DOI 10.15302/J-SSCAE-2016.06.010

Cyberspace Security Competition and Talent Management

Yu Xiangzhan[1], Zhang Hongli[1], Yu Haining[1], Tian Zhihong[2], Zhai Jianhong[1], Pan Zhuting[3]

1. School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China
2. Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, Sichuan, China
3. Beijing Venus Technology Co. Ltd., Beijing 100193, China

Abstract: Competition between talented people, who are commonly referred to as talents, is fundamental to international cyberspace security, and the discovery and tracking of talents is one of its key links. First, the authors investigate the development status of domestic and international cyberspace security competitions. Next, the authors analyze the main problems of cyberspace security competition in discovering and tracking talents. Finally, they propose a long-term policy to discover and track talents based on cyberspace competitions.
Keywords: cyberspace security; competition; talent-discovery; talent-track

1 Introduction

Competition between talented people, who are commonly referred to as talents, is fundamental to international cyberspace security. At the first meeting of China's Office of the Central Leading Group of Cyberspace Affairs, Xi Jinping, General Secretary of the Central Committee of the Communist Party of China, emphasized that China should converge talents in order to build a powerful team which is politically strong, professionally proficient, and excellent in style of work, to build China into a strong cyber power. It is easy to gain a thousand soldiers, but difficult to obtain a general. Therefore, China should cultivate world-class scientists, leading talents in network science and technology, outstanding engineers, and a high-level innovation team. At a symposium on cybersecurity and informatization on April 19, 2016, General Secretary Xi Jinping stated that China should gather global talents to provide strong support for the development of cyberspace security.

Hosting a cyberspace security competition is one of the most effective ways to find talents in offensive and defensive cyberspace, as it provides these talents with a platform to demonstrate their skills. The selected talents are very likely to become leaders in the field of cyberspace security, and may even become the hard core in the field of cyberspace security. Using a competition to find offensive and defensive talents and to guide the direction of their lives as soon as possible can transform these people into reserved talents of the China's cyberspace security team, and can play a more important part in the construction of China's cyberspace security.

2 The development status of cyberspace security competitions at home and abroad

2.1 Capture the Flag competitions

A Capture the Flag (CTF) cyberspace security competition is a fair information security technology competition based on proposition, and it models the comprehensive application of cyberspace security technology. A CTF competition usually includes following three main competition modes: ① Jeopardy. In this competition mode, participants can join in online or offline. Jeopardy is ranked based on the time taken and the score achieved for solved problems, and is often used in online

Received date: 10 October 2016; **revised date:** 18 October 2016
Corresponding author: Yu Xiangzhan, School of Computer Science and Technology, Harbin Institute of Technology, Professor. Major research field is network and information security. E-mail: yxz@hit.edu.cn
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 049–052
Cited item: Yu Xiangzhan et al. Cyberspace Security Competition and Talent Management. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.010

competitions. Major topics include reverse, vulnerability mining and utilization, web penetration, passwords, forensics, steganography, safety programming, and other categories. ② Attack/Defense. In this competition mode, participants perform defensive and offensive maneuvers in cyberspace. Participants score by mining vulnerabilities and attacking opponents' servers, and avoid losing points by repairing their own vulnerabilities. This model is a fierce cyberspace security competition with strong ornamental value and high transparency. ③ Mix. This mode combines jeopardy and attack/defense. For example, participants might get some initial points by solving problems, and then add to their score by attacking or defending, thus winning the game with a higher final score.

At present, famous international CTF events include the following: ① DEFCON CTF, which is based on the DEFCON hacker conference, is the "world cup" of CTF events. ② UCSB iCTF is referred to an international CTF hosted by University of California Santa Barbara (UCSB) and it challenges universities from all over the world. ③ The Plaid CTF is an online problem-solving game that is hosted by the Carnegie Mellon University (CMU)'s hacking team, Plaid Parliament of Pwning (PPP). ④ The Boston Key Party is an online competition that has become popular in recent years. ⑤ XXC3 CTF is Europe's oldest CTF, and it is hosted by the Europe's largest association of hackers, Chaos Computer Club (CCC). ⑥ RuCTF is developed by Russian HackerDom team of Ural Federal University and is a competition to determine the Russian national team. ⑦ RuCTFE is an online offensive and defensive contest hosted by the Russian HackerDom team of Ural Federal University for global teams. ⑧ CODEGATE CTF is the "Grand Prix" of Seoul, South Korea, with a first prize of 30 million Korean Won.

2.2 Crack competitions

Crack competitions are mainly sponsored by enterprises. In these competitions, the enterprise provides a product that has been or will be sold commercially, and encourages the participants to mine vulnerabilities in the online product, and crack it. Famous games and related breach competitions include the following: ① Pwn2Own is the most famous hacking contest and has the highest bonus in the world; it is sponsored by the Pentagon network security service provider, Hewlett Packard (HP)'s TippingPoint Zero Day Initiative (ZDI). Google, Microsoft, Apple, Adobe, and other Internet software giants also support the game in order to improve their own products by this hacking challenge. ② GeekPwn is an international security community focusing in smart life. Created to incorporate the advantages of domestic and overseas security competitions, it innovated and designed the first Internet security "geek carnival" competition platform based on combining intelligent hardware and software. GeekPwn hosts a security carnival (the GeekPwn Carnival) and a security meeting every year. ③ Black Hat is a strong technical information security conference that leads in safety ideas and technology direction. Participants include researchers from various enterprises and governments, as well as some individuals. The agenda includes speeches of all kinds from professionals in the field, and covers topics such as global information security. In addition, the conference demonstrates a large number of vulnerabilities that have been found in digital products, and demonstrates how to attack them.

2.3 Youth cyberspace security competitions

The US National Security Agency and Carnegie Mellon University jointly hold a high school hacking contest that aims to explore and develop the next generation of cyberspace security talents. Youths can participate as individuals or in groups. The organizers claim that participants do not have to be hackers; youths can learn how to identify security vulnerabilities, and then launch attacks in the real world. In addition, the US holds a high school students' network attack competition named the Virginia Governor's Cup Cyber Challenge in order to help the Department of Homeland Security discover cyberspace security talents. The SiBears team from the Russian information security research organization has run a CTF competition for young students since 2010. Unlike other international CTF problem-solving events, this competition focuses on mining teenagers' fundamental knowledge and creativity in cyberspace security, and pays little attention to the level of cyberspace security knowledge and technology. Other countries, particularly Japan and South Korea, run a large number of smaller defense games and creative security games for youth.

In order to discover cyberspace security talents, various universities and social organizations here in China carry out cyberspace security competitions on various levels. These include the Strong Network Cup by the Cyber Security Association of China (CSAC), XDCTF by Xidian University, AliCTF by Alibaba, the Baidu Cup by Baidu, and more. In recent years, most well-known international cyberspace security competitions have been held in China. For example, the GeekPwn Carnival and the GeekPwn security meeting have been held in China. In addition, China's cyberspace security talents have begun to emerge in well-known international hacking contests; examples include blue-lotus team from Tsinghua University (THU), 0ops team from Shanghai Jiao Tong University (SJTU), six stars team from Fudan University (FU), and so on.

3 Main issues regarding talent management and cyberspace security competitions in China

After years of development, China's cyberspace security competitions have begun to take shape, and their effect is gradually being reflected in cybersecurity talent development. On the whole, China's leading role in cyberspace security competitions

for the discovery and tracking of talents requires strengthening. Related issues include the following:

(1) Without the establishment of a long-term mechanism to discover and track talents in cyberspace security using cyberspace security competitions, it is difficult for emerging talents to use their skills and make the best use of their abilities. China has not yet established such a mechanism, and as a result, information on the development direction of many people with natural talent is not being collected or recorded in an effective manner, leading to an inevitable loss of talents. In addition, talents in cyberspace security who are already working within enterprises have few opportunities to become well known, making it difficult for China to make use of their skills.

(2) China lacks cyberspace security competitions for teenagers, making it difficult to discover teenage cyberspace security talents. At present, most of the participants in cyberspace security competitions are college students or technicians from enterprises. Generally speaking, the difficulty, scope of knowledge, and focus of these competitions are not suitable for young people, who may have little experience and who are not yet fully mature. Although it is easy to engage youths' enthusiasm in cyberspace security technology, China does not yet have a means of doing so. The youth cyberspace security knowledge contests and the annual information competition of National Olympiad in Informatics (NOI) held in China both lack elements of actual antagonism in cyberspace security. China currently needs an interest-driven, practice-focused, high-quality cyberspace security competitive platform where teenagers can compete, demonstrate their cyberspace security skills, and enjoy themselves.

4 Policies and suggestions for discovering and tracking talents using cyberspace security competitions

It is proposed to establish a long-term mechanism for the discovery and tracking of cyberspace security talents using cyberspace security competitions. This would include hosting cyberspace security competitions that are supported by CSAC in order to discover talents and establish a record-keeping mechanism for cyberspace security. By discovering talents through such competitions, CSAC would be able to build a solid mechanism that could communicate with universities and enterprises, and establish a China's database of cyberspace security talents by recording competition participants and results in order to track talents in real-time and prevent their loss. In addition, this mechanism is conducive to discovering and then sending talents to the Cyberspace Administration of China (CAC) or to other major departments. China should host a national youth cyberspace security league in order to select teenage cyberspace professionals-to-be. China should establish a grading system for the competitions, and increase the competition awards in order to help grow these teenage talents. China should also establish a cyberspace security youth development fund in order to discover and support young talents. A suggested plan of action is described below.

(1) Hold a yearly cyberspace security competition in order to discover cyberspace security talents, and establish a record-keeping mechanism for cyberspace security competitions. CSAC should propose China's institutions to host cyberspace security competitions targeted especially at teenagers. In addition, CSAC should invite famous international cyberspace security competitions into China to help China discover talents. A record-keeping mechanism for cyberspace security competitions should be established, predominantly by CSAC. All cyberspace security competitions held in China or by China's agencies will submit their record-keeping information—including the competition theme and content, participants' information, and prizewinners' information—to CSAC, giving it a complete grasp of the basic situation regarding cyberspace security talents in China. It benefits China to manage the advantage gained from talents.

(2) Establish a solid talent communication mechanism with universities and enterprises, based on discovering talents through competitions. This mechanism should be established by CSAC. Finding talents through competitions, and building a solid talent communication mechanism that includes professional cyberspace security teachers at universities as well as employment guidance centers, can provide a steady stream of information about talents, particularly about students who take part in international cyberspace security competitions that are hosted overseas. In addition, as CSAC should discover talents through competitions and set up a communication mechanism with enterprises, it can discover cyberspace security talents from enterprises. Such talents can be useful to China through flexible cooperation with enterprises.

(3) Set up a database of cyberspace security talents that carries competition records and other information about talents in order to track talents in real time and prevent their loss. This talent database, established by CSAC, should collect and summarize competition participants' and prizewinners' information and record the skills, natural property, and social property of its members in detail through competition records and the talent communication mechanism, which will become a call-back mechanism to ensure that the talent database is complete and correct and track the direction of the talents' development in order to keep the talent database up to date. This cyberspace security talent database will be a source for team-building, undertaking tasks, and selecting talents to play specific roles in the CAC and other major departments.

(4) Hold a national youth cyberspace security league in order to select young talents in cyberspace security. CSAC should create a cyberspace security league system for China's teenagers, making it interest-driven, high quality, and with a focus on fairness and practical application. These competitions will collect teenage talents in cyberspace security in order to help build China's cyberspace security talent team. Compared with

international hacking competitions, these competitions will differ in their competition style, key points of competition, participants, the difficulty of questions, and scope of knowledge. Participants will be mainly aged 12 to 19. The difficulty of questions will be lower than in international CTF competitions, and will be suitable for teenagers—especially the preliminary contest. One or two testing points should be set in a single-field question, but more than three cycle testing points may be too difficult for the participants to overcome in order to pass the competition.

(5) Create an approved competition grading mechanism, and increase competition awards to assist the growth of teenage talents. Along with other relevant departments, CSAC should create an approved competition grading mechanism. Participants who achieve a prize in a high-level international hacking competition or in a teenager cyberspace security competition will be granted a grade to prove that they have gained a high level of ability in cyberspace security. This grade can be an evaluation index of a talent's chance for further study. In addition, increasing the cyberspace security competition fund will provide teenager-focused development funds, along with any competition funds provided by supporting enterprises, and will benefit teenage talents' further development. For example, a middle school or primary school could enroll excellent talents as special student talents in cyberspace security; colleges that have a cyberspace security major could directly recruit excellent talents; independent college recruitment could increase the final points for the talents. The establishment and enhancement of a grading mechanism can prevent the loss of teenage talents, while providing them with a wider environment to help them develop.

(6) Establish a cyberspace security youth development fund in order to discover and support young talents in cyberspace security. CSAC should create a cyberspace security youth development fund and normalize measures to develop fund management. Developing this fund will ensure the policy of discovering and supporting teenage talents in cyberspace security, help build a better environment for talents to mature in, and establish a long-term mechanism for discovering and supporting teenage talents. Specific tasks of this foundation will include: carrying out a cyberspace security education plan in middle and primary school, hosting cyberspace security competitions for teenagers, training teenagers in hacking, and funding teenage talents in cyberspace security. The main sources of this development fund will be the government, enterprises, and common people. It will be supervised by the local government. The use of the fund, its execution, and its effect should be reported every year.

5 Conclusions

China can discover cyberspace security talents effectively using cyberspace security competitions. Faced with a real demand for cyberspace security talents, China needs to establish and improve discovery and tracking mechanisms for cyberspace security talents, break the existing boundaries that limit it, gather resources, and build a China's database of cyberspace security talents that covers many aspects in order to provide talent support for the construction of a strong cyber power. Meanwhile, China should strengthen investment in cyberspace security competitions aimed at teenagers. This will enable China to attract young people to the field of cyberspace security, discover young talents, and train these talents as quickly as possible, in order to provide young talents for the construction of a strong cyber power.

References

[1] Luo S L, Zhu S, Wang C X. The research on cyberspace security countermeasures simulation model [J]. Journal of Information Security Research. 2016, 2 (8): 712–720. Chinese.

[2] Capture the flag [EB/OL]. (2016-11-03) [2016-09-10]. https://en.wikipedia.org/wiki/Capture_the_flag.