Doc ID: 6586785

(U) NSA's Key Role in Major Developments in Computer Science

PART ONE

(U) Cryptology has historically entailed an intensive application of labor. But since the middle of the last century, automation has been used as a way to greatly ease the making and breaking of codes. The formation and maturation of the National Security Agency (NSA) and the evolution of its missions paralleled in large part the advent of the computer age. As a consequence, the NSA and its predecessor agencies have historically been at the forefront of computer development in the United States.

(U) But the use of computational machines in American cryptology long predated the official birth of NSA. During World War I, the military incorporated use of encryption equipment. During the 1930s, both the Army and Navy cryptologic components acquired devices from International Business Machines (IBM), which allowed them to sort large amounts of data. By the time World War II had broken out, all of the major combatants possessed sophisticated cipher machines for most of their communications generation and security programs.

(U) As the war progressed, the U.S. military services placed many electronic accounting machines into the field in order to process a wide array of enemy signals. The services developed relationships with industry -- Bell Laboratories and Teletype Corporation in the case of the Army, and IBM, Eastman Kodak, and National Cash Register (NCR) in the case of the Navy. A prime example of the benefits of such relationships was the construction of the Navy's cryptanalytic "Bombe," a machine built by NCR to decipher messages from the German ENIGMA machine. The Army and Navy also developed devices of increasing power and capacity during the war. The machines could compile and compare message texts, search for cribs, or seek statistical coincidences. The colorful designators of these machines included DRAGON, COPPERHEAD, RATTLER, MAMBA, DUENNA, MADAME X, and SUPERSCRITCHER. None of these were actual computers, as they lacked memory or the capability to perform outside of their designated computational functions.

(U) Great Britain and the United States became close partners in cryptanalysis, and as a consequence built machines of increasing power and complexity to solve the cryptosystems of their enemies. Near the end of the war, the British government developed a device that could be labeled the first true computer. For rapid exploitation of the German encipherment machine known as TUNNY, British engineers invented the COLOSSUS, which had many characteristics now associated with modern computers. Almost at the same time, American engineers at the University of Pennsylvania also had built a computer, ENIAC, to generate artillery ballistics tables.

[redacted]

Declassified and Approved for Release by NSA on 07-19-2017 pursuant to E.O. 13526: MDR-101721

Doc ID: 6586785

(U) Thus, by war's end U.S. Army and Navy cryptologists had considerable experience with special-purpose devices and even the British proto-computer. This experience made clear to both services that rapid data processing would be vital to American cryptology in the future. The challenge was to transfer their hard-won knowledge from special-purpose machines to the design of a general-purpose computer capable of multiple applications. Although widely recognized that the United States needed rapid data processing for its cryptologic exploitation efforts, unfortunately budgets dropped, many technical experts left government service, and industrial contracts expired during the immediate postwar era. The best that could be done through in-house research was production of cryptanalytic devices known as rapid analytic machines that worked against only one foreign system each. These devices included ALCATRAZ, O'MALLEY, WARLOCK, HECATE, and SLED.

(U~~//FOUO~~) By mid-1946 new advances were occurring in data processing. Programming languages, increased memory, and new processors were being envisaged and discussed at leading academic research centers. Notably, two civilian researchers, James Pendergrass for the Navy and Samuel Snyder for the Army, led the way in discerning applications of advances in commercial data processing for military cryptology. By 1947 both the Army and Navy cryptologic organizations decided to acquire computers.

(U~~//FOUO~~) In 1950 the Navy and industry working together produced the first real general-purpose computer for the government. Built by Electronic Research Associates (ERA), a company headed by Howard Engstrom, who himself had worked on the Navy Bombe during the war, it was called ATLAS. This machine cost nearly $1 million, used 2,700 vacuum tubes, and relied on drum memory technology. ATLAS would perform well in support of cryptanalysis over the subsequent decade in which it was used. One of ATLAS's greatest assignments was to attack isologs in messages codenamed VENONA, intercepts of Soviet espionage communications during the height of World War II.

~~(S)~~ ATLAS had been built by the Navy using outsourcing, but the Army instead relied on in-house work for its own computer research and development. The Army Security Agency (ASA) engaged in considerable design work for its own computer, but had not begun actual production by the time the Armed Forces Security Agency (AFSA) was founded in May 1949. Many cryptologic research functions, including data processing, were consolidated under AFSA, and the outbreak of the Korean War provided the stimulus for more rapid development. Since conventional means proved too slow to validate U.S. encryption tables for wartime use by American forces, AFSA authorized production of ASA's computer design. The result, completed in 1952 under an ASA contract, was ABNER, a general-purpose analytic computer. ABNER consisted of vacuum tubes and held only 16,000 words in its memory, but contributed mightily to reducing calculation speed.

[(U~~//FOUO~~) Kent R. Sieg, Center for Cryptologic History, [redacted]

PL 86-36/50 USC 3605

Doc ID: 6586785

(U) NSA's Key Role in Major Developments in Computer Science

PART TWO

~~(S//SI)~~ Soon after its formation on 24 October 1952, NSA encountered another opportunity for employing electronic data processing. During the mid-1950s, sites around the world were sending 37 tons of intercepts to NSA each month, and conventional machines were not equal to the task of sorting, standardizing, and routing this amount. To deal with this volume, NSA spent more than $3 million dollars on a contract to develop NOMAD. This device, designed to increase computer memory exponentially, failed to deal adequately with the ever-expanding quantity of incoming material.

~~(S//SI)~~ When NOMAD's failure become apparent, NSA developed a number of special-purpose devices to perform the necessary data managing and processing that NOMAD had been slated to do. To meet the many mission requirements it had been tasked with during the height of the Cold War, NSA was among the first organizations to utilize systems that incorporated innovative input techniques and storage devices, including drum storage, tape drives, remote job access, and computer chip technology. SOLO, a computer built in the mid-1950s, became the first machine to replace vacuum tubes with transistors. Special-purpose computers were designed not only for cryptanalysis, but also to generate communications security (COMSEC) material for protection of U.S. communications. Another system named BOGART, originally designed to support NOMAD, used solid state technology for the first time and took advantage of new tape drives for long-term data storage. BOGART also served as the central computer for ROB ROY, one of the first remote job entry systems. Of related significance, ROGUE came out at this time as the first remote job access computer.

~~(TS//SI)~~ By the late 1950s, the highest priority was to cryptanalytically attack Soviet cipher systems. A major study chaired by ex-President Herbert Hoover recommended an all-out offensive program against Soviet cryptosystems similar in scope to the project that had developed the atomic bomb. The first Director, NSA (DIRNSA), Lieutenant General (LTG) Ralph Canine, brought in Howard Engstrom to lead research efforts to solve this problem. Engstrom, who later would become NSA's deputy director, collated ideas from NSA scientists and cryptanalysts regarding both long-term research into super-fast computers and assessments of Soviet cryptosystems. His findings eventually evolved into a proposal for high-speed computer construction known as Project FREEHAND. A subsidiary effort to develop supporting hardware became known as Project LIGHTNING.

~~(S//SI)~~ General Canine wanted the plans begun before he retired, and succeeded in obtaining high-level funding and support for Project FREEHAND. In a meeting with

~~Derived From: NSA/CSSM 1-52~~

~~Dated: 20070108~~

~~Declassify On: 20361231~~

Declassified and Approved for Release by NSA on 07-19-2017 pursuant to E.O. 13526: MDR-101721

EO 1.4.(c)
PL 86-36/50 USC 3605

Canine's successor, LTG John Samford, President Dwight Eisenhower did formally approve Project LIGHTNING. Howard Campaigne became the LIGHTNING program manager and was charged with developing a super-fast computer to meet the country's national security needs. Related advances resulting from these NSA projects included the development of the cryotron to lower computer operating temperatures, component miniaturization, and fast switching devices using the tunnel diode.

~~(S//SI)~~ At the same time LIGHTNING started, the IBM Corporation proposed a parallel research track known as HARVEST. Notably, both Engstrom and Snyder opposed the concept, arguing that the technology involved was not as advanced as needed, and that funding HARVEST would interfere with Project FREEHAND. However, General Samford approved the proposal. With HARVEST, IBM launched a new, state-of-the-art second-generation general-purpose processor.

~~(TS//SI)~~ To be successful, HARVEST had to have a super-high-speed memory and high-speed tape drives beyond anything then in existence. Developed over five years, the most innovative component was TRACTOR, a high-speed tape drive system. It was the first fully automated storage and retrieval system and a precursor to current storage systems. But HARVEST had come in at a higher cost than projected, proved very difficult to use, and had slower processing speed than planned. While NSA personnel wrote innovative programs for it that extended its applications, HARVEST never achieved the goal of multiprogramming. Nevertheless, HARVEST remained in service from 1962 to 1976.

~~(TS//SI)~~ Already by the early 1960s, automation completely overshadowed manual processing. Starting in the middle of that decade, NSA began purchasing commercially developed computers in addition to building its own units. Agency programmers often wrote specialized software that extended the cryptologic capabilities of these on-the-shelf systems. The computer of choice was the IBM 7010. NSA also used the minicomputers PDP-1 and PDP-10 as well as the UNIVAC 490, along with a software developed at NSA known as RYE. The Honeywell Corporation also developed the Honeywell 316 to accept manual Morse data from 128 different sources simultaneously and record it directly onto magnetic tape. As well, collection systems even in remote sites became digitally based. Furthermore, computers also allowed for the collection of a wider variety of signals, including [redacted] By 1968 NSA had over 100 computers, organized in complexes according to the type of processing performed. NSA's five acres of equipment became the largest collection of advanced computers in the United States and probably in the world.

~~(S//SI)~~ HARVEST's advent had marked the domination of computing by large mainframes. NSA had developed six complexes of these mainframes, each dedicated to one specific purpose. UNIVAC and Honeywell computers processed incoming data streams at the communications complex. Five IBM-370s ran batch jobs [redacted] The Rye complex supported current operations. A pair of UNIVAC 1108s ran plaintext. Control Data Corporation (CDC, the successor to ERA) computers processed electronic intelligence. The largest of these six complexes was devoted to cryptanalysis.

PL 86-36/50 USC 3605

Doc ID: 6586785

(U~~//FOUO~~) By the 1980s, NSA's mainframes were becoming congested, and the Agency moved towards deployment of personal computers (PCs). During the middle part of the decade, the IBM PC XT became the standard, and AT&T set up the network for user interface for the dominant operating system at the time, UNIX. Also during that time, NSA established two important centers, one for supercomputer research and the other for computer security.

(U~~//FOUO~~) Although as time passed developments in the computer industry had lost the formerly direct connection to the ever-increasing complexity of cryptology, the Agency continued to remain at the forefront of major progress. In fact, some of the earliest supercomputers were designed and built for NSA. By the early 1970s, the Agency was moving headlong into the era of the supercomputer with the purchase of CDC 6600 and later the CDC 7700. In 1972 former CDC employee Seymour Cray formed his own company and began designing his brand of supercomputers. NSA purchased the first one of his products, CRAY I, in 1976. In 1983 Cray's XMP-22 was the first supercomputer Cray ever actually delivered to a customer site. It was soon upgraded to an XMP-24, arguably the most powerful computer in the world when it came on-line. The XMP-24 used serial processing to conduct 420 million operations per second, and remained in operation from 1983 to 1993.

(U~~//FOUO~~) The second generation Cray, the YMP-90, replaced the older version in 1993. It had a 32-gigabyte memory capacity, some 2,000 times the memory of the better personal computers of that time. The YMP-90 used vector processing, a very powerful form of overlapping coupled with parallel processing, to conduct 2.67 billion operations per second. Working so rapidly that it could melt itself, the designer had installed a cooling system that utilized Flourinert pumped through tubes passing through the circuit boards. The YMP-90, called "Barney" due to its sharing of the purple color belonging to a contemporary popular children's television character, was decommissioned at decade's end.

~~(C//SI)~~ There were other important computer firsts at NSA. A different supercomputer was developed by the Thinking Machine Corporation. This computer was known as the CM-5, or FROSTBURG. Built at a cost of $25 million, the CM-5 had a storage capacity of 500 gigawords and could perform 65 billion calculations per second. Designed to address higher-mathematics- related questions, FROSTBURG was one of the first true parallel processing computers. Also worth mentioning, when installed the PACE 10 was the first analog desktop computer in use at NSA. This computer required the hand wiring of different panels for each type of mathematical calculation to be performed. Of further note, NSA developed many unique and pioneering software systems and databases, such as SOLIS, which held all NSA electronic product reports.

(U~~//FOUO~~) NSA also produced computers for telemetry processing systems. As part of NSA's signals intelligence (SIGINT) mission, telemetry signals were collected by various platforms. Magnetic tape recordings of the intercepted signals were then sent to NSA's National Telemetry Processing Center for processing. These measurements were then transmitted in the form of computer tape to analysis centers that identified the

PL 86-36/50 USC 3605

function of the various transducers and finally developed performance estimates. TELLMAN, the NSA's first telemetry processor to make extensive use of a general-purpose computer, became operational in 1969. In the early 1980's, TELLMAN was replaced with RISSMAN, which processed a wider variety of signals with higher system reliability and lower maintenance costs. RISSMAN's custom-designed hardware used three Intel 8086 microcomputers to perform real-time process control, while Digital VAX-11 computers provided data demultiplexing, data file storage, user-interface, Local Area Network access, digital tape generation, and quality-control plotting services. RISSMAN was in daily use, often processing tapes around the clock, from the date of its delivery through the end of the Cold War.

(U~~//FOUO~~) Storing the data created was another problem that NSA solved with outside assistance. Early efforts involved a photodigital process developed by IBM and a tape storage system from AMPEX. More recently, the Storage Technology (Storage Tek) Corporation has produced much of NSA's recording media storage libraries. Storage Tek designed an automated tape cartridge system for the large, complex, and high-performance environment of NSA. It possessed sufficient capacity for 6,000 tape cartridges each holding 50 gigabytes of data. Using a robotic arm, the StorageTek machine is capable of exchanging 175 cartridges per hour. The entire system can hold 30 terabytes of data.

(U~~//FOUO~~) Since it possesses the world's largest supercomputing facility at its headquarters, NSA therefore has a great demand for microchips.

(U~~//FOUO~~) In recent years, reporting and analysis moved to an on-line basis in order to facilitate rapid dissemination. During the 1990s, the Agency set up the NSA Network (NSANet), an internal classified network. Connectivity to the rest of the IC was established principally through the Joint Worldwide Intelligence Communications System (JWICS), a backbone network connecting all members of the DOD Intelligence Information Systems (DODIIS) community, the military commands, and the IC. Intelink-TS (known to the general NSA population as plain "Intelink") is the TS/SI/TK-rated U.S.-only Web that rides on JWICS to facilitate the easy exchange of information within the IC. The Intelink-S (for Secret) Web rides on the Secret Internet Protocol Router Network (SIPRNet), but there is no physical connection between NSANet and SIPRNet. These and the other members of the Intelink family are directed by the Intelink Management Office (IMO), an IC organization that is hosted at NSA.

(U~~//FOUO~~) To stay at the vanguard of the latest advances, NSA has always sought to reach out to the private sector research and development community.

PL 86-36/50 USC 3605

Doc ID: 6586785

[redacted] The primary areas of research consist of photonic and electronic applications, magnetization, thermal management, material and device fabrication, optical communications, and microelectronics, including the exploration of the processing potential of quantum phenomena.

(U~~//FOUO~~) The development of computers for cryptologic applications did not happen smoothly or directly. NSA research focused on specific problems and how to solve them, not abstract theory, and there were many failures and false starts as well as successes. However, each new system gave enhanced capabilities to NSA's analysts, and in any case provided an excellent learning experience to those involved with basic research. NSA's computers almost always were well in advance of data processing equipment anywhere else. In conjunction with its partners in industry and academia, NSA continues to be a leader in research and development of computer technologies and has been a singular pioneer on the frontiers of computer science and electrical engineering.

(U) For further reading, see:

(U) Bamford, James, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (Doubleday: 2001).

(U) Boak, David G., *A History of U.S. Communications Security* (NSA: 1973).

(U) Burke, Colin B., *It Wasn't All MAGIC: The Early Struggle to Automate Cryptanalysis (Center for Cryptologic History* (CCH): 2002).

(U~~//FOUO~~) Johnson, Thomas R., *American Cryptology during the Cold War, 1945-1989* (CCH: 1995-1999).

(U/~~//FOUO~~) (U) [redacted] *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program* (CCH: 1993).

[(U~~//FOUO~~) Kent Sieg, Center for Cryptologic History, [redacted]

PL 86-36/50 USC 3605

PL 86-36/50 USC 3605