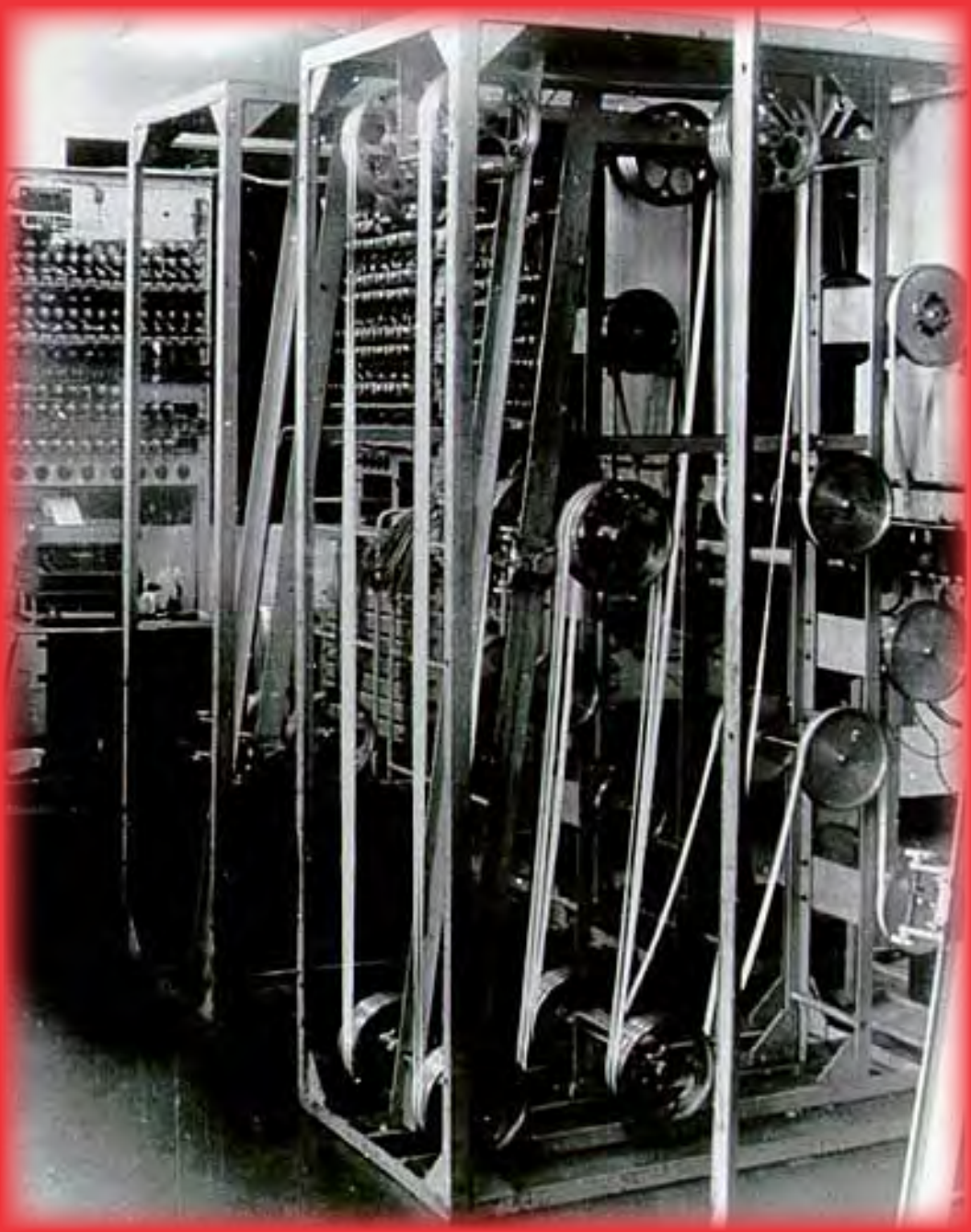
Cryptology's Role in the Early Development of Computer Capabilities in the United States



This publication is a product of the National Security Agency history program. It presents a historical perspective for informational and educational purposes, is the result of independent research, and does not necessarily reflect a position of NSA/CSS or any other U.S. government entity.

This publication is distributed *free* by the National Security Agency. If you would like additional copies, please email your request to history@nsa.gov or write to:

Center for Cryptologic History
National Security Agency
9800 Savage Road, Suite 6886
Fort George G. Meade, MD 20755-6886

Cover: A World War II COLOSSUS computer system.

Cryptology's Role in the Early Development of Computer Capabilities in the United States

James V. Boone and James J. Hearn

Center for Cryptologic History
National Security Agency
2015

Preface

Cryptology is an extraordinary national endeavor where only first place counts. This attitude was prevalent among the participants in the U.K.'s Government Code and Cypher School (GC&CS) activities at Bletchley Park[1] during World War II. One of GC&CS's many achievements during this time was the development and extensive use of the world's first large-scale electronic digital computer called COLOSSUS. The highly skilled military personnel assigned to Bletchley Park returned to the U.S. with this experience and, augmented by the experience from other government-supported development activities in the U.S., their ideas for using electronic digital computer technology were quickly accepted by the U.S. cryptologic community, the U.S. Navy cryptologic organization in particular. Many of the talented people in that organization promoted the rapid expansion of this nation's computer capability as a high-priority task. Some established a new company, others moved on to government organizations, and then, through a series of dynamic and interacting events, the cryptologic-based influence of this group quickly spread into the general marketplace. This over forty-year-long set of events is summarized in this paper.

Introduction

The first "computers" were people who used established mathematical procedures to perform complex calculations in support of activities such as astronomy and navigation. The processes usually consisted of laborious handwork, and were tediously slow. Thus, the results usually contained errors. In the early 1820s, Charles Babbage, a brilliant British inventor, set out to mechanize the performance of some types of calculations. He designed what came to be called "Difference Engine No. 1"; the British government eventually ceased supporting Babbage's work, but his design of "Difference Engine No. 2," although never completed, included concepts of a memory and a processor that would be found a hundred years later in COLOSSUS. His ideas led to the creation of a mechanism to perform what had previously been done only by human thinking. Industry responded rapidly, and relatively soon a number of companies were producing mechanical and electromechanical devices for business use. Examples included the National Cash Register Company of Dayton, OH (founded in 1884), and the predecessor of the International Business Machines Corp. (IBM), the Computing, Tabulating and Recording Corp. (founded in 1911).

Before World War II both the Army and the Navy established organizational elements that were dedicated to cryptology. There are two competing aspects to cryptology. On the defensive side, cryptologists try to construct problems that are difficult, indeed hopefully impossible, for others to solve. On the offensive side, cryptanalysts are trying to solve those problems. Cryptology is a challenging activity, and both sides always need the most advanced tools that can be developed.

Cryptanalytic technology in the late 1930s and in the early years of World War II was based largely on IBM punched cards and electromechanical processes to stack and sort the cards before running them through tabulators. But cryptanalysts often needed to search through millions of characters of cipher text to identify repeats which could lead to determining, for example, the reuse of key to encipher messages or some other improper procedure which could lead to cryptanalytic success. Also, searching, comparing, and iden-

tifying message segments that could possibly be exploited needed to be done quickly—ideally, in little more than the length of time it took to transmit the messages of interest—in order to provide to senior authorities, in a timely manner, an understanding of the underlying plain text. Storage capacity, speed of access, and reliability became major design drivers in the quest for machines to rapidly exploit the enemy's enciphered messages. These important features proved elusive because of the absence of appropriate technology and the resources and time necessary to develop it.

The Army and Navy created a variety of devices to attack enciphered messages. These devices varied in terms of their input-output media (punched cards, paper tapes, film), comparator technology, used to identify similarities or differences between multiple data streams (counters, optical scanning heads) and recording medium (initially, film, and paper or magnetic tape). All of these variations and others related to the wide variety of formats used by the originators of the messages and their transmission systems increased complexity and made it difficult to create a single overall efficient cryptanalytic process.

For example, in one version of such a device, two rolls of paper tape or reels of film, each containing a long enciphered message from the same target entity and from the same time period, and consisting of rows of patterned punched holes that represented the enciphered letters, would be compared using data from photo-optic cells in scanning heads to identify the holes punched in each row. The purpose of the search was to detect repeats common to the messages that were several words long, or enciphered-groups long, as recorded on the two tape rolls. After completing one loop of comparing the groups on the two tapes, one tape would be advanced by one position, and the comparison between the two tapes would be run again to identify repeats. This approach, and others like it, demonstrated the need to constantly find better ways to improve the detection rate of repeats and to perform the comparison, detection, and recording steps.

As the United States entered World War II and the cryptologic units were faced with increasing volumes of enciphered messages,

it became clear that large-scale production and exploitation were required.

To make improvements in managing all the different media and systems employed by the Army and the Navy, Eastman Kodak, National Cash Register, and Gray Manufacturing companies were awarded contracts to manufacture a variety of complex electro-mechanical systems. Although they would not now be considered computers, and were not called that then, they did perform the functions that Charles Babbage had envisioned. A wide variety of these special machines, usually called "RAM" for Rapid Analytic Machines,[2] were developed. They would have made Babbage proud.

This technology was used throughout World War II. Some advanced RAM equipment had the ability to make thousands of comparisons per second from selected enciphered signals recorded on punched paper tape or film. Various versions of RAM systems played a vital role in attacking particular Japanese navy, army, and diplomatic cipher systems.

Other systems were in wide use on different German army, navy, and diplomatic systems. Because there was then no general-purpose device that could accommodate the variety of special cryptanalytic problems across the various target entities, the number of different kinds of RAM systems grew, with particular RAM configurations optimized to address specific cryptanalytic problems. There were always new target communications of interest.

The new challenges would show that even more advanced tools were required. Of course cryptology was not the only area in need of new and improved computational tools. Indeed, a variety of creative activities had been in progress for a very long time. Some of the work was conducted in universities, some in industry, and some in government organizations the world over.

Talented people are always developing new ideas. For example, in 1936 the now-famous mathematician Alan Turing of Cambridge University wrote an extremely important paper, "On Computable Numbers." In this paper he offered a proof that it was possible to

build a computer that was not restricted to solving only one problem. As World War II was evolving, Turing was working, along with many other talented people, at the British codes and ciphers organization at Bletchley Park, and his idea was put to cryptologic use in the early 1940s with great success.

The COLOSSUS Experience of World War II

By 1940 many German strategic communicators were using an electromechanical cryptographic machine that was manufactured by the Lorenz Company. It was considerably more advanced than the now-famous ENIGMA machine in that it was designed to work directly with teleprinters rather than as a manually operated off-line device. One type of that machine is shown in Figure 1.

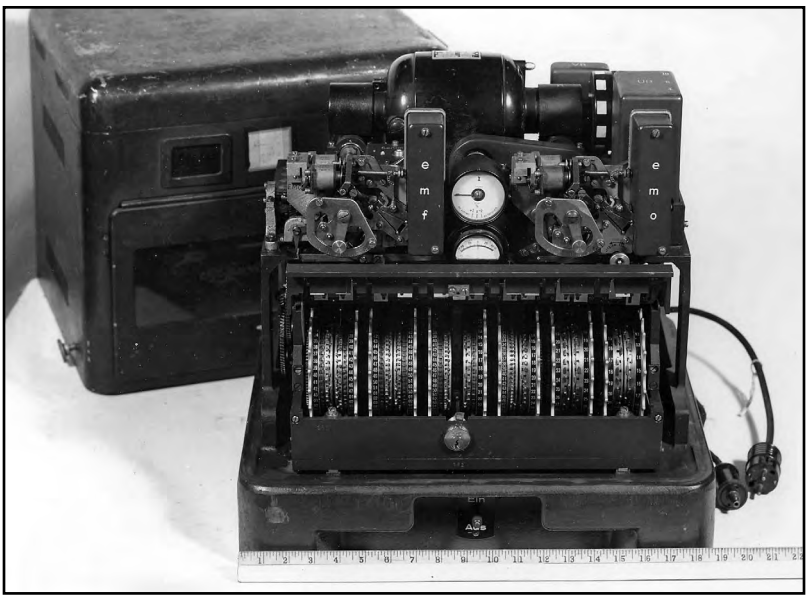


Fig. 1. The World War II German Lorenz machine. This machine was complex cryptographically and was also designed to work directly in-line with the communications systems, thereby speeding up the entire communication process. It was used primarily in support of higher level military organizations. [Photo of machine on display in the National Cryptologic Museum]

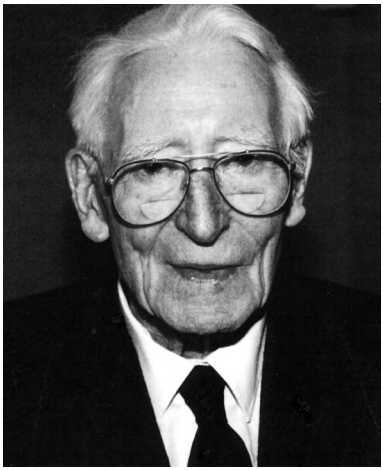


Fig. 2. Dr. Tommy Flowers (1905-1998), ca. 1996. His talents were essential to the successful design and production of the COLOSSUS system. After the war he continued to work at the British Post Office. His wartime accomplishments were not made public until the 1970s. He was made a member of the Order of the British Empire.

It looks complex, and it is. This type of machine can be thought of as one of the primary driving forces of electronic computer development.

By late 1941 the analysts at Bletchley Park, particularly Colonel John Tiltman, British/Canadian mathematician William Tutte, and Dr. Max Newman (previously one of Alan Turing's professors) had developed a method of producing plain text from the Lorenz machine, but the required process was far too complex to be practical without a step-function improvement in analytic tools. By 1942 they had an electromechanical method of producing plain text. It was still far too slow. They knew that being in "second place" was almost worthless, so … in March of 1943 they worked to get back into first place. Under the leadership of Dr. Tommy Flowers, an engineer at the Post Office Research Laboratories, and his team, they created the world's first large-scale electronic digital computer only about seven months after they started the effort. It was called COLOSSUS, and it produced plain text on the first try in January of 1944. The age of electronic computing had arrived.[3]

Prior to the success of the project, there were, of course, skeptics. Dr. Flowers later recalled,

> They wouldn't believe it. They were quite convinced that valves [vacuum tubes] were very unreliable … But I'd intro-

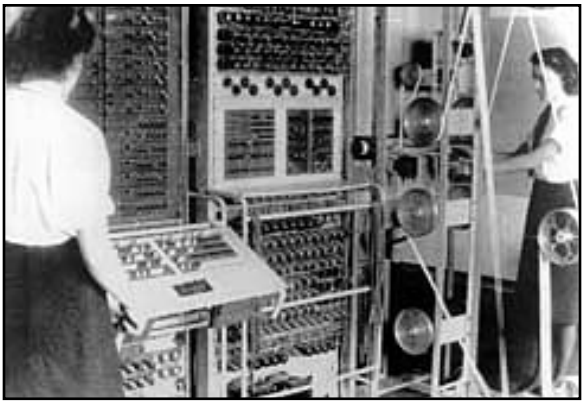


Fig. 3. A World War II COLOSSUS computer system. The system input was by means of punched paper tape on the reel system, called a "bedstead," on the right of this picture. Switch panels and plugboards near the center were used for the programming, and the special electric typewriter on the stand was the output device. (Photo courtesy of Tony Sale)

> duced valves into telephone equipment in large numbers before the war and I knew that if you never moved them and never switched them off they would go on forever.... They decided they would proceed hopefully with the Robinson [an electromechanical RAM], which is what they did and they left the question of whether the valve-based machine would be constructed or not to me.[4]

"They," the overall managers, made a very wise decision to let Dr. Flowers do his own thing. One wonders if they could have really stopped him.

Dr. Flowers's team included linguists, mathematicians, engineers, and skilled technicians and operators. They were not through when they had created the world's first computer. They produced upgraded versions, and by the end of the war, ten COLOSSUS computers were in regular use. These were not toys or experiments. They were large operational systems. Depending on the version, each COLOSSUS contained between 1,500 and 2,400 vacuum

Table 1. COLOSSUS Highlights

- First unit was placed into operation at Bletchley Park in January 1944.
- The cipher text input was provided by means of a 5-hole punched paper tape loop.
- A unique optical sensor system read the input at 5,000 characters per second.
- The system clock rate of about 5 khz was derived from the input tape.
- The system logic was programmed by manual means (cords, plugs, switches).
- The output was provided directly to an electric typewriter.
- Message processing time was improved from weeks to a matter of hours, which drastically improved the value of the output.
- By the end of the war, there were ten improved COLOSSUS systems in regular operation at Bletchley Park, each requiring about 2,500 vacuum tubes.
- For reasons of secrecy, eight of the ten units were destroyed soon after the war ended and the remaining two, along with the documentation, were destroyed in the 1960s.
- The program was not declassified until the 1970s.[5]

tubes. Ten systems were in use by the end of the war. Pictures of one system are shown in figures 3 and 4. A summary of its features is presented in Table 1.

In 2003 the Institute of Electrical and Electronic Engineers (IEEE) placed a bronze plaque at Bletchley Park as part of their history "milestone program." The plaque commemorates the achievements of those who worked there. The inscription reads:

> On this site during the 1939-45 World War, 12,000 men and women broke the German Lorenz and Enigma ciphers, as well as Japanese and Italian codes and ciphers. They used innovative mathematical analysis and were assisted by two

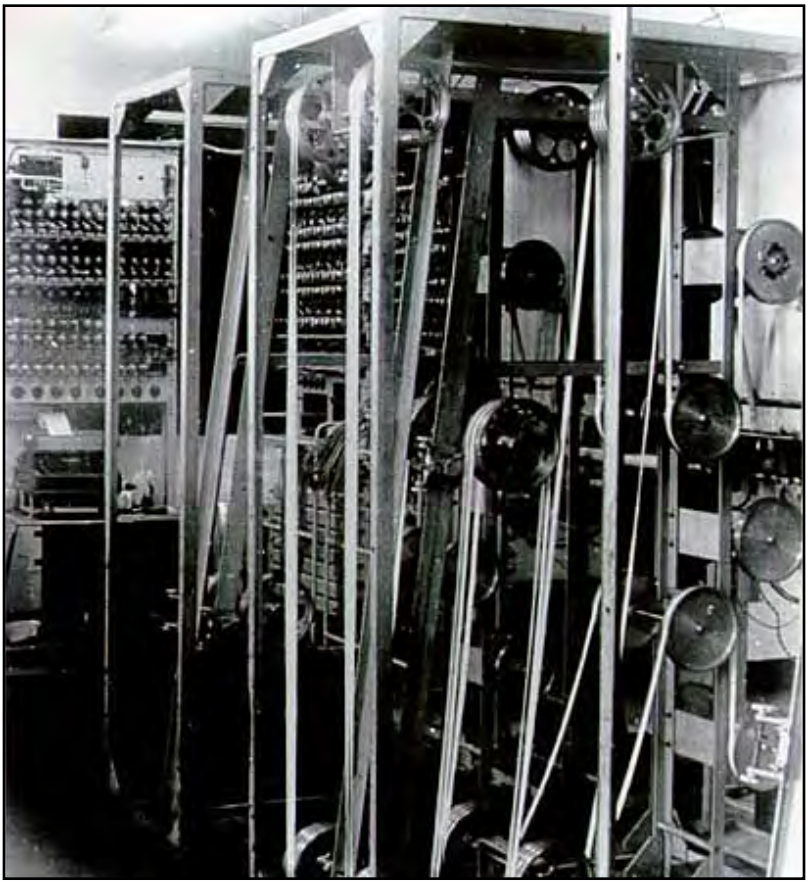


Fig. 4. Another view of the same COLOSSUS system showing more detail of the physical construction. The telephone system heritage of the designers played a large role in this reliable assembly. (Photo courtesy of Tony Sale)

> computing machines developed here by teams led by Alan Turing: the electromechanical Bombe developed with Gordon Welchman, and the electronic COLOSSUS designed by Tommy Flowers. These achievements greatly shortened the war, thereby saving countless lives.[6]

This efficient summary not only emphasizes the creative work of many talented people, but also reminds us that their work was

about much more than the advancement of technology. They were seriously involved in saving our freedom and way of life. COLOSSUS was only a by-product of their efforts, but it did have value of its own.

The Colossus Connection in the United States

How did the COLOSSUS experience affect the computer industry? One thoughtful view is presented by John Hendry, who examined the evolution of the British computer industry in his book that is a part of the *History of Computing* series.[7] Hendry notes that the U.S. would quickly take advantage of the COLOSSUS experience, but the UK would encounter more difficulties. How was the U.S. connection actually made? It was not by top-level policy, nor was COLOSSUS the only factor that led to the rapid growth of this industry in the United States. The critically important connection, however, was made through the efforts of trusted individuals who were deeply involved in cryptology and are briefly described in the following narrative.

During World War II, one of the primary cryptologic organizations in the U.S. was called by the unwieldy name "Navy Communications Supplementary Activity-Washington" or, within Navy circles, CSAW (pronounced "see saw"). Captain Joseph Wenger, USN, directed this organization, located on Nebraska Avenue in Washington, D.C. It was the home of over one hundred of the electromechanical crypt-

Fig. 5. Rear Admiral Joseph Wenger, USN (1901-1970). A 1923 graduate of the Naval Academy, he served in increasingly important roles in the development of the Navy's cryptologic capability including being an early advocate of the development of computers. Among other honors, he was inducted into the NSA Cryptologic Hall of Honor in 2005. (Photo, CCH)

Fig. 6. Lieutenant James T. Pendergrass, USN, ca. 1944. He served at Bletchley Park in World War II, co-authored a key paper that provoked U.S. cryptologic interest in computers, and continued his cryptologic career as a civilian for many years with the Institute for Defense Analyses. (Photo courtesy of the Pendergrass family)

analytic RAMs called Bombes.[8] These machines had been designed and built by the National Cash Register Company (NCR) in Dayton, Ohio, where the work was supervised and shared by a co-located Navy organization, the Naval Computing Machine Laboratory (NCML).

IBM also supported the Navy operations as well as those conducted by the U.S. Army cryptologic element located in Arlington Hall Station, Arlington, Virginia. Intelligence products were exchanged regularly between the U.S. and the UK. So were cryptanalytic techniques and design concepts, and CSAW established liaison officers to facilitate the exchange of technical information. The young officer assigned to the Enigma problem was Lieutenant James T. Pendergrass, USN. In October of 1944 he was assigned to the Government Code and Cipher School at Bletchley Park. A Navy reserve officer, mathematician Dr. Howard Campaigne, was assigned liaison on the Lorenz problem and was also at Bletchley Park. Both became familiar with COLOSSUS.

In this same period, primarily driven by noncryptologic needs, John Mauchly and J. Presper Eckert were leading a large effort, sponsored by the U.S. Army since 1943, at the Moore School of Electrical Engineering of the University of Pennsylvania. ENIAC (Electronic Numerical Integrator and Computer) would be the product. It completed testing and went into operation in 1946.[9] They also proposed

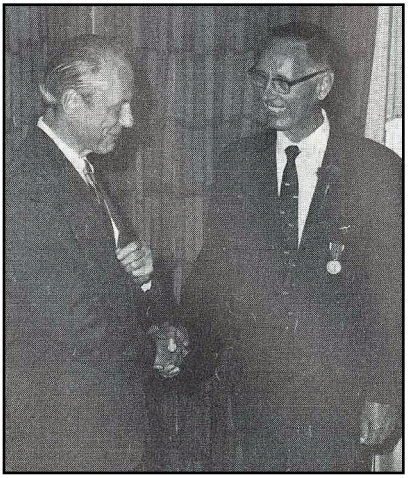


Fig. 7. Dr. Howard Campaigne (r) and Dr. Louis Tordella. Campaigne was also at Bletchley Park in World War II and was the coauthor with Pendergrass of the Navy proposal. He earned his Ph.D. in mathematics in 1938 from the University of Minnesota and worked for NSA for many years in a variety of development activities. (Photo, CCH)

a stored program computer, named EDVAC (Electronic Discrete Variable Automatic Computer) that used binary arithmetic. It was put into operation at the Army's Ballistics Research Laboratory at Aberdeen Proving Ground in Maryland in 1951.

The Army technical lead on these programs was U.S. Army Captain (Dr.) Herman Goldstein, who, during a chance encounter at a Maryland railway station, had interested Dr. John von Neumann in his project. Von Neumann became a contributor, later establishing the computer project at the Institute for Advanced Studies at Princeton University. Later, Goldstein would also work at the Princeton organization and then join IBM in 1958, where he soon became a major contributor to many advanced systems.

The U.S. Navy Takes the Initiative

By 1946 James Pendergrass had been promoted to lieutenant commander and was back at Nebraska Avenue. He was now also the CSAW liaison with the Office of Naval Research. In the summer of 1946, Captain Wenger ordered Pendergrass off leave and told him to attend the computer technology workshops that were being held at the Moore School of Engineering. Many distinguished individuals in industry, government, and academia made presentations at the workshops, and it became clear to Pendergrass that "... this

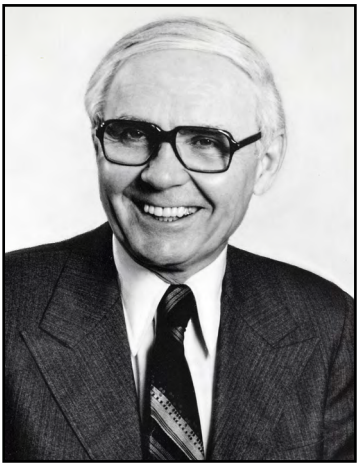


Fig. 8. Lieutenant Commander William Norris (1911-2006). A member of CSAW and a founding member of ERA, he was later founder and CEO of Control Data Corporation. A true innovator and pioneer in the computer industry, he was awarded the National Medal of Technology by President Reagan in 1986. (Photo, 1980, courtesy the Charles Babbage Institute, University of Minnesota)

[programmable computer] was what we wanted as a logic machine for enciphering and cryptanalysis applications." [10] He returned from the workshops and enlisted the aid of Dr. Campaigne. Together, they wrote a classified paper that would soon launch a serious effort in the Navy to advance computer technology with the specific application to cryptologic problems. The paper was formally released in October 1946. It was a successful tool in selling the basic idea, particularly in the Navy, that programmable computers were the wave of the future.

The Navy had a strong desire to preserve and build on their cryptologic knowledge and experience–they knew what powerful tools computers were and, aided by the work of Pendergrass and Campaigne, they knew that this was the time to vigorously promote the development and use of computers. By late 1945 their initial contacts with previous industry partners did not draw much enthusiasm since they were involved primarily in returning to their commercial roots. The University of Pennsylvania team was forming the Eckert-Mauchly Computer Corporation (EMCC) in 1946 but had no cryptologic experience. However, a number of CSAW members were returning to civilian life at the end of the war, and they were intrigued with the potential applications of this new technological tool. Among the principals were Captain (Dr.) Howard Engstrom, USNR, who had been a professor of mathematics at Yale Univer-

Fig. 9. Captain (Dr.) Howard Engstrom, USNR (1902-1962). Engstrom was a technical leader in the Navy's cryptologic work in World War II and continued his participation in many roles after the war. He was awarded the U.S. Distinguished Service Medal and the Order of the British Empire. (Photo, CCH)

sity prior to his call to active duty, where he became the head of the technical activities at CSAW; Lieutenant Commander William "Bill" Norris, an electrical engineer from Nebraska; and the contracting officer of the NCML, Captain Ralph I. Meader.

With the encouragement of Captain Wenger and other Navy officials, this team was able to obtain private financing from a group led by John E. Parker, a 1922 graduate of the Naval Academy; as a result, Engineering Research Associates (ERA) was incorporated in association with an existing glider manufacturing company called Northwestern Aeronautical Corp. (NAC) in St. Paul, Minnesota, in January of 1946.[11] They obtained a sole-source, cost-plus-fixed-fee contract from the Navy in June. By that time a number of other CSAW staff had joined them, and the Navy transferred much of their wartime engineering and supervisory activity from the NCR facilities in Dayton, OH, to the ERA operation. The ERA facility itself was designated as a Naval Reserve Base, and there was on-site supervision of ERA's work by naval personnel who also administered the task-order contracts from the Office of Naval Research and the Bureau of Ships. The first task order called for "... an investigation and report on the status of development of computing machine components."[12] By December 1946 the ERA telephone directory contained the names of 166 employees with a wide variety of experience, skills, and backgrounds. By all reports, it was a very dynamic and enjoyable (if you had the proper security clearances) place to work.

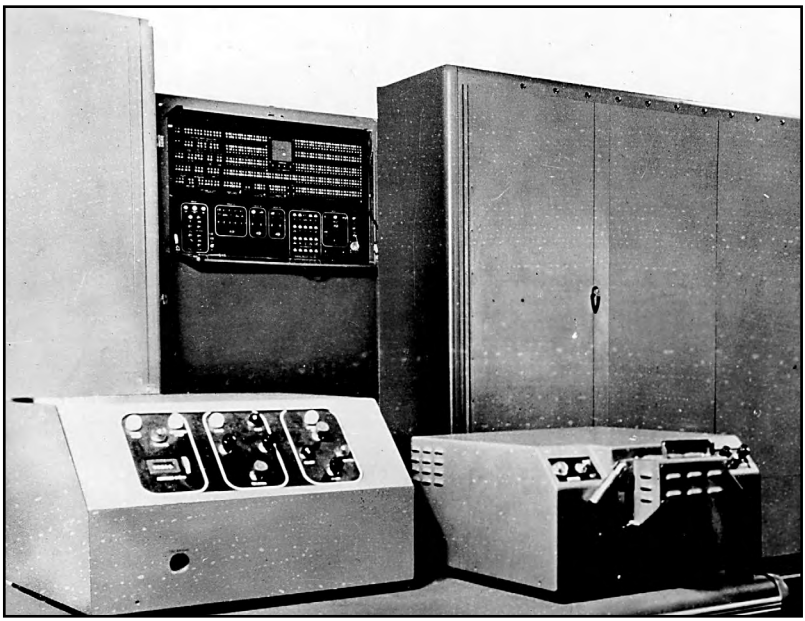


Fig. 10. ATLAS installation, ca. 1954. Although little technical detail is shown, it is obvious that these were large-scale systems. (Photo, CCH)

By 1948 ERA had received the go-ahead on task order 13, which required them to produce a full-scale digital computer for the Navy. It resulted in a computer called ATLAS, which was delivered to the Nebraska Avenue location and put into operation in 1950. ATLAS was a formidable machine that used 24-bit words and required over 2,500 vacuum tubes. Two ATLAS I and two ATLAS II systems (a more advanced 32-bit machine with two-address logic) were delivered between 1950 and 1954, and all were used on operational problems. As with COLOSSUS, these were not experiments; they were full-scale, reliable operational machines that were used by cryptologists in their daily work. ERA also built other systems and subsystems for the cryptologic community. In particular, they were pioneers in the development and use of magnetic drum memories.

ERA had other customers and even tried to be what we would now call a "service provider" by opening their own public computer center in Arlington, Virginia. There were, however, very few custom-

Fig. 11. Dr. Solomon Kullback (1903-1994). A 1999 inductee into the NSA Cryptologic Hall of Honor, he was one of the first three cryptanalysts hired by William Friedman when he started expanding the Army's Signal Intelligence Service. He was a key participant in many aspects of cryptology for his entire career. (Photo, CCH)

ers, with the requisite programming capability, and in 1954 ERA donated their commercial computer (now called the 1101...binary notation to remember task 13) to the Georgia Institute of Technology. It was used at that university into the 1960s.

The Army's Complementary Path

Of course the U.S. Army cryptologic element, the Army Security Agency (ASA), was also vigorously pursuing the potential of the new electronic digital computer at this time. By mid-1948 ASA was working with the National Bureau of Standards (NBS) and using the ENIAC/EDVAC experience with the goal of building an "in-house" electronic digital computer intended for cryptologic applications. This work was taking place within the ASA's Research and Development organization at Arlington Hall Station in Virginia. The organization was headed by Dr. Solomon Kullback, who, as an Army major, had also served at Bletchley Park as a cryptanalyst.[13] Samuel S. Snyder was a major participant in the development and operation of this ASA computer.[14]

ABNER

NBS assisted the ASA analysts and engineers, and when the decision was made for ASA to build its own machine that would use

Fig. 12. Samuel S. Snyder (1911-2007). An early employee of the Army Signal Intelligence Service, he was a versatile performer in the early development and applications of computers in U.S. cryptologic activities. He was an excellent recorder of those early developments and was inducted into the NSA Cryptologic Hall of Honor in 2007. (Photo, CCH)

the four-address logic design of EDVAC, NBS arranged for subcontracts for a mercury delay line memory and for input-output magnetic tape drives from Technitrol Corporation and from Raytheon, respectively. In August 1948 the Army Security Agency and NBS concluded an agreement that provided that NBS would produce a design for a computer that ASA engineers would build. NBS simultaneously would be designing and building a similar computer for themselves. In addition, NBS agreed to place the order for the mercury delay line memories for both machines. Shortly thereafter, several meetings were held to settle on the functional design of the ASA machine, and, to orient ASA engineers in their early design efforts, NBS engineers gave a series of lectures on digital computer logic. The proposed ASA machine was called ABNER. In July 1949 NBS left the partnership to focus on expediting completion of its own machine, the Standards Electronic Automatic Computer, or SEAC.

ASA then decided to build ABNER on its own and estimated that they could build the machine in two years. Meanwhile, the programmers, who had made programming experiments using the several available computer designs, became convinced that ASA operations justified flexibilities in data manipulation not available in these present designs or in ABNER as it was conceived at the time. It was apparent that the elementary computer instructions being programmed to execute typical cryptologic jobs were resulting in excessive operation times and that such jobs were clumsy to imple-

ment. To lessen the programming burden, a series of special-purpose instructions were worked out with the help of ASA engineers. Three principal classes of operations required special attention: character transformations, data-stream manipulations, and paired stream comparisons. These three lines of attention became interrelated and produced a combined solution that was unique at the time and was made possible by the close working relationship between programmers and engineers.

Because the ASA had no prior experience in digital computer design and construction—indeed, no computers of this magnitude and speed range had yet been completed by anyone—ASA engineers faced a number of difficult problems. In addition to the subsystems purchased from Technitrol and Raytheon, other components were ordered from vendors or fabricated in the Agency. The extremely critical electric delay lines used in the logic circuits and operated at 1 megahertz had to be designed and fabricated by ASA engineers and technicians. The power supplies, console, and input-output facilities were also challenging items, primarily because initially they had less reliability than most other parts of the computer system. By September 1951, ABNER I was completed, and the checking out of individual features got under way. This turned out to be a very complex process, partly because of inadequate instrumentation for the 1 megahertz circuits and because of the large number of variations and instruction combinations that were possible.

The design and construction of the ABNER I machine had just begun (April 1949) when ASA analysts began to consider plans for a future improved computer.

In April 1955 the second ABNER was delivered, constructed under contract by Technitrol Engineering Corporation. Logically, it was a copy of ABNER I, but it used quartz instead of mercury in the memory's delay lines.

Compared with ATLAS I neither model of ABNER had high operational reliability, although they had a number of periods of good "up-time." ABNER design and construction laid the foundation for many important later developments. ABNER was among the first

computers in the country to operate successfully up to six magnetic tape drives simultaneously with internal computation. Its analytic instructions and other unique features made it possible to perform many specialized ASA data manipulations more efficiently than certain other computers having inherently higher speed circuitry. For the same reason it was quite popular with programmers. ABNER Serial 1 was operational in April 1952 at Arlington Hall Station. It contained 1,500 tubes and 25,000 diodes. ABNER Serial 2 was operational in June 1955 and was moved to the new National Security Agency (NSA)[15] at Fort Meade, Maryland, in 1957. It was operated there until it was retired in 1960.

The New NSA Accepts a Lead Role

BOGART

The earlier RAM discussion mentioned the problems attending the preparation of input data for World War II-related machine processing. At the time of NSA's founding (1952), these problems still persisted. In 1952 and 1953, suggestions were made for using specially designed digital computers for data conversion and editing and to "clean up" raw data for input to larger computers. This situation was the impetus for BOGART (named after John B. Bogart, a famous city editor of the *New York Sun*), a machine to act as "editor" for data streams requiring subsequent analysis by more powerful machines. The likelihood of needing all the power of the largest computers for sophisticated analyses suggested that it would pay to use a separate "editing" computer to prepare data for input to such jobs. In December 1953 a proposal for the design and construction of such an "editing" computer was approved.

The original idea for BOGART's unit of manipulation was therefore the message character itself (alphabetic or numeric), and the word size of seven bits was specified in the December 1953 proposal. The logic design provided for three-word instructions, both a core memory and a drum memory, and input-output using both punched cards and punched paper tape. In July 1954 ERA contracted to build two models, using a combination of diodes and magnetic cores for

the logic in both arithmetic and control units. It had been decided to eliminate the drum memory and rely on magnetic cores alone.

In July 1955 the contract was modified to provide for construction of four machines instead of two, and to allow for connection of IBM Type 727 magnetic tape drives. These tape drives had just about become the standard for the industry. The logic design was also changed, and the word size became 24 bits, with 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. Subsequently the pilot model of BOGART was modified, and in December 1959 it became the fifth BOGART to come to NSA. The BOGART computers were very reliable and were used on a wide variety of problems. The originally intended application—editing and formatting—became less emphasized because of BOGART's capabilities for higher-priority work and because other cheaper equipment became available for editing. The influence of BOGART stemmed from both its engineering and logic sides. BOGART was probably the first computer in the United States that was designed and built using "design automation" techniques.

Many features of the logic design were unique and carried over into the family of Navy Tactical Data System computers. The UNIVAC 490 included some of BOGART's features such as its index registers and "repetition." Control Data Corporation's CDC 1604 and CDC 160 reflected the early BOGART design experience of that company's founders.

SOLO

By January 1955 the use of transistors in place of electron tubes was increasing, and the apparent advantages of transistors over tubes, such as smaller size, lower heat dissipation, and improved reliability, set the stage for the coming of the new, faster, and mass-produced computers. At NSA the initial step in anticipation of these exciting changes was a training program in the use of the new components. The small group of engineers involved in NSA's special training program formed the nucleus of what became the transistor generation. Among the projects under way at this time was a proposed remote-operation computer, which would make it possible to have terminals in work areas. An alternative proposal to accomplish the same objective was to acquire a number of small computers, built with the new transistor as principal circuit component, and to place one of these desk-size computers in each work area. A project "SOLO" was set up to build the first such machine, and the decision was made to use the logic design of ATLAS II.

In June 1955 Philco Corporation was awarded a contract to build this machine, because Philco at the time was the only firm making reliable surface-barrier transistors (a short-lived technology that 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. While SOLO was successful, the continuing technology development argued against large-scale deployment of this particular design.

Table 2 (next page) contains a brief summary of some of the features of ATLAS and ABNER as well as BOGART and SOLO. All had a major influence on computer design and applications.

Table 2. Selected "Firsts" in the History of Cryptologic Contributions to U.S. Computer Developments[16]

ATLAS I

- Designed and built by Electronic Research Associates (ERA)
- Used a logical design based on von Neumann principles with single-address instructions and forty-one special instructions
- Employed a unique magnetic drum memory with a capacity of 16,383 words of 24 bits each
- Memory access time was 17 milliseconds. The addition of special features brought this down to 32 microseconds.
- Unit No. 1 was delivered in December 1950 and was in operation within one week.

ABNER

- Designed and built in-house at ASA
- Subcontractors made important contributions; Technitrol Corp. provided the mercury delay line memories, and the Raytheon Corporation built the magnetic tape drives.
- It used a four-address design and thirty-one special instructions that emphasized nonarithmetic operations.
- The system could perform computations simultaneously with input and output instructions.
- Operations could be conducted with multiple and mixed input-output devices such as paper tape, magnetic tape, printers, etc.
- First unit was operational in April 1952.

ATLAS II

- Designed and built by ERA
- It used a two-address basic design.

- The first unit of this series used electrostatic storage vacuum tubes for high-speed memory.
- The second unit used magnetic cores for high-speed memory, and it is believed to be the first core-memory computer to be delivered in the U.S.
- The first ATLAS II was delivered in October 1953 and the second in November 1954.

BOGART

- Designed and built by ERA
- Probably the first computer to use magnetic diode/core logic elements in memory. It permitted 20 microsecond cycle times.
- The final version used 24-bit words and IBM type 727 magnetic tape drives.
- It was probably the first computer designed by use of automated design tools and influenced many later designs by Control Data Corporation (CDC).
- The first unit was delivered in July 1957.

SOLO

- Designed by the Philco Corporation in cooperation with NSA; UNIVAC supplied the core-memory and Magnetic Control Corp. the power supplies.
- It was the first computer to rely exclusively on transistors (then of the surface-barrier type) as the principal circuitry component.
- The logic design was a duplicate of ATLAS II.
- It was delivered in March 1958 and was used primarily for testing and training.

A Period of Industry Dynamics and Personnel Moves

Proving again the old saying that "no good deed goes unpunished," there were public accusations of wrongdoing between the Navy and ERA in the early 1950s. The subsequent investigations and the classified nature of the business applications surely drained the energies and cramped the style of the management team which was struggling with an undercapitalized business. In addition, there was by now an active business dynamic in the computer industry of the United States. One result was that by the mid-1950s Remington-Rand had purchased both EMCC and ERA and created what later came to be known as the Univac Division of the Sperry-Rand Corporation. This proved to be an uncomfortable arrangement for some of the pioneers in the business and provoked some people to change their associations again.

Dr. Engstrom served as a vice president of Remington-Rand until the summer of 1956 when he left the private sector for public service in the cryptologic business and joined the recently formed National Security Agency (where Vice Admiral Wenger had become the first vice director) as associate director of the Research and Development Organization. Dr. Howard Campaigne and others were already there. In 1957 William Norris also left Remington-Rand and established another new company, the Control Data Corporation (CDC) in St. Paul. A number of his former ERA employees, including a talented designer and former World War II soldier, Seymour Cray, joined him at CDC. Late in 1957 Dr. Engstrom was appointed to the position of deputy director, NSA, and held that position until he returned to Remington-Rand in 1958.[17]

Dr. Louis Tordella, a mathematician and officer in the Naval Reserve who had also seen service in the World War II cryptologic activities of the U.S. Navy, replaced Dr. Engstrom as deputy director of NSA. The World War II connection continued as Dr. Tordella held that position until his retirement in 1974. He was a powerful lifetime advocate for using the most advanced computers in cryptologic work.

Fig. 13. Dr. Louis Tordella (1911-1996). After obtaining his Ph.D. in mathematics from the University of Illinois, Tordella became a member of the Navy's OP-22 and served throughout World War II. He served as NSA's deputy director from 1958 until his retirement in 1974. The holder of many awards, he was a powerful advocate of the use of advanced computers throughout his life. The NSA Supercomputer center bears his name. (Photo, CCH)

It did not take long for CDC to deliver computing systems. One of their first products was the CDC 1604, delivered in 1960. The customer was the U.S. Navy. The co-workers from CSAW and ERA were continuing their contributions. Soon Seymour Cray had participated in the design and production of what became known as the world's first supercomputer, the CDC 6600, introduced in the early 1960s. NSA was an early customer. But now CDC was not alone, for IBM was fully involved in the business.

Widening of the Government Marketplace

IBM had been aware of CDC's success in the top-end market place and was determined to have a role in that technology-driven market.[18] Los Alamos Scientific Laboratory wanted an advanced computer system, and IBM focused on that about 1955; they won the contract in 1956. A computer called STRETCH was the result. It was designed to use new fast memory and advanced transistor technology that was also delivered in 1959 as a part of the IBM 7090. STRETCH was delivered to Los Alamos in 1961, and for a period of time the nuclear weapons community had the world's most capable computer.

Fig. 14. The HARVEST operating area in 1962. This staged photo does not illustrate the dynamics of this busy area, but it does give a general idea of the size and scope of this landmark system. (Photo, CCH)

There was also a parallel project at IBM sponsored by the cryptologic community. It was called HARVEST. NSA was the customer.

HARVEST was an expanded STRETCH and was the largest computer system IBM had attempted up to that time. The lead engineer on this system was James H. Pomerene, who had previously been a lead engineer in John von Neumann's computer project at the Institute for Advanced Study at Princeton and was now a co-worker with Dr. Goldstein. While a STRETCH computer was at the heart of HARVEST, the most revolutionary aspect of the system was a tape cartridge library called TRACTOR. It used hundreds of special tape cartridges that each contained about 1,800 feet of 1.75-inch-wide tape. A cartridge could store about 120 million characters with a data transfer rate of about 1.4 million characters per second. The library mechanism was a mechanical marvel that could exchange

these large fifteen-pound cartridges in eighteen seconds. It sounds strange today, but then it was clearly the largest electronic data storage capability in the world with a capacity of over fifty billion characters. The HARVEST system went into operation at NSA in 1962. Both the atomic energy community and the cryptologic community had recognized their needs for advanced computational capability and had taken action. They still do.

In the next decade incremental improvements continued, and new competitors were added. Some succeeded and some did not. In 1972 Seymour Cray left CDC and formed his own company, Cray Research, Inc., in Chippewa Falls, Wisconsin. Four years later the Los Alamos National Laboratory and NSA took deliveries of their new Cray-1s. This sixty-four-bit vector-processing machine could achieve 100 million floating point operations per second.

The World War II cryptologic heritage of ERA had now influenced four major computer producers (Univac, CDC, IBM, and Cray Research).

The Transition to Today's Situation and Conclusions

These and other computer companies continued on in this still-dynamic industry, but when William Norris retired as the CEO of CDC in 1986, the direct, first-hand connection of the computer industry's top management to World War II cryptologic activities ended. Some of that experience continued on the government side of the table. All should agree that it had been a great forty-five-year trip. Thereafter, the cryptologic community continued to provide a demanding marketplace to the now-dynamic computer industry. Of course there were other customer sets for the expanding industry, and it is not possible to precisely assign values to how much each contributed to the overall success and growth of the industry and its advancement of "the state of the art." However, it should at least be clear that the cryptologic community had a huge, and very positive, impact on the early computer industry in the United States.

This impact was brought about largely by talented and energetic individuals who pressed on with a job they knew was important. Although their work was often eagerly supported from "above," it was usually not brought about by lengthy and extensive top-level planning. This is often the case when new and innovative technology is being used since, almost by definition, technical consensus is then nearly impossible.

It is much easier to conclude that those who participated in this important activity enjoyed it. Perhaps this quote from Samuel Snyder tells the story of most who participated:

> We who were associated in this pioneering effort in a pioneering industry can look back on one of the most rewarding experiences that can come to anyone, and we are grateful for the support we all enjoyed.[19]

Given the continuing importance of computers in today's cryptologic activities, it is safe to assume that today's cryptologic community continues to be an eager participant in computer research, marketplace expansion, support of academic institutions, and related advanced specialized in-house technical activities. The challenges remain dynamic, and it is still true that only first place counts.

Notes

1. Bletchley Park, located in the city of Milton Keynes, was the center of World War II signals intelligence activities in the UK and the formal home of the codes and ciphers organization. Much of the original area is open to the public today and contains, among other very interesting items, a full-scale working reconstruction of a COLOSSUS computer. More information is available at www.bletchleypark.org.uk. Visitors are sure to enjoy experiencing this historic and important location.

2. For a good discussion of RAM and other matters related to this period, see Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II,* New York: The Free Press, 2000. See in particular pages 246-247. Also see Jennifer Wilcox's bro-

chure (note 6 below) for good detail on one particular RAM development.

3. An excellent summary of the Lorenz problem and the development of COLOSSUS is presented in *The First Computers: History and Architectures,* edited by Raul Rojas and Ulf Hashagen, 2000, Cambridge, MA: MIT Press. The chapter entitled "The Colossus of Bletchley Park–The German Cipher System," by Anthony E. (Tony) Sale, pages 351-364, contains the basics of the story and is highly recommended. It contains a short segment on the contributions to the Allied invasion as well as some information on programming.

4. Quote from Smith, Michael, *Station X: Decoding Nazi Secrets,* New York: TV Books, 1998,193.

5. It seems strange today that these pioneer systems and their documentation were destroyed. It is clear that there was a serious belief that the wide-scale revelation that such advanced technology existed would needlessly put the overall cryptanalytic capability of the allies at risk. We may question the "correctness" of that motivation today, but it dominated the thinking at the time. For a detailed discussion of the reconstruction of the COLOSSUS by a team of talented individuals, many of whom had been involved with the original system, see the website: www.codesandciphers.org/lorenz/colossus.htm. This very informative site also contains further information of the detailed design, reconstruction, and operation of this historic system as well as information regarding the Lorenz encryption machines and how the team at Bletchley Park broke the ciphers. The site was sponsored by Tony Sale.

6. This quote and other information on this subject can be found on the IEEE's Engineering and Technology History Wiki, http://ethw.org/Milestones:Code-breaking_at_Bletchley_Park_during_World_War_II,_1939-1945.

7. See John Hendry, *Innovating for Failure: Government Policy and the Early British Computer Industry,* Cambridge, MA: The MIT Press, 1990. This volume records an extensive analysis of post-World War II events in both the UK and the U.S. The analysis is thoughtful and detailed. For example, in Chapter 13, Conclusions and Policy Implications (161-179), he condenses the experience

of both countries and, in particular (174) comments on the difficulties of developing what he calls "technical consensus" when new technology is involved. He concludes "...in the world of new and complex technologies, technical consensus is quite simply an impossibility." That remains a fact today in many evolving areas of technology.

8. For a brief, interesting, and very readable account of the development of the Bombe, see Jennifer Wilcox, "*Solving the Enigma: History of the Cryptanalytic Bombe,*" Center for Cryptologic History, National Security Agency, 2006. These formidable machines were extremely important in producing plaintext from a variety of the now famous German ENIGMA machines. As you can see from the accompanying photograph of part of the operations area at CSAW's Nebraska Ave. facility, it was a large enterprise.

9. For a complete description of this program and its aftermath, see Scott McCartney, "*Eniac: Triumphs and Tragedies of the World's First Computer,*" New York: Berkeley Books, 1999. ENIAC was an important contribution to the advancement of computing, and some still argue that it was "first" and that is surely true in some aspects, but that is part of the fun of history in any field (including lightbulbs and the telephone). Our vote goes to COLOSSUS.

10. This and other sequence information were obtained by telephone interview with Captain Pendergrass on 22 January 2004. The paper written by Pendergrass and Campaigne was published in redacted form with commentary by Dr. Colin Burke in the journal *Cryptologia,* Vol. 17, No. 2, April 1993, 113-123, under the title "An Introduction to an Historic Document, The 1946 Pendergrass Report, Cryptanalysis and the Digital Computer," and is a very important element in this story for it illustrates not only technical understanding of the new tool, but also the importance of early identification of a demanding marketplace.

11. The Charles Babbage Institute of the University of Minnesota holds an extensive collection of material related to all aspects of ERA and its activities. For background and context for this paper, Audrey and William Boenning, two of the earliest employees of ERA, were interviewed in March of 2004. The article by Erwin Tomash and Arnold A. Cohen, "The Birth of an ERA: Engineer-

Fig. 15. Bombe operations center (see note 8)

ing Research Associates, Inc. 1946-1955," published in the *Annals of the History of Computing*, Vol. 1, No. 2, October 1979, contains significant detailed information on the founding and operations of this company. It also contains many additional references to the details of this complex story.

12. This report was completed and, with the support of the Office of Naval Research, was published in 1950 by McGraw Hill under the title "High Speed Computing Devices," with W. W. Stifler, Jr., as editor. The "author" is noted as "Engineering Research Associates." The task order quote in this paper is from H. T. Engstrom's foreword to the book, page v. This book is very valuable for historical research today because its extensive references and bibliography contain a virtual road map to all relevant work from 1930 to 1950.

13. Dr. Kullback had joined the new Army Signals Intelligence Service in 1930. He was inducted into the NSA Hall of Honor in 1999 for his many technical and managerial accomplishments.

14. Samuel S. Snyder, one of the early employees of the Army Signal Intelligence Service (he joined it in 1936), was inducted into the NSA Hall of Honor in 2007 (at age 96) for his work with the early computer systems. He wrote two papers that describe the ABNER program: "ABNER: The ASA Computer; Part 1:

Design," *NSA Technical Journal*, Vol. XXV, No. 2, Spring 1980, and "ABNER: The ASA Computer; Part II: Fabrication, Operation and Impact," *NSA Technical Journal*, Vol. XXV, No. 3, Summer 1980. These articles contain detailed descriptions of the entire development process and are the source of information for this brief summary.

15. For information on the establishment of the National Security Agency, see the brochure *The Origins of NSA*, a publication of the Center for Cryptologic History, National Security Agency, Fort George G. Meade, Maryland.

16. Another paper by Snyder, unpublished, but written in 1964, "History of NSA General Purpose Digital Computers," is now available at www.governmentattic.org and is the source of much of the information about BOGART and SOLO in this brochure. He also describes several other important computer efforts started prior to 1964 and provides his view of the "Impact of NSA on Commercial Computer Developments" as seen at that time. It is very insightful and a delight to read.

17. Dr. Engstrom continued to serve in an advisory capacity to NSA until his death in 1962. He was one of the forces behind the establishment of a dedicated mathematical research tailored to cryptologic needs. Mr. Norris continued his involvement in technology and civic affairs for many years. He was awarded the National Medal of Technology by President Ronald Reagan in 1986 for "… substantial contributions to the development of digital computer technology." See www.msthalloffame.org/William_Norris.htm for additional details.

18. Much of the IBM-related information can be obtained from another volume in the History of Computing Series: Emerson W. Pugh, Lyle R. Johnson, and John H. Palmer, *IBM's 360 and Early 370 Systems,* Cambridge, MA: The MIT Press, 1991.

19. This quote is from the conclusion of Snyder's second paper in reference 14 above.

James V. Boone obtained a BSEE as an AFROTC Distinguished Military Graduate of Tulane University in 1955. He entered active duty with the Air Research and Development Command and then obtained a MSEE from the Air Force Institute of Technology in 1959. He received an assignment to the Air Force Security Service with duty at NSA where he worked as a design engineer until he converted to civilian status in late 1962. As a civilian, he held a variety of engineering and management positions including an overseas assignment in Germany. In early 1981 he resigned as NSA's Deputy Director for Research and Engineering and went to work in the aerospace industry with TRW, Inc. There he also held a variety of management and staff positions, including the VP and GM of the Electronic Systems Group, until he retired in 1996. Subsequently, he briefly held teaching positions at George Mason University and the Joint Military Intelligence College. He is a recipient of the NSA Exceptional Civilian Service Award (1975) and received the 1994 Outstanding Alumnus award from the Tulane University School of Engineering. He is the author of the Naval Institute Press book *A Brief History of Cryptology*, published in 2005, and has been a volunteer in the Center for Cryptologic History at NSA.

James J. Hearn received a Bachelor of Science degree in electrical engineering from Villanova University and was commissioned as a naval officer in 1959. He served one year as a surface naval warfare officer and four years as a design and test engineer in the U.S. Navy's nuclear propulsion program. Thereafter, he joined NSA and obtained a master's degree. In 1970 he completed his Ph.D. in electrical engineering at the Catholic University of America and two graduate courses in space technology at Johns Hopkins University. In a thirty-four year career at NSA, he held a variety of increasingly responsible positions including deputy director for information systems security (1988-1994) and special U.S. liaison officer, U.S. Embassy, London, in the late 1990s. Hearn served as a department editor for the IEEE publication *Security & Privacy* (2002-2005) and, since 2010, has taught a course in cryptology at Anne Arundel Community College, Arnold, MD. He also held a teaching position at the Joint Military Intelligence College (1999-2001).


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA