



END OF AN ERA, PART I:

THE ROAD TO HELL

John F. Kennedy was dead, and the agency helping investigate his murder was deciding which parts of its own history investigators could see. The House Select Committee on Assassinations later found that Raymond Rocca, a principal CIA contact for the Warren Commission, did not know about the agency's plots against Fidel Castro.

BY NATHAN WALKER

THE REPORT

THE ROAD TO HELL

END OF AN ERA, PART I

3,196

WORDS

51

NUMBERED NOTES

17

DOCUMENTARY IMAGES +
GRAPHICS

6

SECTIONS

REPORT SEQUENCE

I	KENNEDY, CUBA AND VIETNAM	03
II	COVERT FUNDING AND FOREIGN POLICY	06
III	CONTRACTORS AND COMMERCIAL TECHNOLOGY	10
IV	CYBERATTACKS AND SURVEILLANCE IN 2001	12
V	ACADEMIC TIES AND DISEASE SURVEILLANCE	17
VI	METABIOTA, INVESTMENT AND INTELLIGENCE	19

THREE GRAPHICS

GRAPHIC 01	IRAN-CONTRA: WHERE THE MONEY WENT	09
GRAPHIC 02	AN INFECTION COULD LEAVE THE DOOR OPEN	15
GRAPHIC 03	IN-Q-TEL AND METABIOTA: DATA FUSION AND SIMULATION	21

Numbered notes appear beneath the relevant report pages. The complete source register, with full URLs, begins on page 23.

SECTION 1

KENNEDY, CUBA AND VIETNAM

John F. Kennedy was dead, and the agency helping investigate his murder was deciding which parts of its own history investigators could see. The House Select Committee on Assassinations later found that Raymond Rocca, a principal CIA contact for the Warren Commission, did not know about the agency's plots against Fidel Castro. The CIA had kept that information from the official assigned to help the commission. Investigators could ask him about the agency's activities and still miss facts he had never been allowed to learn.¹



The Warren Commission presents its report to President Lyndon B. Johnson in the White House Cabinet Room, September 24, 1964. Courtesy Gerald R. Ford Presidential Library; AV82-31-4854 / NARA 7462161.

CIA historian David Robarge later described Director John McCone's approach as a "benign cover-up." His account described efforts to keep the Warren Commission away from sensitive CIA operations, including the Castro plots. Concealing those operations does not establish responsibility for Kennedy's murder. It does establish that the CIA helped steer the investigation while withholding information investigators needed to examine the agency's own activities.^{2 1}

NOTES

¹ HSCA, CIA cooperation, 1979, pp. 252-253

² Robarge, McCone and Kennedy, 2013

*** The committee agreed that this was an unacceptable explanation for the CIA's failure to inform the Warren Commission of the anti-Castro plots. It was apparent that the Commission was unable to make a specific request for information about the plots since it was unaware of their existence. In this regard, the observations of the Senate committee are worth quoting:**

"Why senior officials of the FBI and the CIA permitted the investigation to go forward, in light of these deficiencies, and why they permitted the Warren Commission to reach its conclusion without all relevant information is still unclear. Certainly, concern with public reputation, problems of coordination between agencies, possible bureaucratic failure and embarrassment, and the extreme compartmentation of knowledge of sensitive operations may have contributed to these shortcomings. But the possibility exists that senior officials in both agencies made conscious decisions not to disclose potentially important information." (46)

House Select Committee on Assassinations, Final Report (1979), p. 253, footnote 8. ¹

The CIA's Cuban operations included plans to help prepare the way for war. Operation Mongoose's March 1962 guidelines called for developing resources inside Cuba that could prepare for and justify eventual American military intervention. The CIA was to conceal American sponsorship. Kennedy's review did not authorize overt military force. The plan nevertheless called for covert action that could help create the conditions later offered as reasons to commit American forces. ³

Kennedy was also considering a reduction in Vietnam. On October 11, 1963, he approved recommendations that included withdrawing 1,000 American military personnel by year's end. The McNamara-Taylor report called for completing much of the American training mission by the end of 1965, based on its assessment of progress. Whether Kennedy's intentions contributed to his assassination remains unknown. His approval of the withdrawal recommendation is documented, preceding the decisions that vastly expanded the war. ^{4 5 6}



USS Maddox (DD-731) off Oahu, Hawaii, March 21, 1964. Photograph by PH2 Antoine, U.S. Navy; Naval History and Heritage Command, NH 97908.

In August 1964, intelligence helped supply the public case for escalation. NSA historian Robert Hanyok concluded that the supposed second North Vietnamese attack in the Gulf of Tonkin had not occurred. His reconstruction described analysts excluding contrary evidence, combining unrelated messages and defending an initial mistake. In his account, almost 90 percent of the available signals intelligence—intercepted signals and messages—was kept out of the later summary. Hanyok did not find a White House order to fabricate the

NOTES

¹ HSCA, CIA cooperation, 1979, pp. 252-253

³ Operation Mongoose guidelines, March 14, 1962

⁴ NSAM 263, October 11, 1963

⁵ McNamara-Taylor report, October 2, 1963

⁶ Hanyok, Gulf of Tonkin study, 2000-01

attack. He found that the people assembling the intelligence made the evidence fit the story they had already sent to their superiors.⁶

~~(S//SI)~~ Instead, three things occurred with the SIGINT. First of all, the overwhelming portion of the SIGINT relevant to 4 August was kept out of the post-attack summary reports and the final report written in October 1964. The withheld information constituted nearly 90 percent of all available SIGINT. This information revealed the actual activities of the North Vietnamese on the night of 4 August that included salvage operations of the two torpedo boats damaged on 2 August, and coastal patrols by a small number of DRV craft. As will be demonstrated later in this chapter, the handful of SIGINT reports which suggested that an attack had occurred contained severe analytic errors, unexplained translation changes, and the conjunction of two unrelated messages into one translation. This latter product would become the Johnson administration's main proof of the 4 August attack.

Robert J. Hanyok, Gulf of Tonkin study, p. 3
(2000/2001; released 2005).⁶

The Warren Commission lacked information about the agency helping it investigate. Officials assessing Tonkin received an account distorted by the analysts who assembled it. Both failures left decision-makers without evidence that might have changed their minds. The officials who controlled the records could shape what other officials believed—and what they did next.¹⁶

NOTES

¹ HSCA, CIA cooperation, 1979, pp. 252-253

⁶ Hanyok, Gulf of Tonkin study, 2000-01

SECTION 2

COVERT FUNDING AND FOREIGN POLICY



Cold War competition also drew the CIA into organizations Americans knew as independent. A 1967 White House compilation reproduced earlier reviews of CIA support to the United States National Student Association and other international youth organizations, including the International Union of Socialist Youth. The stated purpose was to compete with communist organizations. The CIA's anti-communism thus included secret support for selected socialists, depending on which groups could serve American policy. Participants did not all need to know who helped finance their organizations.⁷

A contemporary State Department cable summarized reporting that the money passed through foundations, prominently the Foundation for Youth and Student Affairs. After the arrangement became public, the Katzenbach committee recommended ending covert support to educational and private voluntary organizations, and Johnson accepted its recommendations. The restrictions followed years in which the CIA had used apparently independent organizations to pursue foreign-policy goals without publicly identifying itself as their sponsor.^{8 9}

At home, the search for communist direction became a means of collecting information about Americans. Operation CHAOS began in 1967 under White House

pressure to identify foreign influence over domestic dissent. The Rockefeller Commission described repeated CIA assessments that failed to find the suspected foreign control, even as collection expanded. In 1969, Helms sent Henry Kissinger a study while acknowledging that its domestic component fell outside the CIA's charter. The commission later found improper domestic activity. The CIA kept collecting information about Americans even when its studies failed to find the foreign control the White House suspected.¹⁰

Another copy of the first version of "Restless Youth" was delivered on February 18, 1969, after the change in Administrations, to Henry A. Kissinger, then Assistant to President Nixon for National Security Affairs. Director Helms' covering memorandum of February 18 specifically pointed out the impropriety of the CIA's involvement in the study. It stated:

In an effort to round-out our discussion of this subject, we have included a section on American students. This is an area not within the charter of this Agency, so I need not emphasize how extremely sensitive this makes the paper. Should anyone learn of its existence it would prove most embarrassing for all concerned.

Rockefeller Commission report (June 1975), p. 134, quoting Helms's February 18, 1969 memorandum to Kissinger.¹⁰

Abroad, the CIA helped finance political messages through newspapers. The Senate's Chile investigation recorded funding authorizations of \$700,000 in September 1971 and another \$965,000 in April 1972 for the opposition newspaper El Mercurio. Secret support for a newspaper gave a foreign government a way to

NOTES

⁷ Rostow, covert-action review, February 18, 1967

⁸ State Department, student funding, February 15, 1967

⁹ Katzenbach report and Johnson's response, March 1967

¹⁰ Rockefeller Commission, Operation CHAOS, 1975

¹¹ Senate, Covert Action in Chile, 1975

influence public debate without putting its name on the message. This is along the history of psychological operations: influence the audience while concealing the sponsor.¹¹

Watergate brought intelligence resources into domestic political abuse. The Rockefeller Commission documented CIA technical assistance to E. Howard Hunt and psychological profiles of Daniel Ellsberg. On June 23, 1972, Nixon instructed Haldeman to invoke the CIA

and its Bay of Pigs operation in Cuba to discourage the FBI from following the burglars' money trail. CIA deputy director Vernon Walters conveyed the warning to acting FBI director L. Patrick Gray, although Helms said he knew of no endangered CIA operation. The commission also recorded CIA refusals and found no knowing agency participation in the cover-up conspiracy. Nixon used a claim of national security as a barrier around a criminal investigation.^{12 13}

PRESIDENT: When you get in these people when you...get these people in, say: "Look, the problem is that this will open the whole, the whole Bay of Pigs thing, and the President just feels that" ah, without going into the details... don't, don't lie to them to the extent to say there is no involvement, but just say this is sort of a comedy of errors, bizarre, without getting into it, "the President believes that it is going to open the whole Bay of Pigs thing up again. And, ah because these people are plugging for, for keeps and that they should call the FBI in and say that we wish for the country, don't go any further into this case", period!

| Nixon-Haldeman conversation, June 23, 1972. Trial exhibit 1, p. 16, Richard Nixon Presidential Library. ¹³

The need to counter Moscow also supported decisions that benefited arms sales and intelligence access. In a 1968 interdepartmental review of a proposed \$600 million, six-year military-credit program for Iran, a Joint Chiefs representative did not anticipate a Soviet attack in the near future. The group could not precisely match

the amount of weaponry to a particular threat. Yet Iran's intelligence cooperation and competition with Moscow remained arguments for support. American officials were weighing the access Iran offered alongside the weapons it needed.¹⁴

NOTES

¹¹ Senate, Covert Action in Chile, 1975

¹² Rockefeller Commission, CIA and Watergate, 1975

¹³ Nixon-Haldeman transcript, June 23, 1972

¹⁴ Iran military-credit review, April 5, 1968

Kissinger's July 1972 instructions gave Iran more freedom to choose its weapons. Following Nixon's talks with the Shah, State and Defense were to arrange briefings on advanced aircraft and weapons and provide additional American military technicians. In general, Iran would make the purchasing decisions, with encouragement to buy American equipment. The policy tied American reliance on an armed regional partner to business opportunities for American suppliers.¹⁵

Washington was also planning closer ties with communist China. In June 1972, National Security Council staff member Richard Solomon proposed to Kissinger that a joint committee of the National Academy of Sciences, Social Science Research Council and American Council of Learned Societies manage scholarly exchanges. Cultural exchanges would use the National Committee on United States-China Relations, with the State Department arranging communications and security. The proposal would put respected scholarly institutions to work in a managed diplomatic opening. China's communist government was no obstacle to designing those relationships.¹⁶

American officials could secretly finance anti-communist political activity in one country while planning closer ties with communist institutions in another. Both approaches sought influence through selected partners. Some organizations received covert funding; others appeared in proposals for managed scholarly exchange. Officials were choosing which foreign relationships would receive American resources. Those choices invite a harder question than whether America's leaders opposed communism: what access were they prepared to offer communist institutions to advance their own ambitions?^{7 11 16}

Iran-Contra later exposed how dealings with a publicly opposed government could help finance another secret operation. Independent counsel Lawrence Walsh described the private Enterprise associated with Oliver North, Richard Secord and Albert Hakim: foreign companies, Swiss accounts and proceeds from Iranian arms transactions. His report identified at least \$3.6 million diverted to the Contras. The administration's dealings with Iran and its support for the Nicaraguan fighters had become connected through financial arrangements hidden from public scrutiny. Money from one foreign-policy operation helped sustain another.¹⁷

NOTES

⁷ Rostow, covert-action review, February 18, 1967

¹¹ Senate, Covert Action in Chile, 1975

¹⁵ Kissinger, Iranian weapons purchases, July 25, 1972

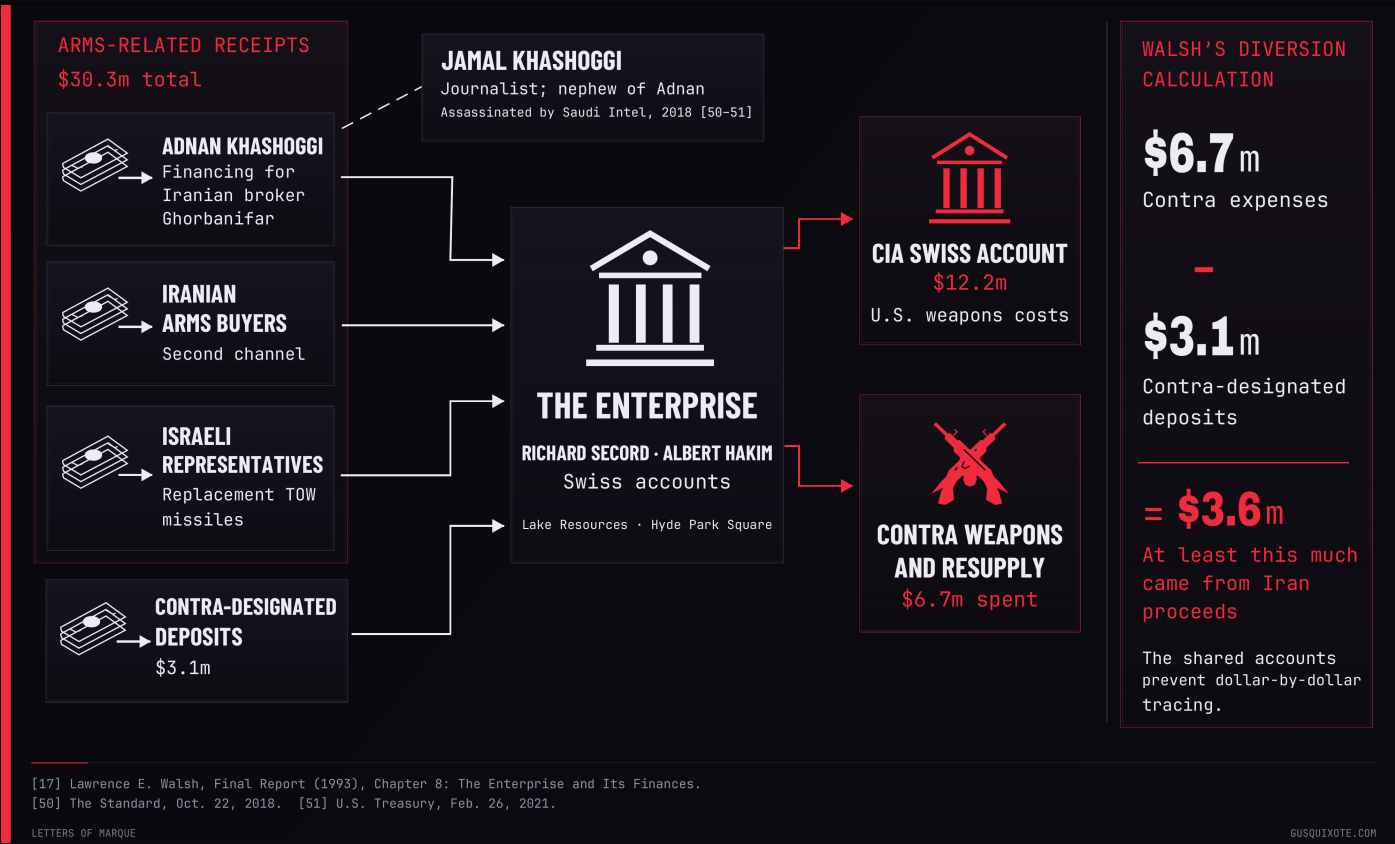
¹⁶ Solomon, Sino-US relations, June 9, 1972

¹⁷ Walsh, The Enterprise, Chapter 8, 1993

GRAPHIC 01

IRAN-CONTRA: WHERE THE MONEY WENT

Selected 1986 cash flows described by Independent Counsel Lawrence Walsh.



1986 cash flows described in Lawrence Walsh’s final report: arms-related receipts entered the Secord-Hakim Enterprise’s Swiss accounts; payments went to a CIA account for U.S. weapons costs and to Contra weapons and resupply. Walsh calculated at least \$3.6 million in diverted Iran proceeds. The separate callout identifies Adnan Khashoggi’s nephew, journalist Jamal Khashoggi, and his 2018 assassination. 17 50 51

NOTES

- 17 Walsh, The Enterprise, Chapter 8, 1993
- 50 The Standard, Jamal and Adnan Khashoggi, October 22, 2018
- 51 U.S. Treasury, Khashoggi murder, February 26, 2021

SECTION 3

CONTRACTORS AND COMMERCIAL TECHNOLOGY



P private industry had been helping organize government programs for decades. The original 1959 paper on PERT—a method for scheduling complex projects—joined Booz Allen authors with the Navy’s Special Projects Office in work associated with Polaris. Private specialists helped government plan the order and timing of its work. When intelligence agencies later sought commercial computing tools, they were extending an established practice of drawing on expertise outside government.^{18 19}

After the Soviet Union’s collapse, one major surveillance dispute reached directly into everyday communications. The Clinton administration’s 1993 Clipper initiative proposed encryption with government-held pieces of an unlocking key, available under legal authorization. Officials argued that criminals and terrorists could use strong encryption to defeat investigators. Their proposal would build government access into the product before any particular investigation began.²⁰

The industry resisted. NIST’s history records strong opposition and very low adoption of the proposed key-escrow arrangement. Clipper’s original design failed to win acceptance. Companies and other opponents had challenged an attempt to make government access a built-in feature of secure communications.^{21 20}

Domestic terrorism renewed the pressure for access. In his April 1996 statement signing the Antiterrorism and Effective Death Penalty Act, Clinton traced additional proposals to the Oklahoma City bombing and the law-enforcement requests that followed. He complained that Congress had refused expanded emergency and multipoint wiretap powers and removed provisions for easier access to records. His proposals against international terrorism had preceded Oklahoma City. He used both threats to press for wider access and portrayed Congress’s refusals as obstacles to protecting the public.²²

The CIA also began working more directly with the companies developing new technology. Its 1999 annual report described In-Q-Tel, incorporated that February, as a way to obtain commercial information technology through relationships with private industry and academia. Intelligence requirements could now help shape which products received support and found customers. The agency could buy a finished tool or help develop one to suit its needs. A product could attract investment by serving both commercial customers and intelligence agencies.¹⁹

While the CIA pursued commercial technology, its intelligence still guided military strikes. On May 7, 1999, American bombs hit China’s embassy in Belgrade.

NOTES

¹⁸ Malcolm et al., PERT paper, 1959

¹⁹ DCI Annual Report, In-Q-Tel section, 1999

²⁰ White House, Clipper initiative, April 16, 1993

²¹ NIST, key escrow and Clipper history

²² Clinton, antiterrorism signing statement, April 24, 1996

²³ Tenet, Chinese embassy bombing, July 22, 1999

Tenet's subsequent testimony described a CIA target nomination based on a mistaken location, reviews that missed the error and a late warning that remained unresolved before the strike. Some intelligence officers knew where the embassy was; the relevant databases did not. Tenet called the bombing accidental. His account showed that knowledge held inside the government had failed to reach the people who needed it before the bombs fell.²³

In March 2000, former CIA director R. James Woolsey publicly acknowledged American spying on European industries. He described using computers to filter the collected information and defended collection aimed at bribery and other prohibited conduct. He denied stealing trade secrets for particular American companies. Instead, he described using intelligence to approach a government receiving a bribe and influence how it awarded a contract. Government officials could use secret commercial information to change a deal without handing it to a competing company.²⁴

Confidential business communications can expose negotiations, dependencies and misconduct that outsiders cannot see. Woolsey described turning that knowledge into pressure over contract awards. Establishing how far intelligence agencies used wiretapping and cyberespionage to manipulate industry requires examining individual transactions. His account supplies a concrete example of the power at stake: secret access to a company's business could give government officials a way to intervene in it.²⁴

In-Q-Tel's agreement with SafeWeb brought the agency into the business of Internet privacy. Announced in February 2001, it covered licensing and development of privacy technology. In-Q-Tel said it then had no ownership stake, board seat or management role. It could work with the company through a development agreement, helping adapt a commercial capability to intelligence needs without owning or managing the business.²⁵

NOTES

²³ Tenet, Chinese embassy bombing, July 22, 1999

²⁴ Woolsey, Why We Spy on Our Allies, March 17, 2000

²⁵ In-Q-Tel-SafeWeb announcement, February 14, 2001

SECTION 4

CYBERATTACKS AND SURVEILLANCE IN 2001

IV

Before September 11, the CIA and Defense Department disagreed over an armed Predator: who would pay, who would operate it and who would take responsibility for lethal action. The 9/11 Commission described those disputes alongside unresolved technical problems, which it said largely determined the timing. The proposed aircraft could observe a target and attack it.²⁶

Government computers were already being hit. According to a 2005 federal guilty-plea announcement, an intruder attacked Defense Information Systems

Agency training computers in Denver around June 10, 2001, defacing pages and deleting logs. Networked computers were disabled for several days. In July, Pentagon spokesman Craig Quigley acknowledged Code Red infections on a small number of computers; he said classified systems and tactical operations were unaffected. GAO also reported that SirCam infected an FBI computer in late July and emailed private documents outside. The Defense Department was also a tenant on 7 World Trade Center's 25th floor, according to NIST. The tenant list does not name a Defense office; the attacked training computers were in Denver.^{27 28 29 30}

SirCam has also reportedly caused some havoc. It is allegedly responsible for the leaking of secret documents from the government of Ukraine. And it reportedly infected a computer at the Federal Bureau of Investigation (FBI) late last month and sent some private, but not sensitive or classified, documents out in an E-mail. There are reports that SirCam has surfaced in more than 100 countries.

U.S. General Accounting Office, Keith A. Rhodes testimony, August 29, 2001, GAO-01-1073T, p. 5. SirCam and the FBI computer.²⁹

NOTES

²⁶ 9/11 Commission, armed Predator, pp. 210-214

²⁷ DOJ/DCIS, Denver computer intrusion, July 28, 2005

²⁸ Reuters, Pentagon Code Red infections, July 24, 2001

²⁹ GAO-01-1073T, August 29, 2001, pp. 4-5

³⁰ NIST NCSTAR 1A, 7WTC tenants, Table 1-1

Table 1–1. Use of floors in WTC 7.

Floor(s)	Tenant or Function ^a
46, 47	Mechanical space, Citigroup
26 through 45	Citigroup
25	U.S. Internal Revenue Service, Department of Defense, Central Intelligence Agency
24	U.S. Internal Revenue Service
23	New York City Mayor's Office of Emergency Management (OEM)
22	Federal Home Loan Bank of New York
21	First State Management Group
19 through 21	The Hartford Insurance Company
18	Equal Employment Opportunity Commission, Teleport, Metropolitan Fiber Systems
15 through 17	Citigroup
14	Vacant
13	U.S. Securities and Exchange Commission, Provident Financial Management, American Express
11, 12	U.S. Securities and Exchange Commission
10, 9	U.S. Secret Service
7, 8	American Express
5, 6	Mechanical floors
4	Meeting spaces, cafeteria
1 through 3	Lobbies, conference center

^a Among those interviewed by the Investigation Team, there was limited recollection of the organizations occupying some of the floors, especially those occupying smaller spaces, and no one had copies of all the tenant leases.

NIST, Final Report on the Collapse of World Trade Center Building 7 (November 2008), p. 9, Table 1-1. Tenants and floor uses as of September 11, 2001. ³⁰

In July 2001, Code Red swept across Internet-connected computers. CAIDA researchers estimated that its July 19 outbreak infected more than 359,000 computers in under 14 hours. On August 4, a separate worm, CodeRedII, appeared. It left persistent backdoors on affected Windows web servers; restarting the computer did not remove them. On August 29, GAO

told Congress that Treasury's Financial Management Service had been infected and forced to disconnect from the Internet. Bank customers were also exposed through a separate breach of third-party purchase data. By early September, Riggs had notified 3,000 customers and First Virginia another 500 that their debit-card information had been compromised, Computerworld reported. Banks

NOTES

²⁹ GAO-01-1073T, August 29, 2001, pp. 4-5

³⁰ NIST NCSTAR 1A, 7WTC tenants, Table 1-1

³¹ CAIDA, Code-Red study and chronology, 2002

³² Computerworld, compromised debit cards, September 10, 2001

³³ Pitt, securities-market recovery, September 20, 2001

had to cancel and replace cards. These outbreaks and breaches were already underway when the September 11 attacks struck. U.S. securities markets reopened on

September 17 after extensive checks of power, telecommunications and computer connections, as SEC chairman Harvey Pitt later described.^{31 29 32 33}

Impact of the Attacks

Reports from various media and computer security experts indicate that the impact of these viruses has been extensive. On July 19, the Code Red worm infected more than 250,000 systems in just 9 hours, according to the National Infrastructure Protection Center (NIPC). An estimated 975,000 servers have been infected in total, according to Computer Economics, Inc. Code Red and Code Red II have also reportedly disrupted both government and business operations, principally by slowing Internet service and forcing some organizations to disconnect themselves from the Internet.

For example, reports have noted that (1) the White House had to change the numerical Internet address that identifies its Web site to the public, and (2) the Department of Defense was forced to briefly shut down its public Web sites. Treasury's Financial Management Service was infected and also had to disconnect itself from the Internet. Code Red worms also reportedly hit Microsoft's popular free E-mail service, Hotmail; caused outages for users of Qwest's high-speed Internet service nationwide; and caused delays in package deliveries by infecting systems belonging to FedEx Corp. There are also numerous reports of infections in other countries.

U.S. General Accounting Office, Keith A. Rhodes testimony, August 29, 2001, GAO-01-1073T, p. 4.²⁹

On September 18, CERT warned of Nimda, which spread through email, infected websites and other routes. It also searched for backdoors left by CodeRedII and earlier attacks. The FDIC attributed unusually high September virus detections inside its firewall to Nimda. World Bank researchers also listed Deutsche Bank among Nimda's September victims. In Japan, Associated Press reporting quoted Tsuru Credit Union spokesman Takao Ide saying its infected website had been shut and

online settlements and transfers suspended. CAIDA continued monitoring Code Red activity into October, reporting no significant change from August until CodeRedII's programmed October 1 shutdown. F-Secure documented another episode on October 11, when hundreds of Nimda-infected emails were sent worldwide. The attacks stretched from July into October, with later malware able to exploit access left behind by earlier infections.^{34 35 36 37 31 38}

NOTES

²⁹ GAO-01-1073T, August 29, 2001, pp. 4-5

³¹ CAIDA, Code-Red study and chronology, 2002

³² Computerworld, compromised debit cards, September 10, 2001

³³ Pitt, securities-market recovery, September 20, 2001

³⁴ CERT CA-2001-26, Nimda, September 2001

³⁵ FDIC, 2001 Performance Report, p. 54

³⁶ World Bank, electronic security, 2002, Table 2

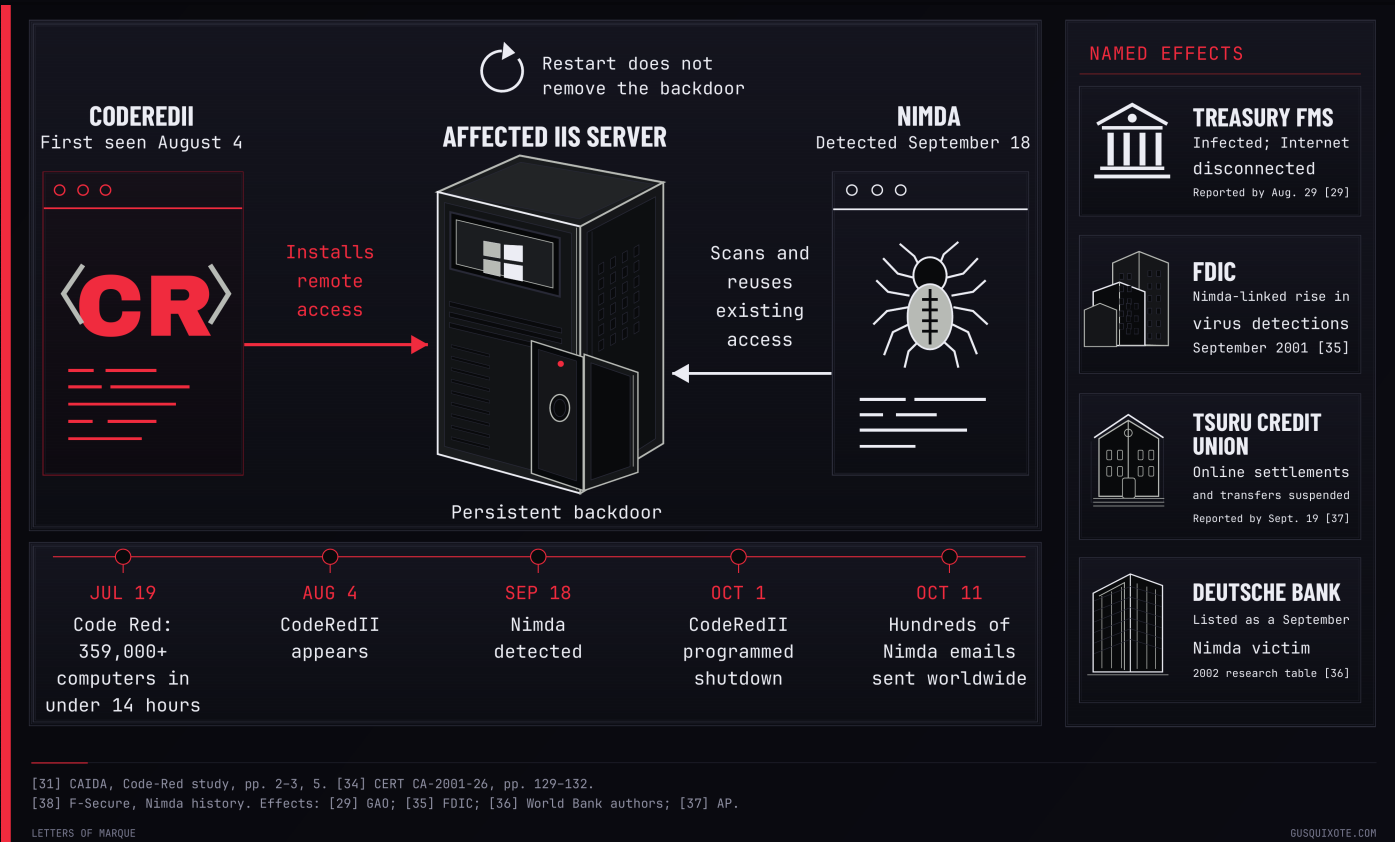
³⁷ AP, Tsuru Credit Union and Nimda, September 19, 2001

³⁸ F-Secure, Nimda technical history

GRAPHIC 02

AN INFECTION COULD LEAVE THE DOOR OPEN

CodeRedII left access that Nimda could reuse. July-October 2001.



CodeRedII could leave persistent access on an affected IIS server; Nimda could search for and reuse that access. The July-October 2001 chronology sits beside separately documented effects at Treasury’s Financial Management Service, the FDIC, Tsuru Credit Union and Deutsche Bank. [31](#) [34](#) [38](#) [29](#) [35](#) [36](#) [37](#)

NOTES

- [29](#) GAO-01-1073T, August 29, 2001, pp. 4-5
- [31](#) CAIDA, Code-Red study and chronology, 2002
- [34](#) CERT CA-2001-26, Nimda, September 2001
- [35](#) FDIC, 2001 Performance Report, p. 54
- [36](#) World Bank, electronic security, 2002, Table 2
- [37](#) AP, Tsuru Credit Union and Nimda, September 19, 2001
- [38](#) F-Secure, Nimda technical history

On October 4, 2001, President George W. Bush authorized the Defense Department, including the NSA, to conduct electronic intelligence collection aimed at preventing further attacks. The Justice Department inspector general later found that, during the President's Surveillance Program's first year and a half, only one Office of Legal Counsel attorney—John Yoo—was cleared to work on it. Keeping other lawyers out of the program also kept them from checking the government's arguments for its legality.^{39 40}

The inspector general called reliance on a single attorney extraordinary and inappropriate. Limited review had contributed to legal analysis that was, at minimum, factually flawed. Once additional attorneys gained access, serious objections emerged. As with the earlier investigative failures, officials could not properly examine information they were forbidden to see. Restrictions imposed around a surveillance program had weakened the government's own legal oversight.^{40 1}

NOTES

¹ HSCA, CIA cooperation, 1979, pp. 252-253

³⁹ DOJ, surveillance authorization documents, December 2014

⁴⁰ DOJ Inspector General, surveillance-program review, 2009

SECTION 5

ACADEMIC TIES AND DISEASE SURVEILLANCE



American funding also supported academic relationships with China. Temple University reported a September 2001 USAID grant of \$1.75 million to expand its rule-of-law program, with Tsinghua among the collaborators. Its newsletter described training Chinese judges and officials and helping China adapt its legal system to world trade. A later Congressional Research Service report documented USAID support for constructing and equipping Fudan's Center for American Studies. Fudan identifies the Washington-based Fudan Foundation as the funding channel. The United States was deliberately investing in relationships with Chinese institutions as a way to advance American interests.^{41 42 43}

In September, 2001 Temple University's Beasley School of Law was awarded a \$1.75 million grant from the U.S. Agency for International Development (USAID) to enlarge its rule of law initiative in China. This is the first federal grant awarded to any American university to support a rule of law program in China. Temple is the lead institution in this collaborative effort, which includes Tsinghua University, China University of Political Science and Law, New York University School of Law and Brigham Young University. USAID is an independent government agency that provides foreign assistance and humanitarian aid to advance the political and economic interests of the United States.

Temple University Beasley School of Law, Temple ESQ., Winter 2001-02, p. 1. Opening paragraph announcing the September 2001 USAID grant and naming the collaborating universities.⁴¹

Office of American Schools and Hospitals Abroad (ASHA). During the past eight years, USAID's ASHA has supported the construction and equipping of the Center for American Studies at Fudan University in Shanghai. ASHA has also assisted the Hopkins-Nanjing Center for Chinese and American Studies in Nanjing and provided a grant to Project Hope to support training for the Shanghai Children's Medical Center.

Congressional Research Service, RS22663, January 28, 2008, p. CRS-6. The ASHA paragraph describes USAID support for construction and equipment at Fudan's Center for American Studies.⁴²

Academic research also opened international relationships for disease surveillance. A 2011 evaluation prepared for NIH described Nathan Wolfe's 2005 Pioneer Award and research that followed a group of people in Cameroon for signs of emerging disease. It

connected that work to his subsequent Global Viral Forecasting Initiative and listed research locations including Cameroon, Congo, Madagascar and China. Researchers needed access to people, samples and information across borders to carry out the work.⁴⁴

NOTES

⁴¹ Temple ESQ., USAID grant, Winter 2001-02, p. 1

⁴² CRS RS22663, assistance to China, 2008, p. 6

⁴³ Fudan, Center for American Studies history

⁴⁴ NIH award evaluation, 2011, pp. C-26-C-27

Nathan Wolfe (2005)



and predict the emergence of infectious diseases globally.

Nathan Wolfe was awarded the NDPA in 2005, two years after becoming an assistant professor in Epidemiology at Johns Hopkins University's Bloomberg School of Public Health. In the same year, Wolfe was named one of the "Brilliant 10" by *Popular Science* magazine, and was a Burroughs Wellcome Fund finalist for the Investigators in Pathogenesis of Infectious Disease Award. For his NDPA project, Wolfe proposed to establish the first system to monitor

IDA Science and Technology Policy Institute, evaluation of the NIH Director's Pioneer Award, July 22, 2011, p. C-26. Nathan Wolfe's profile and the opening description of his 2005 award project. ⁴⁴

Since receiving his NDPA, Wolfe has also founded the Global Viral Forecasting Initiative (GVFI), to research and predict emerging infectious diseases, in international disease "hot spots" within Cameroon, Madagascar, China, Malaysia, Congo, and Laos.

The same NIH-commissioned evaluation, p. C-27. The next page lists GVFI research locations, including China. ⁴⁴

USAID's PREDICT project, initiated in 2009, brought universities, aid officials and other organizations together to watch for emerging viruses. UC Davis's One Health Institute identifies itself as the lead and lists USAID, EcoHealth Alliance, Metabiota, the Wildlife Conservation Society and the Smithsonian as core partners. Its account describes work primarily in Africa and Asia. A private company and several public and nonprofit institutions were participating in the same disease-surveillance project. ⁴⁵

On CNN in December 2011, Wolfe described the work directly: "we do surveillance, biological surveillance around the world." Discussing pandemic prevention with Sanjay Gupta, he explained the difficulty of finding threats among large quantities of specimens and

information. Researchers would gather observations across countries, combine them and look for signs of danger before an outbreak became a disaster. ⁴⁶

American organizations were also building partnerships with Chinese researchers. In September 2012, BGI announced its memorandum with the Bill & Melinda Gates Foundation, combining its ability to study genes and read genetic sequences with the foundation's health and agricultural programs. This was a separate agreement from Wolfe's work and PREDICT. Together, these records show how research partnerships created continuing contact across national boundaries that security officials also treated as lines of strategic competition. ^{47 44 45}

NOTES

⁴⁴ NIH award evaluation, 2011, pp. C-26-C-27

⁴⁵ UC Davis, PREDICT project description

⁴⁶ CNN, Nathan Wolfe interview, December 21, 2011

⁴⁷ BGI-Gates memorandum announcement, September 25, 2012

SECTION 6

METABIOTA, INVESTMENT AND INTELLIGENCE

VI

Metabiota also attracted private investors. A preserved March 2014 Rosemont Seneca Technology Partners investment-committee email preserved among the published Hunter Biden emails described a proposed additional \$250,000 investment that would bring the firm's position to \$500,000. The email records a proposal, not a completed transaction. It places investor interest in Metabiota alongside the company's government and scientific relationships.⁴⁸

Subject: IC Materials
From: John DeLoche
Date: 3/10/14, 2:36 AM
To: Hunter Biden, Devon Archer, Neil Callahan, William Lee <will@rstp.com>

IC Committee,

In the interest of establishing a clear process for our investment approvals I wanted to give you a preview of the agenda for the first IC Committee call, which I hope we can do on our weekly call tmw. In the future we will plan to have full memos distributed to the committee for each deal the Friday before the Monday committee meeting. Apologies we were not able to put together a memo for Metabiota given our front end loading of Lyft. We will put one together for Metabiota shortly.

We have three deals to discuss tmw.

The first is an increase in our investment in Metabiota by \$250k. Docs are attached. They raised about \$2.4mm of which we represent \$500k (250k from the first investment plus this one). They intended to raise a max of \$1.6mm but it was oversubscribed. They way to think about this one is that Palantir is the to the CIA what Metabiota is to the USDA. The company's plan is to take advantage of the current fundraising climate and start raising a series A as soon as this series seed closes. They hope to raise another \$15mm at at least \$80mm pre which would be a nice 5x mark-up to our investment. We are planning to show it to Founders Fund, Andreessen and Google Ventures (among others) as potential leads.

| John DeLoche, investment-committee email, March 10, 2014. Excerpt from the preserved email image. ⁴⁸

NOTES

⁴⁸ John DeLoche investment email, March 10, 2014

By August 2017, In-Q-Tel's relationship with Metabiota was public. An announcement hosted by In-Q-Tel said it and Munich Re, a company that insures insurers, had signed strategic agreements with Metabiota. In-Q-Tel investment partner Eugene Chiu highlighted "open source data fusion and sophisticated epidemic simulations." That meant combining publicly available information and using computer models to explore possible outbreaks. In-Q-Tel was backing the data and software side of biological surveillance.⁴⁹

The same announcement described software to estimate how often epidemics might strike, how long they might last, and their likely severity and cost. Insurers could use the results to price and manage risk; governments could use them to assess preparedness. Metabiota turned information about disease into a commercial product. Intelligence, public-health and insurance organizations could use the same software to make decisions that served their different interests.⁴⁹

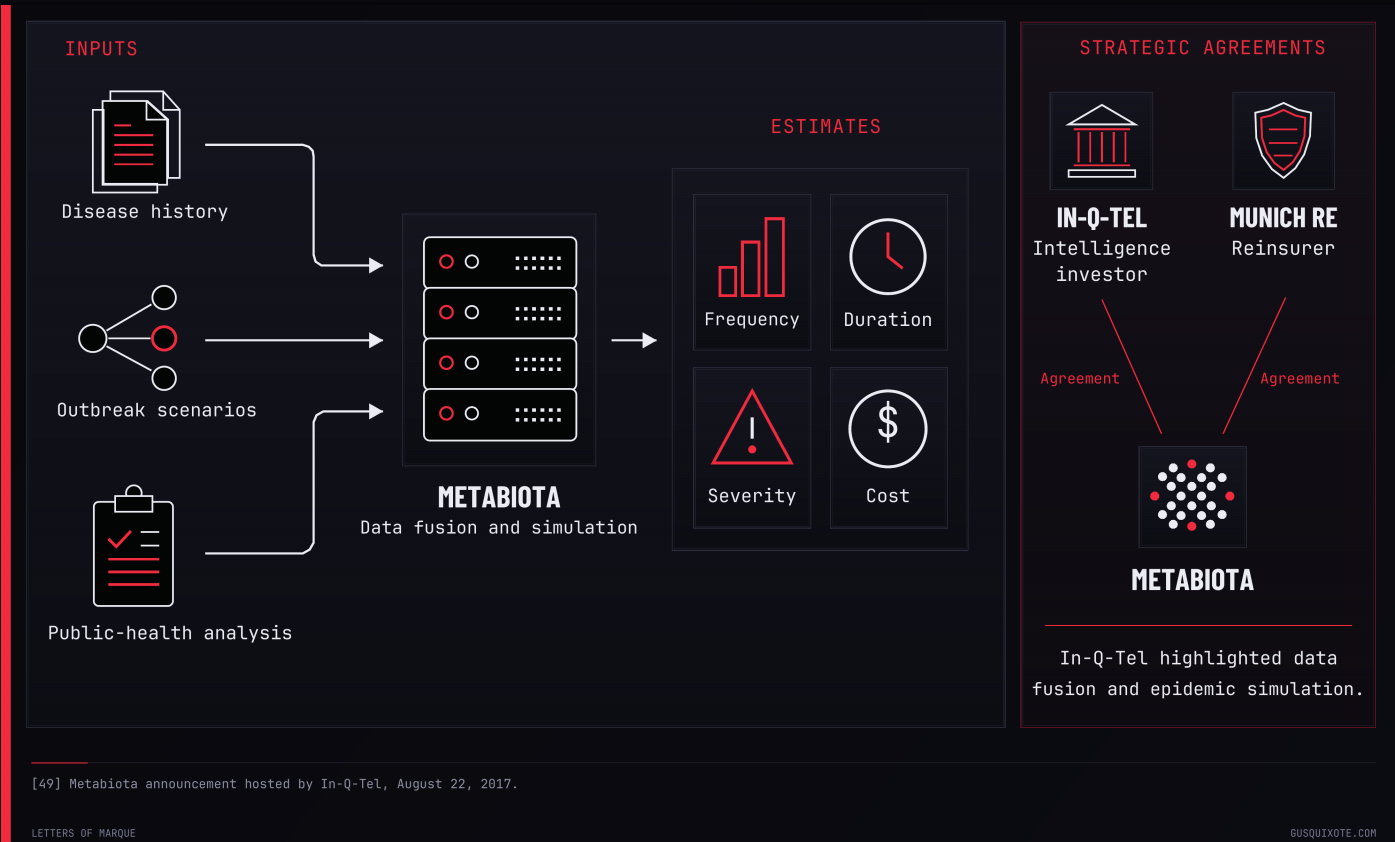
NOTES

⁴⁹ In-Q-Tel-Metabiota announcement, August 22, 2017

GRAPHIC 03

IN-Q-TEL AND METABIOTA: DATA FUSION AND SIMULATION

Epidemic-modeling capabilities and strategic agreements announced August 22, 2017.



Metabiota's August 22, 2017 announcement described data-fusion and epidemic-simulation capabilities combining disease history, outbreak scenarios and public-health analysis to estimate frequency, duration, severity and cost. It announced separate strategic agreements with In-Q-Tel and Munich Re. 49

NOTES

49 In-Q-Tel-Metabiota announcement, August 22, 2017

Control over information repeatedly gave officials power over other people's decisions. Investigators worked from the files they received. Military leaders acted on intelligence that others assembled. Officials could use confidential business information to pressure a government over a contract. Software could organize disease reports into warnings that customers used to make decisions. The people collecting and interpreting the information helped determine what those customers and officials saw—and what they might overlook. ^{1 6 24 49}

By September 2001, demands for more intelligence were already familiar. The attacks gave officials new grounds to seek wider access. Examining who gained that access, what they could do with it and who could check them leads from government offices to the companies building surveillance tools. Their contracts, technology and relationships with intelligence agencies are the subject of the next part of this investigation. ^{22 19 25 39}

NOTES

¹ HSCA, CIA cooperation, 1979, pp. 252-253

⁶ Hanyok, Gulf of Tonkin study, 2000-01

¹⁹ DCI Annual Report, In-Q-Tel section, 1999

²² Clinton, antiterrorism signing statement, April 24, 1996

²⁴ Woolsey, Why We Spy on Our Allies, March 17, 2000

²⁵ In-Q-Tel-SafeWeb announcement, February 14, 2001

³⁹ DOJ, surveillance authorization documents, December 2014

⁴⁹ In-Q-Tel-Metabiota announcement, August 22, 2017

NUMBERED SOURCES

SOURCE REGISTER

- 1 HSCA report, 1979: CIA cooperation with the Warren Commission
Printed pp. 252-253, discussion of Raymond Rocca and Richard Helms.
<https://www.archives.gov/research/jfk/select-committee-report/part-1d.html>
- 2 David Robarge, John McCone and the Assassination of President John F. Kennedy
Studies in Intelligence, September 2013; release approved September 29, 2014; printed pp. 8-9, 12, 20. Derived from the 2005 McCone history.
https://nsarchive2.gwu.edu/NSAEBB/NSAEBB493/docs/intell_ebb_026.PDF
- 3 Guidelines for Operation Mongoose, March 14, 1962
FRUS document 314, paragraphs 1-4 and source note concerning March 16 covering memorandum.
<https://history.state.gov/historicaldocuments/frus1961-63v10/d314>
- 4 National Security Action Memorandum 263, October 11, 1963
FRUS document 194, p. 396, operative paragraph 2.
<https://history.state.gov/historicaldocuments/frus1961-63v04/d194>
- 5 McNamara-Taylor report to Kennedy, October 2, 1963
FRUS document 167, pp. 337-339, section I.B.1-3.
<https://history.state.gov/historicaldocuments/frus1961-63v04/d167>
- 6 Robert J. Hanyok, Skunks, Bogies, Silent Hounds, and the Flying Fish
Cryptologic Quarterly, Winter 2000/Spring 2001; printed pp. 3, 26-28, 38, 44, 48-49.
https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/gulf-of-tonkin/articles/release-1/rell_skunks_bogies.pdf
- 7 Rostow to Johnson with covert-action review chronology, February 18, 1967
FRUS document 171, attachment paragraph d, p. 543; reproduced August 24, 1961 review.
<https://history.state.gov/historicaldocuments/frus1964-68v10/d171>
- 8 State Department circular on CIA student funding, February 15, 1967
FRUS Public Diplomacy VII, document 132, paragraph 4, pp. 412-413.
<https://history.state.gov/historicaldocuments/frus1917-72PubDipv07/d132>
- 9 Katzenbach committee report, March 24, 1967, and Johnson's response
Document 144, attachment sections 1-2, pp. 445-449; March 29 acceptance in editorial note.
<https://history.state.gov/historicaldocuments/frus1917-72PubDipv07/d144>
- 10 Rockefeller Commission report, Chapter 11: Operation CHAOS
June 1975, printed pp. 130-136 and 143-150; Helms cover memorandum reproduced p. 134.
https://www.fordlibrarymuseum.gov/library/exhibits/intelligence/RockComm_Chap11_CHAOS.pdf
- 11 Senate staff report, Covert Action in Chile, 1963-1973
December 18, 1975; pp. 8, 19, 27-29.
<https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-94chile.pdf>
- 12 Rockefeller Commission report, Chapter 14: CIA and Watergate
June 1975; printed pp. 178-185, 199-203, 206-207.
https://www.fordlibrarymuseum.gov/sites/default/files/pdf_documents/library/document/0005/7288237.pdf
- 13 Nixon-Haldeman recorded conversation, June 23, 1972, morning
Trial exhibit 1, printed pp. 3-8 and 16-17.
https://www.nixonlibrary.gov/sites/default/files/researchers/find/tapes/watergate/trial/exhibit_01.pdf
- 14 Interdepartmental review of military credit for Iran, April 5, 1968
FRUS document 277, record of March 21 and April 3 meetings, pp. 497-501.
<https://history.state.gov/historicaldocuments/frus1964-68v22/d277>
- 15 Kissinger instruction following Nixon's talks with the Shah, July 25, 1972
FRUS document 214, items 1-3 and final paragraph, original pp. 1-2.
<https://history.state.gov/historicaldocuments/frus1969-76ve04/d214>
- 16 Richard Solomon to Kissinger, Possible Next Steps in Sino-US Relations, June 9, 1972
FRUS document 229, section II.C, pp. 909-910; notes 4-5.
<https://history.state.gov/historicaldocuments/frus1969-76v17/d229>

NUMBERED SOURCES

SOURCE REGISTER

- 17 Lawrence Walsh, Final Report, Chapter 8: The Enterprise
1993 report, sections on the 1985-1986 Enterprise, foreign accounts and Iran proceeds.
https://irp.fas.org/offdocs/walsh/chap_08.htm
- 18 Malcolm, Roseboom, Clark and Fazar, Application of a Technique for Research and Development Program Evaluation
Operations Research 7(5), 1959, pp. 646-669; DOI 10.1287/opre.7.5.646. The cited material is the publisher abstract and author affiliations.
<https://pubsonline.informs.org/doi/abs/10.1287/opre.7.5.646>
- 19 Director of Central Intelligence Annual Report, 1999
In-Q-Tel section: incorporation February 19, 1999, commercial IT and CIA requirements.
<https://irp.fas.org/cia/product/report-99.html>
- 20 White House statement on the Clipper encryption initiative, April 16, 1993
Full statement, especially law-enforcement rationale and key-escrow description.
<https://clintonwhitehouse6.archives.gov/1993/04/1993-04-16-press-release-on-clipper-chip-encryption-initiative.html>
- 21 NIST cryptography history: key escrow and the Clipper initiative
Key Escrow / Clipper sections, including adoption and 1996 committee discussion.
<https://csrc.nist.gov/nist-cyber-history/cryptography/chapter>
- 22 Clinton statement signing the Antiterrorism and Effective Death Penalty Act, April 24, 1996
Statement paragraphs on February/May 1995 requests, Oklahoma City, wiretaps and stripped provisions; original Public Papers p. 630.
<https://www.presidency.ucsb.edu/documents/statement-signing-the-antiterrorism-and-effective-death-penalty-act-1996>
- 23 George Tenet statement on the Chinese embassy bombing, July 22, 1999
Chronology of Events; Late Concerns About the Target; What Went Wrong?
https://irp.fas.org/congress/1999_hr/990722-tenet.htm
- 24 R. James Woolsey, Why We Spy on Our Allies, March 17, 2000
Wall Street Journal commentary reproduced by Cryptome, then Linas; admission, computer filtering and trade-secret denial paragraphs.
<https://www.linas.org/mirrors/cryptome.org/2001.11.13/echelon-cia2.htm>
- 25 In-Q-Tel commissions SafeWeb for Internet privacy technology
Announcement February 14, 2001; agreement dated November 30, 2000.
<https://www.igt.org/library/in-q-tel-commissions-safeweb-for-internet-privacy-technology>
- 26 9/11 Commission Report, Chapter 6: From Threat to Threat
Printed pp. 210-214, armed Predator discussion; notes 238-258.
https://9-11commission.gov/report/911Report_Ch6.htm
- 27 U.S. Attorney, District of Colorado / DCIS, Venezuelan hacker pleads guilty to attacking Department of Defense computer system located in Denver, Colorado
July 28, 2005 announcement; PDF p. 1, stipulated-facts paragraphs dating the DISA training-system intrusion to about June 10, 2001.
https://media.defense.gov/2005/JUL/28/2001711084/-1/-1/1/venezuelan_08205.pdf
- 28 Reuters, Pentagon thwarts worm, reopens Web sites
July 24, 2001; Craig Quigley statements on limited Code Red infections, classified systems and tactical operations; Susan Hansen restoration statement.
<https://www.chron.com/business/technology/article/pentagon-thwarts-worm-reopens-web-sites-2027514.php>
- 29 Keith Rhodes, GAO-01-1073T: Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures
August 29, 2001 testimony; printed p. 4 / PDF p. 5, Treasury Financial Management Service paragraph; printed p. 5 / PDF p. 6, FBI SirCam paragraph.
<https://www.gao.gov/assets/gao-01-1073t.pdf>

NUMBERED SOURCES

SOURCE REGISTER

- 30 NIST NCSTAR 1A, Final Report on the Collapse of World Trade Center Building 7
November 2008 report, final-revision metadata
January 29, 2009; printed p. 9 / PDF p. 51, Table 1-1 and footnote, tenants as of September 11, 2001.
<https://www.govinfo.gov/content/pkg/GOVPUB-C13-4d4c17460292ee57ef313f6491fa8d1e/pdf/GOVPUB-C13-4d4c17460292ee57ef313f6491fa8d1e.pdf>
- 31 David Moore, Colleen Shannon and Jeffery Brown, Code-Red: a case study on the spread and victims of an Internet worm (2002)
PDF pp. 2-3, Background and Methodology; p. 5, Results A.1. Supplementary institutional chronology:
<https://www.caida.org/archive/code-red/> . July 12/19 and August 4, 2001 outbreak dates; monitoring continued into October.
https://www.caida.org/catalog/papers/2002_codered/codered.pdf
- 32 Dan Verton, Hacker forces some banks to cancel Visa debit cards, Computerworld
September 10, 2001; opening reporting and statements by First Virginia CFO Rick Bowman, Riggs official and Visa about compromised third-party purchase data.
<https://www.computerworld.com/article/1337620/hacker-forces-some-banks-to-cancel-visa-debit-cards.html>
- 33 Harvey Pitt testimony on market recovery, September 20, 2001
Closure, system testing and September 17 reopening paragraphs. Page modified September 21.
<https://www.sec.gov/news/testimony/092001tshlp.htm>
- 34 CERT/CC Advisory CA-2001-26: Nimda
Initial September 18, 2001; revised September 25; printed pp. 129-132, PDF pp. 133-136. Compilation revision/copyright are later.
https://www.sei.cmu.edu/documents/508/2001_019_001_496192.pdf
- 35 FDIC 2001 Program Performance Report
Printed p. 54, PDF p. 56 of 76, Virus Detection; September 2001 reporting.
https://archive.fdic.gov/view/fdic/9521/fdic_9521_DS1.pdf
- 36 Thomas Glaessner, Tom Kellermann and Valerie McNevin, Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues
World Bank Policy Research Working Paper 2870, July 2002; printed p. 8 / PDF p. 13, Table 2, Deutsche Bank entry dated September 20, 2001, and note 14.
<https://documents.worldbank.org/curated/en/985681468739503889/pdf/multi0page.pdf>
- 37 D. Ian Hopper / AP, contemporary Nimda report, September 19, 2001
Tsuru Credit Union spokesman Takao Ide's statement about online settlements and transfers. Contemporary report recovered through indexed article text.
<https://thedailyrecord.com/2001/09/19/new-complex-worm-slows-in-united-states-but-other-countries-hit/>
- 38 F-Secure, Net-Worm:W32/Nimda
Technical Details and History; the October 11, 2001 episode is reported at about 15:00 GMT. The page's original publication and amendment dates are not established.
<https://www.f-secure.com/v-descs/nimda>
- 39 DOJ release concerning surveillance authorized after 9/11, December 12, 2014
Paragraph beginning On Dec. 21, 2013: October 4, 2001 authorization. Page updated February 5, 2025.
<https://www.justice.gov/archives/opa/pr/department-justice-releases-additional-documents-concerning-collection-activities-authorized>
- 40 DOJ Inspector General, semiannual report April-September 2009
The Department's Involvement with the President's Surveillance Program section; report summary dated July 10, 2009.
<https://oig.justice.gov/archives/semiannual/0911/multi.htm>
- 41 Temple Law ESQ., Winter 2001-02: \$1.75 Million Grant Expands Law School's Program in China
Page 1, opening article and continuation in adjacent column; grant September 2001.
<https://law.temple.edu/esq/docs/Temple-Law-ESQ-Winter-2001.pdf>

NUMBERED SOURCES

SOURCE REGISTER

- 42 Thomas Lum, U.S.-Funded Assistance Programs in China, January 28, 2008
CRS RS22663, p. 6, ASHA paragraph; p. 1 for stated democracy/rule-of-law purpose.
https://www.everycrsreport.com/files/20080128_RS22663_3e9e89138bcb565b231aadccc449cc390eb96846.pdf
- 43 Fudan University, Center for American Studies institutional page
Institutional history, ASHA/Fudan Foundation paragraph; current page accessed September 6, 2026.
<https://iis.fudan.edu.cn/en/cas/list.htm>
- 44 NIH-commissioned evaluation of the Director's Pioneer Award, July 22, 2011
IDA/STPI report, Nathan Wolfe (2005), printed C-26-C-27, PDF pp. 148-149.
https://commonfund.nih.gov/sites/default/files/Pioneer_Award_Outcome%20Evaluation_FY2004-2005.pdf
- 45 UC Davis One Health Institute, PREDICT project page
Project description beginning Initiated in 2009; core partner paragraph.
<https://ohi.vetmed.ucdavis.edu/programs-projects/predict-project>
- 46 CNN Anderson Cooper 360 transcript, December 21, 2011
Sanjay Gupta discussion with Nathan Wolfe and Fran Townsend; Wolfe's biological-surveillance description.
<https://transcripts.cnn.com/show/acd/date/2011-12-21/segment/01>
- 47 BGI-Gates Foundation memorandum announcement, September 25, 2012
BGI issuer release, opening and collaboration paragraphs; signing September 24, 2012.
<https://www.prnewswire.com/news-releases/bgi-and-the-bill-melinda-gates-foundation-sign-memorandum-of-understanding-on-collaboration-for-global-health-and-agricultural-development-171139691.html>
- 48 Preserved John DeLoche investment-committee email, March 10, 2014
Canonical row 221; full displayed image; separate email record <https://bidenlaptopemails.com/primary-research/email/127038> ; original context <https://gusquixote.com/threads/2023-08-10-1689455218264596480/index.html> . The preserved email image was checked against a separately preserved text copy in the completed audit.
<https://gusquixote.com/media/twitter/1689455218264596480/F3ImexcXAAEflgI.png>
- 49 In-Q-Tel / Metabiota strategic-agreement announcement, August 22, 2017
Complete announcement, Eugene Chiu attribution and commercial-platform description.
<https://www.iqt.org/library/munich-re-in-q-tel-select-metabiota-to-gain-deeper-insights-into-epidemic-risk-and-global-preparedness-for-infectious-diseases>
- 50 Tom Herbert, Who was Jamal Khashoggi?
Paragraph identifying Jamal Khashoggi as Adnan Khashoggi's nephew.
<https://www.standard.co.uk/news/uk/who-was-jamal-khashoggi-the-saudi-journalist-tortured-and-murdered-a3964576.html>
- 51 U.S. Treasury sanctions announcement concerning the murder of Jamal Khashoggi
Murder of Khashoggi section: October 2, 2018 killing and identified Saudi participants.
<https://home.treasury.gov/news/press-releases/jy0038>



KEEP THE RECEIPTS

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

[GUSQUIXOTE.COM](https://gusquixote.com)