Influence of U.S. Cryptologic Organizations on the Digital Computer Industry

SAMUEL S. SNYDER

This article was originally published in two parts in the Fall 1977 and Winter 1978 issues of Cryptologic Spectrum *(Vol. 7, No. 4 and Vol. 8, No. 2).*

INTRODUCTION

An unfortunate aspect of historical accounts of computer lore in open sources is the omission – conspicuously to some of us – of mention of the U.S. cryptologic organizations, or of the contributions by these organizations which helped in laying the foundation of the computer industry. NSA, and other cryptologic organizations, have been required over the years to observe a policy of anonymity, and with good reason. But in the age of maturing appreciation of the role of computers in nearly all civilized endeavors, it is time to acknowledge, for the first time, their outstanding contributions to the computer industry.

The reader will notice the absence of remarks concerning software efforts by cryptologic organizations. While this side of their operations received its proper share of support, space restrictions preclude its inclusion in this article. Also, the Army and Navy cryptologic services have frequently changed organizational titles throughout the years. Therefore, to avoid confusion in this article, they are, previous to 1945, referred to as "Army," "Navy," "service cryptologic organizations," and the like. Too, NSA's predecessor organization, AFSA, was established in 1949, and NSA in 1952. Consequently, references to "NSA" and "Agency" are, on occasion, used interchangeably, the particular agency referred to depending upon the time period being discussed.

EARLY DEVELOPMENTS

The development of the U.S. computer industry might have been delayed for years if it had not been for the stimulus and financial support of the U.S. government. The details of the Army Ordnance wartime requirement for assistance in calculation of ballistic tables, and the creation of a team of engineers and mathematicians at the University of Pennsylvania's Moore School of Electrical Engineering to design and build ENIAC, are well known.[1,2] Also, the design and construction of UNIVAC for the Bureau of the Census, and of RAYDAC by the Raytheon Corporation for the Naval Research Labs, are important pioneering stages in early computer history. In these cases, and in others as well, the Bureau of Standards exerted important influence as supervisor of the contracts and in furnishing technical guidance.

1. Herman H. Goldstine and A. Goldstine, "The Electronic Numerical Integrator and Computer (ENIAC)," *Mathematical Tables and Other Aids to Computation,* Vol. 2 (July 1946), pp. 97-110.
2. J. G. Brainerd and T. Kite Sharpless, "The ENIAC," *Electrical Engineering* (February 1948), pp. 163-72.

By the time ENIAC was completed, in February 1946, John W. Mauchly and J. Presper Eckert, its designers, had fairly clear ideas about the kinds of features a modern general-purpose computer should have. For example, in addition to high-speed storage for both instructions and data, the computer of the future would require some kind of "discriminate" instructions which would make possible the modification of the course of problem solution. The experience in building and operating ENIAC certainly helped, particularly in emphasizing certain features a computer should *not* have. The total storage capacity of ENIAC was only 20 numbers, and the method of setting up problems to be solved consisted of "plugging up," in proper sequence, large cables interconnecting the registers containing numbers to be operated upon. Also, while ENIAC's circuits were quite fast enough, it contained 18,000 electron tubes, a prohibitively large number.

In addition to the people at Moore School, several other research centers and universities had begun making plans for the design of large-scale computers. The completion of construction of ENIAC provided the impetus for a conference, or series of lectures, in which outstanding researchers could report on their work. The Moore School was a natural setting, and the Office of Naval Research, U.S. Navy, and the Ordnance Department, U.S. Army, provided joint sponsorship. The lectures were conducted from 8 July to 31 August 1946, and the participants included representatives of 20 organizations from government and industry.

The Moore School lectures were noteworthy in several ways. Logic design for both single-address and multi-address instruction systems were described. Engineering principles were presented for dealing with arithmetic operations, as well as several systems for constructing practical computer memories. Numerical methods for attacking mathematical problems were proposed, suitable for use in digital computers. Among the lecturers' names, that of Dr. John von Neumann is worth noting, since he contributed, as a Moore School consultant, a 1945 report[3] in which many of the logic design suggestions were presented for the first time. Also, in June 1946, the first two important Institute for Advanced Study (I.A.S.) reports appeared.[4,5] These reports contained detailed discussions of von Neumann's ideas for computer organization and construction and basic principles, with examples, showing how to program and code problems. The proposed computer logic, which came to be known as "the von Neumann machine," has proved to be the basic system followed in most computers until recent times. Thus, the Moore School lectures and the I.A.S. reports can be said to have laid the foundation for the modern computer industry.

3. John von Neumann, "First Draft of a Report on the EDVAC," Report on Contract No. W-670-ORD-492, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia (30 June 1945).

4. Arthur H. Burks, Herman H. Goldstine, and John von Neumann, *Report on the Mathematical and Logical Aspects of an Electronic Computing Instrument*, 2d ed., Part I: *Preliminary Discussion of the Logical Design of an Electronic Computing Instrument* (Princeton, N.J.: Institute for Advanced Study, 1947).

5. Herman H. Goldstine and John von Neumann, *Report on the Mathematical and Logical Aspects of an Electronic Computing Instrument*, Part II: *Planning and Coding Problems for an Electronic Computing Instrument* (Institute for Advanced Study, Princeton, N.J.) (Vol. 1, 1 April 1947; Vol. 2, 15 April 1948; Vol. 3, 16 August 1948).

PRE-COMPUTER ERA

From about 1935, the military cryptologic organizations began to make good use of machines in support of their missions. An integral and continuing feature was their punched-card installations. Before the advent of modern digital computers, punched-card machines constituted the backbone of machine support; in fact, in general-purpose applicability, the punched-card installation was the natural predecessor of the modern computer.

In addition, both military cryptologic organizations, during World War II, built or had built under contract several special-purpose machines. The Navy, particularly, enlisted the support of several contractors to design and build special-purpose equipment; in some cases these were specialized as to problem and thus were of no use on any other job. In several other instances, the specialization constituted a specific function, such as comparing or counting; these machines had limited applicability, but they were not confined to a single problem. (It is worth pointing out that machines built in this "pre-computer" era utilized high-speed digital circuits similar to, and definitely antedating, techniques later used in electronic digital computer technology.) The Navy used Eastman Kodak, National Cash Register, and several other firms to plan and build these machines. M.I.T.'s Vannevar Bush provided some of the ideas for these early equipments. The Army utilized the services of Bell Telephone Laboratories during the war to design and construct a large complex of relay equipment which was dedicated to one particular problem; other contractors also helped in building other machines.

Punched-card equipment installations of both cryptologic services grew phenomenally during the war, but of particular interest was a series of special-purpose attachments built for the most part by IBM for operation with the IBM Tabulators. These in effect multiplied manyfold the power of the standard punched-card complex.

In most of the foregoing machine-design jobs done by outside contractors, it was necessary to bring contractor personnel into a classified problem area; that is, security clearances for selected personnel were required. This requirement, the necessity to observe physical security regulations, and the feeling on the part of contractors that such limited-application efforts for the government would not be profitable, resulted in refusals by several firms to accept such machine-design contracts after the war. Thus, at the end of the war, a group of naval officers who were acquainted with this situation and were technically able to provide continuing guidance for such machine support, formed Engineering Research Associates, Inc. (E.R.A.). The Navy's Bureau of Ships provided a blanket contract and arrangements for clearance and security.[6] E.R.A. thus began in 1946 what became a most successful arrangement for designing equipment for use by the Navy's Communications Supplementary Activity, Washington (CSAW). The company's operations were regulated by a BuShips contract under which a number of "tasks" could be assigned with minimum notice as long as funds were available. One significant aspect of the Navy's procedure for supervising work under this contract was the BuShip's system for inspection and quality control. Undoubtedly it was largely because of strict adherence to this policy that E.R.A. was able to maintain an excellent record of delivering equipment that "worked." Most of the machines built under this arrangement were quite

6. Kirk Draheim, Richard P. Howell, and Albert Shapero, "The Development of a Potential Defense R & D Complex; A Study of Minneapolis-St. Paul," Stanford Research Institute Project No. IMU-4370; Prepared for OSD, Asst. Director, Engineering Management, D/DRE (July 1966).

specialized in function. Their engineering technology was similar to that being developed for electronic general-purpose digital computers.

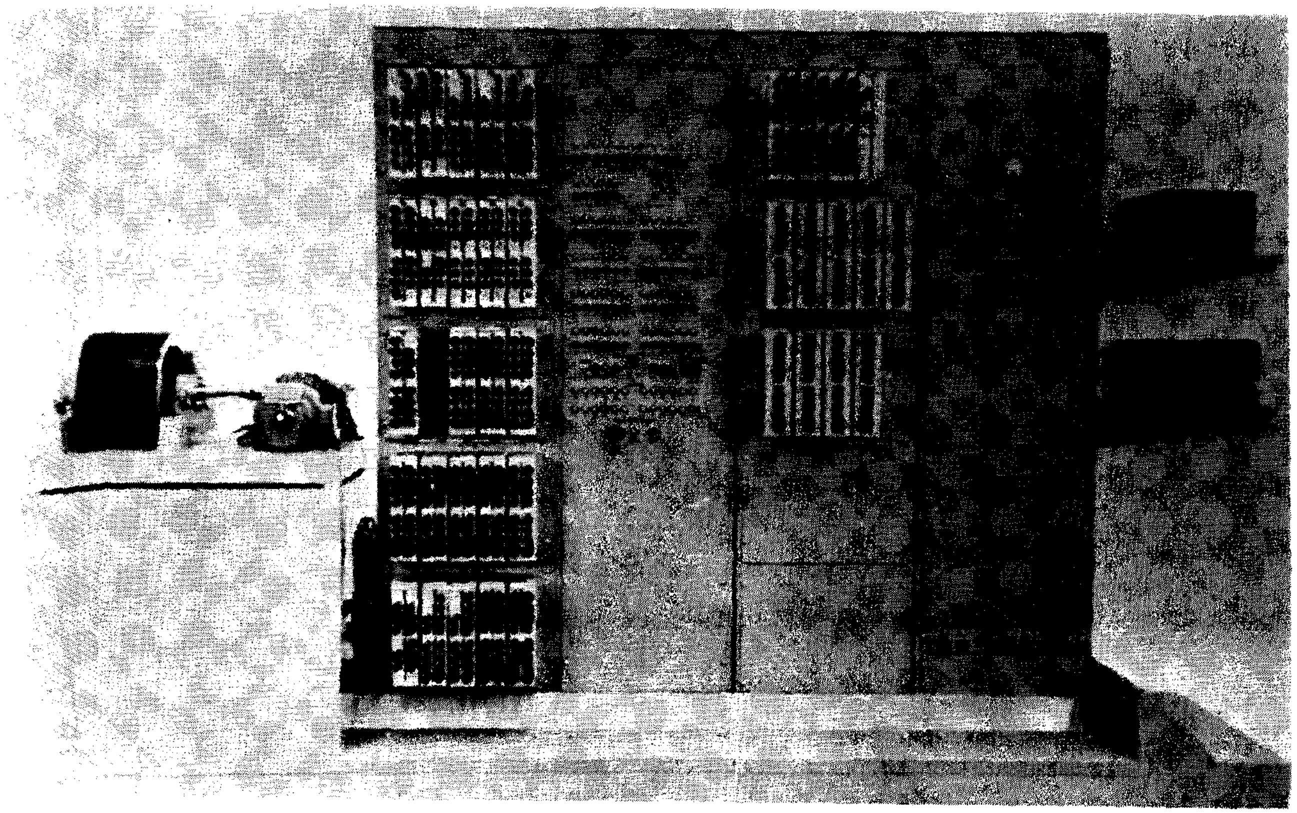
J. M. Coombs,[7] in a report at the 1947 National Electronics Conference, described work on one of the tasks assigned to E.R.A. in August 1946 to investigate magnetic recording on drums and disks. One of the first models constructed to test magnetic drum recording used an aluminum drum, its magnetized surface consisting of paper magnetic tapes glued to the drum's surface. Information was recorded statically, advancing the drum about eight steps per second, by use of a ratchet which moved on signals from the paper-tape reader. Thus, holes in the tape were recorded as magnetic marks on the drum. After recording, the drum was rotated and signals could be read, erased, and rewritten on the same track.

Two new tasks were subsequently levied on E.R.A., calling for construction of practical special-purpose machines using magnetic drums to store data for analysis. Task 9, GOLDBERG, was assigned in 1947; it was to be a comparator-like system with statistical capabilities. Early in 1948 work on Task 21, DEMON, was authorized. DEMON was to use data stored on the drum to perform a specialized version of table look-up. Both used large 34-inch-diameter drums. Although GOLDBERG was assigned earlier, the DEMON project was completed first, and the first of five DEMON equipments was delivered in October 1948. The magnetic drum memory on DEMON was, as far as we know, the first drum memory in practical operational use in the United States. When the first DEMON was delivered, operation of electronic equipment containing large numbers of electron tubes was still in infancy. In spite of routine provisions for cooling, it was found that many tubes burned out when power was turned on. A procedure for identifying "marginal" components was tried and found to be successful; each day, voltages were systematically lowered on separate racks of equipment. Marginal checking on DEMON is believed to be the first regular use of this technique in routine equipment maintenance.

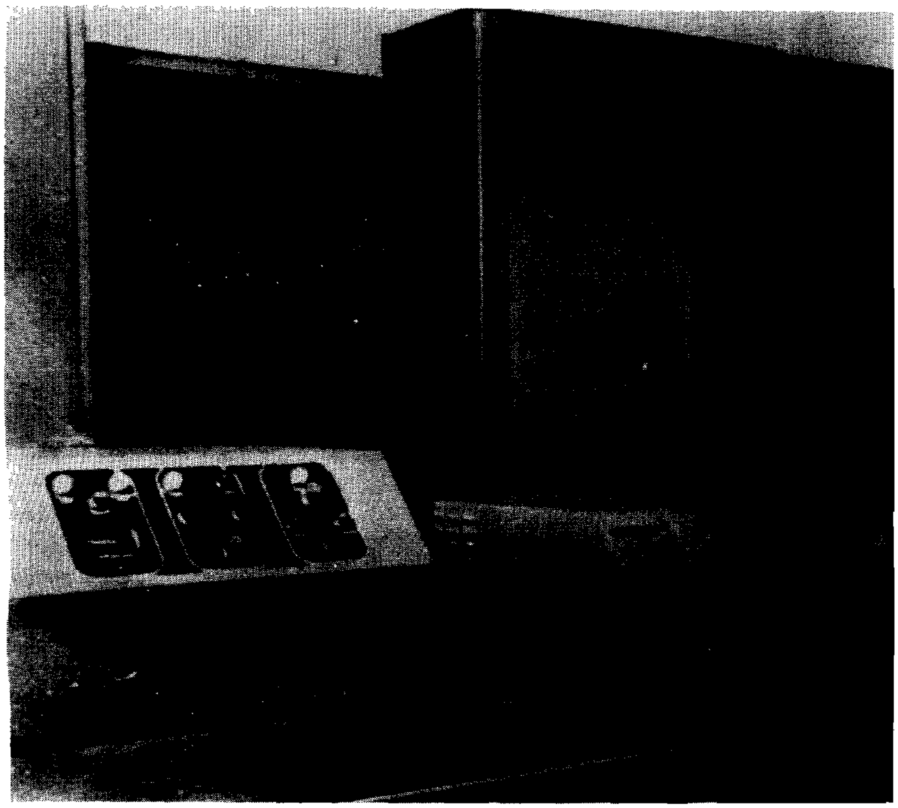
E.R.A. built several other machines for NSA predecessor organizations and for other sponsors who used magnetic drums for storage. Later, improved models utilized sprayed magnetic coating instead of tapes; they were also more compact. The last built for cryptologic use were those delivered with the ATLAS computers described below.

Another example worthy of note is the ABEL computer. ABEL, a slow-speed relay analog of ATLAS I, was built by CSAW engineers in about four months in 1949. Its drum memory, built by E.R.A., was identical to those used on one of the special-purpose machines. ABEL was used primarily for training ATLAS programmers, but it also computed many tables of reference material. After being in successful operation for almost two years, ABEL was donated to the Office of Naval Research (ONR) for use in support of the Logistics Research Project being conducted at George Washington University. The machine, renamed "ONR Relay Computer," is described in a 1952 report.[8]

7. J. M. Coombs, "Storage of Numbers on Magnetic Tape," *Proceedings of the National Electronic Conference*, Vol. 3 (1947).
8. J. Jay Wolf, "The Office of Naval Research Relay Computer," *Mathematical Tables and Other Aids to Computation*, Vol. 4 (1952), pp. 207–12.



ABEL built in 1949



ATLAS I built in 1950

CRYPTOLOGIC-RELATED FIRST GENERATION COMPUTERS

One of those attending the lectures at Moore School was Lieutenant Commander James T. Pendergrass, representing the Navy's CSAW. His supervisor, who had participated in consultations with Dr. von Neumann and others regarding the new computer designs being proposed, had selected Pendergrass to attend the lectures and learn of the possible applicability of such computers to their problems. Pendergrass was particularly impressed by the versatility promised by the proposed designs, since up to that time most machines had been designed to attack a particular problem. But this special-purpose approach often had proved to be expensive and time-consuming. Also, in some situations the problem disappeared by the time a special machine had been designed and constructed. The prospect of having equipment capable of working on any of a whole range of problems was exciting, and Lieutenant Commander Pendergrass's report conveyed that possibility convincingly, by including, among other things, sample programs. Within a few months, negotiations between CSAW and E.R.A. resulted in the establishment of Task 13, providing for the design and construction of the ATLAS computer. Approximately one year later, in November 1948, E.R.A. submitted a report to the National Bureau of Standards (NBS) containing the description of a computer with a design similar to that of ATLAS.[9,10]

The logic design of ATLAS was patterned after that of the I.A.S. machine. M.I.T.'s WHIRLWIND, another machine based on the von Neumann principles, was also under construction about this time. The M.I.T. reports on WHIRLWIND were made available to ATLAS planners, and thus provided valuable support during early stages of ATLAS design. ATLAS differed in word size from the I.A.S. and WHIRLWIND machines, but the instructions for all three were of the one-address type, which turned out to be characteristic of most early parallel machines.

The original proposal for the ATLAS computer called for internal high-speed memory using the Selectron, a specially-designed electrostatic tube being developed at RCA's Princeton Laboratories for the I.A.S. computer. Unfortunately, at the time Task 13 was assigned, the Selectron had not attained the degree of reliability required for computer use, so the decision was made to substitute a magnetic drum type of memory. (The only operational set of Selectron tubes was that used in RAND Corporation's JOHNNIAC, an I.A.S.-type computer finished in March 1954.) The drum memory for ATLAS was much improved over the DEMON drums, and its access time – the time required to locate and read a word from memory into the arithmetic unit, or vice versa – was considerably shorter than that of the earlier drums. Also, the drum memory for ATLAS is believed to be the first in which drum locations ("addresses") were permanently recorded electronically. E.R.A., in December 1947, described its drum research in a report to the ONR;[11] E.R.A. also published a book summarizing the status of electronic digital computing technology as of 1950, one of the earliest publications of its kind.[12] ATLAS's capacity was 16,384 words of 24 bits (binary digits). The feature of "interlace plugging," added after it was delivered, aided programmers in improving access time. ATLAS was delivered in December 1950, and a second machine of identical design was delivered in March 1953.

Several months before ATLAS was delivered, a proposal was made for the design of a successor to be called ATLAS II. Its logic design was unique, in that it is believed to be the first computer with two-address instructions. Its high-speed memory was built with

9. Engineering Research Associates, Inc., "Summary of Characteristics, Magnetic Drum Storage Computer." Report prepared for the National Bureau of Standards, Department of Commerce, under Contract CST-10133 with Engineering Research Associates, Inc., St. Paul, Minn., Part I (30 November 1948).

10. Engineering Research Associates, Inc., "Examples of Coding, Magnetic Drum Binary Computer." Report prepared for the National Bureau of Standards, Department of Commerce, under Contract CST-10133 with Engineering Research Associates, Inc., St. Paul, Minn., Part II (30 November 1948).

11. Engineering Research Associates, Inc., "Selective Alteration of Digital Data in a Magnetic Drum Computer Memory." Report prepared for ONR, under Contract N6onr-240 Task I with Engineering Research Associates, Inc., St. Paul, Minn. (1 December 1947).

12. Engineering Research Associates, Inc. Staff (W. W. Stifler, Jr., Editor), *High Speed Computing Devices* (New York: McGraw-Hill Book Company, Inc., 1950).

electrostatic tubes (so-called "Williams tubes"); there was also a medium-speed drum memory similar to the one used in ATLAS I. ATLAS II was delivered in October 1953, and a second model of ATLAS II, using magnetic cores for high-speed memory instead of electrostatic tubes, was delivered in November 1954. (Incidentally, the second model of ATLAS II is believed to be the first core memory computer delivered to a customer in the United States.) All four machines (the two ATLAS I's and two ATLAS II's) gave excellent service for six to eight years.

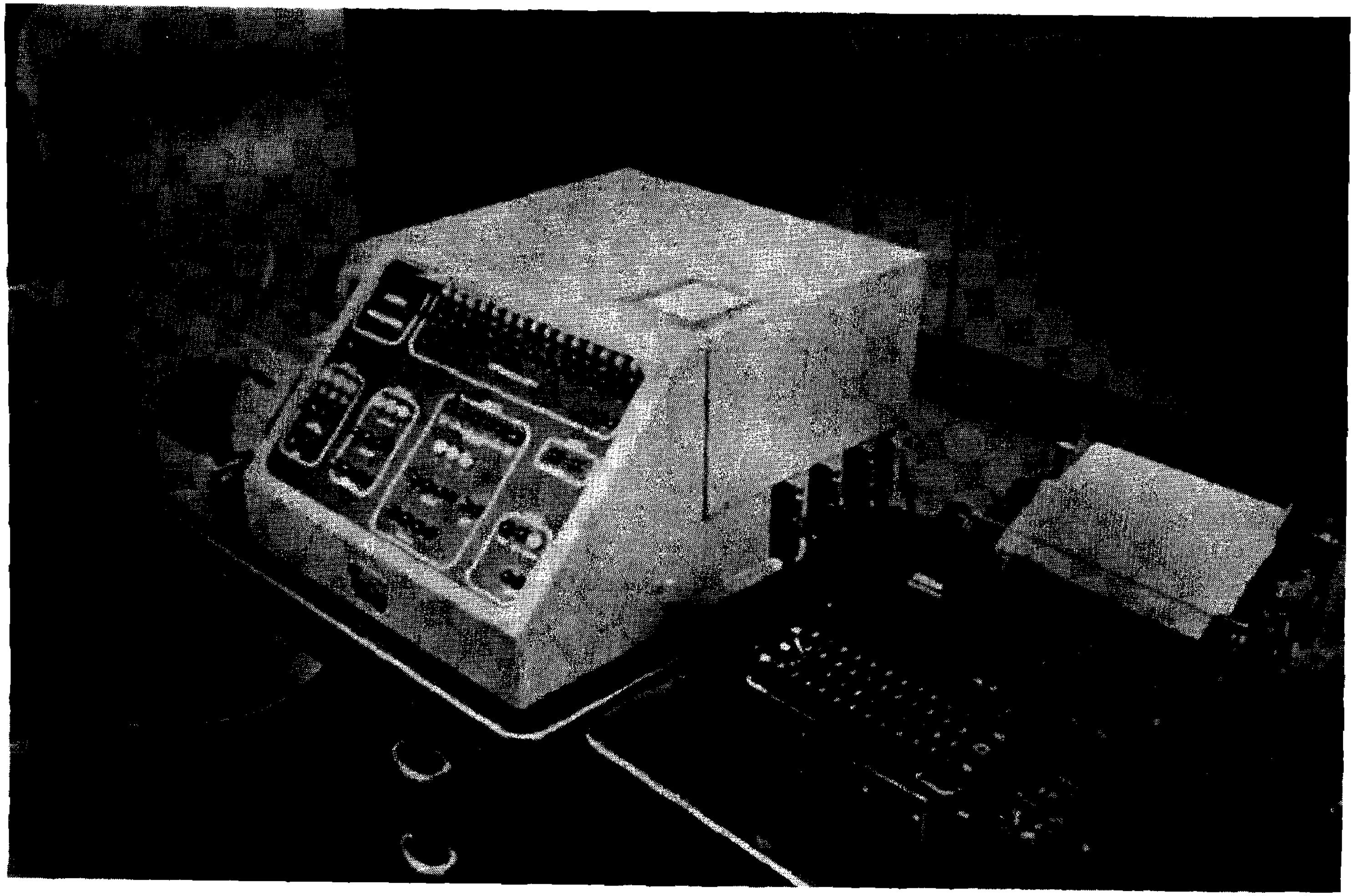
E.R.A. planned to market the ATLAS I commercially, with the designation "E.R.A. 1101," which was the binary equivalent of the ATLAS I task number (13). However, only one such machine was built (for E.R.A.'s Arlington office), because the commercial version of ATLAS II (UNIVAC Scientific 1103), already under way, was a more powerful computer.

Not long after receiving a copy of Pendergrass's October 1946 report on the Moore School lectures, ASA analysts began studies of all extant computer proposals. The machines considered (which were only paper proposals as none had been built) were Raytheon's RAYDAC, UNIVAC, and EDVAC, in addition to ATLAS. ASA analysts wrote experimental programs, estimated operation times to execute typical problems, and visited computer planners at each location. The conclusion of the ASA group was a recommendation to procure a four-address computer like EDVAC. The NBS assisted ASA analysts and engineers in their review, and when the decision was made for ASA to build its own machine, NBS made arrangements for subcontracts for mercury delay memory and for magnetic tape drives, from Technitrol Corporation and Raytheon respectively.

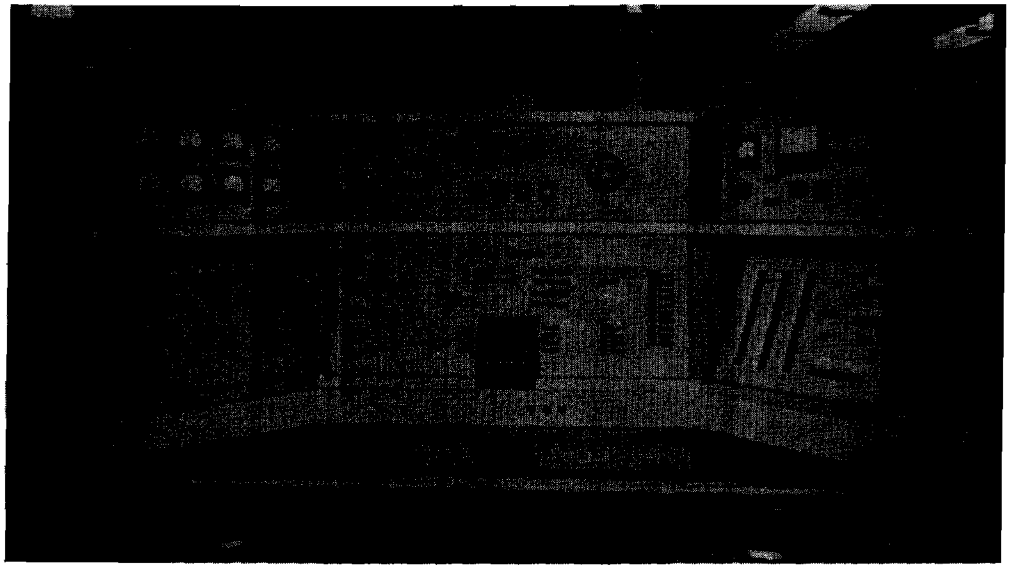
Design and construction of such a machine (named ABNER) was just getting under way when ASA analysts began planning for a future, improved computer. It was apparent that the elementary computer instructions being programmed to execute typical cryptologic jobs were resulting in excessive operation times, and such jobs were clumsy to implement. To lessen the programmer's burden, a series of special-purpose instructions was worked out, with the help of ASA engineers. By the time this additional set of instructions was perfected, the first machine was already partly built, but it was found that the new features could be incorporated into the first machine without excessive delay or the need for additional hardware. It was therefore decided to add the new analytic instructions to ABNER, and instead of a total instruction set of 15 orders, the new code of orders totaled 31, using a five-bit operation symbol. This ABNER instruction set was unique, undoubtedly the first which placed primary emphasis upon nonarithmetic operations.

A second model of ABNER also gave Technitrol an opportunity to further its computer expertise. The second machine, which was built entirely by Technitrol, was a logic copy of the first ABNER. However, it was much improved in construction detail and included additional high-speed memory. The two models of ABNER became operational in April 1952 and June 1955.

Not all of the early research and development efforts were successful, although developmental projects for cryptologic organizations yielded useful equipment in a surprisingly large proportion of cases. When one considers that most of the projects had not been tested or perfected for quantity production, the record is indeed quite good. The following story of NOMAD concerns one such development which, although it did not result in an operational system, yielded techniques and innovations which proved valuable in developing later systems.



ATLAS II (input-output station)



ABNER II (Serial 2 Console)

As early as January 1950, when the Agency's first two computer projects were under construction, a proposal was made for a large-scale super-speed sorting machine. The proposed machine was called NOMAD, and it was based on the idea that data being sorted – that is, rearranged on magnetic tapes – would have no fixed address. E.R.A., under Task 3 of the BuShips contract, had made feasibility studies which produced tentative design specifications of such a computer. In 1951 the decision was made to expedite the project by soliciting competitive bids to respond to a "Purchase Description." In September 1951 the Raytheon Corporation was awarded a letter contract, and in May 1952 a definitive contract was signed for design and construction of the NOMAD system.

One of the most critical components of NOMAD was the rather massive magnetic tape system, which was called Primary Internal Tape Storage (PITS). The tapes were three inches wide and contained 36 information channels; the tape transports were planned to move at 120 inches per second. In order to achieve maximum information storage on a reel and still have an interrecord gap between blocks for starting and stopping tape reels, information was packed solid, one block after another. It was designed, however, so that alternate blocks would be read or written in one direction with a space between successive blocks, which would then be used as information when reading or writing in the other direction.

In operation, the tape drive sounded like a machine gun. Because the tape started and stopped at every block 100 times a second, the bending and snapping of tape delivered a loud, cracking sound. More or less soundproof housing was built, which muffled the noise somewhat. In June 1954, personnel losses of the contractor, as well as delays and cost overruns, led to the termination of this work. Only three engineering test models of this tape drive were built.

About two months after work on NOMAD ended, Raytheon proposed the commercial marketing of a computer to be called RAYCOM, which differed only slightly from the basic design of NOMAD. Later, in 1954, a cooperative arrangement between Raytheon

Corporation and Minneapolis-Honeywell led to the formation of the Datamatic Corporation, resulting in the Datamatic 1000, the first in a series of Honeywell computer models. Raytheon's involvement in the Computer Division of Honeywell was later liquidated, and the H-series computers continue to flourish successfully.

Another result of the NOMAD experience came about when, shortly before cancellation, several top Raytheon engineers who had worked on the project resigned to form a new company. Named the Computer Control Corporation ("3-C"), it began marketing a line of "building blocks" or circuit cards which were designed for flexible recombination into various configurations. These "3-C" cards were partly based on developments under the NOMAD contract and were moderately successful. Computers built from "3-C" cards were among the earliest of the small computers to be marketed in the country.

IMPACT ON GENERAL DATA HANDLING

Because requirements for computer support are often dominated by the need for statistical and other analyses of great masses of data, U.S. cryptologic organizations quite early became preoccupied with improvements in input-output, conversion, and recording equipments. Also, the internal processing operations have often been logical or transformational, rather than strictly computational. This preoccupation with "information processing," as contrasted with computing, was responsible for several early (pre-computer) developments. For example, in the 1930s punched-card specialists in the cryptologic organizations developed procedures for indexing data for analysis, probably before anyone in industry. Long before the advent of modern computers, many variations of this procedure – later known to computer users and programmers as "Key Word in Context" (KWIC) – were practiced by the service cryptologic organizations with punched-card equipments.

One of the earliest commercial high-speed line printers came about at least partly because of experimentation and initiatives by cryptologic engineers. Also, one of the first practical character-sensing machines received early encouragement from the government in the form of a development contract. And much later, after commercial computers were becoming available, several developments by commercial firms became viable only after the first models were tested by Agency engineers, with modifications and improvements made as a result of such tests. Also, NSA, beginning in 1957, was instrumental in bringing about tape standardization and in lowering the costs of magnetic tapes for computer use, leading to the development of testing procedures and the establishment of industry-wide standards.

SECOND GENERATION COMPUTERS: SOLID STATE MACHINES

The original impetus for the system called BOGART came from the early realization that data conversion, formatting, and the like often occupied a large proportion of the programmer's attention. Often, special-purpose equipment had to be built to convert data from one medium to another. And the likelihood of needing all the power of the largest computers for sophisticated analyses suggested that it would pay to use a different "editing" computer to prepare data for input to such jobs. The original idea for BOGART's unit of manipulation was therefore the individual character (alphabetic or numeric), and the word size of 7 bits was specified in a proposal of December 1953. The logic design provided for three-word instructions, both core and drum memory, and input-output using both punched cards and punched paper tape. E.R.A., in July 1954, contracted to build two models, using diode and magnetic core logic for arithmetic and control. Cycle time of the core memory was 20 microseconds, and drum storage was eliminated.

In July 1955 the contract was modified to provide for construction of four instead of two machines and to allow for connection of IBM Type 727 magnetic tape drives. These tape drives had virtually become the standard for the industry. The logic design was also changed – the word size became 24 bits, with the capability of selecting any of three 8-bit portions of a word. Also, several index registers were provided. The four machines were delivered between July 1957 and January 1958. The pilot model of BOGART was subsequently modified, and in December 1959 it became the fifth BOGART to come to NSA. It was subsequently used as the central computer for ROB ROY, a remote-operated system with five outstations.

The BOGART computers were very reliable, and were used on a great variety of problems. Their intended application – editing and formatting – received less emphasis later, probably because of BOGART's capabilities for high-priority work and because other, cheaper equipment became available for editing.

The influence of BOGART can probably be seen in both its engineering and logic sides. First, BOGART was probably the first U.S. computer which used "design automation" techniques. Also, many features of the logic design were unique and carried over into the family of Navy Tactical Data System computers. Additionally, the UNIVAC 490 included features, such as its index registers and "repetition," which were borrowed from or were influenced by BOGART. Control Data Corporation's CDC 1604 and CDC 160 also reflected early BOGART design innovations.

BOGARTS II

By January 1955, the use of transistors in place of electron tubes became increasingly likely, and their apparent advantages over tubes – in size, lower heat dissipation, and improved reliability – set the stage for the new, smaller mass-produced computers. NSA, in anticipation of these changes, began training a small group of engineers in the use and applications of the new components. They were the nucleus of what later became known as the "transistor generation."

One project under way at this time concerned a proposal for a remote-operation computer, with terminals located in work areas. Another proposal, intended to accomplish the same objective, was to acquire a number of small computers, with the new transistors as the principal circuit component. Each desk-size computer was to be located in a different operational area. A project called SOLO was established to build the first such machine, and the decision was made to duplicate the logic design of ATLAS II. In June 1955, Philco Corporation was awarded the contract, because Philco at the time was the only firm making reliable surface-barrier transistors (a short-lived technology which was superseded by junction transistors). Subcontracts for construction of SOLO's core memory and power supplies went to Remington-Rand-UNIVAC and Magnetic Controls Corporation, respectively.

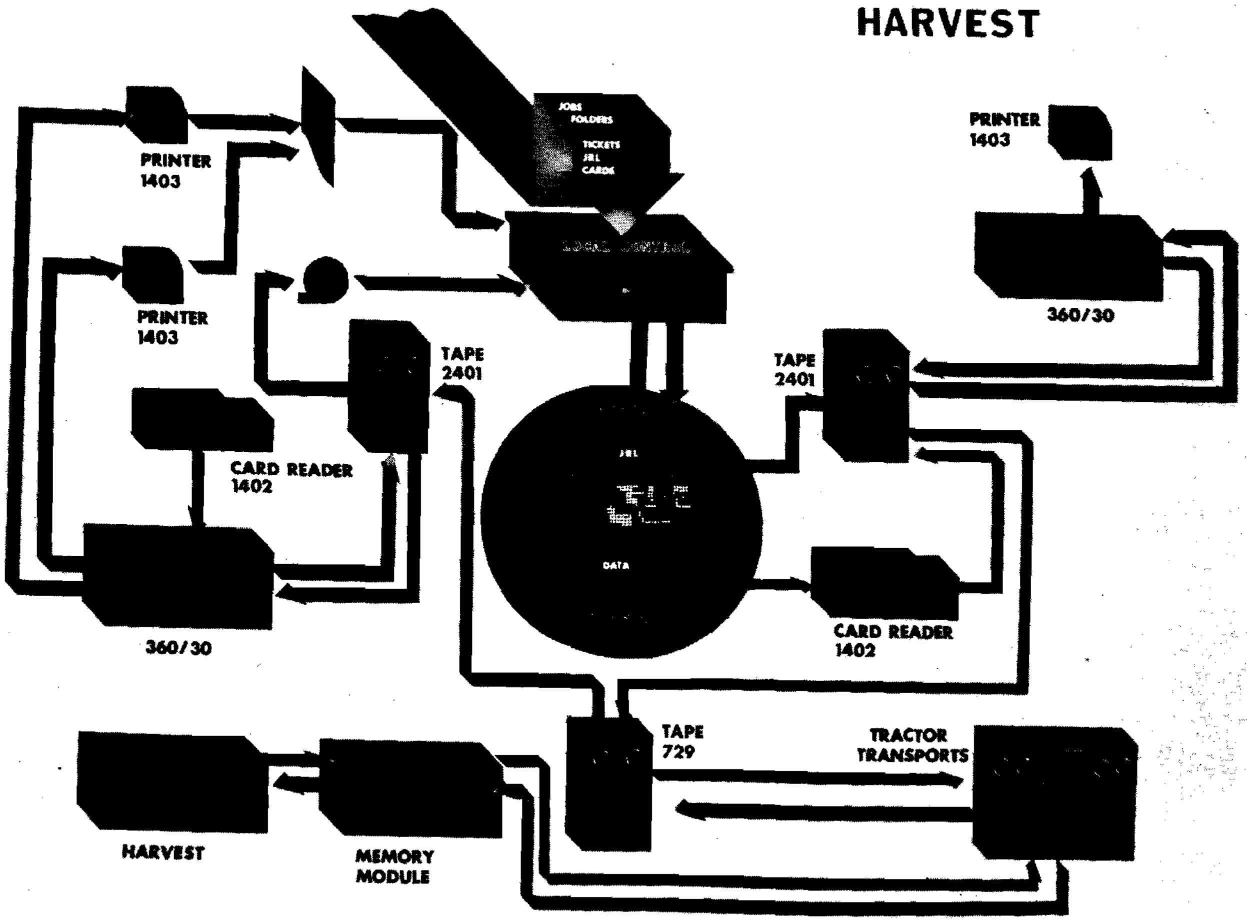
During construction, many difficulties were encountered and corrected, including problems with subcontractor-furnished power supplies and memory. Also, after delivery in March 1958, NSA engineers spent about a year debugging the equipment. Although SOLO was logically a copy of ATLAS II, its memory lacked the supplemental drum of ATAS II, and its input-output equipment was not very reliable. As a consequence, SOLO was not used on large operational problems. Because of these difficulties and delays, the original plan to build many copies of SOLO was abandoned, and the one desk model was used for several years for testing other equipment and for training.

The original objectives for SOLO were twofold: (1) to prove that a reliable computer could be constructed using direct-coupled transistor logic and (2) to train NSA engineers in transistor technology. Both objectives were met; SOLO also holds the distinction of being the first completely transistorized computer designed and built in the United States, and undoubtedly the first in the world. Philco later built a commercial version, marketed under the designation TRANSAC S–1000. A larger and improved computer, the TRANSAC S–2000, was later marketed more successfully. Its design was based on the Navy CXPQ computer, and it was later called the Philco S–2000.

NSA's HARVEST was undoubtedly the most sophisticated computer of the so-called second generation. It was one of the limited number of systems built by IBM as an embodiment of a research program called "STRETCH." Beginning in 1954 the planners at IBM had decided that, on the basis of experiences in the operations of their first successful models – the IBM 701 and 704, 702 and 705 – a quantum leap ahead would be possible. But this "leap forward" hinged on their achieving increases in circuit speed, in lowering memory-access time, in improving the logic design, and in developing higher speed and higher capacity tapes and disks. A project was subsequently launched by the company's research laboratories to stretch the state of engineering art in these directions.

IBM experiments along these lines had progressed, by the spring of 1955, to the point where it was considered desirable to test the new ideas by constructing a STRETCH computer, and two government agencies, NSA and the Atomic Energy Commission (AEC), were approached in this regard, mainly because both had requirements for large-scale computer support.

The IBM STRETCH proposal came to NSA at a propitious time (May 1955). The requirement for a large-volume data processor, and the effort to satisfy that requirement under the ill-fated NOMAD project, had been followed by a proposal called FARMER. This proposal, made in the spring of 1954, called for a modular system of general-purpose



The IBM HARVEST System

and special-purpose machines. By providing flexibility in choosing such modules, it was the intention to maximize the advantages of both special-purpose and general-purpose equipments while minimizing their respective disadvantages. Thus, input-output, data editing, computation, and general storage requirements could be accommodated by a powerful and versatile computer, while needs which justified additional power could be met by special attachments, designed to operate with the main FARMER computer. Also, a FARMER–NOMAD Special Study Group had been created; its members spent several months interviewing specialists in various Agency problem areas. Their report recommended that the FARMER approach be followed in future large-scale systems planning. Thus, the reaction of Agency computer specialists to the logic ideas in IBM's STRETCH was immediate: this system could become the first embodiment of the FARMER concept.

Although IBM's offer to build a STRETCH computer for the Agency for $3.5 million was considered to be a bargain, it was rejected for two reasons: (1) two important components of the proposed system – fast (0.5 microsecond access) memory and advanced magnetic tape external storage – were considered to be insufficiently developed, and (2) over-all system logic was not sufficiently directed toward NSA's requirements to qualify as the basis for FARMER. After some negotiations, however, an agreement was worked out which provided for additional research by IBM in the areas of high-speed memory and high-density tapes and tape transports, and for logic design studies.

The Atomic Energy Commission accepted the IBM proposal in 1955, after a delay of several months, and a contract for a STRETCH computer was signed in 1956. AEC's computer requirements differed from those of NSA in that they emphasized high-speed multiplication, whereas NSA's placed emphasis on manipulation of large volumes of data and on great flexibility and variety in nonnumerical logic processes. Thus, in approximately the same time frame, IBM was engaged in planning two embodiments of the STRETCH computer for two clients having widely differing requirements.

By May 1957 a design proposal for NSA's model of STRETCH was completed, and a careful evaluation was soon under way by an ad hoc group charged with examining the design proposal. The group made time estimates for executing candidate jobs, proposing several design improvements. The group's studies resulted in favorable recommendations, including estimates that the proposed system would be faster than current equipment, in most cases by factors between 100 and 200. After more negotiations, a final contract was signed on 30 April 1958.

Additional and massive programmer training and software development were required to utilize HARVEST's powerful new features, and because of its logic complexity, the system's great potential came into its own only gradually. HARVEST was used for 14 years with emphasis placed on jobs not conceivable for any other computer. It functioned very well throughout.

As already noted, HARVEST was a unique embodiment of the STRETCH computer development, that is, no successor was built, and no commercial models were ever contemplated. HARVEST's most important effect was undoubtedly on the engineers who designed it, since it was a program which brought out the best in all who were involved. HARVEST also exerted a great influence on later computer developments in a number of significant ways. Additionally, in 1962 IBM designers who participated in the development of the STRETCH computer concept, collaborated in the publication of a book which details the STRETCH design experience.[13] Chapter 17, entitled "A Non-Arithmetic Extension," describes NSA's HARVEST.

13. Werner Buchholz (ed.), *Planning a Computer System: Project STRETCH* (New York: McGraw-Hill Book Co., Inc., 1962).

TOWARD THE COMPUTER OF THE FUTURE: LIGHTNING

One of the most costly and far-reaching research programs ever undertaken by NSA was purported to have had its beginning at a cocktail party in July 1956. The story is told of a conversation involving several high-level NSA equipment planners and Lieutenant General Ralph J. Canine, then Director of NSA. There had been some discussion of NSA's perennial problem: the race between analysts' insatiable requirements for new ways to attack ever-increasing volumes of data and the efforts of engineers to design and build bigger and faster computers to meet these needs. Apparently no matter how powerful the new equipment, we never seemed to catch up. The then-current development, HARVEST, was being designed to fill such requirements with an estimated 100-fold improvement over the best current computers, but its completion was several years away. General Canine then forcibly expressed his exasperation by exploding: "Build me a *thousand megacycle* machine! I'll get the money!" Within the next few days, the LIGHTNING project was under way, with a budget of $25 million for a five-year program to develop "thousand megacycle" electronics.

The LIGHTNING project received the approval of the Deputy Defense Secretary in October 1956, and it was endorsed at the Presidential level by Dr. James Killian in a White House conference in December 1956. It also had President Eisenhower's personal backing. Actual work by several contractors was under way by June 1957.

Much of the discussion in the earliest stages of LIGHTNING revolved around clarification of the oft-repeated expression "kilomegacycle computer." Rather than a computer operating at a thousand million pulses per second, the objective was an analytic system accomplishing tests a thousand times as fast as current megacycle equipment. This thousand-fold power increase could be expected to be achieved by (1) faster circuitry, (2) better logic, and (3) other over-all system improvements. The efforts of LIGHTNING researchers were primarily directed toward the first of these goals – faster circuitry – with every effort aimed at the ultimate goal of a performance improvement by a factor of one thousand. Eight major contractors participated in the project, each attacking a different line of research.

Progress reports by contractors involved in the LIGHTNING project were supplied directly to AEC, several Air Force laboratories, ONR, and other government organizations. In addition, the BuShips presented, on three different occasions, three-day symposia featuring reports by the contractors for interested government organizations and laboratories. Published articles in recognized technical journals numbered over 160, and many papers were presented at major technical conferences. A total of 320 patent applications and 71 university theses also resulted from the LIGHTNING project.

One of the direct benefits derived from LIGHTNING concerned the requirement in the address-selection matrix in the high-speed memories of HARVEST for a faster diode. Sperry Rand's Norwalk plant developed, under LIGHTNING sponsorship, a silicon high-conductance avalanche diode which satisfied the requirement. Many other techniques and components which resulted from LIGHTNING research were also used in special-purpose machines for NSA and for other defense agencies. For example, Sperry Rand developed, under LIGHTNING sponsorship, one of the earliest techniques for strip-line manufacture. And what may have been the first magnetic thin-film content-addressed memory was built by the same firm. And many areas of electronic data processing began to make use of LIGHTNING nanosecond techniques. For example, the UNIVAC Model 1107, first delivered in 1962, made use of thin-film techniques for fast memory. Also, LIGHTNING undoubtedly was responsible for inducing commercial firms to speed up their own advanced research efforts. However, most computers which began to appear on the commercial market following LIGHTNING research relied principally on development in semiconductors and microminiaturization – such as transistors and integrated circuits – which could more readily be reproduced in quantity.

Although LIGHTNING support for IBM research in cryogenics was discontinued in 1961, the team of researchers at IBM continued work in this field, but at a somewhat curtailed strength. Several years later, the discovery of ways of putting to practical use the phenomenon known as the Josephson Junction led to a new surge of interest in cryogenics. NSA again contributed partial financial support to speed these developments. It now appears that these high-speed (several picosecond – one trillionth of a second – range-gating time), low power-dissipation components show promise as a possible candidate for the future computer generation.

Chronology of Agency Computer "Firsts"

October 1948	DEMON placed in operation. First practical use of magnetic drum for data storage for analytic operations at electronic speeds.
December 1950	ATLAS I delivered; operational in one week. First parallel electronic computer in U.S. with drum memory. Forerunner of commercial E.R.A. 1101.
April 1952	ABNER operational; designed and built at NSA. Serial computer similar in logic to SEAC and EDVAC. Most sophisticated computer of its time. First use of computation simultaneous with input-output. Most complete complement of input-ouput capabilities (punched cards, punched paper tape, magnetic tape, parallel printer, typewriter, console).
October 1953	ATLAS II delivered; forerunner of commercial E.R.A. 1103 (UNIVAC Scientific 1103). Second model of ATLAS II delivered in November 1954. Equipped with core memory instead of electrostatic store; first core memory computer delivered to customer in U.S.
June 1957	LIGHTNING high-speed circuitry research under way. Believed to be largest computer research effort supported by U.S. Government. Influenced many commercial developments.
July 1957	First BOGART delivered. Believed to be first practical computer using magnetic (diode/core) logic in basic circuitry. Believed to be first computer to utilize design automation. Influenced design of several commercial models built by UNIVAC and Control Data Corporation.
March 1958	SOLO delivered; first completely transistorized computer in U.S. and undoubtedly the first in the world. Model for Philco's TRANSAC S-1000 and forerunner of improved S-2000.
February 1962	HARVEST delivered; most sophisticated model of STRETCH series. The tape system (called TRACTOR) was the first completely automated tape library. Influenced design of IBM System 360.

CONCLUSIONS

Simply stated, the missions of U.S. cryptologic organizations have always been to develop and to protect information. The technical processes required to perform this mission, although quite intricate at times, were carried out entirely without machine assistance into the early 1930s. But as the complexity of the technical processes increased, cryptologic specialists sought the help of machines. World War II gave increased impetus to the use of machines as NSA's predecessors enlisted the help of private industry in developing these early computers.

Although the modern electronic computer did not come along in time to assist in the war effort, several pre-computer special-purpose equipments, built for U.S. cryptologic organizations under contract, employed electronic digital techniques, hastening the start of the computer age. And experience gained in the development of large-scale systems for NSA, up to and including HARVEST, resulted in design improvements subsequently used for commercial computers. Also, LIGHTNING inspired many discoveries in the areas of fundamental materials properties, high-speed circuitry, and component fabrication – discoveries which assisted in the birth of another computer generation. As a consequence, it is generally agreed that the computer industry of the 1970s is approaching maturity. That is, the established leaders in the field are sufficiently secure that budgets for research can be supported for the most part without U.S. Government assistance.

Mr. Snyder, a retired NSA employee, received a B.S. in Chemistry from George Washington University. During his career as a cryptanalyst and computer specialist with NSA and predecessors (1936 to 1964), he was the first punched-card equipment supervisor (1937), directed several successful cryptologic units before and during World War II, helped develop and adapt early computers, and supervised the HARVEST project. He was director of automation activities at the Library of Congress from 1964 to 1966. At Research Analysis Corporation from 1966–1969, he was manager of several study projects for the Army Materiel Command. He is co-author, with anthropologist Ashley Montagu, of *Man and The Computer* (1973) and author of *History of NSA General-Purpose Electronic Digital Computers*. He contributed to the *NSA Technical Journal* and *Spectrum* and worked on a historical account of NSA's pre-computer machines for cryptanalysis.