March 2021

Academics, AI, and APTs

How Six Advanced Persistent Threat-Connected Chinese Universities are Advancing AI Research

CSET Issue Brief

CENTER for SECURITY and EMERGING TECHNOLOGY

AUTHOR
Dakota Cary

Executive Summary

Turning cutting-edge research into operational capabilities is the currency of cyber operations. The vulnerability no one else knows about, one found by someone with highly specific knowledge of a program or coding language, opens a backdoor into an adversary's most sensitive vault. A better understanding of one technology or technique can give cyber operators an advantage over opponents. Governments benefit from compressing the timelines from discovery to exploitation, more rapidly using the insights of researchers for operations.

Artificial intelligence (AI) and its current dominant paradigm, machine learning (ML), almost certainly will not fundamentally alter competition in cyberspace. That said, AI systems will provide both new terrain for cyber operations—as targets that can themselves be hacked—and new tools of cyber operations, as ML aids offensive and defensive efforts. China's military-civil fusion strategy takes a holistic approach to development and aims to seamlessly incorporate private resources and developments for state use, with the goal of shortening the pathway for non-governmental research on AI and cybersecurity to strengthen and diversify government operational capabilities.[1]

There is notable precedent for using university developments in state-sponsored hacking operations. Over the past decade, China's security services have repeatedly turned to select university faculty to conduct research on cyber techniques and, in some cases, run cyber operations. Collaboration between university faculty and cyber operators illustrates China's approach to military-civil fusion. This report identifies six universities that previously worked with China's state-sponsored hacking teams and are now conducting research on the use of ML for cyber capabilities; two universities also host research programs on cyber attack and cyber defense of AI systems. This report summarizes the extent to which these universities, with ties to known state-sponsored hacking teams, might aid China's efforts in these areas.

Key Findings

- **Multiple universities with connections to Advanced Persistent Threat (APT) cyber actors are conducting research on the intersection of cybersecurity and ML.** All six universities employ faculty who are actively conducting research on ML and cybersecurity. At least one known state-backed hacker is researching how to use ML for anomaly detection, a defensive cybersecurity technique. Shanghai Jiao Tong University's School of Information Security Engineering, a school with ties to the PLA, hosts a research institute conducting research on offensive and defensive cybersecurity techniques; the director of that institute published an analysis of ML and cybersecurity trends in a Ministry of State Security periodical. Research on cybersecurity and AI is moving from academic journals to strategy forums for China's security services.

- **Research conducted on the application of machine learning and AI to cybersecurity is extensive, particularly in the areas of anomaly detection systems, malware classification, behavior analysis, and active defense.** Most papers published by faculty from these universities examined how to use machine learning for defensive purposes. Offensively oriented papers noted ML's application to vulnerability discovery and exploitation—a dual-use technique that can secure or wreck software. One paper published by an author at Xidian University and funded by the Key State Laboratory for Information Security's Unclassified Projects Fund concluded that ML could bolster cyber defenses and improve vulnerability discovery.

- **Research on the attack and defense of AI systems was less pervasive than research on applying the technology to cybersecurity.** Two schools favored for recruiting cyber operators for specific hacking groups are researching the vulnerability of AI systems. Zhejiang University offers classes on the attack and defense of AI systems, alongside classes on how to write intelligence reports.[2] Harbin

Institute of Technology is conducting research on the topic, but does not publish its progress.

Governments' use of new technologies affects their relative power and influence in the modern world. Nations that innovate faster and more effectively often build and sustain an advantage over their rivals. In such a competition, ML has the potential to be a game-changing technology, and both China and the United States are racing to exploit its power. More narrowly, the application of ML techniques to traditional cyber operations may prove to be transformative, altering operations' practice and amplifying their potency. Since these operations are a fundamental part of modern statecraft, having an operational advantage, even if only for a moment, can yield lasting gains for governments. By examining the research at select universities, analysts and decisionmakers can better determine how China may try to apply AI and machine learning techniques to cyber operations in search of this advantage. If the cross-pollination from academic research teams to fielded operations occurs for ML-enabled cyber capabilities as it did in earlier cyber operations, then understanding the depth and breadth of the schools' work can shed light on future operational developments and their potential security impacts.

Table of Contents

Introduction

Professor Gu Jian (顾剑) splashed cash on whoever could help him. Standard password cracking techniques and dictionary attacks served no use for the professor—he needed innovators. Only the top talent would do and he did what he could to lure it out. "Believe it or not, our professor has a lot of money," one student said of Professor Gu.[3] With payouts up to RMB 500K ($73,000), the professor threw large sums of money at his problems.[4] "Our teacher says if no one can crack it this time, then he'll increase the money on offer," the student said.[5] Outside of his classroom, Professor Gu scouted talent at hacking competitions on Hainan University's campus and encouraged students to attend by offering cash prizes from one of his shell companies. That company, Hainan Xiandun Technology Company, even listed its address of incorporation as the university's library.[6]

As a former PLA officer in the Guangzhou Military Region's Political Department, Professor Gu was a natural choice for Hainan's State Security Bureau when it sought to stand up its hacking operations. Gu Jian served as a professor in the Information Security Department of Hainan University and used his position to run state-sponsored hacking operations. Beginning in 2013, Professor Gu posted job listings on internal university boards, hosted hacking competitions where he scouted for talent, and offered bounties on technical capabilities to his students and coworkers. By the time *Intrusion Truth*—a cybersecurity blog rumored to be a front for a national intelligence agency—outed Professor Gu and his government contact in early 2020, his hacking team had already victimized companies in the U.S. defense industrial base.[7] Cybersecurity professionals assigned Professor Gu's state-sponsored team a standardized designation, Advanced Persistent Threat 40 (APT40); it was a sign that the hackers were notable operators.

Professor Gu's experience running a state-sponsored APT is not an aberration. Both the Ministry of State Security (MSS) and the People's Liberation Army (PLA) have used universities and their employees to support and conduct cyber operations for many years.[8] Six schools deserve particular scrutiny.

The universities analyzed in this report were chosen because of their connections to known hacking groups. Universities qualified for inclusion if they: 1) previously conducted cyber operations (Hainan University, Southeast University, and Shanghai Jiao Tong University), 2) partnered with specific divisions of the security services that conduct cyber operations (Xidian University), or 3) were noted by US cyber threat intelligence companies as places of recruitment for APTs (Zhejiang University and Harbin Institute of Technology). Other universities, aside from these six, also contribute to China's cyber capabilities albeit without apparent connection to specific APTs, thus falling below the threshold for analysis of this report.[9]

China's *Science of Military Strategy*, a government publication of military doctrine and strategic thinking put forward by the PLA's Academy of Military Science, has long emphasized the integration of civilians into the military's information warfare operations, the domain that includes cyber operations.[10] The CCP's strategy of military-civil fusion aims to leverage private resources for government use. Recent reporting shows that the MSS tasks some companies to analyze bulk data collected from cyber espionage operations—exemplifying one way MCF is put into practice in the cyber domain.[11] Whereas other countries' security services may contract with consenting and interested companies, non-government entities in China accept working with the CCP as a cost of doing business; rejecting the Party's requests may be the death-knell for an organization. As China's security services compete for access to information, cyber operators can leverage close relationships with universities to develop new tactics, techniques, and procedures. This quest for new capabilities pushes academics and operators into new areas of research. The integration of universities and state-sponsored espionage shortens the time required to turn academic research into operational capabilities and creates a window into operators' possible research priorities. Understanding current research can provide insights, and potentially indicators, into possible future capabilities and intentions. Research applying machine learning to offensive techniques and defensive tactics offers China's security services new tools to leverage; research on the attack and defense of AI

systems opens a new battlespace for contest. Competition begets innovation.

It is not this research, in and of itself, that warrants attention. Research on machine learning and AI for cybersecurity, and the attack and defense of those same systems are normal topics for computer science researchers for good reason: machine learning offers new tools for cybersecurity professionals to deploy. ML-based cyber threat detection, malware classification, and inspection of encrypted data flows all promise future gains for cybersecurity. By the same token, AI systems themselves must be secured from attackers. Vulnerable systems proliferate as companies monetize algorithms and governments deploy new tools. Defending these systems requires anticipating how they may be attacked, so researching attack methodologies is one way to gain insight into adversaries' efforts, which in turn could inform efforts to bolster defenses. This dual-use nature of cybersecurity research tints the lens of analysis.

This paper examines the relationship between China's state-backed hacking teams, six universities, and the AI/ML research they do that may affect future cyber operations. To do that, this paper draws on open sources[12] to study the relationship between the MSS, the PLA's Strategic Support Force (PLASSF), which is responsible for computer network operations and technical reconnaissance, and these institutions.[13] The author examined university webpages for each school's cybersecurity (网络空间安全) program and information security (信息安全) program. Faculty web pages with biographical information claiming connection to the security services, and research related to AI/ML are analyzed below. University or government documents from public file sharing sites, such as Baidu Wenku, bearing related search terms are also included. Findings regarding academic papers from the China National Knowledge Infrastructure (CNKI) database reflect papers published by each school's respective degree programs that the CSET data team has determined to be related to AI/ML.

Findings

This table provides a brief overview of all six universities affiliated with Chinese state-backed APTs; whether the cybersecurity program at these schools offers courses on AI and machine learning; whether professors at the school are conducting research on AI and cybersecurity; and if the institution is on the U.S. Commerce Department Bureau of Industry and Security's Entity List. The following subsections provide more details on the links between each university and the security services, as well as any relevant research conducted by faculty and staff of the institution.

Institution's Name in English	Institution's Name in Mandarin	Affiliated APTs	Cybersecurity Courses Include AI/ML?	Individual Professors Researching AI/ML and Cybersecurity?	US Government BIS Entity List[14]
Hainan University	海南大学	APT40	Unknown	Yes	No
Southeast University	东南大学	Deep Panda	Yes	Yes	No
Shanghai Jiao Tong University	上海交通大学	APT1	Yes	Yes	No
Xidian University	西安电子科技大学	APT3	Yes	Yes	No
Zhejiang University	浙江大学	APT1	Yes	Yes	No
Harbin Institute of Technology	哈尔滨工业大学	APT1	Unknown	Yes	Yes

Hainan University (海南大学)

Connections to the Security Services

Hainan University employed a professor conducting cyber operations with APT40, which *Intrusion Truth* attributed to the Hainan Bureau of the MSS (see introduction).[15]

Research on AI/ML + Cybersecurity

Websites for the Hainan University cybersecurity school and related research institutions either failed to load or required passwords to access. It is unclear why the Hainan University Cybersecurity Department's website is password protected—an uncommon security protocol compared to other universities examined in this report. The increased security measures may well have been implemented following the revelation of the school's association with APT40, but this is not easily discernable.

A search of available academic papers uncovered one paper published on using ensemble learning methods, a machine learning framework, to create an early warning system for distributed denial of service attacks.[16] Hainan University has not published any other research related to AI/ML and cybersecurity.

Southeast University (东南大学)

Connections to the Security Services

Professor Song Yubo (宋宇波) and Beijing TopSec, a company known to provide cybersecurity services to the PLA and MSS, hosted a hacking competition in early 2014 for Southeast University students.[17] Unlike normal capture-the-flag competitions where participants hack other teams for points, Professor Song offered students a real-world opportunity to earn points and gain prestige by attempting to access the network of a U.S. DoD contractor, VAE, Inc.[18]

In preparing the computer infrastructure for the hacking competition, Professor Song accidentally left a trail of indicators connecting him, the competition, and the VAE operation. Song set

up websites meant to fool VAE employees into giving up their credentials in the days leading up to the competition; VAE confirmed spearphishing attempts at the same time as the competition.[19] Not only did the timing of the websites align with the competition, but Song used the same registration company and naming conventions to create both the competition registration website and the websites used for the hacking operation. Such overlapping procedures could be coincidental; one registration company can serve many clients. But, Song also made an operational security error when compiling his malware, by accidentally programming his malware to call back to the same IP address he used to register the competition's website, connecting him, the competition, and the malicious websites.[20]

Months after the attempted attacks on VAE, Inc., the same malware from the competition was found on a website targeting Anthem Insurance employees.[21] The 2019 DOJ indictment of Chinese hackers for the Anthem Insurance hacks did not name Song, however. The relative exclusivity of the malware and its connection to Deep Panda, the Crowdstrike designation for a Chinese state-sponsored hacking team, suggests that Song and the team that hacked Anthem Insurance had access to the same tools—either through sharing or centralized distribution.[22] Moreover, Song registered the malicious VAE websites using the name of a Marvel comic book character—the same theme used to register infrastructure for the hack of the U.S. Office of Personnel Management, another major Chinese operation.[23]

Aside from Song Yubo, Southeast University has a strong institutional relationship with China's information warfare programs. A 2012 report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman determined that Southeast University faculty—including Song[24]—received regular funding from five programs for "the modernization of state secrecy, the technical professionalization of the PLA, and the continuing development of information conflict capabilities."[25] As of 2012, funds from these five programs—the 863 National High Technology Research and Development Program (国家高技术研究发展计划), the 973 National Key Basic Research Program (国家高技术研究发展计划), the National 242 Information Security

Program (国家 242 信息安全计划项目), Ministry of State Security 115 Program (国家安全部 115), and the National S219 Information Security Application Demonstration Project (国家 S219 信息安全应用示范工程)—were selectively distributed to a small group of universities; it is unclear if these programs are still disbursing funds. Only two other universities, Harbin University and Zhejiang University, received funding from all five information warfare projects as of 2012—both are tied to APTs and covered in this report.

Southeast University continues to build upon its relationship with the security services in the information domain. A university webpage touts Southeast University partnering with the PLA Strategic Support Force to establish the Purple Mountain Internet Communications and Security Research Lab (网络通信与安全紫金山实验室), which opened in 2018.[26] PLA SSF researchers and Southeast University faculty at the lab work together on "important strategic requirements", computer operating systems, and interdisciplinary cybersecurity research.[27] In the same year, the university established a "security self-investigation and self-correction working group" for the cybersecurity academy's "laboratory and important venues"—perhaps to guard against insider threats to research.[28] Other engagements revolve around hands-on learning and job placement. Southeast University connects students to the security services via job postings and research positions. One post-doctoral position with the MSS 13th division works on "APT attack detection, and vulnerability discovery and exploitation."[29] A web page for prospective students highlights that graduates often go on to work for the MSS, among other possible careers.[30]

Research on AI/ML + Cybersecurity

Professor Song, the academic who facilitated the VAE, Inc. hacking competition, is now researching how to use machine learning for anomaly detection—a technique that looks for unusual patterns of network behavior.[31] Song is just one of many Southeast University professors who has accepted funding from any of the three secretive funding programs for information security research. Dr. Jiang Rui (蒋睿), a three-time recipient of MSS 115 Program (国家

安全部 115) funding, is currently researching data protection technology for distributed machine learning systems on behalf of the Ministry of Public Security.[32] Other professors also received MSS 115 Program (国家安全部 115) or National 242 Information Security Program (国家 242 信息安全计划项目), but do not conduct ML-related cybersecurity research.

Another group of Southeast University faculty also research ML and cybersecurity, but do not appear to receive government funding for their research. Li Tao (李涛) focuses on smartphone security and vulnerabilities, and claims to research AI applications for cybersecurity, but has only listed one publication related to AI.[33] Qin Zhongyuan (秦中元) researches AI for malware classification and attack detection systems—both applications help defenders fortify networks.[34] Another professor, Yang Wang (杨望), invites student applicants to assist with his research on cyber threat intelligence, cyberattack attribution technologies, and security challenges for AI systems.[35] According to Yang's webpage, applicants for research positions should be familiar with machine learning, cybersecurity posture awareness technology, and threat intelligence modeling and analysis.[36] The requisite skills for applicants and declared direction for the research project—automated cybersecurity response (自动化安全响应)—suggests a focus on ML-based anomaly detection and threat attribution technologies.

Shanghai Jiao Tong University (上海交通大学)

Connections to the Security Services

The first murmurs of Shanghai Jiao Tong University's (SJTU) relationship with state-sponsored hackers date back as far as 2010. In an article published by *The New York Times*, unnamed military contractors provided evidence that someone at SJTU was conducting network operations against foreign targets, including Google and the U.S. government.[37] Three years passed before evidence of the relationship surfaced again.

In 2013, Mandiant published its ground-breaking APT1 report that named PLA Unit 61398 as an Advanced Persistent Threat to the U.S. government and non-Chinese companies. Based on the attribution of attacks to Unit 61398, investigative reporters at Reuters identified three computer science articles that SJTU academics co-authored with members of Unit 61398.[38] One of the academic authors implausibly claimed he was unaware of his co-author's ties to the PLA—insisting that the co-author was a graduate student—even though a military unit designation appeared next to the operator's name on the paper.[39] The technical articles demonstrated that the academics were directly contributing to research that could be used for network operations and were doing that research alongside people from military units carrying out those operations. The Reuters journalists also determined that SJTU's School of Information Security Engineering (上海交通大学信息安全工程学院) was co-located on an "Information Security Engineering Base" run by the PLA, establishing another clear connection between SJTU and the PLA. Following the DOJ indictments of Unit 61398 a year later, another report found that one of the hackers had used his university email address to register infrastructure used in a hacking campaign.[40] Rumors about SJTU and its connection to Chinese government cyber operations evolved into irrefutable facts over the four years from 2010 to 2014.

This report finds that the relationship between SJTU and state-sponsored hacking teams almost certainly continues today. The SJTU's Cyberspace Security Science and Technology Research Institute (上海交通大学网络安全技术研究院) stands out for its potential impact on cyber operations and as a vehicle for cooperation. The Network Confrontation and Information System Security Testing (网络攻防与信息系统安全检测) project works on "network and information system testing and evaluation, security testing for intelligent connected networks, APT attack testing and defense, and key cyber range technology."[41] Research priorities, like "APT attack testing and defense," explicitly state the intent to develop offensive and defensive technologies for APT (read: government-backed) cyber operations. Other enumerated areas of research include "password cracking, social engineering, and

creating active honeynets."[42] Password cracking and social engineering are used to gain unauthorized network access and are offensively oriented. While penetration testers can use these tactics against consenting organizations to improve their defensive posture, the institute makes no mention of providing such services. The most likely application is for offensive cyber operations. Additionally, SJTU hosts a few AI research organizations, including the AI Security Laboratory, whose mission is to increase the security and defenses of ML algorithms.[43]

Besides this research, the biographies of two professors stand out for their stated impact on the security services. Dr. Qiu Weidong's (邱卫东) research on AI and graphical processing unit optimization—a key component for training AI systems—led to the widespread adoption of his cryptographic techniques by "many core national security ministries," presumably including the security services.[44] Another professor, Dr. Chen Xiaohua (陈晓桦), served as the Executive Deputy Director (常务副主任)—likely second or third in the chain of command—of the national-level MSS 13th Bureau, known publicly as the China Information Technology Security Evaluation Center (CNITSEC), before becoming a professor.[45] Standard-setting cryptographical research and experience running a bureau of an intelligence service are good indicators of SJTU's reputation among cybersecurity professionals in China.

Research on AI/ML + Cybersecurity

Researchers at Shanghai Jiao Tong University published seven papers on using AI for defensive purposes over the last five years. Researchers published on defensive ML applications such as identifying malicious URLs[46], inspecting web traffic to identify botnets[47], attributing certain types of DDOS attacks[48], and a litany of specialized intrusion detection systems.[49] Other research topics have dual-use applications. One paper funded by the Ministry of Public Security researched the application of machine learning for static vulnerability analysis of software.[50] Vulnerability analysis finds weaknesses in software that can be patched by defenders or exploited by attackers; how vulnerabilities are used after their discovery is up to the user. Another paper proposed a machine learning model that could differentiate Tor web traffic from other

traffic—a tool that would allow a state with comprehensive surveillance and collection capabilities to isolate otherwise obscured internet connections; China has obvious incentives to use such a tool.[51] Other work sheds the veneer of dual-use research and benefits only attackers. A paper published in 2019 increased the accuracy of password guessing attacks by using a machine learning model to generate password attempts.[52]

In addition to the work of individual professors, the Network Confrontation and Information System Security Testing (网络攻防与信息系统安全检测) project, mentioned above, also conducts research on the use of AI and machine learning for computer network attack and defense. Though sourcing for this assertion is limited, the documents available speak volumes. The MSS 13th Bureau published an article by the director of the SJTU research institute in its Cyberspace Strategy Forum periodical.[53] The article considers the potential offensive and defensive applications of AI in computer network operations, as well as the vulnerabilities of AI systems themselves. In one section, the director—concurrently the director for the National Engineering Laboratory for Information Content Analysis Technology (信息内容分析技术国家工程实验室)—highlights using AI to repair software vulnerabilities, support network attack and defense, and find software vulnerabilities for exploitation in the malware development process.[54] The piece concludes by making two arguments. First, AI holds potential for defensive cybersecurity applications like intrusion detection, threat intelligence management, and the ability to construct intelligent-secure networks (构建网络安全智能模型). Second, it contends that further research on AI is the solution to AI's current vulnerabilities. The publication of the article by the MSS 13th Bureau demonstrates the service's interest in such capabilities and illustrates the deference it pays to the research and analysis of SJTU faculty.

Besides the publication, two other pieces of evidence point towards research on ML applications for cyber operations by the Cyberspace Security Science and Technology Research Institute. First, a recent job posting for a training program manager (培训业务主管) gave preference to applicants with a background in cybersecurity and a strong understanding of AI security.[55] Second,

the description of responsibilities for part of the program includes "AI-based vulnerability discovery and testing," the same offensive application the director noted in his article.[56] Taken together, the high-level publication on AI and cybersecurity in an MSS periodical, the job posting seeking applicants with a cross-disciplinary background, and the research institute's description of its own work provides strong evidence that researchers are working on AI for cyber offensive and defensive purposes. In light of one program conducting "APT attack testing and defense" and SJTU's past relationship with PLA cyber operators, it is reasonable to conclude such research could directly support state-sponsored hacking.

Xidian University (西安电子科技大学)

Connections to the Security Services

Guangdong ITSEC, a division of the MSS 13th Bureau and the managing organization for APT3, started working with Xidian University in 2017 to offer a jointly administered graduate program under the Network and Information Security School (网络与信息安全学院).[57] Xidian University awards degrees and handles admissions; Guangdong ITSEC facilitates hands-on education and pairs graduate students with MSS employees serving as mentors.[58] Together, Guangdong ITSEC and Xidian University graduate students pursue research projects that meet the "actual needs" (实际需求) of Guangdong ITSEC—solving technical problems to enable the MSS's work. The relationship between Guangdong ITSEC and Xidian University is unusual; not only is the jointly-administered degree a novel program, but the two institutions are located more than 1,000 miles apart. Xidian University's involvement may be explained by Guangdong ITSEC's collection priorities. APT3 changed its mission to targeting residents of Hong Kong in 2015.[59] Practicing offensive cyber skills on Hong Kongers is no different than an internship with the Ministry of Public Security since China considers Hong Kong to be an "internal affair." This is conjecture, however. There are no reports that Xidian University supported past operations and this is the first report establishing the university's relationship with the Guangdong ITSEC.

Xidian University students are not limited to just one division of the MSS 13th Bureau, however. The university also established a joint research laboratory and internship program with Shaanxi ITSEC in 2017. The two committed to "jointly launch information security assurance and posture evaluation services for China, Shaanxi Province, and Shaanxi's prefecture-level cities" among many other responsibilities.[60] Shaanxi ITSEC is not connected to any publicly known APT groups or hacking campaigns.

Xidian University's relationship with PLA information warfare units extends at least a decade. In 2011, Xidian University established a relationship with the 3PLA and 4PLA, both now under the PLA Strategic Support Force, when it constructed the Collaborative Innovation Center of Information Sensing and Understanding (信息感知技术协同创新中心).[61] This project was a continuation of its historic ties to the CCP—Mao Zedong established the forerunner to Xidian University in 1931.[62]

Research on AI/ML + Cybersecurity

Two Xidian University professors claim an affiliation with China's security services and are conducting research on AI and cybersecurity.

Dr. Zhang Yuqing (张玉清) joined Xidian University after having first served as the director of the National Computer Network Intrusion Prevention Center (国家计算机网络入侵防范中心主任), a government body tasked with securing computer networks, and serving as the Deputy Director of the National Engineering Experimental Laboratory for Technology to Prevent and Cure Computer Viruses (计算机病毒防治技术国家工程实验室副主任).[63] Zhang's research at Xidian is focused on network confrontation, vulnerability discovery and exploitation, and the intersection of AI and cybersecurity.[64] In his most recently published academic paper, Zhang and researchers from the National Computer Network Intrusion Prevention Center—his former employer—surveyed more than 200 papers on using AI for cybersecurity tasks.[65] The paper analyzed possible applications of ML for data mining, vulnerability discovery and exploitation, and automated patching of software vulnerabilities. Zhang and his colleagues determined that using AI

for automated vulnerability discovery was likely the most useful application and made recommendations for future research to overcome the technology's (2018) limitations at the time. The project would likely prove useful to one of its funders, the Unclassified Projects Program at the Key State Laboratory for Information Security (信息安全国家重点实验室的开放课题), which could use the research to inform grant distributions to other academics working on ML and cybersecurity. The actual impact of the report is unknown, however.[66]

A second academic, Dr. Yang Chao (杨超), has active connections to the security services and conducts research on AI applications for cybersecurity.[67] While at Xidian University, Dr. Yang has submitted more than 20 software vulnerabilities to China's National Vulnerability Database (CNNVD, 国家信息安全漏洞库)—a division of the MSS 13th Bureau. Fifteen of these received certification from the government as critical vulnerabilities, though most were apparently related to payment systems within China.[68] His work on cybersecurity earned him a national defense research project funded by the now-defunct PLA General Armaments Department Development Fund and a current "high-level consulting position" with the MSS 13th Bureau Xibei office.[69] Yang describes his research as including "data-driven AI intelligent cyber threat detection and [developing a] "hunter" defense system architecture; AI and big data analysis-based detection of malignancies in encrypted traffic; machine learning-based encrypted traffic (SSL, Tor, VPN, ShadowSocks) / private internet protocol recognition and investigation; data analysis and machine learning-based cyberspace virtual persona recognition, matching, and investigation."[70] Each of Yang's research topics tightly intertwines ML and cybersecurity and could be put to good use in his consulting position at the MSS 13th Bureau's Xibei office.

Academics at Xidian University without acknowledged or known ties to the security services are also conducting similar research. A paper focused on defensive research published in 2019 proposed and demonstrated using machine learning to classify malware samples based on patterns in behavior.[71] The resulting model could be used to detect attacks from new malware with behaviors similar to that of older, known malware. Research using machine learning

for behavioral detection of new attacks is a common theme in current research on AI and cybersecurity.[72] Another Xidian University paper from 2017 proposed a similar ML-based solution to classifying malware, though that research focused on overcoming inadequate training data.[73]

Other academics are conducting research on less defensive, more dual-use topics. An article from 2019 compared algorithms that conduct membership interference attacks on ML systems, an exploit that allows attackers to determine if a given piece of data was part of the model's training data.[74] For example, a membership interference attack on a facial recognition system may allow the attacker to determine if the system can identify a particular face.[75] Though the researchers qualified their research by demonstrating how to defend against such attacks, the paper concluded with examples of attacking commercially available algorithms to evaluate which data sets had been used to train targeted models.

Zhejiang University (浙江大学)

Connections to the Security Services

Zhejiang University is a highly-respected, internationally renowned school for cybersecurity studies. Unsurprisingly, the PLA vigorously recruited graduates of its program at the time Mandiant published its APT1 report in 2013.[76] A report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman found that Zhejiang University received funding from three secretive programs for information security research: China's National 242 Information Security Program (国家 242 信息安全计划项目), the Ministry of State Security 115 Program (国家安全部 115), and the National s219 Information Security Application Demonstration Project (国家 s219 信息安全应用示范工程).[77] The report also concludes that universities which received these funds were selected to conduct "sensitive research and development with information security and information warfare applications."[78]

Though never tied to a specific hacking campaign, this report finds that Zhejiang University has collaborated on research with members of the PLA SSF. Zhejiang University academics co-

authored a research paper with members of PLA Unit 61646 in 2018.[79] Also known as the Air Reconnaissance Bureau, Unit 61646 was originally organized under the PLA General Staff Department's 2nd Department and responsible for military intelligence until its reorganization in 2015-16.[80] The joint paper evaluated SM4, a then-common encryption protocol that played an "important role as a national encryption standard" in China.[81] Together, Zhejiang University academics and members of Unit 61646 concluded that SM4 encryption protocol is weak and easy to circumvent.

Research on AI/ML + Cybersecurity

Classes taught at, and research conducted by, Zhejiang University suggest the school's graduates are well prepared for jobs involving cyber operations, making them great recruits for China's security services and national champion companies alike. Indeed, the joint Zhejiang University-Fudan University team beat the team from Carnegie Mellon in the 2020 DEFCON Capture-the-Flag competition.[82]

Cybersecurity is not the only relevant area of focus at Zhejiang University, as the school is also teaching undergraduate students how to attack and defend AI/ML systems.[83] Under its Applied Security curriculum, Zhejiang University teaches AI-related courses including: Algorithm and Model Security, Backdoors in Models, Data Poisoning, Adversarial Example Attacks, Measures for Defending Against Adversarial Example Attacks, and Certifiable Security for AI (人工智能可证明性安全).[84] In addition, Zhejiang University's Applied Security program is conducting research on "malicious machine learning" (恶意机器学习).[85]

Each of these topics is central to protecting or attacking AI systems. Data poisoning attacks target the training data of a model; manipulating the inputs in such a way that the deployed system fails to function properly.[86] Undetected data poisoning attacks can slow the development of a system, increasing costs and undermining its functionality. Other vulnerabilities allow attackers to make models fail in specific, predictable ways. Backdoors in models allow for the attackers to designate a specific outcome given a certain trigger.[87] A backdoor attack against a

facial recognition model could allow anyone wearing a purple hat to be recognized as a particular person, for example. Defending against these types of attacks is critical for any organization or business integrating AI models into operations.

In the course of their degrees on cybersecurity, AI and information security at Zhejiang University, students pick up some government-focused skills along the way. The program offers courses on intelligence[88] entitled: “the evolution and definition of strategic intelligence, the relationship between induction and deduction in intelligence research, intelligence classification, and crafting [intelligence] reports."[89] Understanding the intelligence cycle and writing intelligence products is likely to be of little relevance to employees outside the national security sector. Combined with classes on AI vulnerabilities—which require familiarity with how systems can be attacked—the evidence suggests that Zhejiang University students are well-prepared for a job in the security services.[90]

Full-time faculty at Zhejiang University who teach AI/ML attack and defense classes are on the cutting-edge of research in the area. Dr. Ji Shouling (纪守领), an international participant on eight US National Science Foundation-funded research projects, recipient of the China’s 1000 Young Talents Program (2017) and the Zhejiang 1000 Talent Program (2016), has his own research institute at Zhejiang University which conducts research on AI for cybersecurity.[91] In an arrangement that typifies the issues of China’s talent programs, Ji simultaneously holds a research faculty position at Georgia Institute of Technology. One non-NSF paper published by Ji proposes a tool called “VulnSniper,” which uses neural networks to find new software vulnerabilities.[92] It is one example from dozens of papers published by Ji’s research program at Zhejiang University.

Dr. Yang Ziqi (杨子祺), another professor in the cybersecurity program, focuses his research on the attack and defense of AI systems. After receiving his doctorate from Singapore National University, Yang conducted research for the Singapore Cybersecurity Agency National Lab, Kaspersky Labs, and Huawei. Yang’s research on AI security includes model inversion,

membership interference, adversarial attack and defense, and backdoors in models.[93] Membership interference attacks pair well with Yang's other research into model inversion of commercially available facial recognition systems.[94] Together, these two techniques can determine whether a particular face is recognized by a targeted facial recognition system. Other applications of Yang's research include using AI to trace the origins of malware binaries based on information about the compiling author.[95]

In addition to full-time professors conducting research, Zhejiang University has hosted many guest lectures on attacking AI systems and defending their vulnerabilities. Topics from guest lecturers have included: Neural Network Inversion in Adversarial Settings[96], Attack and Defense of Deep Neural Network Models[97], Federated Learning-Oriented User Privacy Attacks[98], Data Set Inference and Reconstruction Attacks in Online Learning[99], and Stealthy Attacks Against Automatic Speech Recognition.[100] These attacks pose myriad problems for users of AI systems. Neural network inversions reveal technical details about the data used to train a specific model—potentially exposing sensitive or classified data used in training the model.[101] Other attacks, rather than exposing information, manipulate mundane systems to the attacker's advantage. The presentation on "Stealthy Attacks Against Automatic Speech Recognition" systems demonstrated how to embed secret commands in songs, which when played, can direct virtual assistants—like Google Home, Amazon Echo, or Apple's Siri—to perform certain tasks. Though research of this nature is common in cybersecurity, the relationship between Zhejiang University and China's cyber operators is uncommon. Moreover, a recent CSET report demonstrates how hard it is to defend AI systems—vulnerabilities are pervasive and defensive techniques are often only temporary patches.[102] As more organizations and governments deploy AI systems, the attack surface for such techniques will grow.

Harbin Institute of Technology (哈尔滨工业大学)

Connections to Security Services

The Mandiant APT1 report named Harbin Institute of Technology (HIT) as a recruitment center for Chinese cyber operators in 2013.[103] HIT is not alleged to have supported specific operations, though the university's ties to the military would make any such support unsurprising. As one of the Seven Sons of National Defense—a collection of universities with deep historical ties to the defense industry and PLA—HIT has received an institutional top-secret clearance to work on military projects.[104] HIT's cybersecurity school touts working on nine government-funded research projects, including research done on behalf of the now-defunct PLA General Armaments Department Key Laboratory Fund and the MSS, among other research funders.[105] Legacy webpages show many graduates of HIT's cybersecurity school from 2008 to 2014 went to work for the PLA's 54th Research Institute, formerly part of the General Staff Department's 4th Department (Electronic Intelligence, or ELINT), an organization folded into the PLA Strategic Support Force in 2015.[106] The U.S. DOJ indicted four members of the 54th Research Institute in 2020 for the 2017 Equifax hack.[107]

Research on AI/ML + Cybersecurity

Academics based at the Harbin Institute of Technology published few research articles on ML applications for cybersecurity or AI vulnerabilities. Instead, the vast majority of its faculty's publications (49 of 51) examined the application of AI to other fields, including a significant focus on the medical field. The two papers published on ML and cybersecurity rehashed recurrent themes in the field. One group of researchers built a machine learning model to detect and categorize software vulnerabilities.[108] The other publication proposed using AI to create an intrusion detection system based on behavior analysis.[109]

The relative scarcity of publications on ML and cybersecurity topics is surprising, given HIT's reputation as a cutting-edge cybersecurity school. It may well be the case that the university's

institutional top-secret clearance prevents the publication of such research. Another CSET report on China's defense technology workforce found that China's central government designated a Microsoft-HIT Artificial Intelligence and Machine Translation Joint Laboratory as a Key State Laboratory in 2006.[110] Moreover, the same report found that Microsoft Research Asia worked with HIT to create its computer science curriculum and provided training to professors in 2018 and 2019 on AI and natural language processing technology.[111] In fact, the presence of such international partnerships may be the reason that HIT shies away from publishing or even conducting such research.

But there are more indicators that HIT is performing, but not publishing, research on AI and cybersecurity. The Computer Application/Cyberspace Security Research Center, an affiliate of the cybersecurity school, conducts "research on key technologies in privacy-protecting machine learning."[112] Though the phrase is ambiguous, other sources use the same phrase when discussing the issue of ML model security.[113] Here, the description of HIT's research center denotes work on securing machine learning models from attacks that may divulge information from training data or other aspects of the model. To secure these models, researchers attack newly-developed defenses to test their efficacy. The acknowledgment of defensive research is also a tacit acknowledgment of offensive capabilities, though the attack methodologies used are not necessarily new or developed in-house.

Conclusions

Examination of China's AI/ML research and computer network operations to date demonstrates that six key universities play a major role in not only building technical competencies, but also in moving the research out of the lab and operationalizing it. Research currently conducted at these six universities demonstrates interest in both sides of the AI/ML and cybersecurity divide—ML-based offensive and defensive techniques, and the attack and defense of AI systems themselves. In addition to technical research from all six institutions, two of the schools published high-level strategic papers on the intersection of machine learning and cybersecurity. Xidian University's paper, funded by the Key State Laboratory for Information Security Unclassified Projects Fund, conducted a wide-ranging review of current (2018) research, determining machine learning could make a significant impact on vulnerability discovery and exploitation.[114] The conclusions of that paper were reiterated in an MSS publication written by faculty from Shanghai Jiao Tong University, where affiliated programs are conducting research on AI-based vulnerability discovery and "APT attack and defense."[115] The state of technical research in China is such that work on machine learning and computer network operations has moved from the research lab to strategic policy publications.

The close relationships between universities and the state shortens the path to operationalizing new techniques and provides the security services quick access to talented researchers. As nations and organizations deploy AI systems with unknown vulnerabilities, China's hacking teams will have new avenues of attack. Conversely, China's government and private sector will also seek to defend their own systems. Enhanced protection of China's computer networks and AI systems will be at least one outcome of conducting this research. Though research benefits both offensive and defensive applications, the relationships of these institutions with the security services augur the use of such knowledge in future hacking operations.

Author

Dakota Cary is a Research Analyst at the Center for Security and Emerging Technology.

Acknowledgments

For feedback and assistance, we would like to thank John Bansemer, Ben Buchanan, Scott Harold, Ben Murphy, Anna Puglisi, Helen Toner, Emily Weinstein, Ryan Fedasiuk, Benjamin Pollack, and Kady Arthur.

Document Identifier: doi: 10.51593/2020CA010

Endnotes

[1] Elsa Kania, "A Force for Cyber Anarchy or Cyber Order? —PLA Perspectives on 'Cyber Rules,'" *Jamestown Foundation*, July 6, 2016, https://perma.cc/LZA7-GATT.

[2] 浙江大学网络空间安全学院,"浙江大学网络空间安全学院本科生课程," accessed January 15, 2021, https://perma.cc/BW22-HXXB?type=image.

[3] IntrusionTruth, "Who Is Mr Gu?" *Intrusion Truth*, January 10, 2020. https://perma.cc/6GPX-JP3Q.

[4] 2015 conversion rate of approximately RMB 6.3 to USD 1.

[5] IntrusionTruth, "Who Is Mr Gu?"

[6] IntrusionTruth, "Who Is Mr Gu?"

[7] Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon, Ben Read, "APT40: Examining a China-Nexus Espionage Actor," *FireEye Blogs*, March 4, 2019. https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html.

[8] Evidence for each school's relationship with the security services are available in the Findings section of this paper.

[9] For example, the Beijing Institute of Technology posted a message of thanks to its Information and Electronics Program from the Ministry of State Security for their "significant contribution" to its work. (https://perma.cc/56S5-SB2E) In late 2020, the US Bureau of Industry and Security placed the school on its End-User list for acquiring technology for the PLA. Similarly, Sichuan University touts providing zero-day vulnerabilities to "relevant government ministries" on its homepage. (https://perma.cc/SQ3K-LZKQ) Small, ad-hoc contributions are likely the most common way universities support China's computer network operations. Still other schools' contributions fall somewhere between supplying vulnerabilities and setting up shell companies. Tsinghua University computers conducted network reconnaissance on US targets ahead of a trade meeting, but the university was not connected to a persistent campaign or entity. (https://perma.cc/2MZ4-Q87F) This one-off type of operation may be indicative of a professor moonlighting for extra income or a student trying to pad their resume for future jobs—such activity does not constitute an Advanced Persistent Threat.

[10] Elsa Kania, "A Force for Cyber Anarchy or Cyber Order?"

[11] Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage." *Foreign Policy*, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

[12] e.g. University websites, social media posts, files uploaded to file sharing sites, and academic publications accessible through the CNKI database.

[13] Reports of China's military hacking operations prior to 2016 refer to the Third General Staff Department (3PLA) as the military's cyber espionage department. The PLA SSF incorporated 3PLA into its structure in 2016. John Costello, "The Strategic Support Force: China's Information Warfare Service," *Jamestown Foundation*, February 8, 2016, https://perma.cc/8N9J-YFM8. China's civilian intelligence agency, the Ministry of State Security, conducts cyber operations through its 13th Bureau, which is known publicly as the China Information Technology Evaluation Center (CNITSEC). Peter Mattis identifies China Information Technology Evaluation Center (ITSEC) (中国信息安全测评中心) as the Ministry of State Security's 13th Bureau. The 13th Bureau is responsible for "research and development of investigative tools." Regional bureaus are adorned with their provincial name. Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis, MD: Naval Institute Press, 2019).

[14] Bureau of Industry and Security, "Entity List," Department of Commerce, accessed January 15, 2021, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

[15] IntrusionTruth, "Who Is Mr Gu?"

[16] 张晨，唐湘滟，程杰仁，董哲，and 李俊麒，"基于多核学习的自适应 DDoS 攻击检测方法，" 计算机工程与科学, no. 8 (2019): 7, http://www.cnki.com.cn/Article/CJFDTotal-JSJK201908007.htm.

[17] Ellen Nakashima, "Security Firm Finds Link between China and Anthem Hack," *The Washington Post*, February 27, 2015, https://perma.cc/37P3-3PSJ.

[18] ThreatConnect Research Team, "The Anthem Hack: All Roads Lead to China," ThreatConnect, February 27, 2015, https://perma.cc/ZNQ5-325G.

[19] ThreatConnect Research Team, "The Anthem Hack."

[20] ThreatConnect Research Team, "The Anthem Hack."

[21] ThreatConnect Research Team, "The Anthem Hack."

[22] Deep Panda may be associated with APT19, but this is not confirmed. The MITRE Corporation, "Deep Panda," MITRE ATT&CK, accessed January 15, 2021, https://perma.cc/VW5P-LJJV.

[23] ThreatConnect Research Team, “The Anthem Hack.”

[24] Bryan Krekel, Patton Adams, and George Bakos, “Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage” (U.S.-China Economic and Security Review Commission, March 7, 2012), 62, https://perma.cc/6RXN-XCQS; “宋宇波,” Southeast University, accessed January 15, 2021, https://web.archive.org/web/20201214160633/https://cyber.seu.edu.cn/_s303/syb1/list.psp.

[25] Krekel, Adams, and Bakos, “Occupying the Information High Ground,” 60-62.

[26] “科技部副部长黄卫考察网络通信与安全紫金山实验室,” Southeast University, accessed January 15, 2021, https://perma.cc/Q4XY-SKCK?type=image.

[27] “科技部副部长黄卫考察网络通信与安全紫金山实验室,” Southeast University.

[28] “关于成立网络空间安全学院实验室与重要场所安全自查自纠工作组的通知,” Southeast University, accessed January 15, 2021, https://perma.cc/37GN-8BTV?type=image.

[29] “中国信息安全测评中心博士后科研工作站招聘简章,” Southeast University, accessed January 15, 2021, https://perma.cc/Y34E-7PEK?type=image.

[30] “学院概况,” Southeast University, accessed January 15, 2021, https://perma.cc/4AFA-B7HB?type=image.

[31] “宋宇波,” Southeast University.

[32] “蒋睿,” Southeast University, accessed January 15, 2021, https://perma.cc/7UE9-NPEZ?type=image.

[33] “李涛,” Southeast University, accessed January 15, 2021, https://perma.cc/D6LP-A4BA.

[34] “秦中元,” Southeast University, accessed January 15, 2021, https://perma.cc/TG7P-2QTU.

[35] “杨望,” Southeast University, accessed January 15, 2021, https://perma.cc/MLF3-NPXB.

[36] “杨望,” Southeast University.

[37] John Markoff and David Barboza, “2 China Schools Said to Be Tied to Online Attacks,” *The New York Times*, February 19, 2010, https://perma.cc/9TA6-C8VV.

[38] Melanie Lee, “Top China College in Focus with Ties to Army’s Cyber-Spying Unit.” Reuters, March 24, 2013, https://perma.cc/NC96-EB7B.

[39] Lee, “Top China College in Focus.”

[40] Nicole Perlroth, “2nd China Army Unit Implicated in Online Spying,” *The New York Times*, June 9, 2014, https://perma.cc/6PFZ-NFHZ.

[41] “上海交通大学网络安全技术研究院招生信息，” 上海交通大学–网络安全技术研究院， accessed January 15, 2021, https://perma.cc/6AFP-9E5E?type=image; (基于人工智能的漏洞挖掘与检测，网络与信息系统检测评估，智能网联安全检测，APT 攻击检测与防护，网络空间靶场关键技术) Thanks to Ben Murphy for this translation.

[42] “”研究方向,” 上海交通大学–网络安全技术研究院, accessed January 15, 2021, https://perma.cc/P656-6W5R?type=image (密码破解、社会工程、主动诱捕).

[43] “人工智能安全,”上海交通大学网络空间安全学院, accessed January 15, 2021, https://perma.cc/3HQD-P52X?type=image.

[44] “邱卫东,” 上海交通大学网络空间安全学院, accessed January 15, 2021, https://perma.cc/EH2D-W8CW?type=image.

[45] “陈晓桦,”上海交通大学网络空间安全学院, accessed January 15, 2021, https://perma.cc/MAK6-W7QK?type=image.

[46] 潘司晨, 薛质, 施勇, et al., “基于卷积神经网络的恶意 URL 检测,” *通信技术*, no. 08 (2018): 1918–23, https://perma.cc/J36T-32UL. 李泽宇, 施勇, and 薛质. “基于机器学习的恶意 URL 识别,” *通信技术*, no. 2 (2020): 25, https://perma.cc/QC5W-CTFV.

[47] 周畅 and 黄征, “基于僵尸网络流量特征的深度学习检测,” *信息技术*, no. 4 (2018): 1, https://perma.cc/PTR9-V7FW.

[48] 李林森， 邹福泰， and 吴越, “基于深度学习的放大攻击归因技术,” *通信技术*, 2019, https://perma.cc/3ZEC-SG4B?type=image.

[49] 张涵, 薛质, and 施勇, “基于多层神经网络的 Webshell 改进检测方法研究,” *通信技术*, no. 1 (2019): 32, https://perma.cc/MA8K-UUFW.

[50] 夏之阳, 易平, and 杨涛, “基于神经网络与代码相似性的静态漏洞检测,” *计算机工程*, no. 12 (2019): 21, https://perma.cc/SV96-ZT43.

[51] 潘逸涵 and 张爱新, “基于深度学习的 Tor 流量识别方法,” *通信技术*, no. 12 (2019): 26, https://perma.cc/X6HJ-YEAX.

[52] 夏之阳 and 易平, "基于神经网络的多源密码猜测模型," *通信技术*, no. 1 (2019): 29, https://perma.cc/N5U4-AWGP. Researchers used a recurrent neural network to train GenPASS, a tool for brute-forcing password attacks more easily.

[53] 中国信息安全, 阿里云安全, and App 个人信息举报, "上海交大李建华：人工智能与网络空间安全," accessed January 15, 2021, https://perma.cc/7WSA-Q962.

[54] 基于人工智能的漏洞挖掘技术，同样也可以被用于软件的恶意攻击过程，还可以实现漏洞修复与攻防对抗.

[55] "电院网络安全技术研究院招聘项目聘用人员启事," 上海交通大学-网络安全技术研究院, accessed January 15, 2021, https://perma.cc/QQ8D-RTX4?type=image (网络空间安全、计算机相关专业背景者优先[...]对人工智能及系统安全有一定的了解).

[56] "上海交通大学网络安全技术研究院招生信息," 上海交通大学-网络安全技术研究院, accessed January 15, 2021, https://perma.cc/6AFP-9E5E?type=image (基于人工智能的漏洞挖掘与检测，网络与信息系统检测评估，智能网联安全检测，APT攻击检测与防护，网络空间靶场关键技术). Thanks to Ben Murphy for this translation.

[57] "广东省信息安全测评中心," 西安电子科技大学网络与信息安全学院, accessed January 15, 2021, https://web.archive.org/web/20200820145416/http%3A%2F%2Fce.xidian.edu.cn%2Finfo%2F1112%2F1492.htm.

[58] "广东省信息安全测评中心," 西安电子科技大学网络与信息安全学院"; Mattis and Brazil, *Chinese Communist Espionage: An Intelligence Primer*, 77; Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security behind APT3," Recorded Future, May 17, 2017, https://perma.cc/5LJS-5RHT.

[59] The MITRE Corporation. "APT3." MITRE ATT&CK, accessed February 12, 2021, https://attack.mitre.org/groups/G0022/.

[60] "陕西省网络与信息安全测评中心," 西安电子科技大学网络与信息安全学院, accessed January 15, 2021, https://perma.cc/XA2B-M8EG (共同开展面向国家、陕西省以及省内各地级市信息安全保障与态势评估服务工作). Thanks to Ben M for this translation. (A full translation of the agreement is available here).

[61] "中国建信息感知技术中心 打造中国版林肯实验室," GuanCha, accessed January 15, 2021, https://perma.cc/YXN9-2MV5?type=image .

[62] Edward Wong, "University in Xi'an Opens School of Cyberengineering," *The New York Times*, January 6, 2015.

[63] "张玉清," 西安电子科技大学, accessed January 15, 2021, https://perma.cc/47WD-5M3Y?type=image; https://perma.cc/RQV8-3FBK?type=image (国家计算机网络入侵防范中心主任, 计算机病毒防治技术国家工程实验室副主任).

[64] "张玉清," 西安电子科技大学.

[65] 孙鸿宇, 何远, 王基策, 董颖, 朱立鹏, 王鹤, 张玉清 et al., "人工智能技术在安全漏洞领域的应用," *通信学报* 39, no. 8 (2018): 1–17, https://perma.cc/YW8C-P2LC (http://www.infocomm-journal.com/txxb/CN/10.11959/j.issn.1000-436x.2018137).

[66] (信息安全国家重点实验室的开放课题(2017-ZD-01)).

[67] "杨超," 西安电子科技大学, accessed January 15, 2021, https://perma.cc/5EJM-QYUS?type=image. Thanks to Ben M for this translation. "西电教师个人主页系统–杨超," 西安电子科技大学, accessed January 15, 2021, https://perma.cc/XD3E-9PGY?type=image.

[68] Insikt Group, "China's Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers over Foreign Technology," Recorded Future, August 31, 2017, https://perma.cc/95CZ-QUL7.

[69] "杨超," 西安电子科技大学 (国家信息安全测试西北中心).

[70] "西电教师个人主页系统–杨超," 西安电子科技大学 (大规模异构数据驱动的 AI 智能网络威胁检测与"狩猎"防御体系架构、基于 AI 智能与大数据分析的加密流量恶意性检测、基于机器学习的密文流量 (SSL、Tor、VPN、ShadowSocks) /私有协议识别与审查、基于数据分析与机器学习的网络空间虚拟身份识别对应与审查、基于"云边协同"的安全大数据分析平台与系统等). Thanks to Ben M for this translation.

[71] 胡建伟, 车欣, 周漫, and 崔艳鹏, "基于高斯混合模型的增量聚类方法识别恶意软件家族," *通信学报* 40, no. 6 (2019): 148–59, https://perma.cc/B8H6-MZ2F (http://www.infocomm-journal.com/txxb/CN/abstract/abstract168753.shtml).

[72] "Behavioral detection of malware + machine learning," Google Scholar, accessed January 15, 2021, https://scholar.google.com/scholar?hl=en&as_sdt=0%2C34&q=behavioral+detection+of+malware+%2B+machine+learning&btnG=.

[73] 李兴华, 刘海, 钟成, and 马建峰, "基于半监督学习和信息增益率的入侵检测方案," *计算机研究与发展* 54, no. 10 (2017): 2255-2267, https://perma.cc/YP7Y-JFB3.

[74] 张鹏, 闫峥, and 周晓康, "机器学习训练数据集的成员推理综述," *网络空间安全* 10, no. 10 (2020): https://perma.cc/Z3XW-ZB7T.

[75] Ram Shankar, Siva Kumar, David O'Brien, Jeffrey Snover, Kendra Albert, and Salome Viljoen, "Failure Modes in Machine Learning," Microsoft, November 11, 2019, https://perma.cc/6SCH-KYAT.

[76]Mandiant, "APT1: Exposing One of China's Cyber Espionage Units " (FireEye, February 19, 2013), 11, https://perma.cc/AC3D-2VL4. "中国人民解放军 61398 部队招收定向研究生的通知," 浙江大学计算机科学与技术学院, accessed January 15, 2021, https://perma.cc/9AYT-5JF7?type=image (Zhejiang University Recruitment Event for PLA Unit 61398).

[77] Krekel, Adams, and Bakos, "Occupying the Information High Ground," 60–62.

[78] Krekel, Adams, and Bakos, "Occupying the Information High Ground," 60–62.

[79] 张帆, 黄静, 赵新杰, and 刘会英, "SM4 密码算法的踪迹驱动 Cache 分析," *密码学报* 5, no. 4 (2018): 430-441, http://www.jcr.cacrnet.org.cn/CN/article/downloadArticleFile.do?attachType=PDF&id=272.

[80] Peter Mattis and Elsa Kania, "Modernizing Military Intelligence: Playing Catchup (Part Two)," *Jamestown Foundation*, December 21, 2016, https://perma.cc/T62V-A47N.

[81] 张帆, 黄静, 赵新杰, and 刘会英, "SM4 密码算法的踪迹驱动 Cache 分析."

[82] "DEF CON® Hacking Conference - Capture the Flag Archive," DEFCON, accessed January 15, 2021, https://www.defcon.org/html/links/dc-ctf.html; "白洪欢," 浙江大学教师个人主页," accessed January 15, 2021, https://perma.cc/HQ2Y-KJ9H?type=image.

[83] Course catalogues for graduate students and doctoral candidates are unavailable, but likely share comparable content.

[84] "浙江大学网络空间安全学院本科生课程," 浙江大学网络空间安全学院, accessed January 15, 2021, https://perma.cc/BW22-HXXB?type=image. Thanks to Ben Murphy for this translation.

[85] "浙江大学网络空间安全学院科研方向," 浙江大学网络空间安全学院, accessed January 15, 2021, https://perma.cc/4LH5-34S4?type=image.

[86] Shankar et al., "Failure Modes in Machine Learning."

[87] Shankar et al., "Failure Modes in Machine Learning."

[88] Here, "intelligence" is related to intelligence agencies and the national security use of the term, not AI.

[89] “浙江大学网络空间安全学院本科生课程,” 浙江大学网络空间安全学院, accessed January 15, 2021, https://perma.cc/BW22-HXXB?type=image.

[90] Andrew Lohn, "Hacking AI" (Center for Security and Emerging Technology, December 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Hacking-AI.pdf.

[91] “Index - NESA - Network System Security & Privacy Lab,” NESAlab, accessed January 15, 2021, https://perma.cc/MP58-68X3?type=image.

[92] Yanjun Wu, Mutian Yang, Xu Duan, Jingzheng Wu, Zhiqing Rui, Shouling Ji, and Tianyue Luo, “VulSniper: Focus Your Attention to Shoot Fine-Grained Vulnerabilities,” *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence Main* track, 2019, 4665–71, https://perma.cc/T9KL-K8YG.

[93] “杨子祺,” 浙江大学个人主页, accessed January 15, 2021, https://perma.cc/S2PB-CGEJ.

[94] “杨子祺,” 浙江大学个人主页.

[95] “杨子祺,” 浙江大学个人主页.

[96] Ziqi Yang, “(学术报告)（CCS2019）Neural Network Inversion in Adversarial Setting,” 浙大网安, accessed January 15, 2021, https://perma.cc/9Q5B-MVMU?type=image.

[97] Ling Liu, “(学术报告) Robust Deep Learning Against Deception,” 浙大网安中心, accessed January 15, 2021, https://perma.cc/V5UT-284L?type=image.

[98] 王志波, “(学术报告)面向联邦学习的用户隐私攻击,” 浙大网安中心, accessed January 15, 2021, https://perma.cc/YP7W-WA76?type=image.

[99] “(学术报告) Updates-Leak: 在线学习中的数据集推理和重建攻击,” 浙大网安中心, accessed January 15, 2021, https://perma.cc/Z5UY-4R2S?type=image.

[100] “(学术报告)机器学习应用中的安全问题,” 浙大网安中心, accessed January 15, 2021, https://perma.cc/4VMC-WR3N?type=image.

[101] Shankar et al., “Failure Modes in Machine Learning.”

[102] Lohn, "Hacking AI."

[103] Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units.”

[104] Alex Joske, “The China Defence Universities Tracker” (Australian Strategic Policy Institute, November 25, 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

[105] “科研项目,” 哈尔滨工业大学（深圳）计算机科学与技术学院, accessed January 15, 2021, https://perma.cc/TU2K-MWA8?type=image; Krekel, Adams, and Bakos, “Occupying the Information High Ground," 60–62; National 242 Information Security Program (国家 242 信息安全计划项目), Ministry of State Security 115 Program (国家安全部 115), and the National s219 Information Security Application Demonstration Project (国家 s219 信息安全应用示范工程).

[106] “毕业硕士,” 计算机应用研究中心, accessed January 15, 2021, https://perma.cc/UA6D-DFAD?type=image; Bureau of Industry and Security, “Entity List”; Mattis and Kania, “Modernizing Military Intelligence.”

[107] Department of Justice Office of Public Affairs, “Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax,” U.S. Department of Justice, February 10, 2020, https://perma.cc/47CQ-R3EM.

[108] 何金虎, 吴翔虎, and 曲明成, “基于迁移学习的软件缺陷预测算法研究.” *智能计算机与应用*, no. 5 (2019): 93, https://perma.cc/597L-XNGJ.

[109] 曹为政 and 葛蒙蒙, “多模式匹配算法研究和优化,” *智能计算机与应用* 8, no. 2 (2018): 129–33, http://www.cqvip.com/qk/94259a/201802/675154861.html.

[110] Ryan Fedasiuk and Emily Weinstein, “Universities and the Chinese Defense Technology Workforce” (Center for Security and Emerging Technology, December 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Universities-and-the-Chinese-Defense-Technology-Workforce.pdf.

[111] Fedasiuk and Weinstein, “Universities and the Chinese Defense Technology Workforce.”

[112] “哈尔滨工业大学（深圳）网络空间安全研究中心/计算机应用研究中心面向全国高校招收 2020 年入学硕士生/博士生,” 计算机应用研究中心, accessed January 15, 2021, https://perma.cc/9RLC-6YVN?type=image; (隐私保护机器学习关键技术研究) Thanks to Ben Murphy for this translation.

[113] The previously mentioned publication by the research institute director at Shanghai Jiao Tong University, for example.

[114] 孙鸿宇, 何远, 王基策, 董颖, 朱立鹏, 王鹤, 张玉清 et al., “人工智能技术在安全漏洞领域的应用,” *通信学报* 39, no. 8 (2018): 1–17, https://perma.cc/YW8C-P2LC (http://www.infocomm-journal.com/txxb/CN/10.11959/j.issn.1000-436x.2018137).

[115] “上海交通大学网络安全技术研究院招生信息,” 上海交通大学-网络安全技术研究院, accessed January 15, 2021, https://perma.cc/6AFP-9E5E?type=image.