

END OF AN ERA, PART V:

PAPER TIGER DIPLOMACY

BY NATHAN WALKER

SEPTEMBER 25, 2026

4,349 WORDS / 129 NOTES

PAPER TIGER DIPLOMACY

Opening 03
Before the tragedy 04
Kuala Lumpur 05
Birth of Cyberwarfare 06
The other side of the story 08
Canada 09
Good intentions with unintended consequences 10
Sanjiang 11
Wormhole design 12
The bridge is built 13
Standard American foreign policy 16
The bridge became functional 17
Around the wire 19
Talent and financial funnels 20
The cyber waves 21
October Surprises 24
Spy games 26
Putting 25 years into perspective 31
End notes 38
Additional source material 42

SECTION 1

Opening

01

Before September 11, a Michigan voice-network company[1] had a sales partner in Zhuhai[2] [3] listed within China's Sanjiang aerospace group.[4] Across the water in Hong Kong, a Chinese billionaire linked Canadian finance[5] to Chinese Academy of Sciences technology alliances;[6] a separate Canadian venture shared Sudan's oil-export project with China's state oil company.[7] [8] U.S. records also described Chinese satellite[9] and military-aircraft cooperation with Iran and Pakistan,[10] and missile-technology supply to Iran.[11] These were distinct channels of the U.S.'s normalized relations with China. Yet each placed consequential technology, capital, and intelligence in the hands of aan elite circle spanning national borders, and who had the protections of national security information. While those centers of power blossomed, the CIA knew that terrorists had obtained U.S. visas, but held back a report intended for the FBI; the bureau did not receive later travel information until August 2001.[12] [13] The record existed, but the hindsight for the general public to assemble the full breadth of intelligence did not.

SECTION 2

Before the tragedy

02

In February-March 1998, the Solar Sunrise intrusions reached more than five hundred military, civilian-government and private systems while Washington prepared for possible military operations against Iraq.[14] You read that right: Iraq, 1998. The intruders exploited a known Solaris weakness, gained privileged access, installed password collectors and left backdoors.[14] The immediate attackers were identified, but the episode demonstrated how a campaign against American systems could be misconstrued as a state operation.[14] Later, in August, al-Qaeda bombed the U.S. embassies in Kenya and Tanzania.[15]

Modern cyber disclosures show the duration such access can have. In 2024, CISA, the FBI, NSA and partners reported that PRC state-sponsored Volt Typhoon actors had maintained access to some U.S. critical-infrastructure environments for at least five years.[16] The advisory described stolen credentials, living-off-the-land techniques and repeated returns to victim systems.[16] That is a contemporary case removed from this story, but interconnected with the same organizations. It demonstrates the long-persistence problem the 2001 defenders could scarcely measure at national scale, and the recluctance or negligence by the American national security-state to mitigate those dangers without first exploiting foreseeable downstream crises.

SECTION 3

Kuala Lumpur

03

On April 7, 1999, the U.S. consulate in Jeddah issued 9/11 hijacker Khalid al-Mihdhar a visa.[12] Jeddah was a major Saudi port facing Sudan across the Red Sea, in the country where John Brennan served as CIA station chief during 1996-99. Sometime in mid-1999, Brennan became CIA Director Tenet's chief of staff.[17] When surveillance identified Mihdhar at a January 2000 meeting in Kuala Lumpur, CIA knew he had a U.S. visa.[12] [13] An FBI detailee at CIA drafted a report for FBI channels that included the visa and travel information. A CIA supervisor marked it to be held and it was therefore never sent.[13] By March, CIA also knew Nawaf al-Hazmi had entered Los Angeles. The FBI did not receive that travel information until August 2001.[13]

After a November 30, 1999 intelligence intercept, Jordanian authorities broke up a cell preparing attacks for the millennium.[18] U.S. customs officers stopped Ahmed Ressam as he brought explosives from Canada toward Los Angeles International Airport.[18] Al-Qaeda's attempted strike on the USS The Sullivans in Aden failed in January 2000, but the organization struck the USS Cole there in October.[18] [19] The Kuala Lumpur intel-gathering included operatives connected to the Cole plot as well as men later involved in the 9/11 operation.[18] These were distinct operations and disrupted plans spanning several countries, while select details of the same intelligence remained at separate offices.

SECTION 4

Birth of Cyberwarfare

04

The same pre-9/11 years brought a public fight over encryption access, a federal push to defend computerized infrastructure, and a widely publicized year-2000 ("Y2K") remediation deadline. Technology companies contested proposals for government access to encryption keys.[20] [21] Separately, the 1997 President's Commission on Critical Infrastructure Protection led to PDD-63 in May 1998, and the FBI's National Infrastructure Protection Center began work that year[22].

FedCIRC handled federal civilian incidents, while Carnegie Mellon's CERT Coordination Center received 419 vulnerability reports and handled 8,268 computer-security incidents in 1999.[22] [23] Federal teams also planned heightened monitoring for the millennium rollover.[22] CIA launched In-Q-It in 1999 to connect intelligence needs with private technology companies and universities.[24] This was soon rebranded into its modern "In-Q-Tel" and directed by university, investor, defense, and public-sector executives.[24]

GRAPHIC 01

FEDERAL CYBER RESPONSE

PDD-63

22 MAY 1998 · PRESIDENTIAL DIRECTIVE

FOR OFFICIAL USE ONLY 20365

THE WHITE HOUSE
WASHINGTON

May 22, 1998

PRESIDENTIAL DECISION DIRECTIVE/NSC-63

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF VETERANS AFFAIRS
ADMINISTRATOR, ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
THE ASSISTANT TO THE PRESIDENT FOR ECONOMIC POLICY
THE ASSISTANT TO THE PRESIDENT FOR SCIENCE AND TECHNOLOGY
THE CHAIRMAN, JOINT CHIEFS OF STAFF
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: Critical Infrastructure Protection

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation,

Protect critical infrastructure from physical and cyber attacks.

PDD-63, p. 1 · [22 + directive]

NIPC National Infrastructure Protection Center

Warning and Information Centers

As part of a national warning and information sharing system, I immediately authorize the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, I also direct the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

FBI-based interagency center
Threat assessment · warnings · investigations · response

PDD-63, p. 12 · [22]

CERT® Coordination Center
1999 Annual Report



FedCIRC

Civilian federal incident response
GSA-managed; CERT/CC-operated · OCT 1998

CERT/CC

Carnegie Mellon · vulnerability and incident response
1999: 419 vulnerability reports · 8,268 incidents [23]

SOURCES: PDD-63 · [22] GAO-01-1168T · [23] CERT/CC 1999 Annual Report

SECTION 5

The other side of the story

05

In Tsinghua University's network orbit, the China Education and Research Network established CCERT in May 1999 as an incident-response center.[25] [26] [27] CERNET signed an interconnection agreement with the U.S. Internet2 consortium in 2000.[25] As U.S. technology shares fell after their March 2000 peak,[28] Semiconductor Manufacturing International Corporation began building its first Shanghai wafer fab in August 2000; pilot production began in September 2001 and commercial production in January 2002.[29]

The spate of pre-9/11 cyberattacks' mechanics were being written about inside Chinese universities while similar attacks hit American networks. A 1997 University of Electronic Science and Technology of China paper treated malicious programs as tools of information warfare, including propagation, latency and back-door access.[30] Tsinghua researchers submitted a distributed intrusion-detection design in September 1999 that modeled network scanning and worm spread.[31] In April and May 2001, Southeast University's NJCERT received reports of hosts scanning ports 111 and 80. NJCERT's May 19 analysis described propagation through Solaris sadmind and Microsoft IIS weaknesses, code upload and reboot persistence.[32]

SECTION 6

Canada

06

Canada developed a less publicized, quieter role in the pre-attack picture. Hong Kong-based Sun Wah's archived financial history places its majority stake in Canada's Kingsway International Group in 1998, the year Sun Wah says it began high-technology alliances with Chinese Academy of Sciences (CAS) institutes.[5] [6] A later interview dates Sun Wah president Jonathan Choi's appointment as an economic adviser to the CAS president to 1998, and MSU identified him in that role in 2004.[33] [34] He also appears in the CPPCC's 1998 National Committee membership roster, years before a 2020 Hong Kong exchange filing described him as a Standing Committee member.[35] [36]

Along another Canadian lead, founder Sheema Khan's 2003 affidavit recounted CAIR-branded chapters in Montreal in 1996 and Ottawa in 1998, followed by CAIR-CAN's incorporation in June 2000.[37] [38] NCCM, the successor organization, says it has always been independent of CAIR in the United States but the affidavit identified a U.S. trademark license, later raised in Canadian Senate testimony.[37] [38] [39] Across the border in the U.S., the Wen Ho Lee case linked these advocacy circles in print: Committee of 100 cofounder Henry Tang later recalled that Lee came to the group through defense lawyer Brian Sun; a March 2000 *Minaret* article to which Lee's daughter Alberta contributed invoked a CAIR alert and directed readers to CAIR for legal referrals.[40] [41] Lee was indicted in December 1999 for mishandling classified nuclear-weapons information, not for selling secrets to China.[42]

Another Canadian-Chinese route ran through Sudan. Talisman Energy acquired a 25 percent interest in the Greater Nile Oil Project in 1998 alongside China National Petroleum Corporation's 40 percent stake.[7] [8] The consortium began shipping oil through its pipeline to Port Sudan on the Red Sea in August 1999.[8] There were multiple avenues through the Canadian private sector for exchanges off the books.

SECTION 7

Good intentions with unintended consequences

07

Michigan-based CC&T Technologies was incorporated in February 1998.[1] Lionel Ni and En-Wei Chai built a business around Internet telephony, network-phone servers and the equipment and software needed to move voice traffic through data networks.[1] [2] A contemporary trade reporter described CC&T as a partner of 3JET Network Engineering & Service in Zhuhai, China.[2] An archived 3JET page identified CC&T as its U.S. agent; Sanjiang Aerospace Group's archived site listed Zhuhai Siruijie-3JET-among its companies.[3] [4] This is a well-documented commercial and institutional route running from Okemos, Michigan through Zhuhai into a Chinese aerospace group, documented back to 1998.

SECTION 8

Sanjiang

08

A September 1999 U.S. Army War College study identified Sanjiang's Base 066 as a developer of solid-fueled tactical ballistic missiles, including the M-11.[43] A later corporate filing dates the establishment of its Wuhan import-export company to November 1998.[44] Ni has since recalled securing $2 million in initial 3JET funding and concentrating on product delivery to those investors.[45] The wider U.S.-China technology record was already consequential: Congress's 1999 Cox report found that Hughes and Loral supplied launch-failure analysis affecting China's Long March guidance system,[46] while a 2002 GAO review documented China's acquisition of foreign semiconductor production technology for both consumer electronics and more capable weapons systems.[47]

SECTION 9

Wormhole design

09

C C&T's EMIP-1 was part of that market. An independent August 1999 test examined the Linux-based Internet/WAN emulator supplied on an industrial PC.[48] It could impose bandwidth limits, packet loss and delay, generate background traffic and report packet statistics while developers evaluated networked products.[48] Its usefulness was plain: a vendor could make a local test network behave like an unreliable long-distance one before deploying a voice service. CC&T's own archived product page later said a Chinese government laboratory was using EMIP-1 to evaluate VoIP equipment.[49] The laboratory was unnamed in the page; the contemporaneous claim nevertheless put the product's evaluation inside a Chinese government setting by April 2001.[49]

The American public-research route was visible too. NIST had made its own Linux network-emulation tool, NIST Net, publicly available by 1998.[50] [51] An NSF award beginning in 2000 funded Michigan State University equipment for the EMPOWER network-emulation testbed; Pei Zheng and Ni published an EMPOWER framework in 2002.[52] [53] MSU listed a $30,000 CC&T gift to Engineering for fiscal 2000-01.[54] Ni's student Vibhavasu (Vasu) Vuppala coauthored a 1999 paper with him on virtual network ports.[55] [56] He later co-chaired a distributed-data-services collaboration at MSU's Facility for Rare Isotope Beams (FRIB), whose partners included Brookhaven and Beijing's Institute for High Energy Physics.[57]

SECTION 10

The bridge is built

10

The Chinese-side product record did not stop at a company name. Sanjiang's archived late-2001 catalog listed an NPS Network Integrated System among its Internet-telephony products;[58] its English corporate overview claimed research, manufacturing and intellectual property in Internet-telephone service devices.[59] 3JET's archived product page identified specific NPS gateway models and an accompanying control-and-management system: call routing, charging and account authentication, browser-operated management, and SeeNPS monitoring of real-time system workload and voice quality[60]. CC&T's own operations page described distributed ChargeNPS settlement across multiple network operators and remote technical support through SeeNPS.[61] These were commercial servers, gateways and software with documented operational functions during the shift from conventional telephones to data networks.

GRAPHIC 02

NPS: VOICE, MONITORING & SETTLEMENT

3JET / GATEWAYS + CONTROL [60]

ARCHIVE · 11 DEC 2000

8 Channel Gateway System NPS-E-8

- Support 8 full-duplex voice lines, easy upgradable to 16 channels
- Facilitated with Communication Control System

NPS-E-8 · 8 full-duplex lines, upgradeable to 16

CONTROL / ROUTING + CHARGING

Communication Control System Basic NPS 1.90	Charging System LocalAgent 2.36
Monitoring System See NPS	Network Management System CompanyAgent 2.27 & WebAgent 2.15

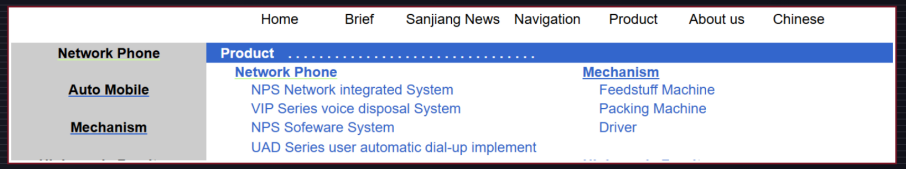
SeeNPS / REAL-TIME MONITORING

See NPS allows real-time monitoring of current system activities and has the following features:

- Web-based design to allow real-time monitoring from any web browser;
- Real-time monitoring of the work status and work loads;
- Real-time monitoring of the voice quality parameter;

Workload · voice quality · remote browser access

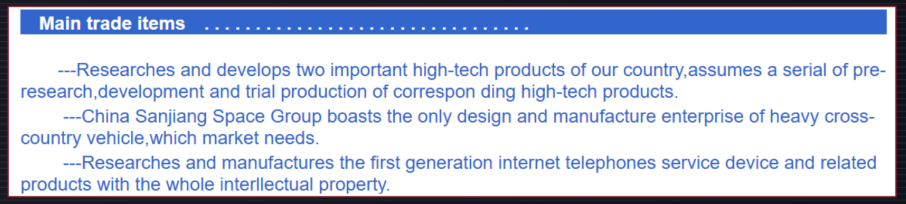
SANJIANG / CATALOG [58]



NPS listed under "Network Phone"

ARCHIVE · 24 DEC 2001

SANJIANG / CORPORATE OVERVIEW [59]



Develops and manufactures Internet-telephone devices and related intellectual property.

ARCHIVE · 15 FEB 2002

CC&T / SETTLEMENT [61]

CC&T Clearing House

As part of the global service network functions, CC&T currently coordinates individual network operators and provide inter-operator settlement for calls made between different POPs. CC&T's ChargeNPS supports a service network with multiple independent companies. Furthermore, the distributed and scalable architecture of ChargeNPS can handle a huge amount of accounts created by different companies. The SettleNPS software also automates the settlement computation among different NPS owners.

ChargeNPS: multiple companies and accounts
SettleNPS: settlement among NPS owners

SeeNPS / REMOTE SUPPORT [61]

Remote identification and resolution of problems

CC&T ARCHIVE · 06 APR 2001

SOURCES: [58–61] ARCHIVED COMPANY PAGES

CONTINUED

The regional technology routes were active in the same years. China's space agency records an April 1998 small-satellite cooperation memorandum with Iran and Pakistan;[9] an August 2000 U.S. Army War College study documents CATIC's military-aircraft exports to both countries and its 1998 fighter co-development agreement with Pakistan.[10] A CIA assessment covering January-June 2000, entered in the Congressional Record on September 6, 2001, described continuing Chinese work on two Iranian nuclear projects and Chinese entities among Iran's largest missile-technology suppliers.[11] Chinese firms also laid fiber-optic links for Iraqi air defenses before the 2003 invasion;[62] the Iraq Survey Group later recovered records of an October 2001 Syrian approach to Chinese air-defense firms on Iraq's behalf.[63]

SECTION 11

Standard American foreign policy

11

The Committee of 100 occupied the foreign and domestic policy side of that landscape. Its own history records a 1998 China-policy paper delivered to National Security Adviser Sandy Berger, 1999 activity around Wen Ho Lee, a 2000 Beijing high-tech financing conference and a 2001 Greater China delegation.[64] Years later, it and the Council on American-Islamic Relations signed the same March 2018 letter seeking a meeting with FBI Director Christopher Wray over his comments about Chinese-origin students and researchers.[65] The coalition was public. This is how civil rights and diaspora politics met in the same institutional arena.

Henry Tang, C100 chair from 1996 to 2002, already knew 7 World Trade Center from inside: a 1992 Labor Department directory listed him as a Salomon Brothers vice president on its 40th floor.[66] [67] A Port Authority alteration record reproduced by NIST still identified that floor as Salomon Smith Barney space in 1999.[68] Retired Maj. Gen. John Fugh, the Army's former Judge Advocate General, joined C100 in 1993 and later guided China operations for McDonnell Douglas, Boeing and Enron.[69] [70] He led its 2001 Greater China delegation; in 2002, he and Tang became C100 co-chairs.[70] [64]

SECTION 12

The bridge became functional

12

Interstellar (Hangzhou), doing business as eBanswers, described itself as initiated and established by CC&T and listed e-commerce, call centers, customer-management and VoIP-gateway work.[71] Its October 8, 2001 notice said LJ Connection had become its Midwest U.S. agent for the e-shop and e-CRM product lines the previous day.[72] LJ's January 2002 product pages described PBX, VoIP, unified messaging, gateway, WebCall and related services.[73] Pages at the same LJ domain later carried Konnech branding with materially similar product descriptions.[74] Michigan records date LJ Connection's incorporation to July 2001 and Konnech's to March 2002; a later Michigan economic-development release described Konnech's business origins as 1999.[75]

GRAPHIC 03

THE COMMERCIAL TRAIL

CC&T → eBanswers [71]

COMPANY ORIGIN

星际（杭州）技术有限公司是一家由美国CC&T公司在中国发起设立的一家高新技术企业，

“Initiated and established” by U.S. CC&T
Products: eCRM · call centers · VoIP gateways

ARCHIVE · 02 SEP 2001

eBanswers → LJ Connection [72]

E-SHOP / E-CRM AGENT APPOINTMENT

Ebanswers 和 LJ Connection 建立合作

2001-10-8 12:55:04

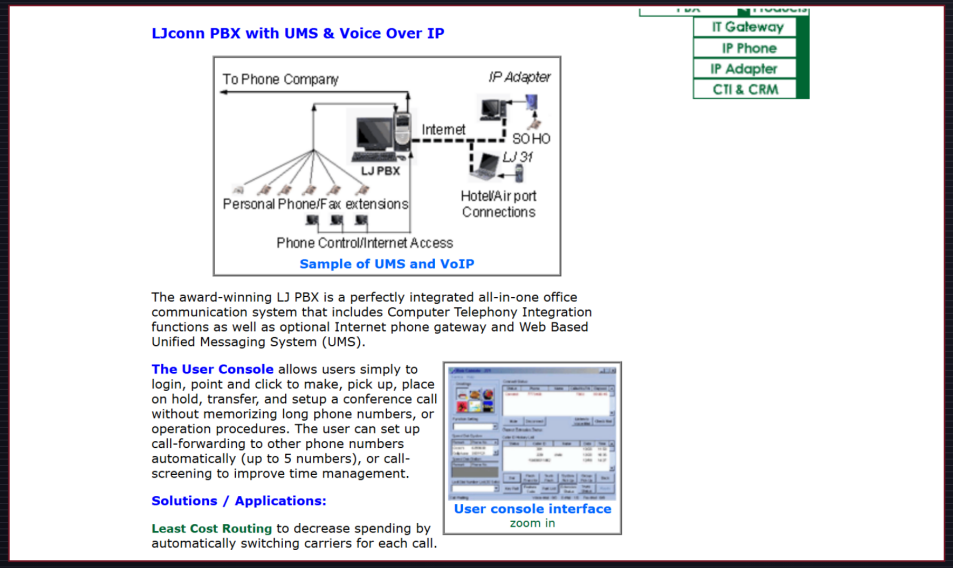
LJ Connection 成为Ebanswers 在美国的代理
十月七日，LJ Connection 成为ebanswers e-shop, e-CRM系列产品在美国的代理商，主要面向美国的中西部地区。

U.S. Midwest agent for e-shop and e-CRM
Effective 07 OCT 2001 · Posted 08 OCT 2001

ARCHIVE · 25 FEB 2005

LJ PRODUCT PAGE [73]

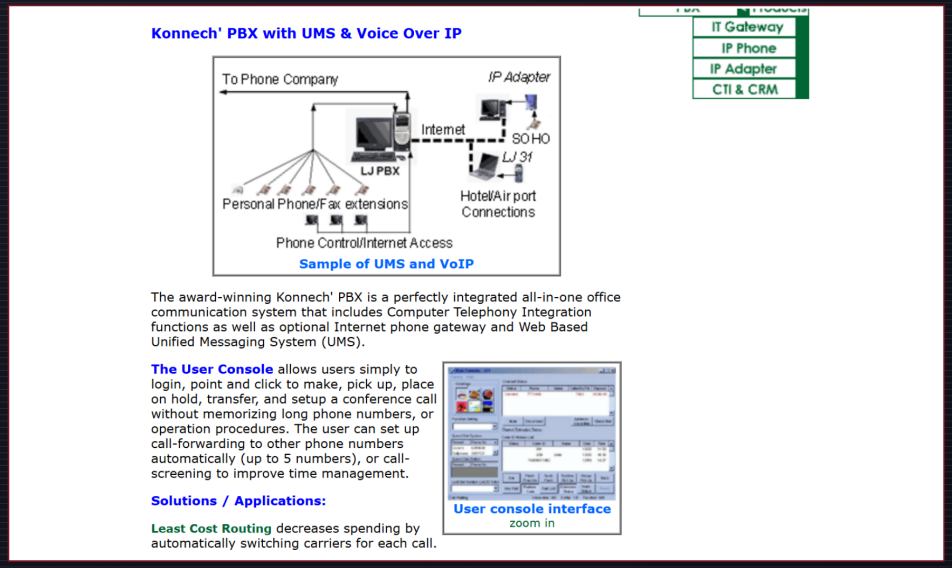
ARCHIVE · 06 JAN 2002



ljconn.com/products/products_pbx.html

KONNECH-BRANDED PAGE [74]

ARCHIVE · 03 OCT 2002



Same domain · later branding

KONNECH HISTORY [75]

Founded 1999 · Incorporated 2002

SOURCES: COMPANY ARCHIVES [71–74] · MEDC, 09 DEC 2021 [75]

SECTION 13

Around the wire

13

Sun Wah established its high-technology group in 1998 and described alliances with Chinese Academy of Sciences institutes and universities.[6] Hong Kong Polytechnic University reported an October 2000 Linux training and development center with Sun Wah Hi-Tech, alongside a Microsoft China academic arrangement.[76] Nanjing University later recorded Sun Wah support for a software research-and-development center beginning in 2002.[77] In 2004, MSU's board recorded a $5 million Sun Wah Education Foundation grant for a U.S.-China education center; the center's governing arrangement divided appointments between MSU and Sun Wah, with Jonathan Choi as first chair.[78] These were named agreements, facilities, funds and board seats.

Sun Wah's Red Flag project was more than a training partnership. An October 2000 release said Sun Wah Hi-Tech had become a shareholder and Red Flag's first authorized master dealer in Asia.[79] It described Red Flag as a Chinese Academy of Sciences Institute of Software venture and presented a server/e-business kit containing browser-based remote Linux monitoring.[79] The same release named enterprises, banks, government departments and the military among markets for the server.[79] The partnership joined a state-rooted operating-system developer to a Hong Kong distributor with university training and overseas sales ambitions.

SECTION 14

Talent and financial funnels

14

AZKEF, the American Zhu Kezhen Education Foundation, offered a direct link from Zhejiang University in Hangzhou, Zhejiang Province to American academia, industry, and infrastructure. AZKEF's early-2000s roster named LJ Connection and Konnech founder Eugene Yu, and Lionel Ni's PhD. student, Xipeng Xiao.[80] A January 2002 Microsoft letter recorded employee gifts eligible for company matching.[81] Zhejiang University later counted $332,762 raised in 1996-2004, 18 U.S.-based lecturers and seven faculty funded for U.S. study.[82] Carnegie Mellon's Chuck Thorpe lectured in 1999, Harvard's Charles Lieber in 2002, and Arizona professor Fei-Yue Wang also held CAS Institute of Automation posts before later leading AZKEF.[83] [84] [85] Parallel U.S. vehicles included the Tsinghua Education Foundation in North America, registered in 1997;[86] Friends of Tsinghua SEM, tax-recognized in 2001;[87] and Fudan's U.S. foundation, registered in 2006.[88]

American institutions sustained these routes. Microsoft Research Asia began its Chinese-university joint-laboratory program in 1999,[89] and a later ministry partnership brought Lionel Ni into an HKUST lab.[90] Boeing subsequently commissioned HKUST aircraft and airport-maintenance wireless research,[91] while Ni's CC&T "seed" Konnech appeared in a 2010 Defense Department software procurement.[92] Alongside Sun Wah's CAS and MSU agreements,[6] [78] these distinct programs show the continuing institutional demand for Chinese-linked research, talent and production even as U.S. authorities documented theft and transfer risks in the same markets.[93] [94] The commercial benefits and the security warnings grew together.

SECTION 15

The cyber waves

15

The aviation attacks of 9/11 arrived amid a rising tide of publicized network incidents. CERT's 2001 record separately dated the vulnerabilities, advisories and active worms: the sadmind/IIS campaign, Code Red in July, Code Red II in August and Nimda in September.[95] [96] Code Red II installed persistent access on affected IIS systems.[96] CERT reported that Nimda scanned for backdoors left by Code Red II and sadmind/IIS while spreading by email, shared files, compromised websites and vulnerable servers.[95] [97] F-Secure reported that ordinary infected user computers could reach intranet websites behind firewalls that Code Red could not reach directly.[97] The technical record itself therefore explains that one wave of exposure led into the next without making all the worms the same code.

The sequence is remarkably important. CERT's Nimda advisory was released September 18 and revised September 25; F-Secure says the first variant was found September 18.[95] [97] Those are announcement and detection dates, but not proof of the first launch.[95] [97] CERT described a host-local registry value under which Nimda would repeat address harvesting and email sending every ten days.[95] At about 15:00 **GMT** on October 11, F-Secure observed hundreds of Nimda.A emails that appeared to come from its research manager's old company domain.[97] F-Secure traced them apparently to an infected machine somewhere in Canada.[97]

GRAPHIC 04

2001: THE CYBER WAVES

08 MAY	19 JUN	19 JUL	06 AUG	18–21 SEP	11 OCT	26 OCT	11 NOV
sadmind/IIS	IIS flaw	Code Red	CERNET	Nimda	~15:00 GMT	Klez / ElKern	Klez.D
Advisory [95]	Disclosure [95]	Advisory [95]	Notice	Advisory / impact	Email burst [97]	First located [98]	First seen [98]

CERNET / CODE RED

06 AUG 2001 · NOTICE

关于防范IIS红色蠕虫病毒CodeRed的紧急通知

2001-08-06

CERNET各地区网络中心、省节点网络中心和各联网单位网络中心：

自7月中旬以来，IIS 红色蠕虫病毒Code Red在互联网上大规模泛滥，8月初进入了第二个高峰期，近日已在一些CERNET联网单位发现这种病毒，并且危害严重。目前正值全国高校网络招生的关键时期，为了确保中国教育和科研计算机网CERNET的安全可靠运行，提高抗攻击能力，特对全网的各级网络运行管理中心发出此紧急通知。

Connected institutions infected; report to CCERT
Spread: mid-July · second peak: early August

CERT/CC / NIMDA [95]

RELEASE · 18 SEP 2001 / REVISION · 25 SEP

26 CA-2001-26: Nimda Worm

Original release date: September 18, 2001
Revised: September 25, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

- from client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

Scans backdoors left by Code Red II and sadmind/IIS.

CCERT / NIMDA WARNING

SIGNED · 19 SEP / RAPID SPREAD · FROM 18 SEP

中国教育和科研计算机网
China Education and Research Network

您当前的位置: 首页 > CERNET > CERNET动态 > 学术动态

关于防范Nimda蠕虫病毒的紧急通知

CERNET各地区网络中心、省节点网络中心和各联网单位网络中心：

9月18日，一种更具破坏力的恶意代码——Nimda worm 蠕虫开始在Internet上迅速蔓延传播。Nimda蠕虫病毒感染Windows 系列多种计算机系统，通过多种渠道传播，其传播速度之快、影响范围之广、破坏力之强都超过Code Red II。

目前已经检测到大量被感染的计算机系统，危害严重，希望各部门紧密关注。为了确保中国教育和科研计算机网CERNET的安全可靠运行，提高抗攻击能力，特对全网的各级网络运行管理中心发出此紧急通知。

同样的，客户端机器会扫描有漏洞的IIS 服务器。Nimda 会搜寻以前的IIS蠕虫病毒留下的后门：Code Red II [IN-2001-09] 和 sadmind/IIS worm [CA-2001-11]； 它也试图利用IIS Directory Traversal 漏洞 (VU #111677)。

HEFEI UNIVERSITY OF TECHNOLOGY

21 SEP 2001 · CAMPUS IMPACT NOTICE

关于防范、清除CodeRed 和Nimda蠕虫病毒的紧急通知

浏览量: 317 时间：2001-09-21

九月以来，红色代码蠕虫病毒CodeRed疯狂肆虐我校网络，感染大量服务器，造成网络信息极度拥塞，尤其是影响了网络中心交换机和路由器，使网络信息中心无法为用户提供正常服务。最近，另一种更具破坏力的恶意代码—Nimda蠕虫开始在校园网上迅速蔓延传播，通过多种渠道传播，感染Windows系列多种计算机系统，其传播速度之快、影响范围之广、破坏力之强都超过CodeRed。目前，网络信息中心已经检测到校园网内大量的计算机系统被感染，使校园网络几度瘫痪，危害十分严重。为了确保我校校园网络的安全可靠运行，提高抗攻击能力，特向全校发出紧急通知，请各单位和个人紧密关注病毒感染的情况，彻底清查本单位的计算机系统，安装补丁，清除病毒。

Many systems infected · repeated network paralysis

11 OCT ~15:00 GMT · NIMDA EMAIL BURST [97]

ARTICLE INFERENCE · TEN-DAY TIMER

11 SEP → 21 SEP → 01 OCT → 11 OCT

SOURCES: [95] CERT · CERNET / CCERT · HFUT · [97–98] F-Secure

CONTINUED

October 11 was thirty days after September 11. A machine first infected on September 11 could, on that ten-day schedule, have sent again around September 21 and October 1 before the observed October 11 burst.[95] [97] The October 11 emails are an observation; the September 11 start and intervening mailings are an inference from the documented timer and the calendar.

The same distinction applies to Klez. F-Secure dated the first located Klez/ElKern infections and its detection update to October 26.[98] It first observed Klez.D in the wild on November 11; that variant sought to terminate processes with names including Nimda and Code Red.[98]

The result in 2001 was not merely a collection of memorable malware names. Compromised servers could remain available to later intruders, especially if left unpatched.[95] [96] The pattern lasted: a 2023 multiagency advisory found that in 2022 attackers exploited older vulnerabilities more frequently than newly disclosed ones, targeting unpatched internet-facing systems.[99] Ordinary workstations became scanners.[95] [97] A preserved corporate-record aggregation dates LJ Connection's incorporation to July 2, 2001[100] [101]-days before Code Red was first reported.[102] Infected web pages carried malicious content into browsing sessions.[95] [97] Defenders had to find an attack's origin while incidents crossed organizations, private networks and countries. The public documentation shows a system in which first discovery could come well after the first compromise-and where repairing one visible worm did not reveal every earlier visitor to the same machine.

SECTION 16

October Surprises

16

On October 4, 2001, George Tenet signed the CIA threat assessment used to support President George W. Bush's first authorization for electronic surveillance inside the United States.[103] [104] The analysts who prepared the continuing assessments initially did not know the surveillance program their work supported.[103] Tenet's chief of staff added a recommendation for domestic electronic surveillance, using language he recalled receiving from White House counsel Alberto Gonzales or Vice President Cheney's counsel David Addington.[103] The authorization was renewed again and again.[103]

On October 7, LJ Connection entered the eBanswers ecosystem.[72] On October 11, F-Secure observed the Nimda email burst from Canada.[97] On October 26, it found the first Klez/ElKern infections.[98] Government was acquiring new powers, commercial networks kept expanding and compromised systems kept producing evidence of earlier access.

On November 23, 2001, U.S. authorities arrested Fei Ye and Ming Zhong at San Francisco International Airport as they tried to leave for China with Sun Microsystems and Transmeta trade secrets.[93] They later pleaded guilty to economic espionage and admitted an intended microprocessor venture financed in part through Hangzhou and Zhejiang interests.[93] In another case, former Boeing engineer and naturalized U.S. citizen Dongfan Chung was sentenced in 2010 after convictions for economic espionage benefiting the PRC.[105] Inside the American aerospace market, Boeing agreed in 2006 to pay $615 million to resolve criminal and civil allegations that included its possession of Lockheed Martin launch-vehicle competition material.[106] Defense secrets and competitive information moved through employees and companies, not merely through foreign intrusions. The later record became more explicit about cyber access and semiconductor production. Su Bin pleaded guilty in 2016 to conspiring to hack U.S. defense contractors and send export-controlled military data to China, including C-17 and fighter-aircraft material.[94] Taiwan's UMC pleaded guilty in 2020 to possessing stolen Micron trade secrets in a DRAM project linked to PRC state-owned Fujian Jinhua; the admitted facts included recruitment from Micron's Taiwan operation and off-network laptops.[107] In 2017, ZTE pleaded guilty to shipping U.S.-origin technology to Iran in violation of sanctions, obstruction and false statements.[108] Its own managers described using intermediary or "isolation" companies to conceal supply routes.[108] These proceedings are separate, adjudicated examples of how personnel, intellectual property, supply chains and jurisdiction can be exploited across the same markets that governments also cultivate.

GRAPHIC 05

BUSINESS ROUTES FOR TECHNOLOGY

01 COMMERCIAL INTERFACE / AEROSPACE GROUP

CC&T TECHNOLOGIES → 3JET / ZHUHAI SIRUIJIE → SANJIANG SPACE GROUP

U.S. agent [3]

Established overseas agents:
CC&T Technologies,Inc.,USA
Tel:+1-517-381-8838
Fax:+1-517-381-0887
Email: sales@cctt.com

3JET DIRECTORY

13 OCT 1999 · ARCHIVE [3]

Sanjiang directory [4]

三江航天集团财务有限责任公司
武汉三江航天网络通信有限公司
武汉三江大地物业发展有限责任公司
武汉三江航天商贸有限责任公司
武汉三江航天进出口有限责任公司
宜昌三江航天储运有限责任公司
孝感宇航事业有限责任公司
珠海斯瑞捷网络工程服务公司

珠海斯瑞捷 3JET link

06 APR 2001 · ARCHIVE [4]

State enterprise group [59]

The predecessor of China Sanjiang Space Group is a large rear enterprise,which belongs to the former China Space Industry Ministry.It established on August 1969,and approved by premier Zhou Enlai personally.It was reorganized to form a large enterprise group on April 1993,which conforms to be one of the first 55 large-sized enterprise groups of the state.

15 FEB 2002 · ARCHIVE [59]

02 SEPARATE EXPORT CHANNELS

AVIC / CATIC → IRAN + PAKISTAN

Aircraft exports · AUG 2000 [10]

attack aircraft. These systems have been sold to countries such as Iran, Pakistan, Myanmar, and Sri Lanka. One of CATIC's most recent deals was the 1998 agreement with Pakistan to co-develop the Super-7/FC-1 aircraft. In

AVIC affiliation / aircraft trading [10]

• China National Aero-Technology Import-Export Corporation Group (CATIC Group). The CATIC Group was a subsidiary organization of the Aviation Industries Corporation of China (AVIC), and is now responsible for trading military and civilian aircraft. The CATIC Group is

CHINESE FIRMS → IRAQ

Air-defense links · reported 2003 [62]

Prior to the Iraqi War Chinese firms laid fiberoptic cables enhancing the efficiency of Iraqi air defense systems and reducing their vulnerability to air attack. Chinese

30 OCT 2003 · USCC p.95 [62] · firms unnamed

CHINA → NORTH KOREA

AUG 2000 · country-level report [10]

arms exports overall, China continues to provide sensitive weapons and technology to a range of recipients Washington views with concern: Iran, Myanmar (Burma), North Korea, Pakistan, and others. Thereislittledoubt that

Exporter unnamed

03 CAS / DISTRIBUTION / UNIVERSITY TRAINING

CAS INSTITUTE OF SOFTWARE → RED FLAG + SUN WAH HI-TECH → HONG KONG POLYU

Red Flag co-founder [79]

The Institute of Software, under the CAS, and several world-renowned venture capitalists formed Red Flag Software Co. Ltd. With international

18 OCT 2000 · RELEASE [79]

Shareholder / Asia distributor [79]



Mr Jonathan Choi (left) and Dr Lui Sun-wing.

Linux center · OCT 2000 [76]



Signed, sealed and delivered: Dr Zhang Yaqin (left) and Prof. Poon Chung-kwong.

Separate agreement PolyU–Microsoft

Research / staff exchange

NOV 2000 [76]

3JET / SANJIANG [3,4,59] · ARMY WAR COLLEGE [10] · USCC [62] · SUN WAH / POLYU [76,79]

SECTION 17

Spy games

17

The surveillance build-out had its own history. Congress's 1994 Communications Assistance for Law Enforcement Act required carriers to make authorized interception technically possible, but industry litigation, standards disputes and deadline extensions delayed implementation. The FBI offered a packet-mode deployment initiative in August 2001.[109] The new counterterrorism bill also underwent negotiation: the Senate passed an early version on October 11 and the House acted the next day.[110] A letter containing anthrax was opened in Senate Majority Leader Tom Daschle's office on October 15;[111] the FBI and Justice Department later attributed its spores to a stock held by Bruce Ivins at USAMRIID, Fort Detrick.[112]

Congress completed the USA PATRIOT Act on October 25 and President Bush signed it the following day.[113] Its sections 215 and 216 widened access to business records and non-content electronic routing and addressing information;[113] section 217 authorized interception of a computer trespasser's communications under specified conditions with the system owner's consent.[113] Lawful demands on commercial data and monitoring of intruder traffic now had broader statutory channels alongside the still-unfinished interception infrastructure. In that environment, products that kept communications observable and analyzable had growing institutional value.

LETTERS OF MARQUE / GRAPHIC 06

ACCESS, AUTHORITY & INTRUSION

1994 CALEA enacted

1998 | 1999 | 2000 | 2001 | 2002

POLICY / INSTITUTIONS

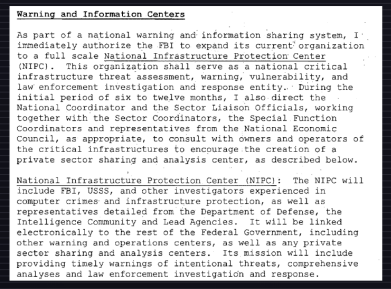
- 1998-05-22 — **PDD-63** — Directive · E4558
- 1998-10 — **NIPC / FedCIRC** — Centers / sponsorship · E4566-67
- 1999-08 — **CALEA / FCC** — Packet-mode mandate [109]
- 2000-08-21 — **CALEA remand** — Four capabilities [109]
- 2001-08 — **FBI packet-mode** — Carrier offer [109]
- 2001-10-04 — **Presidential surveillance** — First authorization [104]
- 2001-10-26 — **USA PATRIOT Act** — §§215-217 [113]
- 2002-04-11 — **FCC remand order** — Due 30 JUN 2002 [109]

INTRUSIONS / WARNINGS

- 01–26 FEB 1998 — **Solar Sunrise** — Incident · E4556
- 1999-03-27 — **Melissa** — CERT advisory · E4282
- 2000-04 — **478 compromised hosts** — NIPC discovery · E4591
- 2001-03-29 ◇ — **Moonlight Maze** — 1998 intrusions reported · E4593
- 2001-07-19 — **Code Red** — CERT advisory · E4336
- 2001-08-04 — **CodeRedII** — Observed / backdoor · E638
- 2001-09-18 — **Nimda** — Advisory / old backdoors · E729

NIPC / WARNING + INVESTIGATION

22 MAY 1998 · PDD-63 p.12 · E4558



Warning and Information Centers

As part of a national warning and information sharing system, I immediately authorize the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, I also direct the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

Assessment / warning / coordination

§217 / INTRUDER TRAFFIC

26 OCT 2001 · P.L. 107-56 [113]

SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.

(2) in section 2511(2), by inserting at the end the following:

"(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

"(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

"(II) the person acting under color of law is lawfully engaged in an investigation;

"(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

"(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.".

Owner authorization + statutory conditions

NIMDA / PRIOR BACKDOORS

18 SEP 2001 · CERT · E729 / E4343

26 CA-2001-26: Nimda Worm

Original release date: September 18, 2001
Revised: September 25, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

- from client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

Code Red II + sadmind/IIS

● Dated — Month / period ◇ Report date PDD-63 · GAO · DOJ OIG · P.L. 107-56 · CERT · CAIDA

CONTINUED

The cost was also measured in military decisions. In February 2002, Tenet described Iraq's contacts with al-Qaeda as tenuous and mutually wary.[114] CIA's June papers treated operational cooperation as a possibility resting on reports of varying reliability.[114] By September, a Counterterrorist Center paper had been circulated to a narrow senior audience, while Pentagon policy officials carried an alternative Iraq-al-Qaeda presentation to White House and vice-presidential staff.[114] [115] [116] The October WMD estimate contained dissent and uncertainty; the public paper did not convey all of it.[115] Later Senate and inspector-general reviews found that important judgments were overstated, caveats lost or differences between products inadequately identified.[115] [116] [117] American forces acted within a picture other people assembled.

One year after the original Tenet assessment, on October 4, 2002, Tenet released a public paper on Iraq's weapons programs.[115] The classified National Intelligence Estimate issued three days earlier contained the State Department's dissent on whether Iraq had reconstituted a nuclear program and the Energy Department's technical judgment about the aluminum tubes at the center of that argument.[115] A Senate investigation later found that the public version omitted important caveats and alternative agency views.[115] [117] Another CIA assessment, *Iraqi Support for Terrorism*, had gone to twelve senior administration officials on September 19.[115] Congress did not receive its copy until October 2003.[115] The audiences were different, but so were the products placed before them.

ATTACKS, PLOTS & CYBER OPERATIONS

1998 · 1999 · 2000 · 2001 · 2002

AL-QAEDA & LINKED PLOTS

- MAR 1998 — **Ressam** — Afghanistan travel
- 16 SEP 1998 — **Salim** — Arrest · Germany
- FEB 1999 — **Ressam** — Return · Canada
- 03 JAN 2000 — **Millennium plans** — Failed / disrupted
- 05–08 JAN 2000 — **Kuala Lumpur** — Gathering
- 12 OCT 2000 — **USS Cole** — Bombing
- 11 SEP 2001 — **9/11** — Commission ch.1

JEMAAH ISLAMIYAH

2000–2001 · Singapore reconnaissance
Boating surveys

08 DEC 2001 · ISD operation

12 OCT 2002 — **Bali bombings** — ISD / MHA 2021

THREAT REPORTS

- 05 MAR 1998 · E2254 — **Three Brothers Islamic Front** — Possible hoax
- 04 DEC 1998 · E567 — **Islamic Group / Islambuli** — Aircraft plans reported
- 30 DEC 1999 · E2445 — **Muslim Hackers Club** — Detainee links / Y2K warning

CYBER INTRUSIONS

- 01–26 FEB 1998 — **Solar Sunrise · E4556** — California / Israeli suspects
- 1998 → 29 MAR 2001 REPORT — **Moonlight Maze · E4593**
- 08 MAY · sadmind/IIS · advisory
- 19 JUL · Code Red · advisory
- 04 AUG · CodeRedII · observed
- 18 SEP · Nimda · advisory
- 26 OCT · Klez/ElKern · observed

MOMBASA

28 NOV 2002 · Hotel bomb / aircraft missiles missed · claims varied · E4609–10

CIA PDB / 30 DEC 1999

p.46 · released 2026 · E2445

(30 December 1999) Terrorism: Near-Term Threat Undiminished

Computer degradations due to Y2K glitches are likely to facilitate opportunistic attacks by groups or individuals, including hackers who may be affiliated with terrorist organizations. Bin Ladin affiliates arrested this month in Pakistan, for instance, are linked to the extremist Muslim Hackers Club.

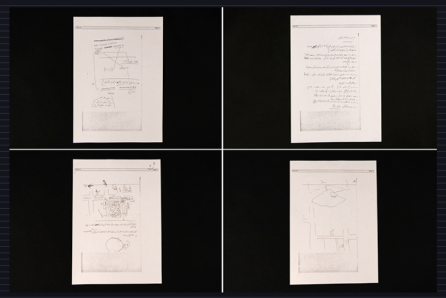
MOONLIGHT MAZE / GAO 2001

GAO-01-341 p.5 · E4593

Even as greater attention has been paid to incident response, cyber threats and attacks continue to affect the operations of DOD and other federal systems and networks. Since 1998, a number of federal systems have been subjected to a series of recurring, "stealth-like" attacks, code-named Moonlight Maze, that federal incident response officials have attributed to foreign entities and are still investigating. More recently, the "ILOVEYOU" virus attack affected electronic mail and other systems worldwide.[3]

SINGAPORE JI / PLOT EVIDENCE

ISD / MHA 2021 · E4624 / E4637 / E4638



Notes / route maps
Yishun MRT / Sembawang





Reconnaissance
Water facilities / pipelines

Surveillance / camera
08 DEC 2001 · ISD operation

CONTINUED

The attacks beyond the United States continued. Singapore's Internal Security Department began arrests of a Jemaah Islamiyah cell in December 2001 after its members had surveyed diplomatic, military and infrastructure targets.[118] On October 12, 2002, Jemaah Islamiyah bombed Bali.[119] On November 28, bombers struck a hotel in Mombasa while a missile attack missed a departing Israeli Boeing 757.[120]

SECTION 18

Putting 25 years into perspective

18

Between 1998 and 2002, American funding and customers helped sustain cross-border laboratories, server businesses and semiconductor production[1] [6] [78] while U.S. investigations warned of technology flowing into China's military-commercial system.[46] [47] The hijackers used international finance, travel, flight training and public computers[121] [122] during the same years that intelligence about particular men failed to reach the agencies that could act on it.[12] [13] Worms and backdoors made network access harder to date or even attribute.[95] [96] After the attacks, surveillance authority expanded[103] [104] and the Iraq case showed how differently scoped intelligence products-or the withholding of them-could steer global decisionmaking.[115] [117]

An FBI report places Mohamed Atta at a Las Vegas cybercafé on June 28-30, 2001, Khalid al-Mihdhar and Nawaf al-Hazmi at New Jersey public computers on August 9, and Atta at Fort Lee's Web Station on August 12.[121] The Moussaoui indictment records Ziad Jarrah's August 22 purchase of GPS equipment and Boeing 757 cockpit diagrams.[122] In 2004, 9/11 Commission staff described the training value of commercial cockpit software and the navigational possibilities of a 757/767 flight-management computer.[123] The NTSB's recovered-data study more specifically found Mode Control Panel inputs steering Flights 77 and 93 during their hijacked segments and autopilots disengaged before the final impacts.[124] The reports establish distinct preparations, capabilities and observed flight modes. They also define the next disclosure question: what surviving onboard, airline and ground-system records were examined together with the cyber-incident record, and what would their joint analysis show?

RESEARCH & NETWORK ACCESS

SOUTHEAST UNIVERSITY / NJCERT [32]

19 MAY 2001 · MANUSCRIPT FINALIZED

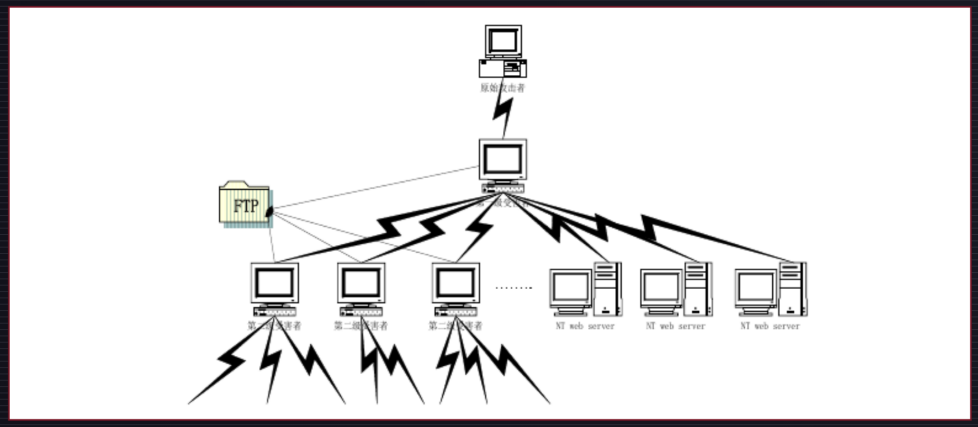
AUGUST 2001 · PUBLISHED

CUC- A Self-pervading Network Attacking System

Rui Suying GongJian

(Southeast University, Computer Science Dept. , 210096 Nanjing, P.R.China)

【Abstract】The behavior pattern and the architecture of a self-pervading network attacking system -CUC is analyzed in this paper, and its pervading mechanism is also studied. Besides, this paper provides a complete description of the vulnerabilities exploited in this system and comparison between CUC system and Worm which was spasmed in 1988.



Infected hosts become new scanners.

TSINGHUA / DIDAPPER [31]

08 SEP 1999 · RECEIVED

23 NOV 1999 · ACCEPTED

2001 · PUBLISHED · JOURNAL OF SOFTWARE 12(2)



(a) Network scanning
(a) 网络的扫描

(b) Worm spread
(b) 蠕虫的传播

Fig. 2
图 2

DISTRIBUTED INTRUSION DETECTION

IP traps: abnormal-traffic recognition

Shared traffic specimens

BP neural-network traffic classification

CERT/CC: NIMDA AND EARLIER BACKDOORS [95][96]

Original release date: September 18, 2001
Revised: September 25, 2001
Source: CERT/CC

- from client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

Nimda scanned earlier Code Red II / sadmind-IIS backdoors.

2001 · 18 SEP release / 25 SEP revision

[31] Tsinghua DIDAPPER · [32] NJCERT CUC · [95–96] CERT/CC 2001

RESEARCH INTO BUSINESS

TSINGHUA → UNISPLENDOUR / BITWAY

11 APR 2000 · ANNOUNCED · WB 4216

清华紫光自1999年11月上市之初，就推出了以自有技术为核心的"防火墙"等网络安全产品；今年3月又组建 了北京清华紫光顺风信息安全有限公司，向业界提供多层次的计算机信息安全产品。本次设立的清华紫光比威网络技术公司计 划出资2000万元向清华大学购买网络技术方面的科研成果，并以此为基础组建清华紫光比威网络技术研究院，该研究院将 聘请我国四大骨干网之一的中国教育科研网（CERNET）专家委员会主任、清华大学网络中心主任、计算机系博士生导师 吴建平教授出任院长，专业从事与网络技术相关的软硬产品研究开发工作。作为我国著名的网络技术专家，吴教授及其所领导 的清华大学网络中心和计算机系的数十位国内顶尖网络技术人才，先后承担了国家"九五"科技攻关项目"高性能多协议路由器"和"多功能协议测试系统"，以及国家"九五"国际互联网安全科研项目"安全路由器"等的研究任务，这些科研成果在 网络安全和网络管理等方面已达到国际先进水平，并先后通过了国家科技部、教育部、中国人民解放军总参谋部等国家主管部 门的鉴定。清华紫光比威网络技术公司将以清华大学和清华紫光比威网络技术研究院作为自己强大的技术后盾，推出以具有自 主知识产权和技术的高端多协议安全路由器为龙头的全线网络产品。清华紫光比威网络技术公司的设立将是清华紫光提供网络 应用总体解决方案的又一重大举措。

Planned RMB 20m research purchase

Secure routers · protocol testing

Network management

REPORTED APPRAISALS

Science/Technology and Education ministries

PLA General Staff

DCI REPORTED [11]

Iran · North Korea · Libya · Pakistan

CC&T / 3JET → SANJIANG CATALOG

2000–2002 · ARCHIVE CAPTURES [58–61]

Network Phone

NPS Network integrated System

VIP Series voice disposal System

NPS Sofeware System

UAD Series user automatic dial-up implement

24x7 Technical Support Center

CC&T believes that the Company's service priority is the guarantee of customer satisfaction. CC&T's technical support center has been operating its full functions 24 hours a day 7 days a week and serving customers all over the world, with our core engineers on call for quality consulting and support services. Upon request, our engineers are also sent to a clients' site to identify and resolve problems. Through SeeNPS, the technical support staff should be able to identify the problem even before the customers become aware of them.

NPS: marketing · overseas support

Sanjiang: Internet telephony products

CHINESE FIRMS → OVERSEAS PROGRAMS

JAN–JUN 2000 · DCI REPORT PERIOD [11]

Chinese missile-related technical assistance to Pakistan continued to be substantial during this reporting period. With Chinese assistance, Pakistan is rapidly moving toward serial production of solid-propellant SRBMs. Pakistan's development of the two-stage Shaheen–II MRBM also requires continued Chinese assistance. In addition, firms in China provided missile-related items, raw materials, and/or assistance to several other countries of proliferation concern—such as Iran, North Korea, and Libya.

WB 4216: Sina, 11 Apr 2000 · [58–61] Corporate archives
[11] DCI report, Jan–Jun 2000 · Congressional Record, 6 Sep 2001

CONTINUED

A 1992 federal directory placed Henry Tang at Salomon Brothers on the 40th floor of 7 World Trade Center; he later chaired the Committee of 100.[66] [67] The Committee's co-founder I.M. Pei had, through his firm, joined Silverstein Properties in the separate Federal Triangle development bid,[64] [125] while retired Army general John Fugh helped lead the Committee's 2001 China delegation.[64] For the next 25 years, the Committee of 100 maintained direct lines to government, industry, commerce, technology, and academia, in large part as a result of their bonds forged in the events surrounding 9/11. Years after the tragedy, Jonathan Choi appeared on Hong Kong's Maritime Silk Road Society's roster as an honorary president.[126] [127] The Society also published a Chinese-language CV for engineer Patrick Ng (吳惠明), a former chair of the Hong Kong Institution of Engineers' Public Relations Committee.[128] [129] It says his media work on technical crises included the collapse of the World Trade Center on September 11.[128] [129]

LETTERS OF MARQUE / GRAPHIC 09a

THE SHARED CHRONOLOGY

MAR 1998 [E4557]
Ressam: Afghanistan travel

05 MAR 1998 · PDB [E2254]
Three Brothers Islamic Front · Possible hoax

07 AUG 1998 [15]
U.S. embassy bombings

16 SEP 1998 [E4565]
Salim arrested: Germany

04 DEC 1998 · PDB [E567]
Islamic Group / Islambuli

FEB 1999 [E4573]
Ressam returns to Canada

07 APR 1999 [12]
Mihdhar visa: Jeddah

MAY 1999 [25]
CCERT established

08 SEP 1999 · RECEIVED [E4159]
DIDAPPER manuscript

23 NOV 1999 · ACCEPTED [E4159]
DIDAPPER manuscript

30 DEC 1999 · PDB [E2445]
Muslim Hackers Club

2000–2001 [E4624/E4637]
Singapore reconnaissance

03 JAN 2000 · PLANNED [E2252]
Millennium plots: disrupted

05–08 JAN 2000 [E4198]
Kuala Lumpur gathering

12 OCT 2000 [E2252/E3484]
USS Cole bombing

FEB 2001 · ISSUE [E4159]
DIDAPPER published

19 MAY 2001 · FINALIZED [E4158]
CUC attack analysis

28–30 JUN 2001 [121]
Atta: Las Vegas cybercafé

AUG 2001 · PUBLICATION [E4158]
NJCERT CUC paper

09 AUG 2001 [121]
Mihdhar / Hazmi: computers

12 AUG 2001 [121]
Atta: Fort Lee Web Station

22 AUG 2001 · INDICTMENT [122]
Jarrah: GPS / cockpit diagrams

11 SEP 2001
9/11 attacks

08 DEC 2001 [E4638]
Singapore arrests begin

12 OCT 2002 [E4608]
Bali bombings

28 NOV 2002 [E4609/E4610]
Mombasa attacks

INTELLIGENCE REPORTING

HIJACKER PREPARATIONS

UNIVERSITY RESEARCH

TERRORIST OPERATIONS

1998 · ONSET YEAR [E4593]
Moonlight Maze

1998 · YEAR [6]
Sun Wah high-tech alliances

01–26 FEB 1998 [E4556]
Solar Sunrise

13 FEB 1998 [E2877]
CC&T incorporated

22 MAY 1998 [E4558]
PDD-63

OCT 1998 [E4566/E4567]
NIPC / FedCIRC

27 MAR 1999 · ADVISORY [E4282]
Melissa

AUG 1999 [109]
FCC CALEA standards

JAN–JUN 2000 · REPORT PERIOD [11]
Chinese missile assistance

APR 2000 · DISCOVERY [E4591]
478 compromised hosts

11 APR 2000 · ANNOUNCED [E4216]
BITWAY venture

21 AUG 2000 [109]
CALEA court remand

11 DEC 2000 · CAPTURE [60]
3JET NPS catalog

29 MAR 2001 · REPORT [E4593]
Moonlight Maze

06 APR 2001 · CAPTURE [61]
CC&T overseas / NPS support

08 MAY 2001 · ADVISORY [E4328]
sadmind/IIS

19 JUN 2001 · NOTICE [95]
IIS vulnerability

19 JUL 2001 · ADVISORY [E4336]
Code Red

AUG 2001 · OFFER [109]
FBI packet-mode initiative

04 AUG 2001 · FIRST SEEN [E638]
CodeRedII

06 AUG 2001 · NOTICE
CERNET: Code Red

18 SEP 2001 · ADVISORY [E729/E4343]
Nimda

19 SEP 2001 · NOTICE
CCERT: Nimda

21 SEP 2001 · NOTICE
HFUT campus impact

04 OCT 2001 · AUTHORIZED [104]
Presidential surveillance

11 OCT 2001 · OBSERVED [97]
Nimda email burst

26 OCT 2001 [113]
USA PATRIOT Act

26 OCT 2001 · LOCATED [E4662]
Klez / ElKern

11 NOV 2001 · FIRST SEEN [98]
Klez.D

24 DEC 2001 · CAPTURE [58]
Sanjiang telephony catalog

11 APR 2002 [109]
FCC remand order

1998 1999 2000 2001 2002 31 DEC 2002

INTRUSIONS & WORMS

BUSINESS / TECHNOLOGY

LAW, POLICY & INSTITUTIONS

THE SOURCE DOCUMENTS

CIA PDB / GAO

30 DEC 1999 / 29 MAR 2001

(30 December 1999) Terrorism: Near-Term Threat Undiminished

Computer degradations due to Y2K glitches are likely to facilitate opportunistic attacks by groups or individuals, including hackers who may be affiliated with terrorist organizations. Bin Ladin affiliates arrested this month in Pakistan, for instance, are linked to the extremist Muslim Hackers Club.

E2445 / E4593

Even as greater attention has been paid to incident response, cyber threats and attacks continue to affect the operations of DOD and other federal systems and networks. Since 1998, a number of federal systems have been subjected to a series of recurring, "stealth-like" attacks, code-named Moonlight Maze, that federal incident response officials have attributed to foreign entities and are still investigating. More recently, the "ILOVEYOU" virus attack affected electronic mail and other systems worldwide.[3]

CERT / NIMDA

18 SEP 2001 · E729 / E4343

26 CA-2001-26: Nimda Worm

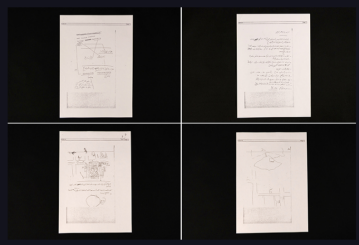
Original release date: September 18, 2001
Revised: September 25, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

- from client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

SINGAPORE ISD

E4624 / E4637 / E4638





PUBLIC LAW 107-56

26 OCT 2001 · §217 · [113]

SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.

(2) in section 2511(2), by inserting at the end the following:

"(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

"(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

"(II) the person acting under color of law is lawfully engaged in an investigation;

"(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

"(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.".

NJCERT / CUC

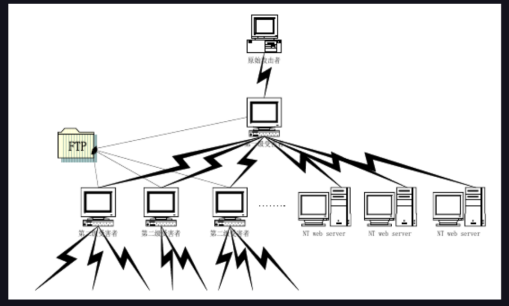
Southeast University · E4158

CUC– A Self-pervading Network Attacking System

Rui Suying GongJian

(Southeast University, Computer Science Dept. , 210096 Nanjing, P.R.China)

【Abstract】The behavior pattern and the architecture of a self-pervading network attacking system -CUC is analyzed in this paper, and its pervading mechanism is also studied. Besides, this paper provides a complete description of the vulnerabilities exploited in this system and comparison between CUC system and Worm which was spasmed in 1988.



DCI / CHINA

JAN–JUN 2000 · REPORT PERIOD [11]

Chinese missile-related technical assistance to Pakistan continued to be substantial during this reporting period. With Chinese assistance, Pakistan is rapidly moving toward serial production of solid-propellant SRBMs. Pakistan's development of the two-stage Shaheen–II MRBM also requires continued Chinese assistance. In addition, firms in China provided missile-related items, raw materials, and/or assistance to several other countries of proliferation concern—such as Iran, North Korea, and Libya.

CONTINUED

The same interests surrounding the cyberattacks and the calamity of 9/11 are now the very same interests surrounding the AI discussion, the surveillance conversation, geopolitical discourse, race relations, and preserving the billionaire class from the consequences of their own incompentence and irresponsibility.

If industrial and defense knowledge could move through lawful partnerships and illicit markets at once, the history of 9/11 cannot end with the airport checkpoint. It must reckon with who could assemble the intelligence, technology-transfer and cyber records before the attacks, why they remained apart, and which original evidence is still withheld from investigators. Robert Mueller had answers until he didn't. The man with the answers now is John O. Brennan.

NUMBERED END NOTES

END NOTES

1 CC&T archived corporate page.

2 EE Times, October 1, 1999.

3 3JET archived agents page.

4 Sanjiang archived company page.

5 Sun Wah archived financial history.

6 Sun Wah high-technology history.

7 Talisman SEC filing, 1998 acquisition of its Greater Nile interest.

8 2000 U.S. House hearing, Sudan oil consortium shares and August 1999 pipeline shipments.

9 China National Space Administration, China's Space Activities (2000), regional cooperation.

10 U.S. Army War College, Chinese Arms Exports (August 2000), pp. 48-49.

11 DCI unclassified proliferation report for January-June 2000, printed in the Congressional Record, September 6, 2001.

12 9/11 Commission, terrorist-travel staff monograph, chapter 2.

13 DOJ Inspector General, FBI handling of pre-9/11 intelligence, chapter 5.

14 U.S. Senate Judiciary Committee, 1999 cyber-threat hearing, Solar Sunrise account, pp. 24-25.

15 9/11 Commission, Chapter 4, the August 1998 U.S. embassy bombings.

16 CISA, NSA, FBI and partners, advisory AA24-038A, February 2024.

17 archived White House Brennan biography.

18 9/11 Commission, Chapter 6, millennium plots and the Kuala Lumpur meeting.

19 DOJ, USS Cole indictment.

20 1999 Congressional Record on proposed limits to compulsory key escrow.

21 Senate encryption-policy hearing.

22 GAO account of PDD-63, NIPC, FedCIRC and Y2K incident preparations.

23 CERT/CC 1999 annual report.

24 CIA announcement of In-Q-It, September 30, 1999.

25 CERNET history, 1999 CCERT and 2000 Internet2 agreement.

26 CERNET account dating CCERT's formation to May 1999.

27 CERNET National Center at Tsinghua.

28 Federal Reserve, June 2001 account of the U.S. technology-stock correction.

29 SMIC SEC Form 20-F, company and Shanghai fabrication timeline.

30 UESTC paper on computer viruses and information warfare, June 1997.

31 Tsinghua DIDAPPER intrusion-detection paper, submitted September 1999.

NUMBERED END NOTES

END NOTES

32 Southeast University/NJCERT analysis, May 19, 2001.

33 Shanghai Securities News interview dating Choi's CAS adviser appointment to 1998.

34 MSU, Partners, fall 2004, Choi adviser role.

35 People's Daily, January 24, 1998, CPPCC National Committee membership roster.

36 Hong Kong Exchange 2020 filing, later Standing Committee title, p. 69.

37 Sheema Khan's 2003 affidavit, archived copy.

38 NCCM account of its 2000 founding and independence.

39 Canadian Senate testimony quoting the affidavit's trademark-license terms.

40 Committee of 100, Trade Secrets and Economic Espionage seminar transcript, September 16, 2015, pp. 1, 12-13.

41 Maha El-Genaidi, "FBI and Muslims," The Minaret, March 2000, pp. 19-21.

42 DOJ, December 1999 Wen Ho Lee indictment description.

43 U.S. Army War College, China's Strategic Modernization (September 1999), Appendix I, Base 066.

44 Sanjiang subsidiary table in 2018 corporate prospectus, p. 3-3-1-35.

45 Lionel Ni's retrospective account of 3JET financing.

46 U.S. House Select Committee, U.S. National Security and Military/Commercial Concerns with the People's Republic of China (1999), pp. xviii-xx.

47 GAO, Rapid Advances in China's Semiconductor Industry (April 19, 2002).

48 TMC, independent EMIP-1 review, August 1999.

49 CC&T archived EMIP-1 product page.

50 NIST, network-emulation tool account.

51 RFC 2398, §2.4.

52 NSF award EIA-9911074.

53 Zheng and Ni, EMPOWER paper, 2002.

54 MSU corporate gifts, fall 2001.

55 Vibhavasu Vuppala and Lionel M. Ni, "Virtual Network Ports: An Inter-network Switching Framework," 1999.

56 MSU graduation record naming Ni as Vuppala's major professor.

57 Argonne/EPICS, FRIB Introduction and FRIB Controls, May 2013, slide 23.

58 Sanjiang archived Internet-telephony product page.

59 Sanjiang corporate overview.

60 3JET NPS gateway and software product page, archived December 2000.

61 CC&T worldwide operations and NPS support page, archived April 2001.

62 2003 U.S.-China Economic and Security Review Commission hearing, Iraqi air-defense fiber-optic links, p. 95.

NUMBERED END NOTES

END NOTES

63 Iraq Survey Group, Comprehensive Report, recovered procurement records.

64 Committee of 100 institutional highlights.

65 Committee of 100, March 2018 coalition letter.

66 U.S. Department of Labor, Glass Ceiling Commission Members, revised November 24, 1992, p. 2.

67 Committee of 100 chairpersons, 1996-2002.

68 NIST, Port Authority record W99-7172, Table 4-7, p. 118.

69 Committee of 100, John Fugh biography.

70 Committee of 100, Committee Bridges, Summer 2002, pp. 3-4.

71 Archived Interstellar/eBanswers About page.

72 eBanswers announcement posted October 8, 2001, describing LJ Connection's October 7 appointment.

73 LJ January 2002 PBX page.

74 Konnech-branded October 2002 page at the LJ domain.

75 Michigan Economic Development Corporation, Konnech history.

76 Hong Kong Polytechnic University account.

77 Nanjing University account.

78 MSU board minutes, February 13, 2004.

79 Sun Wah Hi-Tech and Red Flag Software press release, October 18, 2000.

80 AZKEF archived roster.

81 Microsoft matching-gifts letter.

82 Zhejiang University, AZKEF retrospective, May 31, 2005.

83 AZKEF lecturers.

84 AZKEF fellows.

85 UCAS Fei-Yue Wang biography.

86 TEFNA history.

87 Friends of Tsinghua SEM IRS-derived record.

88 Fudan University account of its 2008 New York foundation event and 2006 registration.

89 Microsoft Research Asia joint-lab history.

90 Microsoft/HKUST joint-lab history.

91 HKUST-Boeing announcement.

92 DoD FVAP source-selection record.

93 DOJ, Fei Ye and Ming Zhong guilty pleas.

94 DOJ, Su Bin guilty plea.

95 CERT/CC, 2001 Advisories, Code Red and Nimda sections.

96 CERT/CC, 2001 Incident Notes, Code Red II.

97 F-Secure, Nimda technical history.

98 F-Secure, Klez chronology and variant descriptions.

NUMBERED END NOTES

END NOTES

99 CISA, NSA, FBI and international partners, 2022 Top Routinely Exploited Vulnerabilities, August 3, 2023, summary.

100 LJ Connection Michigan corporate-record aggregation, preserved image.

101 OpenCorporates entity record.

102 CERT/CC, 2001 incident-note collection, Code Red entry.

103 Joint Inspectors General, President’s Surveillance Program review, volume II, pp. 7-10.

104 volume I, p. 10.

105 DOJ, Dongfan Chung sentence.

106 DOJ, Boeing settlement.

107 DOJ, UMC guilty plea.

108 DOJ, ZTE guilty plea and isolation-company scheme.

109 DOJ Inspector General, CALEA implementation history, including standards disputes, deadlines and the FBI's August 2001 packet-mode initiative.

110 Congressional Record, October 11-12, 2001 counterterrorism-bill proceedings.

111 U.S. Senate anthrax chronology.

112 DOJ/FBI, Amerithrax investigative summary.

113 USA PATRIOT Act, Public Law 107-56, sections 215-217.

114 Senate Intelligence Committee, Iraq-al-Qaeda public-statement review, pp. 62-63.

115 Senate prewar-assessments report, pp. 286-313, 361-63.

116 WMD Commission, note 834.

117 Senate committee, 2008 Phase II findings.

118 Singapore Ministry of Home Affairs, Jemaah Islamiyah cell investigation.

119 9/11 Commission hearing, 2002 Bali attribution.

120 Congressional Record, Mombasa attack chronology.

121 FBI, 9/11 FBI Report, February 2004, Mohamed Atta and New Jersey public-computer chronologies, pp. 44, 51.

122 DOJ, Moussaoui indictment, overt act 77.

123 9/11 Commission, January 27, 2004 hearing, staff statement on the four flights.

124 NTSB, study of Flight 77 and Flight 93 autopilot and navigation activity, February 13, 2002.

125 Washington Post, November 16, 1997, Delta Partnership’s separate Federal Triangle bid.

126 Maritime Silk Road Society, fourth-anniversary brochure (2019), society roster listing Jonathan Choi among its honorary presidents.

127 Society's current organization roster.

128 Maritime Silk Road Society, Chinese-language CV of Ir Patrick Ng (□□□), p. 1, public-relations paragraph.

129 archived November 30, 2022.

ADDITIONAL SOURCE MATERIAL

Background and parallel records for readers following the wider source trail; the footnotes above identify the records used for particular statements.

Earlier reporting in this series: End of an Era, Part I, Part II, Part III, Part IV, and The Phantom Hack.

Broader 9/11 investigations: the complete 9/11 Commission Report, its Terrorist Financing Staff Monograph, and Congress's Joint Inquiry into Intelligence Community Activities Before and After the Attacks.

Federal cyber-defense background: the White House National Plan for Information Systems Protection, GAO's critical-infrastructure protection review, and GAO's FedCIRC review.

Incident-response record: Carnegie Mellon CERT/CC's 1999 annual report summary and 2001 incident-note collection.

World Trade Center technical investigations: NIST's final report on the towers and its separate final report on Building 7.

Wider technology-transfer context: the House Select Committee's 1999 U.S.-China national-security report and GAO's 2002 review of China's semiconductor industry.

Other records retained from the former bundled notes

Sun Wah archived technology account.

IRS-derived FUEDF record.

DOJ declassification notice.

Gus Quixote, “Theory No More, Part One: Frien-emies,” May 25, 2023.



KEEP THE RECEIPTS

INDEPENDENT INVESTIGATIONS · FULLY FOOTNOTED REPORTS

DOCUMENTARY EVIDENCE · ORIGINAL RECORDS

GUSQUIXOTE.COM

END OF AN ERA, PART V: PAPER TIGER DIPLOMACY

NATHAN WALKER · LETTERS OF MARQUE

4,349 WORDS / 129 NOTES