西安交大教授沈超：

數字識別我是誰

攻防雙向護私隱

沈超，男，漢族，1985年9月生，西安交通大學教授，現任網絡空間安全學院副院長，國家自然基金委「優青」，參與中國科技部網絡空間安全創新指南、網絡與信息安全學科「十四五」戰略規劃等編制工作。

研究聚焦網絡空間安全技術領域，在信息物理系統安全和可信人工智能技術等方面持續開展創新研究，主持國家重點研發計劃課題、中國國家自然科學基金、國防預研重點項目等30餘項，申請與授權發明專利20餘項，研發的安全產品應用於800餘家政府和企事業單位。在國內外權威刊物上發表SCI等論文70餘篇，榮獲7次學術會議最佳/優秀論文獎，擔任7個國際期刊副主編或編委、20多個學術會議程序委員會主席或成員。

一次揮手，一個微笑，生活中這些不經意的小動作，在人工智能高速發展的今天，有可能成為洩露私隱的漏洞。「這並不是天方夜譚，這種竊取手法不僅簡單、快速，而且還很廉價。而我的工作就是想方設法去阻止它。」作為一名年輕的中國科研工作者，深耕數字世界十餘載的西安交通大學網絡空間安全學院副院長沈超，原創性地提出基於人機交互行為分析即「行為數據驅動」的新型身份識別理論和技術，而立之年便已成為全球業界公認的智能系統青年精英。

他既是數字世界信息安全的「守護者」，也是行業赫赫有名的頂尖「獵手」，既要防禦，也要出擊。沈超笑稱，這就如同是左右互搏，看似矛盾，但卻是實現信息物理融合系統可信計算和安全應用的最有效手段。 ■香港文匯報記者 李陽波 西安報道

■沈超（右）與團隊在實驗室一起探討技術上遇到的問題。 香港文匯報記者李陽波 攝

互聯網業界曾有這樣一句話，網絡世界沒有絕對的安全，只有此消彼長的過程。

2014年，沈超完成在美國的深造後回到母校，面對自己最為熟悉的網絡安全領域，沈超倍感壓力。「雖然當時我國互聯網及電商發展一日千里，但大家的安全意識卻極為薄弱。」沈超透露，彼時通過對幾千萬密碼樣本分析發現，超過60%的密碼都是12345或ABCDE類似的簡單形式，而很多手機用戶設置的密碼手勢也僅僅是簡單的「Z」或者「L」圖形。「這樣的密碼形同虛設，隱私安全根本無從保障。」

數字密碼暗藏隱患，那麼人臉識別和指紋驗證總該安全了吧？沈超給出的答案同樣是不。

「2013年，德國國防部長在一次會議中僅僅因為招了招手，便被記者利用高清攝像機提取了指紋。而人臉識別更容易蒙混過關。」沈超表示，在這樣的背景下，「數字身份識別」就成為保證用戶數據和隱私安全的關鍵。「數字世界中的數字身份識別是物理身份與數字身份的相對應，通過數字身份識別可有效保障隱私數據安全、極大降低客戶接入成本、顯著降低詐騙率，以提高互聯網的經濟價值。」

捕捉動態細節 精準識別身份

在此之前，縱觀全球業界，也很少有人深度涉及數字身份識別領域，在很多技術和理論層面都是空白。「數字身份識別中最基本的一個問題，就是人們需要用這個技術來證明『自己是誰』。」面對這一世界性的難題，沈超和團隊從一開始，逐層深入，原創性地提出了基於人機交互行為分析的新型身份識別理論和技術，填補了人機行為理解、人機行為身份建模、身份主動識別等方面的研究空白。

具體來說，在此基礎上建立的數字身份識別系統，相較五六年前的識別系統，通過對指紋、人臉的動態細微變化即「行為數據」的捕捉和識別能力，有了質的飛躍。

通俗地講，就是以用戶發出的「行為」作身份載體，通過分析和採集用戶在人機交互過程中所展現出的行為動態特徵，比如指紋、人臉、語音等，建立起多平台、多場景的通用人機行為數據庫，使信息物理系統更智能、更可靠，最終實現機器對用戶身份的精準識別。

在圓滿解決「自己是誰」的難題之後，針對IT信息系統、移動互聯網、互聯網金融等4個典型應用環境，沈超團隊研發了多個適用於多場景多終端的人機行為身份認證與監控系統，並在大型企事業單位進行了成功的應用。相比原有手段的數據安全保護性能提高了約2倍以上，為約3億用戶提供了服務，並極大地降低了客戶接入成本以及系統運營成本。此外，幾年來，沈超及其團隊還率先提出並驗證了行為數據驅動的身份安全防護技術，構建了當前最大規模的行為安全數據庫，形成具有自主知識產權的人機行為認證與系統安全分析工具，研發出網絡信息安全監控與防衛系統。這些成果被20多家國內外研究單位、800餘家政府部門和企事業單位採用，服務了近10億用戶。

信息安全知多點

Q：密碼如何設置才安全？

沈超：從技術上講，網絡世界沒有絕對的安全，但也不必過分驚慌。

首先，密碼設置不要過於簡單，盡量使用數字+子母+字符等組合密碼；

其次，密碼設置盡量不要和生日、姓名、年份掛鈎，多個賬戶不要使用同一密碼；

第三，不要在無法辨別的地方輸入自己的密碼。

最後，如果實在不放心，那就經常更改密碼。

Q：如何防止App過度收集個人信息？

沈超：App違法違規收集個人信息，主要表現為存在強制授權、過度索權、超範圍收集個人信息等。

一方面，不要隨意下載和使用陌生App，慎用一鍵授權，一定要仔細閱讀涉及個人隱私內容（如通訊錄、短信等）的權限獲取申請。

另一方面，不要隨便掃描陌生人發來的二維碼和陌生鏈接，不要隨意連接免費WiFi。

「用一生為母校作貢獻」

「今天真是太忙了，實在不好意思。」35歲的沈超給人的第一印象就是一個字：忙。回憶起自己在西安交大一路走來的這17年，沈超坦言或許正是這種忙碌才成就了自己。「其實本科我學的是自動化專業，直到大三時偶然的一次見習才將我和網絡信息安全綁在了一起。」2006年，沈超作為見習生進入中科院院士管曉宏牽頭組建的「智能網絡與網絡安全教育部重點實驗室」，或許當時連沈超自己都沒想到，第一次接觸便就此改變了他的人生軌跡。

2011年，經實驗室和課題組推薦，沈超前往美國卡內基梅隆大學學習。「這所大學在計算機科學與技術領域排名全球第一，所以我非常珍惜這次機會。」在美期間，沈超總是把自己的時間安排得滿滿的，幾乎每個夜晚都是坐最後一班校車離開。而在研究最為關鍵的時候，他索性買了個睡袋，太困就直接睡在實驗室地上。2014年完成學業後，沈超放棄了國外較為優越的待遇，毅然回國。「我希望用自己的一生為母校作貢獻。」

除了科研，沈超最喜歡的便是他的教師身份。「我的課堂上，學生才是主角，他們自主設計實驗、自己動手解決問題、自主思考形成思路，有時我甚至會空出半個小時，讓他們上台自己講。而我只是一個引導者。」沈超有點「小清新」式的教學，也讓他的課備受學生歡迎。

自2014年擔任本科生班主任以來，沈超結合自己的研究專長陸續開設主講了《網絡與信息安全》等課程，「我也經常會邀請國外包括香港高校在內的很多專家朋友，線上給學生們講課。」沈超坦言，自己最擔心的就是課堂上的學生與社會實際脫節脫鈎。「我不僅要將課堂變成學生主宰的實踐場合，活學活用，將書本內容轉變成實用知識。同時通過國外專家的授課，讓學生們始終站在國際學科的最前沿，放眼世界，方能大有作為。」對於學生們的作業，無論是學術論文還是科研報告，沈超都會逐字逐句進行批改，「因為這不僅是學生的心血，更預示着他們的未來。」

特稿

「挑刺」讓AI系統更聰明

「其實人工智能更像是一把雙刃劍，給生活帶來便利的同時也帶來很多隱患，用好利己，用不好損己。」對沈超而言，給人工智能「挑刺」幾乎成爲他的日常。「我的目的只有一個，那就是希望這把雙刃劍，永遠不會展現出它傷人的一面。」

沈超在研究中發現，現在所有的人工智能系統幾乎都是基於數據訓練得到的，不僅容易產生不公平的現象，同時也容易被愚弄和欺騙。「比如，一對小夫妻需要網貸，往往都是丈夫去操作，此時系統通過分析會得出男性缺錢的概念，學習和記憶之後，就會做出放寬男性貸款，收緊女性貸款的誤判。」沈超指出，再比如一幅貓畫，如果你稍微加上一些狗的因素，人工智能系統就會識別成狗。「所以我一方面需要去不停地主動出擊，給人工智能系統『挑刺』、糾偏、查找漏洞和隱患；一方面要進行防禦，補漏補缺，提高系統的感知，讓機器更『聰明』，讓入侵者無機可乘。」

2020年12月10日，沈超入選《麻省理工科技評論》2020年中國區「35歲以下科技創新35人」榜單，組委會評價其致力於智能系統的行爲感知和可信計算，實現在對抗環境下智能系統的安全可靠和可信計算。「目前我們的技術和成果國內領先，國際上與歐美相比也不落下風。」沈超坦言，雖然與歐美技術水平相當，但總體來看，中國網絡信息安全領域總體力量還甚爲薄弱。「歐美國家和企業每年投入巨資，匯聚大批科學家進行夜以繼日研發，我們也必須要跟得上世界的步伐。」

沈超表示，希望今後網絡信息安全領域能多一些同道者，甚至是競爭者。「我衷心希望能有更多的朋友們加入，大家一起攜手，築牢網絡安全之基，爲國家和民衆信息安全構築最強大『防護牆』。」

■沈超教授與團隊討論。受訪者供圖