



ACCS Briefing Paper #4

Profiles of Chinese Cyber Security Universities

Greg AUSTIN and ZU Haoyue

January 2018



UNSW
A U S T R A L I A

Australian Centre for
Cyber Security

UNSW Canberra

PROFILES OF CHINESE CYBER SECURITY UNIVERSITIES

ACCS Briefing Paper No. 4

Greg Austin and Zu Haoyue

Australian Centre for Cyber Security
University of New South Wales Canberra
January 2018

About the authors

Greg Austin is a Professor in the Australian Centre for Cyber Security. He also serves as a Professorial Fellow at the East West Institute, where as Vice President from 2006-2011 working from London and Brussels he helped set up and lead its Worldwide Cyber Security Initiative beginning in 2009. Greg has held senior posts in the International Crisis Group and the Foreign Policy Centre (London). Other assignments include service in government, defence intelligence, academia and journalism. Greg is the author of several books on China's strategic policy, including *Cyber Policy in China* (Wiley 2014) and *Cyber Security in China: The Next Wave* (Springer 2018).

Zu Haoyue is a PhD candidate in the School of Humanities & Social Sciences, UNSW Canberra, at the Australian Defence Force Academy. She received her Bachelor's degrees from Chengdu College of University of Electronic Science and Technology of China. She has been a visiting scholar at the University of Michigan and has served as a research assistant at the Australian Centre for Cyber Security at UNSW.

ABOUT ACCS

The Australian Centre for Cyber Security (ACCS) at the University of New South Wales Canberra is two things. First, it is a focal point for 60 scholars from various faculties across UNSW who conduct research work on different aspects of cyber security. Second, it is a unit based in Canberra at the Defence Force Academy that provides both advanced research as well as undergraduate and graduate education on cyber security. ACCS brings together the biggest concentration of research and tertiary education for the study of cyber security in any single university in the Southern hemisphere. A number of ACCS scholars, in areas ranging from information technology and engineering to law and politics, have significant international reputations for their work.

Contents

Introduction	1
Xidian University	1
Wuhan University	3
University of Electronic Science and Technology of China (UESTC)	4
Shanghai Jiaotong University (SJTU)	5
Beijing University of Posts and Telecommunications (BUPT)	6
Sichuan University	7
Institute of Information Engineering (IIE)	8
Tsinghua University	8
CAS Centre of Excellence in Quantum Information and Quantum Physics	9
References	10

Introduction

This briefing paper assembles public source information on Chinese universities and several research institutes that are prominent in cyber security studies in China. It is based largely on material from the websites of the various institutions. In many cases, the material is simply a translation of entries in Chinese on the websites. The authors have not sought to verify any of the information from independent sources. The briefing paper was prepared as part of the background research for a project culminating in the publication of *Cybersecurity in China: The Next Wave* (Springer 2018). The selection was based on information from Chinese sources about the most important research education centres. Some centres, such as the Harbin Institute of Technology, which is among these leading universities, have not been addressed in this note. Readers may be interested to consult the Chapter Two of the book referred to above to see how this material informed judgements on related topics.

Xidian University

Based in the western historic city of Xian, Xidian is the short name for this university (based on the Chinese characters *xi* [西] from *Xian* [西安] and “*dian*” [电] from *dianzi* [电子] meaning “electronic”, in the formal name: Xian University of Electronic Science and Technology. It is widely regarded as the country’s pre-eminent university in cryptography and it now sees itself as a leader in the “re-establishment of the national cyber and information security system” (Xidian website). Though ranked in the middle of the top group, Xidian appears to have research strengths and a degree of innovation (broader understanding than in peer universities in the field).

Having started life as a radio school for the PLA in 1935, Xidian acted more quickly than most of its peers to adjust to the new strategic demands laid down by Xi’s cyber power speech by setting up a new School of Cyber Engineering (SCE) in December 2014, albeit based around existing capabilities. The speed of response suggests that in fact Xidian was directed by the central government to act. The SCE website reports that the initiative was undertaken in close consultation with Party and government leaders. The school has set itself two strategic goals: contributing to safe and controllable cyberspace by cultivating top innovative talents; and building within five years a world-famous and nationally prominent academic centre for talent training, scientific research, and collaborative innovation.

In 2017, SCE had about 50 full-time faculty members, all with PhDs, of whom 60 per cent had overseas experience. Of these seven are professors and 29 are associate professors (Xidian Handbook 2017). The school is led by two well known scholars: Professor Cai Ning, an IEEE Fellow, who is widely published, including in collaboration with international scholars; and Professor Ma Jianfeng, appointed under the Cheung Kong Scholars Program, a national initiative set up in 1998 to boost recruitment of highly qualified scholars. Until 2012 at least, Ma had been the single most prolific academic researcher in the field of information security in the world (Olyniuk 2014: 95)

SCE offers two undergraduate programs in Information Security and Cyber Engineering, and master and doctoral programs in Computer Science, Telecommunication Engineering, Cryptography, and Information Security. It has approximately 240 undergraduates, 200 master students, and 30 Ph.D. candidates each year, covering majors including Cyber and Information Security, Cryptography, Computer Science and Telecommunication Engineering. In a

somewhat unique position among universities in China in this field, SCE organises joint training with commercial firms to “upgrade the quality of cybersecurity talents and meet the urgent national need of high level cybersecurity engineers”.

Between 2010 and 2017, the number of new undergraduate students in the information security specialisation in the school each year has varied within the range of 120 (in 2010) and the peak of 183 (in 2013), with the number dropping back since then (to 134 in 2017) in spite of the higher priority accorded the subject (Xidian Handbook 2011, 2013, 2014, 2015, 2016, 2017). The similar annual figure for cyberspace engineering (also heavily oriented to security) has been the peak of 80 in 2010 and 2011, with a low point of 20 in 2013, and the 2017 plan providing for 52.

Every year, the university has reported, almost 20 per cent of bachelor’s graduates are recommended for direct entry (without needing to sit the entrance examination) into graduate study. Most others are employed by the leading Chinese corporations, such as Tencent, Alibaba, Baidu, Huawei, ZTE, China Mobile, China Unicom, and China Telecom Operators. Some join information security enterprises such as Qihoo 360 and TOPSEC, as well as government agencies (Xidian website http://ce.xidian.edu.cn/?page_id=103).

By way of comparison, the size of SCE looks roughly similar to or even somewhat smaller than that of the School of Electronics, Electrical Engineering and Computer Science at Queen’s University Belfast (an academic staff of around 50, with almost 250 students Ph D and Master’s students, 35 research fellows, and about 1000 undergraduate students across ten degree pathways. This Belfast school is home to the Centre for Secure Information Technologies (CSIT) which is one of the UK’s accredited centres of excellence in cybersecurity. CSE at Xidian is smaller than the CyLab at Carnegie Mellon University which, with more than 50 faculty and 100 graduate students, is arguably one of the world’s leading universities in the field.

Xidian University is not one of the country’s leading universities but performs strongly in computer science, ICT engineering, and information security. According to its website, it is one of 35 universities in the country to have a School of Software and one of nine to have a School of Microelectronics. It has joint laboratories with leading foreign corporations, such as Microsoft, IBM, Intel and SAP. It claims academic relations with more than 80 institutions worldwide, high level of faculty exchanges, about 600 foreign students from 43 countries, and runs joint venture undergraduate degrees with second-tier but specialised universities, one from France and one from Scotland.

Its leading research fields have been cryptography, wireless cybersecurity and cloud computing security but these do not map exactly with its new priorities which are described as cryptography, cyber and system security and content security. At its foundation, SCE established a collaborative innovation centre in information security with China Electronics Corporation (CEC), the leading state-owned enterprise in the field of cybersecurity, and with the Institute of Information Engineering of CAS. Table 1 (next page) shows the research fields for the school in 2017.

Xidian is the alma mater of one of China’s most famous entrepreneurs in the ICT field, Liu Chuanzhi, current Chairman of Lenovo, the world’s biggest producer of PCs, and co-founder of Legend (which is the forerunner of Lenovo) in 1984 as an offshoot of the Chinese Academy of Sciences (CAS). According to a Chinese website, in the Cultural revolution, Liu was

denigrated as an intellectual for telling his classmates at Xidian that the revolution was a bad idea (ZSP 2011). He was forced to the countryside as a farm labourer between 1968 to 1970, when he joined CAS as an engineer-administrator.

Table 1: Infosec Research Specialisations in Xidian University

<p><u>Cyber and System Security</u> system architecture heterogeneous cybersecurity access and integration security incident discovery, mining and tracking, policy-based automation social security modelling, emulating and comprehensive evaluation analysis network and system protection and testing vulnerability detection and penetration attack the controllability, observability and control theory of complex network systems software security verification theory and tools network trust management</p>	<p><u>Cloud Computing Security</u> cross-domain security cloud storage technology data security in the cloud computing environment and privacy protection secure computing in the cloud environment cloud architecture's computing architecture and security monitoring and control virtualization security technologies</p>
<p><u>Security Cryptographic Protocol Design</u> a verifiable security model based on computational complexity and theory formalized design based on location cryptographic protocol identity authentication and confidentiality and integrity protection financial password agreement dynamical and high-efficient group key management broadcast and multicast protocol of anonymous security</p>	<p><u>Cognitive Security and Trust Management</u> trusted computing and trust management information awareness and content security combinatorial theory of service security research on influence maximization algorithm security attributes of big data and the security of data manipulation privacy protection technology for big data storage flexible resource scheduling, fault prediction and adaptive-migration research on big data trust</p>

Wuhan University

Situated on the Yangtze River in one of China's oldest urban areas in the Han Kingdom, Wuhan University in 2001 was among the first to set up studies in information security for undergraduates, building on this in 2003 with graduate studies (Ph D and Master's) and post-doctoral offerings as well. This background and its continuous evolution contributed to a national award in 2014 for teaching excellence in the field of information security (Yu Jian 2017). The university prides itself on being the first one to develop an undergraduate courses system, teaching program, and course outline for information security; publishing the first series of domestic teaching materials for information security; and establishing the first domestic information security professional laboratory (Wuhan U. website 2017a).

The university remains nationally prominent in the field. In November 2015, it set up a new Cyberspace Security Institute (Wuhan U. website 2015). In February 2017, the university signed an agreement with the Wuhan Linkong Harbour Economic & Technological Development Zone (Mao H. 2017) to set up a National Cybersecurity School together (Guo Y. 2017). The university reports that most of its graduates in the field are employed in Tencent, Baidu, and Google, while a national report suggests that some its "excellent graduates" are employed by IBM and Microsoft.

The School of Computer Science, which was founded in 1978, was among the first such undertakings in the country. The Information Security Department is one of seven in the school. (Wuhan U. website 2017b). Two of the School's seven Ph D graduate programs are Information Security and Security Emergency Information Technology, topics that are replicated as two of the ten Master's level specialisations. Information security is one of its three undergraduate majors. The School has several national laboratories and centres, including the Key Laboratory of Aerospace Information Security, and Ministry of Education Trusted Computing, and National Network Security Virtual Simulation Experiment Teaching Centre.

The School of Computer Science currently has a total of 202 faculty, including 57 Professors and 87 Associate Professors. Currently, there are about 1500 undergraduate candidates across all three majors, of which one is information security. It is a four-year degree. Like all universities, its undergraduate curriculum includes subjects in Marxism and ideology. Each year, the School takes 280 master's student each year across the ten specialisations and 80 doctoral candidates across seven specialisations (of which only two relate to information security). Its Ph D course work includes a subject on future computer networks.

In 2016, the graduation rates in information security were around 100 with bachelor's degrees, 32 with Master's degree, and 6 with doctorates (about 30 per cent of the total for the School of Computer Science (Wuhan U. website 2017e). Based on earlier annual reports, it appears that these figures were not too different from the two previous academic years, except for small increases (5-10 per cent) in bachelor degrees. Though Wuhan had set up the first information security major in China in 2001, its graduate numbers between 2005 and 2011 were only about 60-70 bachelor's graduates per year (Zhang and Du 2014), compared with 100 per year in 2016. By 2013, there had been four reforms of the education plan in information security, which had seen the requirements change from 6 courses (three compulsory, three elective) to 18 courses (seven compulsory and 11 elective). That represented a significant deepening and broadening of the content of the information security program, but will with largely technical focus.

When Wuhan University opened its National Institute of Cyberspace Security in 2016, it only recruited 50 freshmen and sophomores from its School of Computing and School of International Software (Yu Jian 2017). In July 2017, Wuhan University announced it would recruit 60 students through a drive open to students at all levels. The university believes it is on track to produce 160 bachelor graduates in the field of information security by 2021.

University of Electronic Science and Technology of China (UESTC)

As might be expected for China's education system, one of the strongest research and education centres in the country in the field is a university specially established as a technical college in association with an industrial sector. This was typical of the new China that the Communist Party was trying to create in the 1950s. UESTC started life as the Chengdu Institute of Radio Engineering in 1956 and offered a major in computer science at that time. It has undergone several transformations. After the Cultural Revolution and at the start of the Reform Period, the Department of Computer Science was established in 1979, and a Microcomputer Institute opened in 1984 (UEST 2017a). In 1995, the current School of Computer Science and Engineering (CSE) was founded. It offered information security as one of its sub-disciplines, but it was not until July 2015 that the university set up a School of Cybersecurity (UEST

2017b), and in 2016, it began to recruit doctoral students in its own right after being authorised to do so (UEST 2017a).

The new school set up in 2015 has five research concentrations based on pre-existing capability: network and data security, secure communication, electromagnetic space security, cryptographic theory and applied algorithms, and cloud computing and big data security (UEST 2017a). Prior to 2015, the CSE had three Departments: Computer Engineering, Computer Software and Theory, and Information Security. It has two cyber ranges: a Computer Experiment and Teaching Demonstration Centre and the National Information and Network Security Virtual Simulation Experiment Teaching Centre. According to the CSE website, the School was ranked 12th in its field among Chinese Universities in the discipline evaluation by the state council in 2012 (CSE UEST 2016), and UESTC was ranked 54th in the world in the discipline of computer science by US News in 2017 (U.S. News 2017). This latter result for the computer science discipline is remarkable since the university as a whole is ranked at 584th. UEST has about 1 per cent of its students from overseas, of which 100 were in CSE. CSE ranks very highly (66th) in the computer science discipline for its global international collaboration. It ranks 36th globally for total citations in the field.

CSE has three specialisations in undergraduate training: Computer Science and Technology, Information Security and Digital Media Technology (the first two being national special majors). The 2017 student cohort comprised 3,000 full-time students, including some 1700 undergraduate students, 1117 masters, 171 doctoral students, and 100 international students.

The staff profile for CSE is strong. It has more than 200 staff, including more than 130 full-time teachers, one member of the Chinese Academy of Sciences, 11 awardees of the Recruitment Program of Global Experts. Around 90 per cent of the teachers have Ph Ds, and 80 per cent have studied overseas.

Shanghai Jiaotong University (SJTU)

SJTU describes itself as “one of the oldest and most prestigious and selective universities in China”. Its School of Information Security (SIS) was constituted as such in December 2016, based on the School of Information Security Engineering set up jointly in 2000 by the MOE, the Ministry of Science and Technology (MOST), the national government, the Shanghai Municipal Government, and the university. It claims to have been the country’s first university department that serves as a national talents training base in the field of information security”. The school advertises three primary disciplines: cybersecurity, communication and information system security, and security of computer applications technology. It teaches at undergraduate, master’s and doctoral levels. It has a faculty of 32: seven doctoral tutor professors, one research professor, 11 associate professors, 8 associate research professors, and five senior engineers at associate professor level. This staff is complemented by over 20 adjunct professors. The faculty includes 2 members of the CAS, and a number of other top talents recognised through various national and municipal hiring initiatives. SIS reports that it has won significant research grants from the national government, including the Ministry of Defence. It claims over 80 approved patents and proudly boasts of its role in shaping national information security standards and regulations.

The research priorities of SIS focus on diverse aspects of cybersecurity (content security analysis, Internet of Things (IOT) security, wireless security, mobile security, large data mining and analysis, and cryptography. SIS sees itself as building a “close connection between the

fundamental theories of information security and the major demands of national information security”. It takes project guidance from the Reform Commission Office of the Central Leading Group on Cybersecurity. SIS hosts a number of R&D laboratories: The National Engineering Laboratory for Information Content Analysis Technology (2009); Engineering Research Centre for Network Information Security Management and Service (Ministry of Education)(2006); Shanghai Key Laboratory for Integrated Administration Technologies in Information Security (SKLAITIS)(2002); SJTU Laboratory for Information Security Technology Service; and Joint Research Laboratory on Security and Trust with Telecom Paris Tech, one of France’s leading research institutions in the field.

Of these key labs, SKLAITIS is especially noteworthy, dating its origins back to 2002. It was set up in partnership with Shanghai Koal Software. The lab claims “great influence in the field of information security in China”. The website lists its research priorities as: integrated management and monitoring technology for large scale networks, integrated management and monitoring technology for network media content security, technology and applications for Public Key Infrastructure and privilege management infrastructure, network attack and defence and security evaluation, and E-government engineering and public services.

In addition, SJTU’s School of Computer and Information Technology (CIT) opened in March 2000 on the basis of the amalgamation of the pre-existing departments, including the Institute of Information Science founded in 1978. None of its six departments has an exclusive focus on information security, but it does offer an inter-disciplinary option in the field that is atypical for Chinese universities. At the undergraduate level, this focusses on the technology and management of ICT, electronic information, e-commerce, electronic finance, electronic government, military affairs and law. The students can undertake information security research, development, application and management. Courses offered include cryptography and cryptographic protocols, network security attack and defence, deception, advanced programming, security protection technology, and artificial intelligence (<http://scit.bjtu.edu.cn:8080/en/UndergraduatePrograms.html>). In 2017, there were 178 teaching staff in the CIT, of whom there was one member of Chinese Academy of Engineering (part-time), 18 Ph.D. supervisors, 17 professors, 45 associate professors, and 10 senior engineers. The total enrolment of the CIT is about 1826, including 1061 undergraduates, 645 master candidates, and 120 doctor candidates.

According to the CIT website, its graduates have found work with the Ministry of State Security (MSS), Ministry of Public Security (MPS), National Administration for the Protection of State Secrets, Bank of China, ICBC (Industrial and Commercial Bank of China), China Mobile, Baidu, Sina and Sohu.

Beijing University of Posts and Telecommunications (BUPT)

BUPT occupies a special place in Chinese government plans for cybersecurity, due in no small part to its unique role in servicing the powerful ministries represented by its current missions and its location in Beijing. It has one of the biggest and most rapidly-formed new centres in the country, becoming one of the first five “training bases” to help correct the country’s skills gap (BUPT 2017a).. BUPT set up a new School of Cyberspace Security in January 2016 into which existing students already majoring in Information Security or Computer Science and Technology transferred (some 390 undergraduate and almost 500 doctoral or Master’s students) (BUPT 2017b). BUPT is one of the 27 universities authorised in 2016 to grant Ph Ds in “cyberspace security”. It also has doctoral and master’s degree programs in “Information

Security”, as well as two undergraduate programs—Cyberspace Security and Information Security.

Its staff complement is much bigger than that in the peer department in Tsinghua, and it has a correspondingly larger student body. The new School of Cyberspace Security has one member of the Chinese Academy of Science (Fang Binxing), two Distinguished Great Wall Scholars, twelve full professors, 22 associate professors, 14 lecturers, 17 doctoral supervisors, and 51 master’s supervisors. In response to the urgency of the skills problem, BUPT sought to recruit 30 per cent more undergraduates to the field in 2017 compared with recent years (91 compared with 70/71 from 2014-2016). But this figures of 91 is just a little higher than the 84 recruited in 2013. The 2017 student intake would also see a shift of students from the one degree in information security to fill out the new degree of cyberspace security, with some 30 fewer places taken in the pre-existing degree (BUPT 2017c). In 2016, some 84 students were admitted for postgraduate study in information security, of whom 25 were judged to be sufficiently talented to be admitted without competitive examination (BUPT 2017d).

The 2017 student cohort for Master’s study in the School was 159, of which 9 were taking a major that might be called network security “light”; 22 were taking complex network security (the pre-existing information security degree); 68 were taking the new degree in cyberspace security, which included additional courses in network security confrontation, electromagnetic space information security, and cognitive network and data fusion; and 60 were taking a professional degree in ‘computer technology’ similar to the pre-existing degree in information security (BUPT 2017e). There were 20 Ph D students enrolled in 2017, whose coursework was split between the three specialisations above, but with cyberspace security having advanced research options as coursework units (BUPT 2017f). Between 2014 and 2016 (three academic years), BUPT produced 212 bachelor’s graduates, 221 Master’s graduates, and 19 Ph Ds in the field of information security (BUPT 2017g). This represented only 3-5 per cent of all graduates from the Schools of Computer Science. This, one of China’s top 30 (biggest and best) cybersecurity schools in the field, even with some allowance for growth, is on track for the next few years to produce no more 200 to 250 graduates per year to fill an unmet national need estimated to be in the hundreds of thousands by 2020.

Sichuan University

Based in Chengdu, Sichuan University (SCU) provides a useful comparison with BUPT. The latter is a specialized university, and the former a comprehensive educational institution. Chengdu is one of China’s technology capitals, with around 300 Fortune 500 companies maintaining some sort of presence in the city. Numerous defence industries are located in or near the city. In 2015, SCU set up the Research Institute of Cybersecurity for the purpose of establishing the field as first-level discipline in the university (SCU 2017a). This was followed in 2016, with the opening of the College of Cybersecurity. SCU was one of 29 universities granted the right in 2016 to award Ph.D. degrees in cyberspace security.

SCU is a national talent training base in two related fields: cyberspace security and secrecy for national security (in the College of National Secrecy at the College of Cybersecurity). The Institute and College have about 20 faculty, of whom 17 are full-time academics, with one member of the Chinese Academy of Engineering, eight Senior Professional Technicians, seven associate senior professional technicians, and 14 master’s and doctoral supervisors.

The curriculum is more mathematics-oriented than BUPT (with subjects like cryptography, mathematical logic, data structure and algorithm) but has some additional topics of interest such as information content security, deception, network attack and defence technologies, and malware analysis (SCU 2017b). In 2016, the planned intake of master's degree candidates was 60, of whom 35 candidates would major in cyberspace security, 17 in computer technology (specialising in cyberspace security), and 8 candidates in electronics and communications engineering (specialising in information security)(SCU 2017c). This student cohort was about two-thirds of that planned for BUPT.

Institute of Information Engineering (IIE)

IIE in the Chinese Academy of Sciences was set up in 2011. Its main research priorities are password theory and security protocols, information intelligent processing, data security, communications and electromagnetic security, network and system technology, information system evaluation. In March 2016, its staff comprised 898 people, including 616 research specialists, 57 senior professional and technical personnel, and 126 other professional staff. It had 1127 students, of whom 450 were master's level and 311 were doctoral candidates. The activities of the 366 students were not specified, but normally CAS does not accept undergraduates. They may well be professional development students from state-related cyberspace security agencies.

In March 2016, IIE launched the *Journal of Information Security*, seen at the time as an important and timely corrective to the country's lack of influence in academic journals (CAS 2016a). In 2016, IIE's State Key Laboratory of Information Security (SKLOIS) hosted the 15th International Workshop on Digital Forensics and Watermarking and 14th international Theory of Cryptography Conference in Beijing. The latter was jointly sponsored by the International Association for Cryptologic Research (IACR). CAS also has, as one would expect, its own cybersecurity support services but these were also upgraded in 2016 (CAS 2016b).

SKLOIS is probably the primary information security research hub for IIE. Set up in 1991, it has 135 faculty (two members of the Academy, 34 professors, 22 associate professors). It hosted its first international (and therefore public) Conference on Information Security and Cryptography in 2005. The conference proceedings were published by Springer, based on 33 papers approved for publication by an international organising committee (Feng, Ling and Yung 2005).

Tsinghua University

At Tsinghua, the country's premier science and technology institution for research and education, the leading centre for cybersecurity is the Institute for Network Science and Cyberspace, which sits inside the School of Information Science and Technology. The Institute, set up only in 2012 (Tsinghua 2017a), has five primary disciplines: fundamentals of cyberspace security, cryptology and its application, system security, cybersecurity, and application security (Tsinghua 2017b). Its staff compliment reported in 2017 was one member of the Chinese Academy of Science, two Distinguished Great Wall Professors, two recipients of National Outstanding Youth Foundation awards, seven professors, 17 associate professors, nine persons qualified for Ph.D. supervision, and numerous engineers and technicians. As is typical of universities outside China, the share of Tsinghua's information science faculty engaged in security aspects is quite small (less than five per cent).

The number of cybersecurity graduates is small. In the five-years prior to 2017, 90 students graduated from the Institute (of which 30 were postgraduates) (Tsinghua 2017e). At Tsinghua University, the graduate and undergraduate programs are taught by staff of the leading centre for cybersecurity mentioned above, the Institute for Network Science and Cyberspace, of the 14 subjects taught only a small number have security in the title.

The faculty follow rather predictable pursuits and impressive career profiles. For example, one of the professors, Duan Haixin, blogs regularly on topics such as the U.S. National Security Agency. He is a prolific scholar, with some 90-100 academic publications, in Chinese and international journals and proceedings, and nearly 1500 citations. His most highly cited paper addressed the security of Chinese university networks (Duan 2015). He teaches Network Security Engineering and Practice (undergraduate level) and Computer Network Secure Technology (graduate level)(Tsinghua 2017c). In 2012, he presented a co-authored paper on “Investigating the Chinese Underground Economy of Information Security” at a joint workshop in the United States organised with the University of California San Diego and the U.S. Naval War College (IGCC 2012: 10-11). He has participated in meetings of the Internet Engineering Task Force. He represented CNCERT/CC at an international conference in Tokyo in 2002, the Asia Pacific Security Incident Response Coordination Conference. He has participated in “white hat” hacking conferences in China to demonstrate flaws in automatic teller machines. He was an inaugural member of the (ISC)² Advisory Board for Asia set up in 2004.

Tsinghua also hosts the Research Centre on Cryptographic Theory, which also works on applied cryptography and quantum computing (ATIP 2015: 12).

Tsinghua is also operating at the forefront in China for new technologies that will make cyberspace more secure, including quantum computing and secure computing. This is a highly internationalized operation, led by the Institute for Interdisciplinary Sciences (IIS). The three most important centres from a security point of view in IIS (Quantum Information, Machine Intelligence and Secure Computing) were set up in 2011, at the same time as IIS. Its subordinate centres have partnerships with the Massachusetts Institute of Technology, Aarhus University (Denmark), Waterloo University (Canada), and the Chinese University of Hong Kong. The first agreement with Waterloo, covering a range of disciplines, including computer science, was signed as early as 2005. The Dean of IIS, Professor Andrew Chi-chih Yao, is a prize-winning graduate of National Taiwan University, Harvard and the University of Illinois. He holds two Ph Ds, and is a foreign member of the US National Academy of Sciences and the American Academy of Arts and Sciences. He has held academic posts in Stanford, UC Berkeley, MIT and Princeton. His specialisations include quantum computing, artificial intelligence, computational and communications complexity, and cryptographic protocols (Tsinghua 2017d).

CAS Centre of Excellence in Quantum Information and Quantum Physics

China’s commitment to information security research took a step up when it created a new “networked” Centre of Excellence in Quantum Information and Quantum Physics in 2014 as part of a wider program of centres of excellence launched under the Pioneer Initiative (Wang M. 2017). The research topic was already well established in China but the new measure was intended to accelerate the development of basic research and more importantly its application. The goal of the Pioneer program is to set up new centres that can “lead in academic excellence

at the frontiers of science and technology worldwide, cultivate a national talent pool for innovation, and develop advanced think-tank teams and world-class scientific research institutions”. The Quantum Computing CoE, the first in the Pioneer Program, brings together researchers from CAS, the University of Science and Technology of China (USTC), the Shanghai Institute of Technical Physics of the CAS, Institute of Semiconductors of the CAS, Institute of Optics and Electronics of the CAS, and other domestic research institutions. Its remit is wider than information security, but it has set itself the goal of building a “wide-area quantum communication network, to apply the quantum communication in national defense, government affairs, [and] finance” and “to create strategic industries with China taking a leading international role and a next-generation national information-secure ecosystem” (Wang 2017). As Wang points out, “Quantum key distribution (QKD) overcomes the security risk of classical encryption and, to date, has been proven as the only unconditional[ly] secure communication method”.

One of the projects absorbed by the new CoE demonstrates the determination of the researchers and the government to rush the technologies into operation. The project, launched in in 2013 with a diverse array of Chinese institutional sponsors, is to build a ‘backbone line’ for secure communications between Beijing and Shanghai, taking in cities along the route, and on that basis establish a wide area network (Wang 2017).

References

- ATIP 2015 Cyber Security Research in China. Defense Technical Information Center.
www.dtic.mil/get-tr-doc/pdf?AD=ADA619229
- BUPT 2017a. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
<http://scss.bupt.edu.cn/xygk/xyjj.htm>.
- BUPT 2017b. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
http://zsb.bupt.edu.cn/content/content.php?p=7_50_581.
- BUPT 2017c. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
 Various pages. http://zsb.bupt.edu.cn/content/content.php?p=4_5_514,
http://zsb.bupt.edu.cn/content/content.php?p=4_5_515,
http://zsb.bupt.edu.cn/content/content.php?p=4_5_394,
http://zsb.bupt.edu.cn/content/content.php?p=4_5_395,
http://zsb.bupt.edu.cn/content/content.php?p=4_5_11,
http://zsb.bupt.edu.cn/content/content.php?p=4_5_2.
- BUPT 2017d. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
http://yzb.bupt.edu.cn/content/content.php?p=3_8_207. Accessed 26 September 2017
- BUPT 2017e. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
http://yzb.bupt.edu.cn/content/content.php?p=8_4_209.
- BUPT 2017f. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
http://yzb.bupt.edu.cn/content/content.php?p=8_3_213
- BUPT 2017g. Website of Beijing University of Posts and Telecommunications. (In Chinese.)
 Various pages.
<http://xxgk.bupt.edu.cn/upload/file/201701/20161229%E5%B0%B1%E4%B8%9A%E8%B4%A8%E9%87%8F%E6%8A%A5%E5%91%8A.pdf>;
<http://xxgk.bupt.edu.cn/upload/file/201601/%E5%8C%97%E4%BA%AC%E9%82%AE%E7%94%B5%E5%A4%A7%E5%AD%A62015%E5%B9%B4%E6%AF%95%E4%B8%9A%E7%94%9F%E5%B0%B1%E4%B8%9A%E8%B4%A8%E9%87%8F%E5%B9%B4%E5%BA%A6%E6%8A%A5%E5%91%8A.pdf>; <http://xxgk.bupt.edu.cn/upload/file/201412/%E5%8C%97%E4%BA%AC%E9%82%AE%E7%94%B5%>

- [E5%A4%A7%E5%AD%A62014%E5%B9%B4%E6%AF%95%E4%B8%9A%E7%94%9F%E5%B0%B1%E4%B8%9A%E8%B4%A8%E9%87%8F%E5%B9%B4%E5%BA%A6%E6%8A%A5%E5%91%8A.pdf](#).
- CAS 2016a. Seminar on the Launch and Further Development of the “Journal of Information Security”. In Chinese. 21 March 2016.
http://www.iie.ac.cn/xwdt_101144/tpxw/201603/t20160321_4568384.html
- CAS 2016b. Computer Network Information Center website.
http://english.cnict.cas.cn/RS/departments/201611/t20161111_170334.html
- CSE UEST. 2016. About CSE . School of Computer Science and Engineering of the University of Electronic Science and Technology of China. 2016.
<http://www.ccse.uestc.edu.cn/english/list?type=18>. Accessed 27 September 2017
- Duan Haixin. 2015. CERNET Campus Network Security Analysis and Countermeasures. China Education Network. 3.1. In Chinese.
<https://scholar.google.com/scholar?oi=bibs&cluster=6923009092818443675&btnI=1&hl=en>
- Feng Denguo, Lin Dongdai and Yung Moti. Eds. 2005. Information Security and Cryptology: Proceedings of the First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005. Springer Science and Media Business.
- Guo Y. 2017. Signing of a Cooperation Agreement between our School and the Wuhan Airport to build a National Network Security Institute. In Chinese. [Online]. Wuhan University News Network. Available: <http://news.whu.edu.cn/info/1002/48010.htm>. Accessed 26 September 2017.
- IGCC 2012. China and Cybersecurity: Political, Economic, and Strategic Dimensions. Report from Workshops held at the University of California, San Diego April 2012,
<https://www.usnwc.edu/Academics/Faculty/Derek-Reveron/Documents/China-and-Cybersecurity-Workshop-Report-final.aspx>.
- Mao H. Wuhan Linkonggang Economic & Technological Development Zone. [Online]. The Editorial Office of Hubei Provincial People’s Government Official Web Portal. Available: http://en.hubei.gov.cn/business/zones/201510/t20151014_728663.shtml.
- Olijnyk, N.V., 2014. Information Security: A Scientometric Study of the Profile, Structure, and Dynamics of an Emerging Scholarly Specialty. Long Island University, CW Post Center.
- SCU 2017a. Website of Sichuan University (In Chinese.) <http://ccs.scu.edu.cn/about.html>
- SCU 2017b. Website of Sichuan University (In Chinese.)
<http://ccs.scu.edu.cn/bksjx/201610/0470.html>
- SCU 2017c. Website of Sichuan University (In Chinese.)
<http://ccs.scu.edu.cn/yjszs/201610/71.html>
- Tsinghua. 2017a. Faculty Overview. In Chinese.
<http://www.tsinghua.edu.cn/publish/wyy/10761/index.html><http://www.tsinghua.edu.cn/publish/wyy/10761/index.html>. Accessed 21 August 2017.
- Tsinghua 2017b. Graduate Professions Overview. In Chinese.
<http://www.tsinghua.edu.cn/publish/wyy/10800/index.html><http://www.tsinghua.edu.cn/publish/wyy/10800/index.html>. Accessed 21 August 2017.
- Tsinghua. 2017d. Chao Andrew Chi-chih. <http://iis.tsinghua.edu.cn/en/yao/>.
- Tsinghua. 2017e. Tsinghua University Institute for Network Science and Cyberspace.
<http://www.tsinghua.edu.cn/publish/wyy/10824/index.html>
- UEST 2017a. Website of the University of Electronics and Technology (In Chinese.)
<http://www.ccse.uestc.edu.cn/view?type=10&id=5211>
- UEST 2017b. Website of the University of Electronics and Technology (in Chinese).
<http://www.ccse.uestc.edu.cn/view?type=10&id=4290>

- U.S. News. 2017. University of Electronic Science and Technology of China.
<https://www.usnews.com/education/best-global-universities/university-of-electronic-science-and-technology-of-china-506780>.
- Wang, M. 2017. CAS Center for Excellence in Quantum Information and Quantum Physics: exploring frontiers of quantum physics and quantum technology. *National Science Review*. 4 (1). 144–152. <https://doi.org/10.1093/nsr/nwx025>
- Wuhan U. website. 2017b. Overview [Online]. Available:
<http://cs.whu.edu.cn/plus/list.php?tid=53> [Accessed 26 September 2017].
- Wuhan U. website. 2017c. Organization [Online]. <http://cs.whu.edu.cn/plus/list.php?tid=55>. Accessed 26 September 2017.
- Wuhan U. website. 2017d. College Introduction. In Chinese.
<http://cs.whu.edu.cn/plus/list.php?tid=2>. Accessed 26 September 2017.
- Wuhan U. website. 2017e. Annual Report on Employment Quality of 2016 Graduates of Wuhan University. In Chinese. [Online]. Wuhan University. Available:
<http://info.whu.edu.cn/info/1781/166860.htm>. Accessed 26 September 2017.
- Zhang, H. & Du, R. 2014. The Current Situation and Problems of Information Security Personnel Training in Wuhan University. In Chinese. China Education and Research Network. http://www.edu.cn/xjh/fei/zxz/201410/t20141016_1190565.shtml. Accessed 26 September 2017.
- ZSP 2017. Liu Chuanzhi. Website Zhongguancun Science Park. Compiled by China Daily, drawing on Wikipedia entry. Accessed 2 September 2017.
http://www.chinadaily.com.cn/m/beijing/zhongguancun/2011-11/14/content_14025993.htm.

