



FROM QTFY TO FUDAN

THE PART THEY CAN'T SEIZE

In August the Justice Department shut down two Chinese hacking platforms that had been in commercial service for eight years. It took three domain names. The report follows the commercial and institutional structures that remain beyond the seized domains.

BY NATHAN WALKER

THE REPORT

WHAT THE SEIZURE ACTUALLY EXPOSED

In August the Justice Department shut down two Chinese hacking platforms that had been in commercial service for eight years. It took three domain names. The report follows the commercial and institutional structures that remain beyond the seized domains.

43

BUREAUS I-SOON SOLD TO
ACROSS 31 PROVINCES

200+

BREAK-IN SCRIPTS
IN QSCAN'S LIBRARY

ABOUT

600

ORGANIZATIONS REACHED
BY SALT TYPHOON

97%

31 OF 32 STUDIED
CHINESE-APT CVEs; U.S.
PUBLISHED BEFORE CNNVD

REPORT SEQUENCE

I	THE SHUTDOWN	THREE DOMAIN NAMES, HARD-CODED	03
II	WHAT THE COMPANY SOLD	QSCAN, QTROUTER, AND THE DOORS	05
III	WHO ELSE WAS IN THE ROOM	SALT TYPHOON, I-SOON, CNITSEC	07
IV	WHERE THE PEOPLE COME FROM	973, DUAL-USE RESEARCH, LEXBELL	11
V	THE BUILDER	CHOI, NANJING, FUDAN, FORTINET	14
VI	WHAT CAN'T BE SEIZED	THE PART WITH NO ORG CHART	23

SIX FIGURES, PRINTED LANDSCAPE

GRAPHIC 01	What was sold, and what was seized	04
GRAPHIC 02	Eight years of picking the same kind of lock	06
GRAPHIC 03	One company's address book	10
GRAPHIC 04	One funding instrument, two generations	13
GRAPHIC 05	Choi: authority and cross-border infrastructure	18
GRAPHIC 06	Ming Hsieh: federal biometrics, Fudan, Fortinet	22

NUMBERED NOTES APPEAR THROUGHOUT THE REPORT. THE COMPLETE REGISTER, WITH FULL URLS PRESERVED IN PLAIN TEXT, BEGINS ON PAGE 25.

PHOTOGRAPHS CARRY THEIR CAPTION AND SOURCE BENEATH THE IMAGE.

SECTION 1

THE SHUTDOWN

On the morning of August 26, at the request of federal prosecutors in San Diego, three internet registrars locked a set of domain names and redirected them to servers belonging to the FBI.¹



Department of Justice headquarters, Washington. Prosecutors in the Southern District of California obtained the orders that sent qt-team.com, qt-proxy.org and qtproxy.xyz to FBI servers on the morning of 26 August 2026.

PHOTOGRAPH APK • CC BY 4.0 • WIKIMEDIA COMMONS

The names — qt-team.com, qt-proxy.org and qtproxy.xyz — were not websites anyone visited. They were the addresses a piece of Chinese hacking software checked when it needed instructions, and the addresses it consulted to confirm a customer had paid for access. Redirect them and the software keeps running, keeps calling home, and reaches nobody.

No one was arrested that day and no indictment named anyone. The government asked a court for three domain names, got them, and two platforms that had

been in continuous commercial service since 2018 stopped working.

The platforms were called QScan and QTRouter. The company that built and ran them was registered in Nanjing in 2018 as Nanjing Xinjiuwei Network Technology — XJW — and U.S. agencies track its personnel under the name QTfy. The Justice Department says the paying customers included China's Ministry of State Security, the country's principal civilian intelligence service, and the People's Liberation Army.¹

Over eight years, according to the advisory the FBI, the National Security Agency and the Cyber National Mission Force published the same day, the platforms were used against NASA, the Federal Reserve, the Departments of Energy, Justice, and Health and Human Services, the National Institutes of Health, and the U.S. Senate.¹ The longer list in the advisory runs through defense contractors, telephone and internet carriers, semiconductor firms, hospitals, power companies, water utilities, universities and state election systems — the last of those approached without success in July 2019 and again in June 2026.² The FBI had been working the case since 2019.³

Taking the domains removed two products from a market that has other suppliers. The most useful material in the advisory is not the malware analysis but a section near the back, listing the other companies and government offices XJW did business with.

NOTES

- ¹ U.S. Department of Justice, "Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure," 26 Aug. 2026.
- ² FBI, National Security Agency and U.S. Cyber National Mission Force, Joint Cybersecurity Advisory, 26 Aug. 2026, TLP:CLEAR.
- ³ Greg Otto, "Officials disrupt Chinese espionage operation that hit multiple federal agencies," CyberScoop, 26 Aug. 2026.

QTFY: WHAT WAS SOLD, AND WHAT WAS SEIZED

State customers, a private operator, two complementary platforms, borrowed infrastructure – and one shared dependency that ended it.

01 / PLATFORM ARCHITECTURE

LAYER 01

STATE CUSTOMERS

MINISTRY OF STATE SECURITY · PEOPLE'S LIBERATION ARMY

IDENTIFIED BY DOJ

The Justice Department names both as paying users of the seized platforms. The MSS is China's principal civilian intelligence service.

LAYER 02

COMMERCIAL OPERATOR

NANJING XINJIUWEI NETWORK TECHNOLOGY – XJW / QTFY

REGISTERED 2018 · NANJING

Also tracked as QT and QTCYBER. Staff include former People's Liberation Army personnel who leveraged those contacts for critical-infrastructure contracts, traded in China's freelance exploit-brokering networks, and competed on the offensive side of the domestic HW/HVV exercises.

LAYER 03

TWO PLATFORMS

QSCAN · DISTRIBUTED SCANNING AND EXPLOITATION

FIND THE UNPATCHED DOOR

- More than 200 proof-of-concept exploits written in Python
- More than two million tasks in a single day, 2024
- Crawls pages, harvests TLS certificates, enumerates subdomains, fingerprints plugins – then breaks in

QTRouter · TRAFFIC OBFUSCATION

ARRIVE FROM NEXT DOOR

- Custom OpenWrt firmware on captured consumer routers
- Chained through the Clash proxy framework
- Mixes compromised devices with commercial proxies and leased cloud, so traffic looks residential and local to the target

LAYER 04

BORROWED INFRASTRUCTURE

COMPROMISED IOT · COMMERCIAL PROXIES · LEASED CLOUD

QSCAN SUPPLIED · QTRouter CHAINED

Replaceable by design. Any one node could be lost without ending the service – which is precisely why the seizure did not target them.

LAYER 05

VICTIMS

NASA · FEDERAL RESERVE · DOE · DOJ · HHS · NIH · U.S. SENATE

DOJ-NAMED · 2019-2026

The joint advisory's wider target set: cleared defence contractors, telecommunications carriers, semiconductor firms, hospitals, power companies, water utilities, universities, local government – and state election systems, approached without success in July 2019 and again in June 2026.

02 / SHARED DOMAIN DEPENDENCY

HARD-CODED INTO THE MALWARE ITSELF

qt-team[.]com

Earlier QScan task and result messaging; QTRouter jump infrastructure.

qt-proxy[.]org

Current QScan task and result messaging; QTRouter jump infrastructure.

qtproxy[.]xyz

QTRouter administration, node lists and platform authentication.

COURT-AUTHORISED · SOUTHERN DISTRICT OF CALIFORNIA · 26 AUG 2026

REGISTRY LOCK + DNS REDIRECTION

All three control domains were redirected to FBI-designated servers. No arrests. No indictment. No defendants named in open court.

3

DOMAINS SEIZED

200+

PYTHON EXPLOITS

2M

TASKS IN ONE DAY

8

YEARS 2018-26

SOURCES: DOJ OFFICE OF PUBLIC AFFAIRS, 26 AUG 2026 · U.S. ATTORNEY'S OFFICE, SOUTHERN DISTRICT OF CALIFORNIA · FBI / NSA / U.S. CYBER NATIONAL MISSION FORCE JOINT CYBERSECURITY ADVISORY, 26 AUG 2026 (TLP:CLEAR)

SECTION 2

WHAT THE COMPANY SOLD

Q Scan did the finding. It held a library of more than two hundred break-in scripts written in Python, each built to exploit a specific published flaw in a specific product, and it ran them at a scale that is difficult to picture: on one day in 2024, customers pushed more than two million scanning and testing jobs through it.² It crawled websites, collected encryption certificates, guessed at hidden subdomains, identified which plugins a site was running, and when it found something unpatched, it broke in.

QTRouter did the hiding. Its operators wrote their own version of OpenWrt — the open-source software that runs inside consumer internet routers — and installed it on machines they had taken over. Those routers were chained together with rented commercial proxy services and leased cloud servers, so that traffic arriving at an American network appeared to come from an ordinary residential connection nearby rather than from an office in Nanjing.²

The list of products QTFY attacked shows the pattern. Pulse Secure. Fortinet. Citrix. Microsoft Exchange. F5. Kentico. Log4j. Atlassian Confluence. Ivanti. Check Point. CrushFTP. BeyondTrust.² Almost every one of them does the same job: it sits at the edge of a network and lets authorized people in from outside. A VPN appliance is the door an employee uses from home. A file-transfer server is the door a contractor uses to send drawings. A remote-support tool is the door the help desk uses to reach your laptop. Each of these is a lock on a door the owner installed on purpose.



A Fortinet FortiGate 6501F. Appliances of this class — the network edge — make up most of the QTFY exploitation record. CVE-2018-13379, in Fortinet's FortiOS SSL VPN, entered that record in October 2019.

PHOTOGRAPH PREMEDITATED · CC BY-SA 4.0 · WIKIMEDIA COMMONS

The company also kept pace with public disclosure. In August 2019 it used a flaw in Pulse Secure's VPN software against the Justice Department, the Federal Reserve and NASA. In December 2021 it was exploiting Log4Shell within weeks of that vulnerability becoming public. In May 2024 it used a flaw in Check Point's gateway product to take data from more than three hundred organizations worldwide. In September 2024 it was using three flaws in Ivanti's software for which no patch yet existed. The most recent exploit in that product list is February 2026 — a flaw in BeyondTrust's remote-support product, used against a state government and an American water district. The advisory's activity record runs later still, into March and June 2026.²

A company that can do this is reading the same vulnerability disclosures as every network defender on earth and turning them into working tools faster than defenders can install the fixes, which describes a supplier rather than a spy service. The advisory goes on to describe the rest of the supply chain.

NOTES

² FBI — see register

EIGHT YEARS OF PICKING THE SAME KIND OF LOCK

Almost every product in the federal QTFY record does one job: it sits at the edge of a network and lets authorized people in from outside.

01 / EXPLOITATION RECORD, BY YEAR

2019

VPN AND REMOTE ACCESS

AUGUST 2019 PULSE SECURE VPN CVE-2019-11510 Used against the Justice Department, the Federal Reserve and NASA.	OCTOBER 2019 FORTINET FORTIOS SSL VPN CVE-2018-13379 No target named in the advisory's timeline.
---	---

2020–21

ENTERPRISE AND NETWORK
EDGE

JAN 2020 CITRIX ADC / GATEWAY CVE-2019-19781 Numerous U.S. targets.	MAR 2021 MICROSOFT EXCHANGE CVE-2021-26855 ProxyLogon.	JUL-AUG 2021 F5 BIG-IP CVE-2020-5902 State government and a retailer.	AUG 2021 KENTICO CMS CVE-2019-10068 A U.S. telecommunications company.	DEC 2021 LOG4J / LOG4SHELL CVE-2021-44228 Exploited within weeks of public disclosure.
--	---	--	---	---

2023–24

GATEWAYS AND MANAGEMENT

OCT 2023 ATLASSIAN CONFLUENCE CVE-2023-22515 Exploit used by QTFY.	MAY 2024 CHECK POINT QUANTUM GATEWAY CVE-2024-24919 Power and telecom scanning; data exfiltrated from more than 300 organizations worldwide.	SEPT 2024 · ZERO-DAYS IVANTI CLOUD SERVICES APPLIANCE CVE-2024-8190 · 8963 · 9380 DOE labs · NIH · HRSA · a security-device manufacturer. No patch existed.
---	---	--

2025–26

FILE TRANSFER AND
REMOTE SUPPORT

APRIL 2025 CRUSHFTP CVE-2025-31161 Exploited at a U.S. biotechnology company.	FEBRUARY 2026 BEYONDTRUST REMOTE SUPPORT CVE-2026-1731 A state government and a U.S. water district.
--	---

02 / PRODUCT CATEGORY

A VPN APPLIANCE The door an employee uses from home.	A FILE-TRANSFER SERVER The door a contractor uses to send drawings.	A REMOTE-SUPPORT TOOL The door the help desk uses to reach your laptop.	A GATEWAY OR FIREWALL The door the whole organisation is behind.
--	---	---	--

03 / FORTINET – TWO ADVISORY RECORDS

TWO SEPARATE ADVISORY RECORDS

QTFY RECORD · OCTOBER 2019
FORTIOS SSL VPN
CVE-2018-13379 appears in the QTFY exploitation timeline. The same flaw was used by effectively every significant state and criminal actor of that period.

SAME VENDOR · SEPARATE ADVISORIES

SALT TYPHOON ADVISORY · 2025
FORTINET FIREWALLS
Cisco, Ivanti, Citrix and Palo Alto appear in the same advisory.

Listed among additional devices those operators may target. The advisory's emphasis is on internet-facing edge devices and compromised routers generally.

12
PRODUCTS
IN THE
FEDERAL
RECORD

300+
ORGS
BREACHED
IN
ONE
CAMPAIGN

3
ZERO-DAYS
IN A
SINGLE
MONTH

SOURCES: FBI / NSA / U.S. CYBER NATIONAL MISSION FORCE JOINT CYBERSECURITY ADVISORY, 26 AUG 2026 · DOJ OFFICE OF PUBLIC AFFAIRS, 26 AUG 2026 · CISA AND INTERNATIONAL PARTNERS, SALT TYPHOON JOINT ADVISORY, 27 AUG 2025

SECTION 3

WHO ELSE WAS IN THE ROOM



As of June 2026, the advisory says, XJW had business relationships with two units of the Ministry of State Security, with a regional branch of China's national vulnerability agency, and with at least four other private security firms.²

MSS Unit 0718. XJW did business with it. So did a company called Sichuan Zhixin Ruijie Network Technology, which U.S. and allied agencies associate with Salt Typhoon.²

Salt Typhoon is the operation that got inside American telephone and internet backbones and stayed there. In August 2025 thirteen countries signed a joint advisory describing a worldwide campaign against the routers that carry traffic between carriers and their customers, reaching telecommunications, government,

transport, hotel and defense networks.⁴ Reporting at the time put the total near six hundred organizations, including roughly two hundred American companies across eighty countries.⁵ That advisory named three Chinese firms working for the MSS. One, Sichuan Juxinhe, had been sanctioned by the Treasury Department in January 2025. Another was Sichuan Zhixin Ruijie.⁶

The earlier public record placed QTFY in the general neighborhood of Salt Typhoon. The 2026 advisory places it in the same client's address book as a named Salt Typhoon contractor, one intelligence unit apart.

MSS Unit 9086, in Guangxi. XJW did business there too. In 2019, Unit 9086 held contracts with a company called i-Soon.²



A server rack, photographed by the FBI. XJW's business relationships as of June 2026 run to two units of the Ministry of State Security, a branch of China's national vulnerability agency, and at least four other private security firms.

PHOTOGRAPH FEDERAL BUREAU OF
INVESTIGATION · PUBLIC DOMAIN ·
WIKIMEDIA COMMONS

NOTES

² FBI — see register

⁴ CISA, NSA, FBI and international partners, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," 27 Aug. 2025.

⁵ "13 countries warn against China's Salt Typhoon group in joint advisory," SC Media, Aug. 2025.

⁶ Kevin Collier, "China used three private companies to hack global telecoms, U.S. says," NBC News, Aug. 2025.

i-Soon is the one the public already got to read. Its internal files leaked in February 2024 and exposed the working economics of China's hacking-for-hire market in the vendor's own spreadsheets. In March 2025 the Justice Department charged twelve people connected to it. According to those charges, i-Soon billed the Ministry of State Security and the Ministry of Public Security between \$10,000 and \$75,000 for each email inbox it successfully broke into, and sold the results to at least 43 separate government bureaus across at least 31 provinces and municipalities.⁷ Its American victims included a religious organization that sent missionaries to China, news outlets critical of the Party, the New York State Assembly and the Treasury Department.⁷

Two companies with no known relationship to each other were selling into the same intelligence service, through different units, in different provinces, years apart.

CNITSEC. The advisory records XJW's relationship with the Jilin branch of the China Information Technology Testing and Evaluation Center, and notes that as of September 2021 the branch was supplying vulnerabilities to the MSS 13th Bureau for review before publication.²

CNITSEC runs CNNVD, China's national vulnerability database — the government body whose stated job is to warn Chinese industry about newly discovered software flaws so they can be fixed. Researchers at Recorded Future identified CNITSEC as MSS-run and documented shared building addresses and telephone numbers between CNITSEC and CNNVD. Their analysis also measured the publication calendar. In their sample of 32 vulnerabilities exploited by malware linked to Chinese APT groups, the American national database beat CNNVD to publication 97 percent of the time, reversing CNNVD's usual speed advantage. They put the odds of that happening by chance at less than one in ten million.⁸



The Treasury Department, Washington. Treasury is among the American victims named in the i-Soon charges of March 2025, which priced a successfully opened mailbox at \$10,000 to \$75,000.

PHOTOGRAPH CAROL M. HIGHSMITH · PUBLIC DOMAIN · LIBRARY OF CONGRESS VIA WIKIMEDIA COMMONS

NOTES

- ⁷ U.S. Department of Justice, "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns," 5 Mar. 2025.
- ² FBI — see register
- ⁸ Recorded Future (Insikt Group), "China's Influence on National Network Vulnerability Publications."

The sequence that describes is a flaw arriving at the national disclosure body, and intelligence officers getting to decide whether it is worth more to the state unpatched. The advisory places a QTFY business partner inside that process.

The rest of the list reads like a defense-trade directory. Nanjing Lexbell won a June 2025 contract to build data-mining and analysis tools for command-and-control system design. Bozhi Security Technology, which trades as Elextec, submitted three bids to the National University of Defense Technology the same month for power-system vulnerability detection. Fujian Ares Network Technology was finalist or winner on at least six of that university's projects between May 2023 and October 2025. Changyang Technology, known as Cy-Tech, describes itself as working in industrial internet security.²

Two further details from the advisory are worth reading closely. XJW's staff took part in China's freelance exploit-brokering networks, buying and selling access to already-compromised victim networks as a commodity, and competed on the attacking side of the domestic HW/HVV network exercises, where the state finds talent and the talent finds one another. And for the two years before the seizure, the group had been working hard to build artificial intelligence into its process.²

"Discovery of private companies building networks for China is becoming more frequent," Ryan English of Lumen's Black Lotus Labs said after the seizure.³ Describing the Salt Typhoon contractors a year earlier, the SentinelOne analyst Dakota Cary put the arrangement's strangeness plainly: "It is inconceivable the U.S. would ask a private company to hack Xi's phone."⁶

NOTES

² FBI — see register

³ Greg Otto — see register

⁶ Kevin Collier — see register

ONE COMPANY'S ADDRESS BOOK — SELECTED ENTRIES

Selected business relationships recorded as of June 2026. The advisory lists further entries, including Zhengzhou Hanjiang and a Hunan office, not shown here.

01 / SHARED INTELLIGENCE CLIENTS

MINISTRY OF STATE SECURITY

UNIT 0718

BUSINESS RELATIONSHIP · JUNE 2026

XJW / QTFY
Nanjing Xinjiuwei Network Technology

Operator of QScan and QTRouter; platforms seized 26 August 2026.

SAME UNIT

ASSOCIATED CONTRACTOR

SICHUAN ZHIXIN RUIJIE
Network Technology

Named in the August 2025 thirteen-country advisory as one of three Chinese firms working for the MSS on **Salt Typhoon**. A second, Sichuan Juxinhe, was sanctioned by the Treasury in January 2025.

Salt Typhoon, August 2025 advisory: thirteen signatory countries · roughly 600 organizations worldwide · some 200 U.S. companies across 80 countries · provider-edge and customer-edge routers.

MSS · GUANGXI PROVINCE

UNIT 9086

BUSINESS RELATIONSHIP · JUNE 2026

XJW / QTFY

The same operator, a different province, a different decade.

SAME UNIT

CONTRACTS · 2019

I-SOON
安洵信息技术

Internal files leaked February 2024. **Twelve people charged by the Justice Department, March 2025.**

PRICE PER MAILBOX

\$10,000 - \$75,000

Billed to the MSS and the Ministry of Public Security for each inbox successfully broken into.

CUSTOMER COUNT

43 BUREAUS

Across at least **31 provinces and municipalities.**

U.S. VICTIMS

TREASURY · NY ASSEMBLY

Also a missionary-sending religious organization and news outlets critical of the Party.

02 / VULNERABILITY DISCLOSURE AND PROCUREMENT

JILIN BRANCH · BUSINESS RELATIONSHIP

CNITSEC

A FLAW IS FOUND

CNITSEC operates **CNNVD**, China's national vulnerability database — the body whose stated job is to warn Chinese industry about new software flaws so they can be fixed.

→

INTELLIGENCE REVIEWS IT FIRST

As of September 2021 the Jilin branch was supplying vulnerabilities to the **MSS 13th Bureau for review before publication.**

→

PUBLICATION IS DECIDED

Officers get to decide whether a flaw is worth more to the state **unpatched.**

Recorded Future: CNITSEC shares building addresses and telephone numbers with the MSS. For vulnerabilities later found in Chinese state malware, the U.S. National Vulnerability Database published before CNNVD **97% of the time**, reversing CNNVD's usual speed advantage. Odds by chance: **under one in ten million.**

OTHER NAMED FIRMS — RECORDED BIDS AND CONTRACTS

JUNE 2025 · WINNING BID

NANJING LEXBELL

Networked data-mining and analysis tools for **command-and-control system design.**

JUNE 2025 · THREE BIDS

BOZHI SECURITY / ELEXTEC

Power-system vulnerability detection, to the **National University of Defense Technology.**

MAY 2023 – OCT 2025 · SIX PROJECTS

FUJIAN ARES NETWORK TECH.

Finalist or winner on at least six of that university's projects.

SELF-DESCRIBED

CHANGYANG / CY-TECH

Industrial internet security.

ALSO RECORDED IN THE ADVISORY

THE COMMODITY MARKET

XJW staff took part in China's **freelance exploit-brokering networks**, buying and selling access to already-compromised victim networks — and competed on the attacking side of the domestic HW/HVV exercises, where the state finds talent and the talent finds one another.

THE LAST TWO YEARS

Before the seizure the group had been working hard to **build artificial intelligence into its process.**

SOURCES: FBI / NSA / CNMF JOINT ADVISORY, 26 AUG 2026 · DOJ, 26 AUG 2026 · DOJ I-SOON CHARGES, 5 MAR 2025 · CISA AND INTERNATIONAL PARTNERS, SALT TYPHOON ADVISORY, 27 AUG 2025 · NBC NEWS, AUG 2025 · U.S. DEPARTMENT OF STATE, 17 JAN 2025 · RECORDED FUTURE, INSIKT GROUP

SECTION 4

WHERE THE PEOPLE COME FROM

IV

A market this deep needs a steady supply of trained people, and in China a great deal of that supply has come through one funding mechanism that predates every company named above.

The 973 Program — the National Basic Research Program — paid for large, multi-institution science projects across Chinese universities and academies. Its recipients were not secret and its work was not classified.

Lionel Ni joined the Michigan State University computer science faculty in January 1981 and stayed until June 2003, and from August 1995 to July 1996 he ran the U.S. National Science Foundation's Microelectronic Systems Architecture Program in Arlington.⁹ He moved to the Hong Kong University of Science and Technology, and from September 2006 to August 2011 he was chief scientist of 973 project 2006CB303000, "Research on Fundamental Theory and Critical Technologies for Wireless Sensor Networks."¹⁰ From November 2004 to December 2014 — a decade — he directed HKUST's IT Key Lab jointly with China's Ministry of Education and Microsoft Research Asia.¹⁰ He has held guest and adjunct appointments at the Chinese Academy of Sciences, Fudan, Beihang, Shanghai Jiao Tong and Tsinghua.⁹



The Hong Kong University of Science and Technology. Lionel Ni was chief scientist of 973 project 2006CB303000 here from September 2006 to August 2011, and directed the Ministry of Education / Microsoft Research Asia joint laboratory from November 2004 to December 2014.

PHOTOGRAPH COGDOG BLOG · CC0 · WIKIMEDIA COMMONS

Each of those is an ordinary distinguished-career entry. Together they describe one person holding open, for two decades, a channel running between an American university, an American federal science agency, a Chinese national research program, four mainland universities and Microsoft.

The same machinery turns up on a narrower branch, traceable through two papers eight years apart.

In 2014 the Journal of Software ran a survey of IP geolocation — the techniques for working out where in the physical world a given internet address actually sits. Its lead author was Wang Zhanfeng, and the listed affiliations were the PLA University of Science and Technology and 93615 PLA Troops in Tianjin. The work was supported by 973 grant 2012CB315806 and four grants from the National Natural Science Foundation.¹¹

NOTES

⁹ Lionel M. Ni, biographical sketch, HKUST Department of Computer Science and Engineering.

¹⁰ Lionel M. Ni, complete curriculum vitae, University of Macau Rector's Office. Chief Scientist (9/06–8/11), National Basic Research Program of China (973) project 2006CB303000.

¹¹ 王占丰, 冯径, 邢长友, 张国敏, 许博, 「IP定位技术的研究」(Research on the IP Geolocation Technology), 软件学报 (Journal of Software) 25(7), 2014, pp. 1527–1540.

In 2022 the same journal ran a survey by the same lead author on protocol reverse engineering — how to work out the structure of a proprietary communications protocol purely by watching the traffic it produces, with no documentation and no source code. Wang had moved to Southeast University. His co-authors were listed at Southeast University, at the PLA Army Engineering University's College of Command Control Engineering, at CNCERT — China's national computer emergency response center — and, in the case of Ma Weijun, at Nanjing Lexbell Information Technology.¹²

Nanjing Lexbell is the company that appears in the August 2026 advisory as an XJW business relationship, and that won a contract in June 2025 to build data-mining and analysis tools for command-and-control system design.²

The connection here is not direct or personal. It is the centrally planned institutional mechanism: national funding instruments, appearing across different

generations, moving different people toward the same ends.

What that money bought is dual-use by construction. Working out where an internet address physically sits is how a streaming service routes traffic efficiently and how an operator locates a target. Reconstructing an undocumented industrial protocol is how an engineer audits a power plant's controller and how an intruder learns to talk to one. The knowledge is the same; only the customer differs.

None of this was concealed. China's 13th Five-Year National Informatization Plan stated that a system for civil-military integration in cyberspace had already been established, and called for shared laboratories, joint talent programs, movement of technology and capital between military and commercial sectors, military purchasing of commercial information products, and overseas research and data platforms.¹³ The contractor market did not grow up outside the state system. It grew up inside a published plan.



Southeast University, Nanjing. Wang Zhanfeng wrote the 2014 IP-geolocation survey from the PLA University of Science and Technology and 93615 Troops. By the 2022 survey on protocol reverse engineering he was listed here, beside a co-author at Nanjing Lexbell.

PHOTOGRAPH ZHOU GUANHUI · CC BY-SA
4.0 · WIKIMEDIA COMMONS

NOTES

- ¹² 王占丰, 程光, 马为俊, 张佳伟, 孙中豪, 胡超, 「基于网络轨迹的协议逆向技术研究进展」(Research Progress of Network Protocol Reverse Engineering Technologies Based on Network Trace), 软件学报 (Journal of Software) 33(1), 2022, pp. 254-273.
- ² FBI — see register
- ¹³ State Council of the People's Republic of China, 国务院关于印发「十三五」国家信息化规划的通知 (Notice issuing the 13th Five-Year National Informatization Plan), 国发〔2016〕73号, 27 Dec. 2016.

ONE FUNDING INSTRUMENT, TWO GENERATIONS

How China's national basic-research program connects an American university to a PLA unit – and, eventually, to a company named in a federal advisory.

NATIONAL BASIC RESEARCH PROGRAM OF CHINA

THE 973 PROGRAM

State framework funding large, multi-institution basic science across Chinese universities and academies. Two funded scientists below, separate projects. The grants are dated 2006 and 2012.

BRANCH ONE • GRANT 2006CB303000

WIRELESS SENSOR NETWORKS

Fundamental theory and critical technologies • chief scientist Sept 2006 – Aug 2011

CHIEF SCIENTIST

LIONEL M. NI

倪明选 • Michigan State faculty Jan 1981 – Jun 2003; NSF programme director, Microelectronic Systems Architecture, Aug 1995 – Jul 1996; then HKUST chair professor.

MSU • NSF • HKUST

JOINT LABORATORY

MOE / MICROSOFT RESEARCH ASIA

Ni directed HKUST's IT Key Lab jointly with China's Ministry of Education and Microsoft Research Asia, Nov 2004 – Dec 2014 – a full decade.

JOINT PHD SUPERVISION • INTERNSHIPS • RECRUITMENT

GUEST AND ADJUNCT POSTS

CAS • FUDAN • BEIHANG

Also Shanghai Jiao Tong and Tsinghua.

LATER APPOINTMENT

UNIVERSITY OF MACAU

Rector's office; complete vitae published there.

BRANCH TWO • GRANT 2012CB315806

NETWORK MEASUREMENT AND IP GEOLOCATION

Traceable through two survey papers in the same journal, eight years apart

2014 • JOURNAL OF SOFTWARE 25(7), PP. 1527-1540

IP GEOLOCATION – 「IP定位技术的研究」

Lead author Wang Zhanfeng 王占丰. Affiliations: PLA University of Science and Technology (Institute of Meteorology and Oceanography; College of Command Information Systems) and 93615 PLA Troops, Tianjin. Supported by 973 grant 2012CB315806 and four NSFC grants.

2022 • JOURNAL OF SOFTWARE 33(1), PP. 254-273

PROTOCOL REVERSE ENGINEERING

Same lead author, now at Southeast University. Co-authors listed at Southeast University, at CNCERT – China's national computer emergency response centre – at the PLA Army Engineering University, and, in the case of Ma Weijun 马为俊, at Nanjing Lexbell Information Technology.

FBI / NSA / CNMF ADVISORY • 26 AUGUST 2026

NANJING LEXBELL

Listed among XJW's business relationships as of June 2026. Won a June 2025 contract to build networked data-mining and analysis tools for command-and-control system design.

SURROUNDING INSTITUTIONAL CONTEXT

MICHIGAN STATE → TSINGHUA

ANIL K. JAIN

University Distinguished Professor of biometrics; lists Tsinghua among his visiting appointments. Elected a foreign member of the Chinese Academy of Sciences, 17 December 2019.

MICHIGAN STATE → SUN WAH → HKUST

JONATHAN CHOI

MSU's trustees recorded a \$5m Sun Wah Education Foundation grant on 13 February 2004. Choi is a court member at HKUST, where Ni ran the 973 project.

PUBLISHED STATE PLAN

13TH FIVE-YEAR INFORMATIZATION PLAN

States that a system for civil-military integration in cyberspace had already been established, calling for shared laboratories, joint talent programmes and military purchasing of commercial information products.

SOURCES: JOURNAL OF SOFTWARE 25(7) 2014 AND 33(1) 2022 • LIONEL M. NI COMPLETE VITAE, UNIVERSITY OF MACAU • HKUST • MSU BOARD OF TRUSTEES, 13 FEB 2004 • MSU TODAY, 17 DEC 2019 • STATE COUNCIL OF THE PRC • FBI / NSA / CNMF JOINT ADVISORY, 26 AUG 2026

SECTION 5

THE BUILDER



Jonathan Choi Koon-shum has run the Hong Kong conglomerate Sunwah Group — 新华集团, Xinhua Group — since 1976.

He sits on the Standing Committee of the Chinese People's Political Consultative Conference, the body that formally advises the Communist Party leadership and whose membership is the clearest public marker of political standing available to someone outside the Party apparatus. He was re-elected to its 14th term in March 2023 and filed thirteen policy proposals that session, most of them on Greater Bay Area development.¹⁴ He is a vice president of the China Overseas Friendship Association, one of the organizations through which the Party's United Front Work Department maintains relationships with ethnic Chinese communities abroad.¹⁵

Alongside that he is chairman of the Hong Kong Chinese General Chamber of Commerce, chairman of the Guangdong-Hong Kong-Macao Greater Bay Area Entrepreneurs Alliance, an economic adviser to the president of the Chinese Academy of Sciences, an independent non-executive director of BOC Hong Kong, chairman of the listed financial group Sunwah Kingsway, and chairman of VinaCapital in Vietnam. He was Hong Kong's representative to the APEC Business Advisory Council from 2015 to 2020. He holds the Grand Bauhinia Medal, Hong Kong's highest honor; France's Légion d'honneur; Japan's Order of the Rising Sun; Vietnam's Friendship Order; Cambodia's Royal Order of Sahametrei; and an honorary doctorate from Michigan State University.¹⁵



Hong Kong. Jonathan Choi Koon-shum has run Sunwah Group — 新华集团 — from the city since 1976. He holds the Grand Bauhinia Medal, Hong Kong's highest honour, and sits on the Standing Committee of the CPPCC in Beijing.

PHOTOGRAPH BENH LIEU SONG · CC BY-SA
4.0 · WIKIMEDIA COMMONS

NOTES

¹⁴ 香港新华集团, 「蔡冠深博士连任十四届全国政协常委 13份提案聚焦大湾区及一带一路建设」, Mar. 2023.

¹⁵ Sunwah Group, official biography of Dr. Jonathan K.S. Choi, Chairman.

Nanjing. Sunwah formed its technology arm in 1998. Its relationship with Nanjing University dates to the 1990s. In 2002 Choi put RMB 700,000 into establishing the Choi Koon Shum Software R&D Centre, which worked on embedded-system software and hardware design. The host Electronic Engineering Laboratory listed among its projects embedded operating-system development, Linux system testing, and China's national Linux public testing platform.¹⁶ In March 2006 Nanjing University and Xinhua Science and Technology (Nanjing) System Software jointly filed a patent application for a method of booting a Linux operating system from a portable hard drive; it was published as CN101038551A on 19 September 2007.¹⁷ In January 2025 Choi gave the university ten million yuan for a 2,408-square-metre building, named 蔡继有楼 after his father, Choi Kai Yau. Inside it are the university's information-technology management center and a jointly built data center carrying Choi's own name.¹⁸



Nanjing. Xinjiuwei Network Technology registered here in 2018. Other Nanjing links include the Choi Koon Shum Software R&D Centre, patent CN101038551A, NandaSoft and Bozhi Security.

PHOTOGRAPH HAHAI69 · CC BY-SA 4.0 · WIKIMEDIA COMMONS

Nanjing University matters once more. NandaSoft — 南大苏富特, listed in Hong Kong as Jiangsu NandaSoft Technology, stock code 8045 — grew out of the university's software research and commercialization environment. Fu Tao was deputy director of the NandaSoft research institute before founding Bozhi Security in Nanjing on 7 August 2009.¹⁹ Bozhi calls itself a leading force in domestic cyber ranges, building for national defense cybersecurity and network confrontation and selling industrial-control security into defense, government, energy and transport; Fu Tao is its chairman.²⁰ It submitted three bids to the National University of Defense Technology in June 2025 and appears in the 2026 advisory as an XJW business relationship.²

NOTES

- ¹⁶ 南京大学, 「电子工程实验室」 / Laboratory of Electronic Engineering, 18 Dec. 2014 — records Choi Koon Shum's RMB 700,000 investment establishing the 蔡冠深软件研发中心 in 2002, its work in embedded-system software and hardware design, Professor Du Sidan as director.
- ¹⁷ Patent application publication CN101038551A. Filed 16 March 2006; published 19 September 2007. Full applicants and source: register note 17.
- ¹⁸ 南京大学, 「南京大学『蔡继有楼』捐赠冠名揭牌仪式举行」, 13 Jan. 2025. RMB 10m; 2,408 m² building; houses the university's information-technology construction and management service centre and the jointly built 蔡冠深数据中心.
- ¹⁹ 36Kr / PitchHub company record for 博智安全 (Bozhi Security): founded 7 Aug. 2009 by Fu Tao (傅涛), registered in Yuhuatai District, Nanjing.
- ²⁰ 博智安全 (Bozhi Security / Elextec), 「博智安全董事长傅涛荣获2025年IDC中国网络安全十大人物」, 2025 — describes the company as a leading force in domestic cyber ranges for national defence cybersecurity and network confrontation.
- ² FBI — see register

Michigan State. In February 2004 the university's board of trustees recorded that Michigan State "has received a \$5 million grant from the Hong Kong-based Sun Wah Education Foundation to study and compare the Chinese K-12 system with the U.S. K-12 system."²¹ Choi holds an honorary Michigan State doctorate. Lionel Ni spent twenty-two years on the Michigan State faculty before taking the HKUST post from which he ran the 973 sensor-network project, and Anil Jain, Michigan State's University Distinguished Professor in biometrics, lists Tsinghua among his visiting appointments.²²

Fudan. Choi has been a member of Fudan University's board since 1997, serving all eight consecutive terms — twenty-eight years, by the university's own count in May 2025. The board is not a corporate governing body: Fudan's Ministry-approved charter describes it as consultative and deliberative, a link between the university and society and a means of raising resources.²³ A lecture hall bearing his name opened at the Journalism School in 2004 and a humanities building in 2005. On 29 May 2025 Sunwah and Fudan signed a renewed strategic cooperation agreement covering international cultural exchange, shared international platforms, academic development and talent cultivation, with named focus areas including journalism, finance, life sciences and global governance.²⁴



Fudan University, Shanghai. Choi has sat on its board since 1997, through eight consecutive terms; Ming Hsieh has been a trustee since 2011. The lecture hall carrying Choi's name opened at the Journalism School in 2004.

PHOTOGRAPH PRCMISE · CC BY-SA 4.0 · WIKIMEDIA COMMONS

NOTES

- ²¹ Michigan State University Board of Trustees, minutes of 13 Feb. 2004, agenda item 3 (President's Report), p. 2.
- ²² Anil K. Jain, curriculum vitae, Michigan State University Department of Computer Science and Engineering — University Distinguished Professor; Tsinghua University listed among visiting appointments.
- ²³ 复旦大学章程 (Fudan University charter), Article 62: 「学校董事会是由热心教育事业并且关心支持学校发展的社会各界人士、知名校友、著名学者和学校代表组成的咨询和议事机构」 — the board is a consultative and deliberative body, not a governing one.
- ²⁴ 复旦大学教育发展基金会, 「复旦大学与蔡冠深校友企业新华集团签署战略合作协议、捐赠协议」, 29 May 2025. Records Choi as a founding board member since 1997 across eight consecutive terms; 蔡冠深演讲厅 (2004) and 蔡冠深人文馆 (2005).

The hall — 蔡冠深报告厅 — has been used repeatedly for state and Party communications work. A national speaking tour organised by the Central Propaganda Department, the State Internet Information Office, the broadcasting and publishing regulator and the All-China Journalists Association opened its Shanghai leg there in December 2014. A lecture in March 2016 on implementing Xi Jinping's directives for Party news and public-opinion work was held in the same room, covering Marxist journalism, internet content governance and “telling China's story well.” In March 2017 it hosted the Shanghai promotional session for an international “Telling China's Stories Well” creative communication competition. And it is where the Shanghai municipal propaganda department and Fudan run their “China in the New Era” national-conditions lecture series, in 2022 and again in 2024 — one strand of a co-construction program that the university's 2022 account put at twenty-one years old and reaching six Shanghai universities.²⁵ Speaking at the signing on 29 May 2025, Choi put the relationship at twenty-eight years himself, named journalism and communication among the five fields the agreement targets, and said Sunwah now runs more than ten Choi Koon Shum cultural exchange centres worldwide, which he described as “actively serving as a bridge for people-to-people diplomacy,” inviting Fudan to hold joint events at them.²⁴

The Fudan board is also where this story touches the American security industry. Ming Hsieh has been a Fudan trustee since 2011, sitting on the board Choi has served on since 1997, and Fudan's current governance page lists him, as 谢明, among the regular members of its eighth board. Fulgent Genetics — the genetic-testing company Hsieh runs — repeated the trusteeship in the proxy statement it filed with the Securities and Exchange Commission in March 2026.²⁶ He has attended in person: Fudan's record of the third session of its seventh board, on 16 December 2022, lists 谢明 among the trustees who advised the university on its future direction. At a Greater Bay Area cooperation meeting in Guangzhou on 25 February 2023 he was represented by Liu Haiqing, sales director of Fulgent's Chinese arm, 福君基因.²⁷

Hsieh was born in Shenyang in 1956, came to the University of Southern California in 1981, and in 1990 founded Cogent Systems, which built the automated fingerprint identification systems used by the FBI and the Department of Homeland Security. He took Cogent public in 2004, sold it to 3M in 2010, and now runs the genetic-testing company Fulgent. Since April 2013 he has been a director of Fortinet.²⁸

NOTES

²⁵ Fudan University and School of Journalism, records of events in the Choi hall, 2014-2024. Full titles, dates and seven source URLs: register note 25.

²⁴ 复旦大学教育发展基金会 — see register

²⁶ Fulgent Genetics, Inc., Schedule 14A proxy statement, filed 31 Mar. 2026: “Mr. Hsieh has served as a trustee at the University of Southern California since 2007 and at Fudan University in China since 2011.”

²⁷ 复旦大学, seventh board of trustees, third session, 16 Dec. 2022 — 谢明 (Ming Hsieh) listed among attending trustees advising on the university's development.

²⁸ Fortinet, Board of Directors — Ming Hsieh, director since April 2013.

JONATHAN CHOI: AUTHORITY + CROSS-BORDER
INFRASTRUCTURE

Named records · dates · functions

01 / OFFICES HELD

FORMAL + COMMERCIAL NODE

JONATHAN K.S. CHOI

蔡冠深 · Chairman, Sunwah Group (新华集团) since 1976
Boards: Fudan 1997– (eight terms) · Nanjing University honorary director · Tsinghua Advanced Research Center Foundation chair, 2025 · HKUST and HK PolyU court member

NATIONAL POLITICAL OFFICE

CPPCC STANDING COMMITTEE

Re-elected to the 14th term, March 2023; filed 13 policy proposals that session.

OVERSEAS-LIAISON OFFICE

COFA VICE PRESIDENT

China Overseas Friendship Association – united-front body for Chinese communities abroad.

CONVENING OFFICES + COMMERCIAL PLATFORMS

Chairman, HK Chinese General Chamber of Commerce · Chairman, Greater Bay Area Entrepreneurs Alliance · Co-chair, Belt & Road Alliance

Board chair, Sunwah Kingsway Capital · Independent non-executive director, BOC Hong Kong · Chairman, VinaCapital

BRANCH TWO OF THE 973 PROGRAMME

Wang Zhanfeng · grant 2012CB315806 · PLA UST and 93615 PLA Troops · Ma Weijun at Nanjing Lexbell, named in the same 2026 advisory

SEE GRAPHIC 04

02 / DOCUMENTED INSTITUTIONAL CIRCUITS

A / NANJING — SOFTWARE, INTELLECTUAL PROPERTY, DATA

1998

SUN WAH HI-TECH

Technology arm formed, CAS and university project platform.

2002 · RMB 700,000

CHOI SOFTWARE R&D CENTRE

蔡冠深软件研发中心

Embedded-system software and hardware design. Director: Prof. Du Sidan.

HOST LABORATORY

EMBEDDED + LINUX

Embedded OS development and industrialisation · Linux system testing · China national Linux public testing platform

Mar 2006 — NJU and Xinhua Science and Technology (Nanjing) jointly file patent CN101038551A, booting Linux from a portable drive.

13 JAN 2025 · RMB 10M

蔡继有楼 + DATA CENTRE

2,408 m². Named for Choi's father, Choi Kai Yau; houses NJU's IT centre and the 蔡冠深数据中心.

B / MICHIGAN STATE — HKUST — BEIJING: RECORDS IN DATE ORDER

JAN 1981 – JUN 2003

LIONEL NI AT MSU

Computer science faculty. NSF program director, Microelectronic Systems Architecture, Aug 1995 – Jul 1996.

13 FEB 2004 · \$5M

MSU TRUSTEE MINUTES

"A \$5 million grant from the Hong Kong-based Sun Wah Education Foundation to study and compare the Chinese K-12 system with the U.S. K-12 system." Recorded eight months after Ni's MSU appointment ended.

NOV 2004 – DEC 2014

MOE / MSRA JOINT LAB

Director for a decade of HKUST's IT Key Lab with China's Ministry of Education and Microsoft Research Asia.

SEPT 2006 – AUG 2011

HKUST · 973 CHIEF SCIENTIST

► branch one of two – see Graphic 04

Project 2006CB303000 – fundamental theory and critical technologies for wireless sensor networks.

C / SHANGHAI — GOVERNANCE, NAMED FACILITIES, POLITICAL-COMMUNICATIONS PROGRAMMING

1997 – 2025

FUDAN BOARD · 8 TERMS

Founding board member, twenty-eight years. The charter calls the board consultative and deliberative, not a governing body.

2004 · 2005

NAMED FACILITIES

蔡冠深演讲厅 (2004) · 蔡冠深人文馆 (2005) · Journalism School hall 蔡冠深报告厅.

2014 · 2016 · 2017 · 2022 · 2024

WHAT THE HALL HOSTS

Central Propaganda Department national tour · lecture on Xi's Party-news directives · "Telling China's Stories Well" session · "China in the New Era" series with the Shanghai propaganda department.

29 MAY 2025

AGREEMENT RENEWED

Fudan-Sunwah strategic cooperation, signed for the group by Cai Jesi.

D / NANJING — COMPANY CHAIN

UNIVERSITY COMMERCIALISATION

NANDASOFT

南大苏富特 · HKEX GEM 8045

Jiangsu NandaSoft Technology, out of Nanjing University's software research and commercialisation environment.

PERSONNEL

FU TAO 傅涛

Deputy director, NandaSoft research institute. Degree from Nanjing University of Science and Technology, 2002 – a different institution from Nanjing University.

FOUNDED 7 AUG 2009 · NANJING

BOZHI SECURITY

博智安全 / Elextec · Fu Tao, chairman

Self-described "leading force in domestic cyber ranges," building for national defence cybersecurity and network confrontation. Three bids to NUDT, June 2025.

FBI / NSA / CNMF · 26 AUG 2026

XJW / QTFY

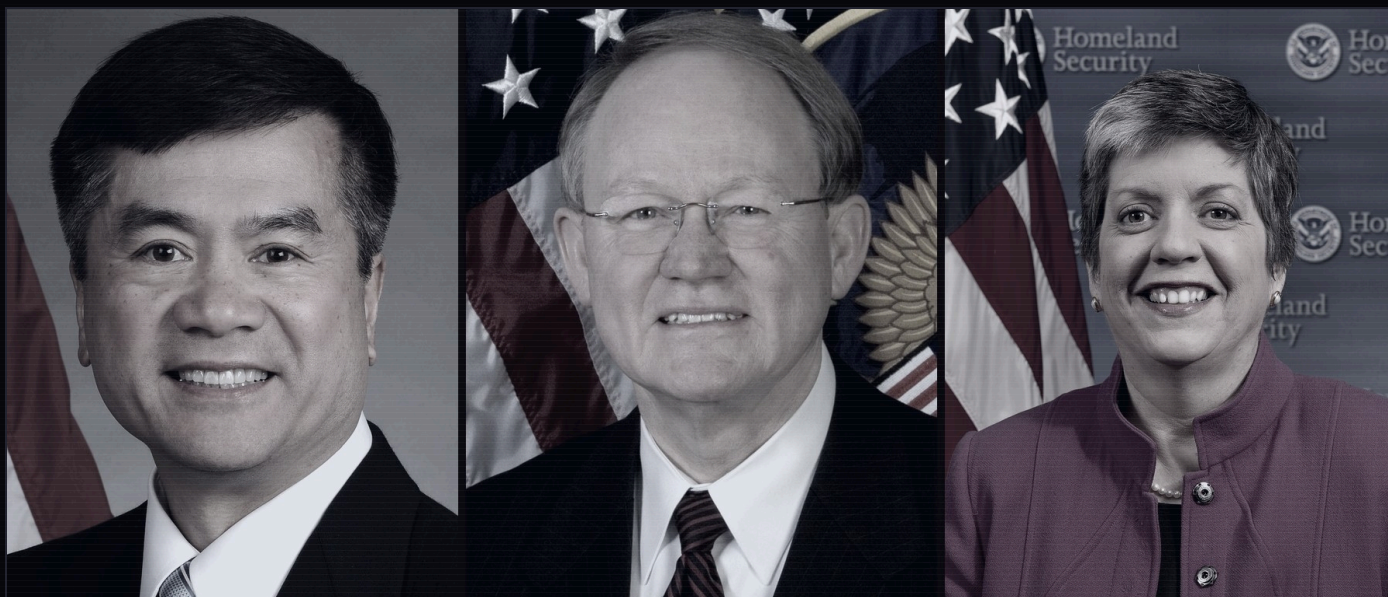
The advisory lists Bozhi among XJW's business relationships as of June 2026.

PRIMARY RECORDS: CPPCC · COFA · SUNWAH GROUP · NANJING UNIVERSITY · PATENT CN101038551A · HKEX · BOZHI/ELEXTec · 36KR · MSU BOARD OF TRUSTEES · LIONEL NI
COMPLETE VITAE (UMAC) · FUDAN UNIVERSITY · FBI/NSA/CNMF JOINT ADVISORY

Fortinet's board is one of the densest concentrations of American national-security leadership in the technology industry. Gary Locke — governor of Washington, secretary of commerce, and United States ambassador to China from 2011 to 2014 — joined it in September 2015.²⁹ When the company launched its federal subsidiary in May 2017, that subsidiary's board included Mike McConnell, a retired Navy vice admiral who had directed the National Security Agency and then served as director of national intelligence.³⁰ In November 2024 the parent board added Janet Napolitano, secretary of homeland security from 2009 to 2013.³¹

A flaw in Fortinet's FortiOS VPN software appears in the QTFY exploitation timeline for October 2019, and

Fortinet firewalls are named in the 2025 Salt Typhoon advisory among devices those operators may target.^{2,4} Being targeted is the ordinary condition of every company selling network-edge equipment; the same advisories name Cisco, Ivanti, Citrix and Palo Alto. The unusual part is the composition of the room — a company whose equipment is a standing objective for Chinese state operators, governed in part by the people who ran the American agencies charged with stopping them, and in part by a founder who built the federal government's fingerprint infrastructure and sat on the board of a Shanghai university beside a member of the CPPCC Standing Committee.



Gary Locke, Mike McConnell and Janet Napolitano in their federal official portraits. Locke joined Fortinet's board in September 2015; McConnell was named to the board of Fortinet Federal in May 2017; Napolitano joined the parent board in November 2024.

OFFICIAL PORTRAITS U.S. DEPARTMENT OF
COMMERCE · OFFICE OF THE DIRECTOR OF
NATIONAL INTELLIGENCE · U.S.
DEPARTMENT OF HOMELAND SECURITY ·
PUBLIC DOMAIN

NOTES

- ²⁹ Fortinet, "Former Governor, U.S. Commerce Secretary, and U.S. Ambassador, Gary Locke, Joins Fortinet Board of Directors," 28 Sept. 2015. Governor of Washington 1997–2005; U.S. Secretary of Commerce 2009–2011; U.S. Ambassador to China 2011–2014.
- ³⁰ Fortinet, "Fortinet Launches Fortinet Federal, Inc. and its Board of Directors," 15 May 2017. Subsidiary board as announced; full roster: register note 30.
- ³¹ Fortinet, "Fortinet Appoints Distinguished Public Sector Leader Janet Napolitano to its Board of Directors," 12 Nov. 2024.
- ² FBI — see register ⁴ Salt Typhoon advisory (2025) — see register

The academic side shows the same compression. Anil Jain, Michigan State's University Distinguished Professor of biometrics, wrote the textbooks that defined the field Cogent commercialized — and in April 2010 the U.S. Army awarded Cogent a contract worth \$1.12 million to prototype a handheld device fusing face, fingerprint, iris, voice and periocular recognition for field use. Cogent held the prime award. The universities underneath it were Michigan State, USC and West Virginia — Jain's institution, the school whose electrical-engineering department Hsieh endowed, and a forensic-science program that in November 2007 had received \$5.5 million from him, part cash and part in-kind gifts of Cogent biometric systems, and had dedicated a building as Ming Hsieh Hall; he gave the same program a further \$250,000 in May 2014.³² Jain described the arrangement himself to the Army Science Board in March 2011: “Current ARL funding to Cogent Systems (with MSU, USC, WVU) is prototyping a system with face, finger, iris, voice and periocular traits.”³³

Michigan State's audited federal-award schedules record what reached it — \$112,092 in the year to June 2011 and \$35,400 the year after, booked as “COGENT DOD,” grantor Cogent, Inc.³⁴ Hsieh was Cogent's chairman, president and chief executive when the contract was signed. A filing that September put his holding, with entities he controlled, at roughly 39 percent of Cogent's shares as of 27 August 2010.³⁵ Defense money moving through his company into Jain's department is not the same thing as a gift from him, and the public record shows no personal Hsieh grant to Jain.



Nanjing University. Sunwah's software centre opened here in 2002; the university and Xinhua Science and Technology (Nanjing) filed the CN101038551A patent together in 2006; NandaSoft came out of the same commercialisation environment; and in January 2025 Choi gave ten million yuan for a building named after his father.

PHOTOGRAPH 猫猫的日记本 · CC BY-SA 3.0 · WIKIMEDIA COMMONS

NOTES

- ³² Army contract W91CRB10C0064, signed 20 April 2010; \$1,124,780 total obligations. USC, MSU and WVU supporting records: register note 32.
- ³³ Anil K. Jain, "Fusion Aspects of Non-Cooperative Biometrics," presentation to the U.S. Army Science Board, 28 Mar. 2011.
- ³⁴ MSU federal-award schedules, FY2011 and FY2012, p. 15: COGENT DOD, \$112,092 and \$35,400. Full audit links: register note 34.
- ³⁵ Cogent Schedule 14D-9, filed 10 September 2010: Hsieh and controlled entities held approximately 38.9% as of 27 August 2010. Register note 35.

In December 2019 the Chinese Academy of Sciences elected Jain a foreign member, in Michigan State's own words "for his scientific achievements and contributions to promoting the development of science and technology in China."³⁶

Ming Hsieh's own career carries the whole span. Cogent built the fingerprint systems the FBI and the Department of Homeland Security run on, and its Army prime contract routed federal biometrics money through Jain's department at Michigan State — the department from which Jain held his Tsinghua visiting appointment and was elected to the Chinese Academy of Sciences. Hsieh sold Cogent to 3M in 2010, took over Fulgent, and joined Fortinet's board in April 2013: the company whose FortiOS VPN flaw sits in the QTFY exploitation record and whose firewalls are named in the 2025 Salt Typhoon advisory. And since 2011 he has sat on Fudan's board beside Choi — in the room himself in December

2022, and represented by the sales director of his Chinese subsidiary in February 2023.

Choi is not named in the QTFY case, and no record cited here alleges wrongdoing by him. What the record shows is narrower and more durable: for forty years he has built and maintained the channels through which people, money, technology and access move between China and everywhere else, in public, with his name on the buildings.



Beaumont Tower, Michigan State University. MSU's audited federal-award schedules record \$112,092 in the year to June 2011 and \$35,400 the year after, booked as COGENT DOD. Lionel Ni spent twenty-two years on the faculty; Anil Jain is its University Distinguished Professor of biometrics.

PHOTOGRAPH GPWITTEVEEN · CC BY-SA 3.0
· WIKIMEDIA COMMONS

NOTES

- ³⁶ Michigan State University, "Anil Jain elected Foreign Member by the Chinese Academy of Sciences," 17 Dec. 2019.

MING HSIEH: FEDERAL BIOMETRICS, FUDAN, FORTINET

One board seat in Shanghai • one Army contract • one boardroom

01 / MING HSIEH — OFFICES AND BOARD SEATS

PERSON AT THE CENTER

MING HSIEH

谢明 • b. Shenyang 1956 • USC 1981

Founded **Cogent Systems**, 1990 — automated fingerprint identification for the **FBI and the Department of Homeland Security**. IPO 2004; sold to 3M, 2010. Now chairman and chief executive of **Fulgent Genetics**.

SHARED TABLE • SHANGHAI

FUDAN TRUSTEE SINCE 2011

Fudan's Ministry-approved charter defines the board as consultative and deliberative.

Fudan's live governance page lists 谢明 among the regular members of its **eighth board**. Fulgent's SEC proxy of **31 March 2026** states he "has served as a trustee ... at Fudan University in China since 2011."

Jonathan Choi has held a seat on the same board since **1997** — all eight terms.

A / FUDAN BOARD ATTENDANCE RECORD

NOV 2011

FIFTH BOARD INAUGURATION

Fudan's record of the ceremony names **Bai Xuefeng** as Hsieh's representative.

→

16 DEC 2022

IN PERSON

Seventh board, third session. Fudan lists 谢明 among trustees advising on the university's direction.

→

25 FEB 2023

GUANGZHOU • BY PROXY

"谢明校董代表、福君基因销售总监刘海情" — **Liu Haiqing**, sales director of Fulgent's Chinese arm.

→

31 MAR 2026

STILL SEATED

Restated in Fulgent's definitive proxy to the SEC.

B / ARMY CONTRACT AND FUNDING ROUTE

20 APR 2010 • \$1,124,780

ARMY CONTRACT W91CRB10C0064

Army Research Laboratory to **Cogent, Inc.** — prototyping a handheld device fusing face, fingerprint, iris, voice and periocular recognition for field use.

→

CONSORTIUM BENEATH THE PRIME

MSU • USC • WVU

Anil Jain's institution, the school whose EE department Hsieh endowed, and a forensic-science program that in **November 2007** took \$5.5m from him — part cash, part in-kind gifts of **Cogent biometric systems** — and dedicated **Ming Hsieh Hall**. A further **\$250,000** followed in May 2014. No source ties either gift to a specific Jain project.

→

CORPORATE POSITION

HSIEH HELD ~38.9% AT 27 AUG 2010

Chairman, president and chief executive of Cogent per its SEC Schedule 14D-9 of 10 Sept 2010. 3M's acquisition was announced **30 Aug 2010** — after the contract.

02 / AUDITED EXPENDITURE AND AFFILIATIONS

C / AUDITED MSU EXPENDITURE — DEFENSE PASS-THROUGH

MSU FISCAL YEAR	AUDIT CLASSIFICATION	EXPENDITURE
Year ended 30 June 2011	CFDA 12.431 • award “COGENT DOD” • grantor Cogent, Inc.	\$112,092
Year ended 30 June 2012	CFDA 12.431 • award “COGENT DOD” • grantor Cogent, Inc.	\$35,400
Audited total	Same named pass-through, two schedules	\$147,492

D / ANIL K. JAIN — AFFILIATIONS AND HONOURS

MICHIGAN STATE

ANIL K. JAIN

University Distinguished Professor of biometrics. Wrote the textbooks that defined the field Cogent commercialized. Fingerprint work funded in part through **CITeR**, the NSF industry-university center — whose university sites include **West Virginia**. The archived CITeR affiliate roster of 9 May 2008 does not list Cogent.

17 DECEMBER 2019

CAS FOREIGN MEMBER

Elected by the Chinese Academy of Sciences, in Michigan State's own words, “for his scientific achievements and contributions to promoting the development of science and technology in China.”

“Current ARL funding to Cogent Systems (with MSU, USC, WVU) is prototyping a system with face, finger, iris, voice and periocular traits.”

ANIL K. JAIN • U.S. ARMY SCIENCE BOARD • 28 MARCH 2011

E / FORTINET — PARENT BOARD AND FEDERAL SUBSIDIARY BOARD, AS ANNOUNCED

MING HSIEH

Founder of the FBI's and DHS's fingerprint supplier

PARENT BOARD • DIRECTOR SINCE APR 2013

GARY LOCKE

Governor of Washington • U.S. Secretary of Commerce • U.S. Ambassador to China, 2011-14

PARENT BOARD • JOINED 28 SEPT 2015

MIKE MCCONNELL

Director of National Intelligence • Director, NSA • Vice Admiral, U.S. Navy (ret.)

FORTINET FEDERAL SUBSIDIARY BOARD • ANNOUNCED 15 MAY 2017 • NOT THE PARENT BOARD

JANET NAPOLITANO

Secretary of Homeland Security, 2009-13

PARENT BOARD • JOINED NOV 2024

PRIMARY RECORDS: FULGENT GENETICS SEC PROXY 31 MAR 2026 • COGENT SCHEDULE 14D-9 • USASPENDING W91CRB10C0064 • MSU SCHEDULES OF EXPENDITURES OF FEDERAL AWARDS FY2011-12 • JAIN, ARMY SCIENCE BOARD 28 MAR 2011 • USC SAIL • CITER ARCHIVED AFFILIATE ROSTER, 9 MAY 2008 • WVU TODAY, NOV 2007 AND MAY 2014 • FUDAN FIFTH-BOARD INAUGURATION, NOV 2011 • FUDAN UNIVERSITY • WVU • MSU TODAY • FORTINET INVESTOR RELATIONS • FBI/NSA/CNMF JOINT ADVISORY

SECTION 6

WHAT CAN'T BE SEIZED

VI

American counterintelligence is built to find chains of command. It looks for the officer who gave the order, the cable that carried it, the money that paid for it, and when it finds them it seizes infrastructure, unseals indictments and imposes sanctions. On August 26 it took the infrastructure. No indictment was unsealed, no arrest was announced and no sanction was imposed, and the part it did do, it did competently.

The structure it disrupted has no chain of command. XJW sold capability. National research programs paid for the underlying science. Universities trained the people and companies hired them. Foreign partners — Microsoft, Michigan State, USC and the ordinary machinery of academic exchange — made those careers portable. Intelligence and military customers bought finished work from private vendors, which meant no single organization chart ever contained all the contributors.

The American side has its own version of the same compression. Fortinet's parent board seated a former ambassador to Beijing in 2015 and a former secretary of

homeland security in 2024, alongside the founder who built the FBI's fingerprint systems and sits on a Shanghai university board; the board announced for its federal subsidiary in 2017 included a former director of the National Security Agency who went on to be director of national intelligence. These are public appointments, and the cited records do not allege wrongdoing on that basis. What it means is that the people who understand both ends of this transaction tend to be the same small set of people, moving between government and the vendors government buys from.

Ming Hsieh is the part of that room that complicates it hardest. Cogent sold the federal government the fingerprint infrastructure the FBI and Homeland Security run on, and the Justice Department — the FBI's own department — sits on the QTFY victim list. He has been on Fortinet's board since 2013 and on Fudan's since 2011. The former officials named on Fortinet's parent and federal-subsidary boards led agencies that write the advisories those companies appear in, and Fortinet's own equipment appears in both: a FortiOS flaw in the QTFY exploitation record, Fortinet firewalls in the Salt Typhoon advisory.



FBI headquarters, Washington. The bureau had been working the QTFY case since 2019. On 26 August the three control domains were redirected to its servers.

PHOTOGRAPH AJAY_SURESH · CC BY 2.0 ·
WIKIMEDIA COMMONS

The cited records describe public activities, many of which are also admirable when looked at alone. A joint doctoral program is a good thing. A funded data center is a good thing. Forty years of philanthropy honored by France, Japan, Vietnam and Hong Kong is, on the public record, forty years of philanthropy.

The difficulty for anyone trying to respond is that a modern state can draw operational power from institutions that look entirely ordinary one at a time, and the people who build those institutions are not hiding. The cited QTFY records do not allege wrongdoing by the named researchers or university partners.

The Justice Department took two platforms off the market in a morning. Everything upstream of them opened for business the next day.

HOW THIS REPORT IS SOURCED

Every factual claim above is drawn from a government release, a court filing, a corporate or patent filing, a university publication, or named press reporting, and each is linked below. Where a document is published only in Chinese, the citation gives the original title and a direct URL. Statements about who conducted, directed or paid for an intrusion appear only where an official record makes them.



Networking equipment, photographed by the FBI. What the Justice Department took on 26 August was three domain names. The research programs, the university channels and the vendor market upstream of them were not part of the action.

PHOTOGRAPH FEDERAL BUREAU OF
INVESTIGATION · PUBLIC DOMAIN ·
WIKIMEDIA COMMONS

COMPLETE NUMBERED REGISTER

SOURCES

NOTES 1-10. FULL URLS PRESERVED IN PLAIN TEXT FOR DIRECT REVIEW.

- 01** U.S. Department of Justice, "Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure," 26 Aug. 2026.
<https://www.justice.gov/opa/pr/justice-department-and-fbi-seize-platforms-operated-and-used-china-state-sponsored-hackers>
- 02** FBI, National Security Agency and U.S. Cyber National Mission Force, Joint Cybersecurity Advisory, 26 Aug. 2026, TLP:CLEAR.
<https://www.ic3.gov/CSA/2026/260826.pdf>
https://media.defense.gov/2026/Aug/26/2003986916/-1/-1/0/JCSA_CHINA_QTFY_MALICIOUS_SYSTEMS.PDF
- 03** Greg Otto, "Officials disrupt Chinese espionage operation that hit multiple federal agencies," CyberScoop, 26 Aug. 2026.
<https://cyberscoop.com/qtfy-china-espionage-group-infrastructure-seized/>
- 04** CISA, NSA, FBI and international partners, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," 27 Aug. 2025.
<https://www.cisa.gov/news-events/alerts/2025/08/27/cisa-and-partners-release-joint-advisory-countering-chinese-state-sponsored-actors-compromise>
- 05** "13 countries warn against China's Salt Typhoon group in joint advisory," SC Media, Aug. 2025.
<https://www.scworld.com/news/13-countries-warn-against-chinas-salt-typhoon-group-in-joint-advisory>
- 06** Kevin Collier, "China used three private companies to hack global telecoms, U.S. says," NBC News, Aug. 2025. · U.S. Department of State, "U.S. Takes Action Against PRC-Linked Cyber Actors for Treasury Hack and Salt Typhoon," 17 Jan. 2025. · U.S. Department of the Treasury press release, 17 Jan. 2025
<https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543>
<https://2021-2025.state.gov/office-of-the-spokesperson/releases/2025/01/u-s-takes-action-against-prc-linked-cyber-actors-for-treasury-hack-and-salt-typhoon/>
<https://home.treasury.gov/news/press-releases/jy2792>
- 07** U.S. Department of Justice, "Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns," 5 Mar. 2025. · FBI/IC3 PSA, 5 Mar. 2025
<https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global>
<https://www.ic3.gov/PSA/2025/PSA250305>
- 08** Recorded Future (Insikt Group), "China's Influence on National Network Vulnerability Publications."
<https://www.recordedfuture.com/blog/chinese-mss-vulnerability-influence>
- 09** Lionel M. Ni, biographical sketch, HKUST Department of Computer Science and Engineering.
<https://www.cse.ust.hk/~ni/biography.html>
- 10** Lionel M. Ni, complete curriculum vitae, University of Macau Rector's Office. Chief Scientist (9/06-8/11), National Basic Research Program of China (973) project 2006CB303000; Director (11/04-12/2014), HKUST China Ministry of Education / Microsoft Research Asia IT Key Lab; MSU faculty 1/81-6/03; NSF Program Director 8/95-7/96.
https://rto.um.edu.mo/wp-content/uploads/2019/03/Ni_CompleteVitae_UMAC.pdf

COMPLETE NUMBERED REGISTER

SOURCES, CONT.

NOTES 11–18. FULL URLS PRESERVED IN PLAIN TEXT FOR DIRECT REVIEW.

- 11** 王占丰, 冯径, 邢长友, 张国敏, 许博, 「IP定位技术的研究」(Research on the IP Geolocation Technology), 软件学报 (Journal of Software) 25(7), 2014, pp. 1527–1540. Affiliations: PLA University of Science and Technology (Institute of Meteorology and Oceanography; College of Command Information Systems) and 93615部队, Tianjin. Funding: 973 Program grant 2012CB315806; NSFC grants 61371119, 61379149, 61103225, 61070173.
<http://www.jos.org.cn/html/2014/7/4621.htm>
- 12** 王占丰, 程光, 马为俊, 张佳伟, 孙中豪, 胡超, 「基于网络轨迹的协议逆向技术研究进展」(Research Progress of Network Protocol Reverse Engineering Technologies Based on Network Trace), 软件学报 (Journal of Software) 33(1), 2022, pp. 254–273. Affiliations: Southeast University (School of Computer Science and Engineering; College of Cyber Science and Engineering); Nanjing Lexbell Information Technology Co. Ltd.; CNCERT; College of Command Control Engineering, Army Engineering University of PLA. Funding: National Key R&D Program grants 2017YFB0801703 and 2018YFB1800200, and others.
<https://jos.org.cn/html/2022/1/6303.htm>
- 13** State Council of the People's Republic of China, 国务院关于印发「十三五」国家信息化规划的通知 (Notice issuing the 13th Five-Year National Informatization Plan), 国发〔2016〕73号, 27 Dec. 2016. Section on 网信军民融合 records that a civil-military integration system in cyberspace has been established and calls for 军地网信人才融合发展计划 (joint talent development) and military acquisition of commercial information products by purchase and outsourcing.
https://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm
- 14** 香港新华集团, 「蔡冠深博士连任十四届全国政协常委 13份提案聚焦大湾区及一带一路建设」, Mar. 2023.
<https://www.sunwahgroup.cn/content/865.html>
- 15** Sunwah Group, official biography of Dr. Jonathan K.S. Choi, Chairman. · Corroborating: 上海大学法学院, 「全国政协常委、香港新华集团主席蔡冠深博士受聘上海大学法学院名誉院长」
<https://en.sunwahgroup.cn/column/268.html>
<https://law.shu.edu.cn/info/1328/23453.htm>
- 16** 南京大学, 「电子工程实验室」/ Laboratory of Electronic Engineering, 18 Dec. 2014 – records Choi Koon Shum's RMB 700,000 investment establishing the 蔡冠深软件研发中心 in 2002, its work in embedded-system software and hardware design, Professor Du Sidan as director, and the host laboratory's Linux and embedded-systems projects including 嵌入式操作系统开发和产业化, Linux系统测试 and 中国国家Linux公共测试平台项目. · On the 1990s origin of the relationship
<https://sbc.nju.edu.cn/jb/sysyl/dzkxygcxy/20140606/i2060.html>
<https://www.nju.edu.cn/info/1055/394141.htm>
<https://www.nju.edu.cn/info/1056/394331.htm>
- 17** Patent CN101038551A, 「在移动硬盘上实现启动Linux操作系统的方法」 (Method for booting a Linux operating system on a mobile hard drive). Applicants: 新华科技(南京)系统软件有限公司 (Xinhua Science and Technology (Nanjing) System Software Co. Ltd) and Nanjing University. Filed 16 Mar. 2006; published 19 Sept. 2007.
<https://patents.google.com/patent/CN101038551A/zh>
- 18** 南京大学, 「南京大学『蔡继有楼』捐赠冠名揭牌仪式举行」, 13 Jan. 2025. RMB 10m; 2,408 m² building; houses the university's information-technology construction and management service centre and the jointly built 蔡冠深数据中心.
<https://www.nju.edu.cn/info/1055/394141.htm>

COMPLETE NUMBERED REGISTER

SOURCES, CONT.

NOTES 19–25. FULL URLS PRESERVED IN PLAIN TEXT FOR DIRECT REVIEW.

- 19** 36Kr / PitchHub company record for 博智安全 (Bozhi Security): founded 7 Aug. 2009 by Fu Tao (傅涛), registered in Yuhuatai District, Nanjing; Fu graduated from Nanjing University of Science and Technology in 2002 and previously served as deputy director of the NandaSoft (南大苏富特) research institute. · Jiangsu NandaSoft Technology Company Limited, HKEX GEM stock code 8045
<https://pitchhub.36kr.com/project/1678330172142593>
https://www.hkexnews.hk/listedco/listconews/gem/2023/1110/2023111000962_c.pdf
- 20** 博智安全 (Bozhi Security / Elextec), 「博智安全董事长傅涛荣获2025年IDC中国网络安全十大人物」, 2025 – describes the company as a leading force in domestic cyber ranges for national defence cybersecurity and network confrontation.
<https://www.elextec.com/company-news/2631.html>
<https://elextec.com/>
- 21** Michigan State University Board of Trustees, minutes of 13 Feb. 2004, agenda item 3 (President's Report), p. 2.
<https://onthebanks.msu.edu/recordFiles/157-544-992/FEBRUARY132004.pdf>
- 22** Anil K. Jain, curriculum vitae, Michigan State University Department of Computer Science and Engineering – University Distinguished Professor; Tsinghua University listed among visiting appointments.
https://cse.msu.edu/~jain/JainVita_15Feb11.pdf
- 23** 复旦大学章程 (Fudan University charter), Article 62: 「学校董事会是由热心教育事业并且关心支持学校发展的社会各界人士、知名校友、著名学者和学校代表组成的咨询和议事机构」 – the board is a consultative and deliberative body, not a governing one. · 教育部关于同意复旦大学章程部分条款修改的批复, Ministry of Education, 16 Dec. 2019
<https://www.fudan.edu.cn/452/list.htm>
http://www.moe.gov.cn/srcsite/A02/zfs_gdxxzc/201912/t20191216_4122276.html
- 24** 复旦大学教育发展基金会, 「复旦大学与蔡冠深校友企业新华集团签署战略合作协议、捐赠协议」, 29 May 2025.
 Records Choi as a founding board member since 1997 across eight consecutive terms; 蔡冠深演讲厅 (2004) and 蔡冠深人文馆 (2005).
<https://fuedf.fudan.edu.cn/35/ea/c29767a734698/page.htm>
- 25** 复旦大学新闻学院 and 复旦大学 records of programmes held in the 蔡冠深报告厅: the 「好记者讲好故事」 national tour, Shanghai opening, 29 Dec. 2014; a lecture on implementing Xi Jinping's speech on Party news and public-opinion work, 2 Mar. 2016; the Shanghai promotional session of the first 「讲好中国故事」 international creative communication competition, 27 Mar. 2017; and the 「新时代中国」 national-conditions lecture series, first session 18 Oct. 2022, sponsored by the Shanghai Municipal Propaganda Department and Fudan University and organised by the School of Journalism, whose page records the propaganda department and journalism school co-construction programme at twenty-one years and six Shanghai universities; and the 2024 series opening, 21 Nov. 2024. Sources in that order, with archive copies for the first two
<https://news.fudan.edu.cn/2014/1229/c4a57176/page.htm>
<https://jd.fudan.edu.cn/0f/e1/c13570a135137/page.htm>
<https://news.fudan.edu.cn/2016/0302/c4a56334/page.htm>
<https://jd.fudan.edu.cn/11/0c/c13570a135436/page.htm>
<https://news.fudan.edu.cn/2017/0327/c40a67682/page.htm>
<https://wxxy.fudan.edu.cn/c6/d8/c41234a509656/page.htm>
<https://news.fudan.edu.cn/2024/1121/c3126a143260/page.htm>

COMPLETE NUMBERED REGISTER

SOURCES, CONT.

NOTES 26-31. FULL URLS PRESERVED IN PLAIN TEXT FOR DIRECT REVIEW.

- 26** Fulgent Genetics, Inc., Schedule 14A proxy statement, filed 31 Mar. 2026: "Mr. Hsieh has served as a trustee at the University of Southern California since 2007 and at Fudan University in China since 2011." · 复旦大学 治理架构, 复旦大学校董会 (第八届) — 谢明 listed among the 校董: · Fulgent Genetics investor-relations biography, repeating the Fudan trusteeship
- <https://www.sec.gov/Archives/edgar/data/1674930/000167493026000020/flgt-20260331.htm>
- <https://www.fudan.edu.cn/448/>
- <https://ir.fulgentgenetics.com/board-member/ming-hsieh/>
- 27** 复旦大学, seventh board of trustees, third session, 16 Dec. 2022 — 谢明 (Ming Hsieh) listed among attending trustees advising on the university's development. · Fudan University, inauguration ceremony of the fifth university board, November 2011 — Bai Xuefeng recorded as Hsieh's representative: · 复旦大学校友会, Greater Bay Area cooperation and development conference, Guangzhou, 25 Feb. 2023 — "谢明校董代表、福君基因销售总监刘海情" (Trustee Xie Ming's representative, Fujun Gene sales director Liu Haiqing).
- <https://news.fudan.edu.cn/2022/1217/c234a133602/page.htm>
- <https://www.px.fudan.edu.cn/0b/8e/c13570a134030/page.htm>
- <https://alumni.fudan.edu.cn/61/46/c29410a483654/page.htm>
- 28** Fortinet, Board of Directors — Ming Hsieh, director since April 2013. · Cogent Systems: founded 1990, IPO 2004, acquired by 3M 2010; Fulgent Genetics.
- <https://investor.fortinet.com/board-directors/ming-hsieh>
- 29** Fortinet, "Former Governor, U.S. Commerce Secretary, and U.S. Ambassador, Gary Locke, Joins Fortinet Board of Directors," 28 Sept. 2015. Governor of Washington 1997-2005; U.S. Secretary of Commerce 2009-2011; U.S. Ambassador to China 2011-2014.
- <https://investor.fortinet.com/news-releases/news-release-details/former-governor-us-commerce-secretary-and-us-ambassador-gary/>
- 30** Fortinet, "Fortinet Launches Fortinet Federal, Inc. and its Board of Directors," 15 May 2017. Board as announced: Mike McConnell (former Director of National Intelligence; former Director, NSA; Vice Admiral, U.S. Navy, ret.); Gary Locke; Phil Quade (Fortinet CISO, former NSA Cyber Task Force); John Whittle; Mike Bossert.
- <https://investor.fortinet.com/news-releases/news-release-details/fortinet-launches-fortinet-federal-inc-and-its-board-directors>
- 31** Fortinet, "Fortinet Appoints Distinguished Public Sector Leader Janet Napolitano to its Board of Directors," 12 Nov. 2024.
- <https://www.globenewswire.com/news-release/2024/11/12/2979300/0/en/Fortinet-Appoints-Distinguished-Public-Sector-Leader-Janet-Napolitano-to-its-Board-of-Directors.html>

COMPLETE NUMBERED REGISTER

SOURCES, CONT.

NOTES 32-36. FULL URLS PRESERVED IN PLAIN TEXT FOR DIRECT REVIEW.

32 USAspending.gov, Department of the Army contract W91CRB10C0064, awarding office W6QK ACC-APG, signed 20 Apr. 2010, period of performance from 16 Apr. 2010, total obligations \$1,124,780; recipient recorded under Cogent's later name, Gemalto Cogent, Inc. · University of Southern California, Signal Analysis and Interpretation Laboratory project listing, "Improving Accuracy, Speed and Usability of Multi-Modal Biometric Handheld Devices," sponsor Army Research Laboratory, collaborator Cogent Systems. · Michigan State University Department of Computer Science and Engineering, "Biometric Fusion," announcement of 5 Oct. 2010. · West Virginia University, "California businessman, company donate \$5.5 million to WVU," 14 Nov. 2007, and "Ming Hsieh Hall to be dedicated Nov. 14," 12 Nov. 2007. · West Virginia University, "Entrepreneur Ming Hsieh Donates \$250K to WVU Forensics Program," 21 May 2014. Sources: Army award; WVU gifts; archived MSU announcement; USC project list. Full URLs follow.

https://www.usaspending.gov/award/CONT_AWD_W91CRB10C0064_9700_-NONE_-NONE-

<http://wvutoday-archive.wvu.edu/n/2007/11/14/6326.html>

<https://wvutoday-archive.wvu.edu/n/2014/05/21/entrepreneur-ming-hsieh-donates-250k-to-wvu-forensics-program.html>

<https://web.archive.org/web/20221101114906/http://www.cse.msu.edu/About/highlight/?id=352>

<https://sail.usc.edu/projects/>

33 Anil K. Jain, "Fusion Aspects of Non-Cooperative Biometrics," presentation to the U.S. Army Science Board, 28 Mar. 2011.

http://biometrics.cse.msu.edu/Presentations/MultiBiometrics_ASB_MArch28.pdf

34 Michigan State University, Federal Awards Supplemental Information, Schedule of Expenditures of Federal Awards, years ended 30 June 2011 and 30 June 2012, schedule p. 15 in each: "COGENT DOD," grantor Cogent, Inc., CFDA 12.431 — \$112,092 (FY2011) and \$35,400 (FY2012), \$147,492 combined. Classified as Defense pass-through expenditure, not a private gift. FY2011; FY2012.

<https://edge.sitecorecloud.io/michigansta4a14-msu70a4-prod718c-8cd0/media/project/msu/controller/docs/fa/financialstatements/a13320102011.pdf>

<https://edge.sitecorecloud.io/michigansta4a14-msu70a4-prod718c-8cd0/media/project/msu/controller/docs/fa/financialstatements/a13320112012.pdf>

35 Cogent, Inc., Schedule 14D-9, filed with the Securities and Exchange Commission 10 Sept. 2010: "Mr. Hsieh and certain entities controlled by Mr. Hsieh held approximately 34,369,965 Shares on August 27, 2010, representing approximately 38.9% of Cogent's outstanding Shares." · Joint press release of Cogent, Inc. and 3M Company, filed as exhibit (a)(5)(D) to the same Schedule; 3M investor-relations copy.

<https://www.sec.gov/Archives/edgar/data/1289434/000119312510208203/dsc14d9.htm>

<https://www.sec.gov/Archives/edgar/data/1289434/000119312510208203/dex99a5d.htm>

https://investors.3m.com/financials/sec-filings/content/0001104659-10-046504/a10-16536_1ex99d1.htm

36 Michigan State University, "Anil Jain elected Foreign Member by the Chinese Academy of Sciences," 17 Dec. 2019.

<https://msutoday.msu.edu/news/2019/12/anil-jain-elected-foreign-member-by-the-chinese-academy-of-sciences>



KEEP THE RECEIPTS

INDEPENDENT INVESTIGATIONS • SOURCE-LINKED THREADS
DOCUMENTARY EVIDENCE • IMAGES AND VIDEO

GUSQUIXOTE.COM