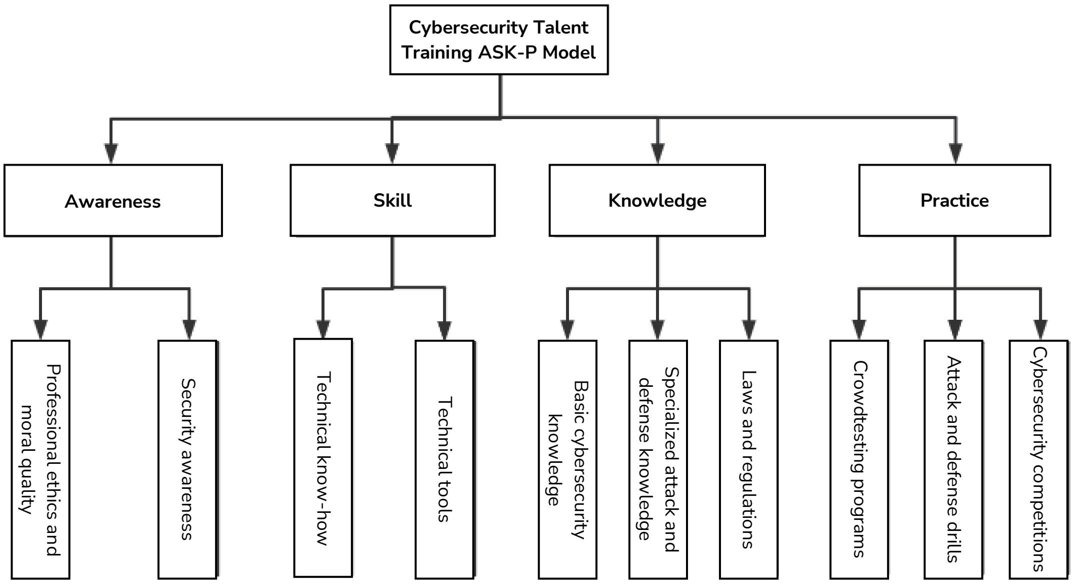

Cybersecurity Talent Training ASK-P Model
Awareness
Skill
Knowledge
Practice
Professional ethics and moral quality
Security awareness
Technical know-how
Technical tools
Basic cybersecurity knowledge
Specialized attack and defense knowledge
Laws and regulations
Crowdtesting programs
Attack and defense drills
Cybersecurity competitions

Figure 5-5ASK-P Framework

From the perspective of the model, K (knowledge) is the easiest to obtain, S (skill) requires continuous training, comprehensive P (practice) can only be obtained in actual engineering practice, and A (awareness) runs through the entire process.

Security Awareness System - Improve Security Awareness (A)

First, we must let cybersecurity practitioners establish a good professional quality, and starting from the level of awareness, recognize and attach value to cybersecurity-related jobs. The acquisition of security awareness is a matter of subjective thinking, which is used to assign value and influence behavior. It is individuals' perceptual awareness, prevention awareness, and behavioral awareness as regards cybersecurity risks during operations and activities in the use of network equipment and network systems. This all involves people's attitudes and emotions. The formation of security awareness must go through at least two stages of value judgment and emotional response. In addition to the behavioral factors that directly affect security, it also includes indirect factors such as morality, professionalism, and sense of responsibility for work. Therefore, security awareness training serves to let everyone realize "why we study security," understand the knowledge and skill requirements of this job, and appreciate the value of security awareness training and self-growth in terms of value judgment, so as to establish a good professional quality.

Security Skills System - Improve Application Skills (S)

Second, at security positions, personnel are required to have practical operation capabilities. No matter what position they occupy, they must be able to assume the responsibilities of the position and have the skills to handle the work of the position. On the premise of having a high degree of security awareness, we must strengthen skill training to meet the needs of projects and work. The acquisition of security skills is a matter of practical training. Through training methods such as cybersecurity skill improvement testing, professional training in simulated environments, and practical drills, the technical capabilities, practical skills, and collaboration and communication skills of personnel are improved. In this way, personnel can apply the skills they have learned.

Security Knowledge System - Master Professional Knowledge (K)

Third, we must develop a series of courses according to the knowledge systems required by the talent levels of cybersecurity positions. The knowledge domains can be divided into security knowledge, professional knowledge, expanded knowledge, and equipment and tool knowledge. We must ensure the professional knowledge of the positions and lay a theoretical foundation for the subsequent comprehensive practice. The acquisition of security knowledge is a matter of objective memory, and cybersecurity is an interdisciplinary subject. In addition to natural science knowledge such as mathematics, communications, and computer science, it also involves social science knowledge such as law and psychology. The study of cybersecurity knowledge involves the creation of a complex multi-field knowledge system. Knowledge can be systematically and actively learned, directly acquired from experience, or indirectly acquired through teaching by others. Brain studies in the field of cognitive psychology have found that knowledge is stored in the human brain in a tree-like structure. Therefore, people who want to master security knowledge must study and reflect on the knowledge.

Security Practice System - Conduct On-the-Job Practice (P)

Finally, through practical forms such as live-fire attack and defense drills and attack and defense competitions, we must conduct on-the-job practice to improve business capabilities. We must integrate knowledge and skills, comprehensively utilize various technical and non-technical means, dynamically improve engineering practice capabilities in live-fire attack and defense operations, tap into the potential of cutting-edge technologies, discover security risk trends, output accumulated knowledge content, and then form a virtuous cycle for a new round of training.

Cybersecurity is a practical discipline emphasizing live-fire capabilities. Especially in the face of the complex cyberspace environment of the "Internet of Everything," the cybersecurity threats we face may come from technological and non-technological attack methods, such as exploiting "computer vulnerabilities" to launch technological attacks and using "human brain vulnerabilities" to launch social engineering attacks. It is not possible to master security awareness, security knowledge, and security skills in isolation. Instead, we must integrate awareness, knowledge, and skills in order to possess comprehensive live-fire capabilities.

5.4.2 Accreditation for Live-Fire Attack and Defense Cybersecurity Capability Courses and Training

Training by colleges and universities, including general universities, higher vocational schools, and private colleges and universities, is the main way to cultivate talent in bulk. It is also an important guarantee for education that provides basic knowledge reserves and systematic theoretical support for talents. However, while the training system of colleges and universities is characterized by systematization, theorization, and academicization, it has deficiencies in pertinence, practicality, flexibility, and skills.

Corporate training is generally carried out with a focus on specific positions or tasks, which gives it high pertinence, practicality, flexibility, and an emphasis on practical skills. However, this training lacks systematic and theoretical guidance and is insufficient for long-term talent development.

In institutional society-oriented training,[14] the trainees often aim to obtain certificates or improve their ability in order to obtain employment. In terms of cybersecurity, especially in the field of cyber attack and defense, a steady stream of new technologies and methods are emerging, and they often form hot spots. Training institutions flock to these hot spots, resulting in an endless stream of training certifications, so it is difficult to judge the quality of these certifications.

We recommend forming a batch of certified (accredited) courses or certified (accredited) certificates among those offered by universities, enterprises, and training institutions on the basis of a unified "capability framework."

Colleges, enterprises, and training institutions that offer relevant courses and training programs can report to relevant institutions for approval if the content covers

[14] Translator’s note: “Institutional society-oriented training” (机构社会化培训) is probably a reference to privately operated classes, tutoring, cybersecurity bootcamps, and the like.

sufficient knowledge points and skill points in the "capability framework" (similar to degree certification).

According to the requirements of different fields and different specialties, [taking] courses that cover sufficient knowledge points and skill points to receive an accreditation certificate or pass accreditation is equivalent to obtaining a capabilities certification of the corresponding level. Corresponding courses and certificates can also become one of the bases for corporate recruitment.

5.4.3 Normalized Attack and Defense Talent Growth Channels

We recommend leaning from the model of the U.S. Cyber Challenge (USCC) and establishing a normalized training method of "competition-based selection, categorized improvement, and career guidance" to open up an attack and defense cyber talent growth channel linking colleges and universities and the actual needs of enterprises.

The U.S. Cyber Challenge (USCC) [https://www.uscyberchallenge.org/] is a national program supported by DHS that conducts competitions and on-site training for high school, college, and graduate students to identify and support talented young Americans so they can develop their skills, obtain high-level training, and be recognized for scholarships, internships, and jobs. It is an important program that allows the United States to select, attract, train, recruit, and absorb a new generation of cybersecurity-related professionals.

The USCC consists of two programs: the Cyber Quests competition and the Cyber Camp program.

Cyber Quests competitions are generally held 1-2 times a year, in spring and autumn. The competition is a set of online challenges that test basic information security knowledge and hands-on capabilities, including tasks from secure coding to network monitoring. Based on their performance in Cyber Quests, participants are invited to participate in one of the Cyber Camps organized by the USCC.

Cyber Camps are generally held in the summer and take place at universities or research institutions across the country. Each camp is a week-long offline workshop (online in 2022) that includes hands-on labs, hacker competitions, instruction on new concepts and security techniques from leading universities and top industry professionals, and mentoring in penetration testing, pseudo-packet (伪数据包) crafting, cyber warfare, and even career development paths.

1. Competition-based selection:

Competition-based selection can be done in a variety of ways, such as online CTF, crowdtesting, and vulnerability mining, or a combination of multiple tracks. The purpose is to give more independent participants a channel for further advancement. It should get them to realize that competitions are not a spectator sport with only a few players, but an admission ticket to a larger and broader growth space.

Following the example of DEF CON, we can set up some authorized wild card competitions (外卡赛), or the Chinese iSpring and Autumn Cup can use iSpring and Autumn points to evaluate personal capabilities for iSpring and Autumn certification. Personnel who obtain wildcards or sufficient points can apply for the next stage of training and improvement.

During the selection process, the following points should be noted:

- We must realize a correspondence between the competition-based selection of talents and the formulated "capability framework."
- We must pay attention to the standardization of evaluation and assessment across different competitions and for participating individuals and groups.
- We must set up different alliances for participants of different ages and different skill levels to form competition echelons.

2. Categorized improvement

Outstanding personnel from different tracks, different technical levels, and different age groups selected through competitions are assigned to enter the corresponding national training camps or seminars held every summer or to conduct concentrated training on different themes, with a focus on strengthening certain aspects and improving live-fire attack and defense capabilities.

3. Career guidance

During training, senior corporate personnel are selected and assigned to provide guidance to the trainees in terms of career development and growth paths. They can also guide cybersecurity personnel to enter the professional and career track early and devote themselves to cybersecurity work by recommending internships and practical projects.

By having events take place at a relatively fixed time each year and using the normalized "competition-based selection, categorized improvement, and career guidance" method, we can attract more and a wider range of students and people from society to devote themselves to cybersecurity work and focus on the improvement of attack and defense capabilities. In this way, the cultivation of cybersecurity talents in China will inevitably form a virtuous cycle.

For practitioners in various industries and fields, it is undoubtedly more important to improve the capabilities relevant to the practices of their job positions. They differ from the student population in this respect. The behavior of practitioners in spontaneously improving their personal capabilities and [their access to] the various capability improvement channels created or provided by their enterprise units represent the personal growth channels of the practitioner population. In a word, the training method centered on "practice-based selection, echelon construction (梯队建设), and value-oriented guidance (价值引领)" can not only promote the improvement of the overall capabilities of employees, but can also achieve the ultimate goal of the complementary and mutual success of both talent training and corporate development.

1. Practice-based selection

The biggest difference between practitioners and students in improving their personal capabilities lies in their positions and responsibilities, which are also a type of practical experience. By organizing a series of practical activities such as attack and defense drills and competitions, enterprises conduct normalized personnel inspection and training. This not only allows them to discover and deal with security risks in a timely manner and effectively test their overall cybersecurity protection level and emergency response capabilities, but also allows them to train their teams and select talents. In addition, as corporate employees, by actively participating in internal and external security competitions, attack and defense drills, and even crowdtesting and other practical activities, while improving their practical capabilities, their achievements can also be used as a basis for effective selection [for promotion or raises] and as evidence of their own capabilities and value.

2. Echelon construction

We must grade and categorize cybersecurity practitioners in different departments, positions, and directions through various practice-based methods, build a multi-level specialized cybersecurity personnel echelon, and carry out professional matching between personnel and work positions according to practical experience and skills. According to their own career development, employees can clarify their growth paths and carry out targeted capability improvement.

3. Value-oriented guidance

On the one hand, enterprises acknowledge the honors employees have gained in practice and show their recognition through direct and effective means such as promotions and raises. On the other hand, various localities and organizations have successively issued benefits policies for cybersecurity technical talents, which have greatly increased the enthusiasm of employees. For the practitioners themselves, actions such as independent learning and improvement based on the company's rigid regulations and requirements or efforts based on future development and planning can all be regarded as examples of value-oriented guidance on the path of personal growth. At the micro level, the different wants and values that drive each employee are reflected at the macro level. After the results produced are all coordinated and balanced in combination with knowledge, skills, and on-the-job experience, there is a positive interaction between the improvement of personal capabilities and the steady development of the corporation.

Chapter 6 | Summary and Recommendations

6.1 Recommendations for the Construction of College and University Talent Training Systems

6.1.1 Theoretical Teaching System Construction

The discipline of cybersecurity is a discipline with a high degree of practicality. It is oriented towards the cultivation of the live-fire capabilities of cybersecurity talents. The talent training systems of colleges and universities should offer targeted practical courses, and at the same time provide courses and training related to live-fire attack and defense operations. They should have higher requirements for the depth and systematic nature of the course content and cultivate students' ability to combine theory with practical applications to comprehensively analyze problems, explore cutting-edge technologies, understand attack and defense game ideas, and comprehensively build a knowledge system, so as to improve students' practical cybersecurity capabilities.

Corporate lecturers should be stationed in theoretical and practical classrooms to bring students the latest and real-time content from enterprises at the front lines. We should encourage enterprises to deeply participate in the training of cybersecurity talents in colleges and universities and strengthen cooperation with colleges and universities in various areas, such as training objectives, curriculum setting, teaching material preparation, laboratory construction, practical teaching, topic-based research, and joint training bases.

According to the teaching syllabi and plans formulated by schools, enterprises should cooperate with teachers to prepare teaching materials and design supporting practical teaching content so that theoretical teaching and practical needs can be more closely combined. Taking knowledge point requirements and application as the main line, they should systematically introduce various technical fields via a classic + cutting-edge method, ensure the integrity and cutting-edge nature of the teaching materials, simultaneously carry out the construction of experimental resources and interactive teaching platforms, and improve the quality of course construction.

6.1.2 Practical Teaching System Construction

The live-fire capabilities of cybersecurity talents still do not match the needs of industry enterprises, and their ability to solve practical problems is still insufficient. It is necessary to promote school-enterprise cooperation, participate in the construction of cybersecurity courses, establish off-campus practice and training bases, and organically combine actual practical needs with course learning. Through various methods such as teachers and students going to enterprises and enterprises coming to campus, schools and enterprises should jointly cultivate high-level practical cybersecurity talents that meet the needs of enterprises.

They should establish joint innovation R&D institutions to speed up the practical application of industrial technology and share the results of technological R&D. Schools and enterprises should extensively carry out project-based cooperation and carry out construction cooperation projects. They should carry out extensive and in-depth collaborative education projects, set up high-quality joint innovation R&D laboratories, establish school-enterprise collaborative innovation centers, and accelerate the industrialization of scientific research results through collaborative innovation in order to assist the high-quality development of related industries.

Schools should cooperate with cybersecurity enterprises to carry out various forms of school-enterprise cooperation, guide enterprises in the industry to join the innovation and entrepreneurship talent training system, and strengthen cooperation with colleges and universities in various areas, such as training objectives, curriculum setting, teaching material preparation, laboratory construction, practical teaching, topic-based research, and joint training bases. They should actively explore cooperation modes between students and the scientific research teams of colleges and universities, to allow students to experience the work of actual scientific research teams in the process of scientific research and truly participate in actual scientific research activities, enrich students' own cybersecurity skills, and comprehensively improve cybersecurity projects and live-fire attack and defense capabilities in the process.

We should promote the integration of science and education, which not only includes the combination of institutions of higher learning and scientific research institutes, but also the integration of the scientific research activities and teaching activities within schools. We should realize the organic integration of scientific research and education, promote the close integration of the whole process of scientific and technological (S&T) innovation and the whole process of personnel training, make converting scientific research and innovation achievements into practical applications part of course content, transform scientific research projects into student project practice cases, and transform first-class scientific research platforms and scientific research facilities into learning platforms and practice environments for students.

We should promote industry-academia integration, which not only gives full play to the main role of enterprises in engineering practice, but also closely aligns with the needs of society for talents. We should deepen industry-academia integration, implement school-enterprise cooperation, reform the talent training model, innovate assessment mechanisms, innovate cooperation models, summarize the problems and deficiencies in the implementation process, and further innovate and improve the quality of professional talent training as the core of the "integrated industry-academia-research institute" task-based-teaching talent training model as well as the teaching model that uses real enterprise projects as tasks, and combine and fuse teaching, learning, production, innovation and other stages in the teaching process. This is a better way to improve students' learning results, actual hands-on capabilities, and professional quality. In addition, it is more conducive to cultivating students' innovative practical capabilities and comprehensive application capabilities.

6.2 Recommendations for the Construction of Corporate Talent Training Systems

Corporate talent training construction includes personnel training, competitions and drills, advanced studies at colleges and universities, and joint training with colleges and universities. It is necessary to continuously implement and organically combine these methods to form a path for improving the live-fire attack and defense capabilities of corporate cybersecurity talents and to promote the cultivation, growth, and emergence of cybersecurity talents.

Enterprises should strengthen personnel training and cultivation and regularly hold special training lectures on topics such as live-fire attack and defense cybersecurity operations, and cybersecurity management. After completing training, personnel can be assessed on their cybersecurity knowledge to strengthen the cybersecurity awareness of enterprise personnel. Through training, education, assessment, and many other measures, enterprises can give enterprise cybersecurity personnel the capabilities to deal with cybersecurity risks. During training, senior cybersecurity personnel are selected and assigned to provide guidance to trainees in terms of career development and growth, forming a virtuous cycle for the cultivation of the enterprise's cybersecurity talent.

Enterprises should carry out cybersecurity attack and defense competitive drill exercises and competitions, organize employees to participate in national cybersecurity competitions, evaluate the cybersecurity level of corporate employees in practical operations, discover, test, and train cybersecurity talents in practical operations, and improve the live-fire cybersecurity capabilities and level of corporate employees.

We should support colleges and universities in their recruitment of high-end talents in the field of cybersecurity from enterprises and support talents in the field of cybersecurity who go to colleges and universities for further training. In this way, the combination of theory and practice can improve the knowledge structure of enterprise cybersecurity talents participating in the training and further enhance their live-fire attack and defense cyberspace capabilities.

We should encourage enterprises to participate in the training of cybersecurity talents in colleges and universities. Schools and enterprises should work together to set up talent training programs, build a multi-level talent system of "elite talent recruitment + basic talent cultivation + practical talent training," and create healthy and sustainable cybersecurity talent echelon construction. We should encourage corporate employees to participate in the training of talents in colleges and universities, coordinate the allocation of their superior resources, actively improve the layout of the cybersecurity academic discipline, train special talents for different positions, cultivate "academic-oriented + application-oriented hybrid talents, promote the formation of a talent cultivation model that is oriented to industry needs and based on job capabilities, and accelerate the cultivation of high-level, multidisciplinary, innovative, and practical talents and teams.

Building teams of "doubly qualified teachers" (双师型) who combine rich industry and enterprise experience with teaching experience is an extremely important measure for improving the level of cooperation between schools and enterprises. According to the needs of enterprises, we should implement joint on-campus + in-enterprise training; enterprise mentors and case-plus-practice sharing; establish a dual-mentor system between enterprises and schools, highlight the practicality and effectiveness of talent training, and cultivate hybrid talents.

6.3 Government Support Policy Recommendations

In the cybersecurity talent training system, government support policies should play an important role. Governments at all levels need to actively participate in providing guidance. As an external force, the government has gradually shifted its focus to constructing norms for overall school-enterprise cooperation and promoting the formulation and construction of laws, standard frameworks, and industry-university platforms and alliances. As the external support and guarantee [that compensates] for the limitations of schools and enterprises, it is also an adaptive environment necessary for the orderly operation of the entire cooperation process and the promotion of the internal motivation of both parties. In terms of policy, the government should formulate more favorable policies and systems, such as for scientific planning, atmosphere creation, entrepreneurship encouragement, and simplification of company registration procedures, hold some activities to promote alliances between enterprises and schools, and channel public opinion.

We recommend that the government greatly increase financial investment in vocational education and support colleges and universities as they improve conditions in an orderly manner and adapt to the needs of industrial development and market employment. The government should guide, encourage, and support enterprises in participating in university education. The key here is to issue relevant policies and regulations to increase the initiative and enthusiasm of enterprises to participate. From the perspective of local economic and social development, governments at all levels should plan the development of vocational schools and enterprises, coordinate school-enterprise cooperation, use school-enterprise cooperation tasks as an important means of promoting regional economic development, and establish a new school-enterprise cooperation development mechanism led by the government, with vocational schools and enterprises as the main entities, and industry associations as the intermediaries.

For school-enterprise cooperation, only with the overall planning and support of the government can departments, enterprises, and schools establish effective cooperation models and mechanisms for school-enterprise cooperation. Only in this way can school-enterprise cooperation be truly realized and achieve its mutually beneficial goals. From the perspective of local economic and social development, governments at all levels should plan the development of vocational schools and enterprises, coordinate school-enterprise cooperation, use school-enterprise cooperation tasks as an important means of promoting regional economic development, and establish a new school-enterprise cooperation development mechanism led by the government, with vocational schools and enterprises as the main entities, and industry associations as the intermediaries. We should adhere to the reform directions of industry-education integration, education-industry cooperation, school-enterprise integration, and work-study integration and increase the ability of vocational education to serve regional economic development and improve the people's livelihoods.