The WWII Cryptologic Heritage of the United States' Computer and Communications Industries

James V. Boone
Life Senior Member, IEEE
National Cryptologic Museum Foundation, Inc.

Abstract

The secret cryptologic activities of World War II played crucial roles in determining the evolution of both the communications and computer industries of the post-war United States. The process was influenced heavily by individuals who had participated in either cryptanalysis activities aimed at the axis powers or those who had been involved in protecting the voice communications of the allies. Their wartime experiences and their creative drive provided a foundation for the development of new technological marketplaces. These individuals worked in both government and industry and combined to push and pull the national industrial base forward. Formal government policy was essentially non-existent, but several government entities did serve as informed and influential customers. The examples of SIGSALY, the first digital voice security system, and the linkage of individuals with cryptologic experience to the early US computer industry illustrate this early evolutionary process. Whether or not this technology-growth model has modern policy applications is an open item of current national interest.

Introduction

World War II provoked many important technological developments that would later be applied in world-wide marketplaces. Radar is probably the most widely known example in the field of electronics, while medicine and atomic energy are good examples of other fields. Sometimes the wartime heritage of a technology has been clear, as is the case for radar, but in other cases the connections have been obscured by the security classifications of that time. Two particularly interesting examples have a common heritage as both grew from the wartime cryptologic activities of the U.S. and the U.K.

The term "cryptologic" encompasses both cryptography and cryptanalysis. There are obvious valid reasons for conducting such work under the protection of strict security precautions. In WWII, and still today, both the cryptographer and the cryptanalyst try to use technologies and tools that "the other side" would not expect could even exist. This type of work, which after all attempts to create and solve some of the most challenging technical problems that humans can generate, naturally attracts the most advanced tools of the time. Fortunately, some of the individuals who use these tools in secret may often also have an advanced understanding of their potential for broader application. The abbreviated stories that follow illustrate how individuals and organizations that were involved in WWII cryptologic activities made important contributions to the computer and communications industries in the post-war United States.

The Computer Example

By 1940 many German communicators were using an electro-mechanical 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 with teleprinters rather than as a manually operated off-line device. The allies called the resulting class of messages by the name FISH and the specific machine came to be known as TUNNY. A TUNNY machine is shown in Figure One. It looks complex, and it is. In a peculiar way, this machine can be thought of as one of the primary driving forces of electronic computer development for its messages drove the design and development of COLOSSUS. There is little disagreement about the historic nature of this large-scale vacuum-tube programmable computer. COLOSSUS was a first! [1]

As is the case with many technological advances, there were many individuals involved in the COLOSSUS development and all were important. What we would now call the "requirements" were generated by the mathematician and cryptanalyst Max Newman. The very talented staff of the Post Office Research Laboratories in London, led by the outstanding engineer Tommy Flowers, started this ambitious project in March of 1943. By January 1944 the first COLOSSUS was in operation at Bletchley Park!

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.[2] But how was the U.S. connection actually made? It was not by top-level policy, nor was COLOSSUS the only factor. But as we will see, the critically important connection was made through the efforts of individuals who were deeply involved in cryptologic activities.

During WWII, 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 "sea saw"). This organization, located on Nebraska Avenue in Washington, D.C. (in the present location of the new Department of Homeland Security), was directed by CAPT Joseph Wenger, USN. It was the home of over a hundred of the electro mechanical cryptanalytic machines called BOMBEs.[3] These machines had been designed and built by the National Cash Register Company (NCR) in Dayton, OH 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 that was located in Arlington Hall Station, Arlington, VA. Intelligence products were exchanged regularly between the U.S. and the U.K. 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 LT 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 "Howie" Campaign, was the assigned liaison on FISH and was also at Bletchley Park. Both became familiar with COLOSSUS.

In this same general time-frame, primarily driven by non-cryptologic 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.[4]

The Navy had a strong desire to preserve, and build upon, their cryptologic knowledge and experience, but 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 CAPT (Dr.) Howard Engstrom, USNR who had been a professor of mathematics at Yale University prior to his call to active duty, LTCDR William "Bill" Norris, an electrical engineer from Nebraska, and the contracting officer of the NCML, CAPT Ralph I. Meader. With the encouragement of CAPT Wenger and other Navy officials, this team was able to obtain private financing from a group lead by John E. Parker, a 1922 graduate of the Naval Academy, with the result that 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.[6] 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."[7] 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 place to work.[8]

By 1946 James Pendergrass had been promoted to LCDR and was back at Nebraska Ave. He was now also the CSAW liaison with the Office of Naval Research. In the summer of 1946 CAPT Wenger ordered LCDR Pendergrass off of 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 was what we wanted as a logic machine for enciphering and cryptanalyis applications."[5] He returned from the workshops and enlisted the aid of Dr. Campaign. Together, they wrote a classified paper that would soon launch a serious effort within 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 within the Navy that programmable computers were the wave of the future.

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 Ave. location and put into operation in 1950. A photograph of an early ATLAS installation is shown in Figure Two. The photo does not really do justice to the formidable machine that used 24-bit words and required over 2500 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 was the case 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 sub-systems 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, VA. However, there were very few customers 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 1960's.

Proving again the old saying that "no good deed goes unpunished", there were public accusations of wrong-doing between the Navy and ERA in the early 1950's. The subsequent investigations, and the classified nature of the business applications surely drained the energies and cramped the style of the management team who were struggling with an under-capitalized 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-1950's 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 VADM Wenger had become the first Vice Director) as Associate Director of the Research and Development Organization.[9] Dr. Howard Campaign 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. He was joined at CDC by a number of his former ERA employees including a talented designer, and former WWII soldier, Seymour Cray. 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.[10]

Dr. Engstrom was replaced as Deputy Director of NSA by Dr. Louis Tordella, a mathematician and officer in the Naval Reserve who had also seen service in the WWII cryptologic activities of the U.S. Navy. The WWII 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.

It did not take long for CDC to deliver computing systems. One of their first products was the CDC 1604 that was 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 that was introduced in the early 1960's. NSA was an early customer. But now CDC was not alone for IBM was fully involved in the business.

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.[11] Los Alamos Scientific Laboratory wanted an advanced computer system and IBM focused on that about 1955 and they won the contract in l956. 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 the atomic energy community had the world's fastest computer. There was also a parallel project at IBM sponsored by the cryptologic community. It was called HARVEST.

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. While a STRETCH computer was at the heart of HARVEST, the most revolutionary aspect of the system was a tape cartridge library called TRACTOR.

TRACTOR used hundreds of special tape cartridges that each contained about 1800 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 l5-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 50 Billion characters.

The HARVEST system went into operation at NSA in 1962. A photograph of the operations area is shown in Figure Three. Both the atomic energy community and the cryptologic community recognized their needs for advanced computational capability. They still do.

In the next decade incremental improvements continued and new competitors were added. Some succeeded and some did not. In l972 Seymour Cray left CDC and formed his own company, Cray Research, Inc., in Chippewa Falls, WI. Four years later the Los Alamos National Laboratory and the NSA took deliveries of their new Cray-l 's. This 64 bit vector-processing machine could achieve 100 Million Floating Point Operations per second. The WWII cryptologic heritage of ERA had now influenced four major computer producers (Univac, CDC, IBM and Cray Research).[12]

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 industry top-management to WWII cryptologic activities ended. Some of that experience continued on the government side of the table. All should agree that it had been a great 45-year trip!

The Communications Example [13]

Before the U.S. became fully involved in WWII, the senior leaders of the U.S. and the U.K. were using transatlantic high-frequency radio for voice communications that employed an analog voice privacy system called the A-3. While this system provided reasonable privacy against a casual eavesdropper, it was vulnerable to anyone with sophisticated unscrambling capability. There was no satisfactory alternative.

Fortunately, the technical groundwork for a solution was in place. About 1936, Bell Telephone Laboratories (BTL) started to explore a technique to transform voice signals into digital data that could be reconstructed (or synthesized) into intelligible voice. It was called a "vocoder" for voice coder. An early demonstration of the voice synthesizer portion was a part of the 1939

World's Fair in New York. Stimulated by the approaching war, BTL investigators researched the subject and determined that while there were about eighty patents issued on the general topic of voice security, none were really satisfactory from a national security viewpoint. New technology was required.

Encouraged by initial experiments with the vocoder, BTL proceeded on their own to develop the capability for voice security and was soon able to demonstrate it to the U.S. Army and an Army contract was awarded in 1942 for the production of the first two systems. This system eventually came to be known as SIGSALY and was first deployed in 1943. A photograph of an early deployed system is shown in Flgure Four. It was a large and impressive system involving a large assortment of vacuum tubes, relays, synchronous motors, turntables, and other unique electromechanical equipment. It was power hungry and a typical installation weighted about 55 tons. The design was based on using a twelve-channel vocoder with ten channels each devoted to measuring the power of the voice signal in a portion of the voice frequency spectrum. The work was essentially completed in 1942 and patents were filed. Most patents would be kept secret until 1976! BTL had invented not only the fundamental of digital encrypted voice, but they also invented the means to transmit it.

A 1983 review of this system was published by the IEEE and attributed no fewer than eight "firsts" to SIGSALY[14]. They are:

1) The first realization of enciphered telephony
2) The first quantized speech transmission
3) The first transmission of speech by Pulse Code Modulation (PCM)
4) The first use of companded PCM
5) The first examples of multilevel Frequency Shift Keying (FSK)
6) The first useful realization of speech bandwidth compression
7) The first use of FSK-FDM (Frequency Shift Keying-Frequency Division Multiplex) as a viable transmission method over a fading medium, and
8) The first use of a multilevel "eye pattern" to adjust the sampling intervals.

It was an astonishing system and required the inventive efforts of many people. Important patents were filed by Homer W. Dudley, Ralph K. Potter, and Robert C. Mathes. The historian David Kahn noted that Harry Nyquist and Claude Shannon made important contributions and that the British cryptographer Alan Turing was briefly involved in the development and approved the security aspects of the system for the British.[15]

The importance of this development was not lost on BTL. At the formal opening of SIGSALY service in the recently-completed Pentagon on 15 July 1943, Dr. O. E. Buckley, President of BTL, said:

> We are assembled today in Washington and London to open a new service, - secret telephony. It is an event of importance in the conduct of the war that others here can appraise better than I. As a technical achievement, I should like to point out that it must be counted among the major advances in the art of telephony. Not only does it represent the achievement of a goal long sought - complete secrecy in radiotelephone transmission - but it represents the first practical application of

> new methods of telephone transmission that promise to have far-reaching effects.
>
> To achieve the result represented by this system, there have been done several very remarkable things. Speech has been converted into low frequency signals that are not speech but contain a specification or description of it. Those signals have been coded by a system that defies decoding by any but the intended recipient. The coded signals have been transmitted over a radio circuit in such a way that an interceptor cannot even distinguish the presence or absence of the signals. At the receiving end, the signals have been decoded and restored and then used to regenerate speech nearly enough like that which gave them birth that it may be clearly understood.
>
> To do these things called for a degree of precision and a refinement of techniques that scarcely seemed possible when the researches that led to this result were undertaken. That speech transmitted in this manner sounds somewhat unnatural and that voices are not always recognizable should not be surprising. The remarkable thing is that it can be done at all.
>
> All of the elements of this system were developed by the Bell Telephone Laboratories in the interests of advancing the art of telephony. Early in the course of the development, the system was discussed with representatives of the Signal Corps who at once recognized its possible military value and encouraged our efforts. When it had reached the point where its principles could be demonstrated, the Signal Corps took prompt steps for its procurement. In the present embodiment of the system, manufactured by the Western Electric Company, representatives of the Signal Corps have worked closely with us and are prepared to install and operate it.
>
> We of Bell Telephone Laboratories and the Western Electric Company are proud of this achievement in which the efforts of a large number of our people were involved. We hope that it will be a help in the prosecution of the war, and we are indebted to the Signal Corps for the opportunity to put into practical use this new system of telephony.[16]

Those "far-reaching effects" are with us today. They proved to be useful in WWII as well. Terminals were eventually established in Washington, D.C., London, Paris, North Africa, Hawaii, Guam, Manila, and Australia, among others. Systems were also deployed after the conclusion of the war in other locations including Berlin, Frankfurt and Tokyo. In London, the bulk of the SIGSALY equipment was housed in the basement of an annex to Selfridge's Department Store while the actual instrument used by Churchill and his staff was about a mile away in the War Rooms under the Admiralty Building.

SIGSALY was taken out of service during the post-war demobilization. Some of the documentation and most of the equipment was destroyed, but people involved with the system continued to work on the problems of digitizing voice. The BTL leader of the SIGSALY development program, A. B. Clark, joined NSA and led the Research and Development activities there from 1954 to 1955. Others who had acquired experience with the system while in the Army continued on in government service and at least two, Mahlon E. Doyle and Fred E. Buck, later became engineering executives with NSA.

Transistor technology was introduced quickly into the system designs. By about 1953 a 12-channel vocoder system using early transistors was used in a voice security system that brought the system weight down to under 600 lbs; It was a big improvement from 55 tons, but still limited applications. As solid state technology improved, the weight continued to drop, but it was not until the BTL-government team (there were now government members other than NSA and additional industrial participants began to appear) took a new approach to voice signal processing that dramatic advances were made. This new approach permitted abandoning analog components and tuned circuits and concentrated on a computer-based concept of signal processing which came to be called Linear Predictive Coding (LPC). Soon, new solid-state bit-slice processors were being used and voice processing was quite different from the WWII days. A new generation of equipment came into use.

In 1974 the Justice Department filed anti-trust actions against the Bell System. In many ways this action had as much effect on the communications industry as did the many important technological innovations. Yet the innovations continued to be applied and in this same time-frame; soon all digital voice signal processing systems were being simulated on computer models. Today's Code Excited Linear Prediction (CELP) speech coder which is used in the desk-top secure voice system introduced in the 1980's called the STU-III (and is the foundation of Federal Standard 1016) grew directly from the extensions of the LPC work and design simulations.

Since a modified form of CELP is also used in many of today's digital cellular systems, it is not a stretch to say that WWII cryptologic "DNA" is now in your cell phone.

Summary and Comments

Allied participants in the cryptologic activities of WWII shared a broadly based understanding that the Axis forces threatened their very way of life. They were not really working on market-driven applications; they were working on the survival of all that they held dear. Consequently they were highly motivated. The remarkable technological achievements of the time represent evidence of the success of their efforts. Yet they were not unaware of other peacetime potentials for their work. The post-war demobilization period, and then the continued threat of the Cold War period that followed quickly, continued to challenge governments and individuals. The nature of their responses to the challenges was important.

John Hendry notes in his previously referenced work that the complexity of any high level planning process involving technology is extremely difficult. At one point he notes that consensus is usually a prerequisite for decisions on government sponsorship, particularly at high levels. He then observes:

> Unfortunately, in the world of new and complex technologies, technical consensus is quite an impossibility.

In the early post-war U.S. cryptologic community it seems that the decision-making was carried out at relatively low levels by talented and experienced individuals who were, at least by this time, creative risk-takers. They continued their wartime experiences in the private sector with great confidence. Their superiors believed in them, the surrounding secrecy actually limited the size of the reviewing population in a useful way, and action followed quickly. Other government support was available in the computing field and played an important role. Robert Seidel succinctly describes this case:

> As the midwife for the computing industry, the government made it possible to emerge from the womb of war to the world of peace.[17]

It was not very peaceful in this particular womb, and the world of peace had different kinds of dangers, but the analogy works. The success in both the computer and communications fields also seemed to be dependent upon a type of personal interaction that is rare today. Figure 5 illustrates the primary connectivity between individuals, organizations and products that grew from our examples of WWII cryptologic activities.

Most developers of technology would agree that nothing is better than working with a customer who is knowledgeable of the potential technological advantages and is able to explain the details of the application. Similarly, most buyers of new technology would agree that the best developers are those who know their specialties in-depth and can still appreciate the details of the applications. Both sides must have detailed knowledge if the application is likely to succeed. The knowledge must be personal. It cannot be supplied efficiently by third parties (outside contractors, consultants, or those from the "intentionally not-for-profit" community). In the immediate post-WWII environment, there seemed to be a relationship between the parties that could be described as "creative, competent, and cooperative." That is a rare situation today when the government-industry relationship is more often characterized by "broad area announcements", "service contracting" and "open competitive bidding". In fact, many budget reviewers seem to think that "cooperation" is a sign of potential corruption. Apparently, that is not a new idea either.

A number of building-blocks must exist for this generalized WWII-type of government-industry technology model to be successful. Both government and industry must have:

Organizational structures that support centers of true technical excellence,

Influential individuals who have personal understanding of both the technical aspects of the technologies and strategic interests in the potential applications, and

The capacity for rapid decision-making within their organizations.

Creating and maintaining this situation is extremely challenging in any time period and eventual long-term success is never guaranteed.

Nevertheless, today's policy makers in both government and industry will hopefully consider the examples given here and work actively toward improving the "creative, competent, and cooperative" atmosphere of their development processes.

In the end however, all will depend on the creative talents and knowledge of individuals. That much is exactly as it was in the WWII period.

FIGURES, REFERENCES AND NOTES

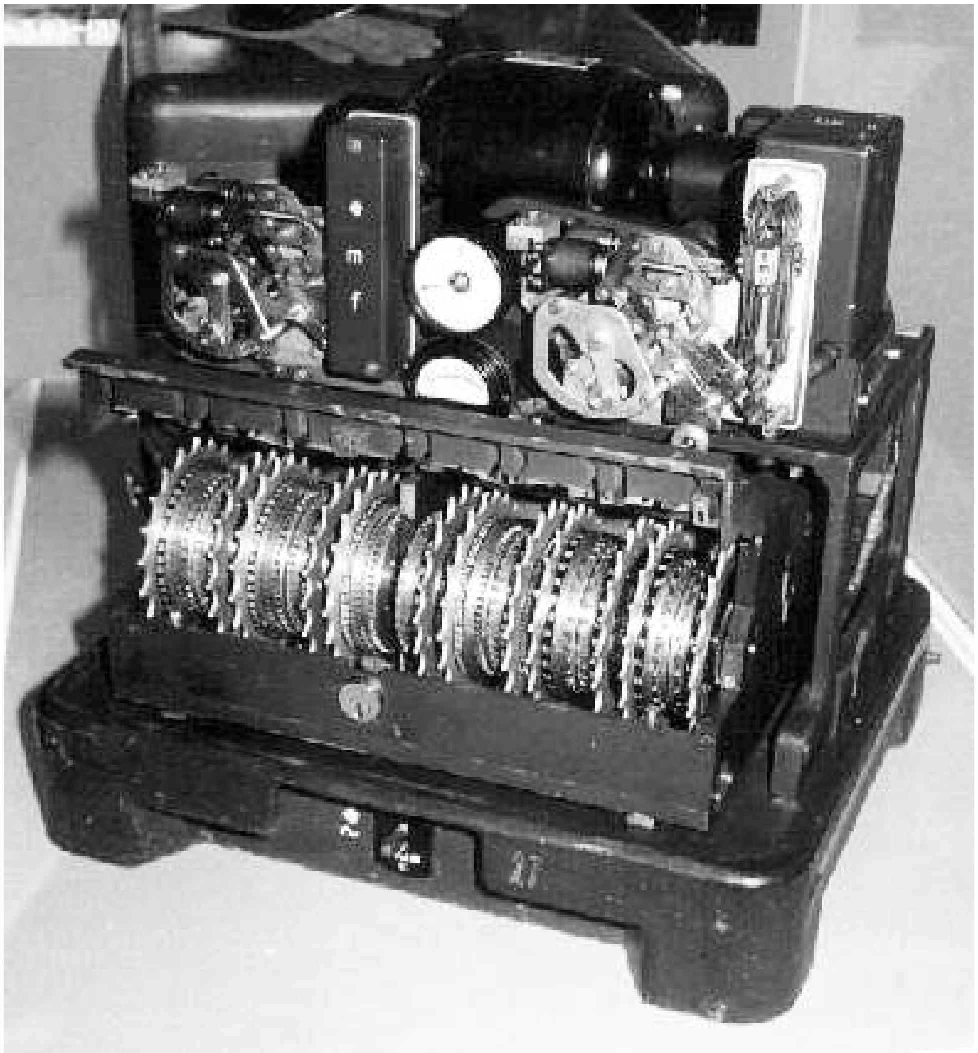


Figure One

TUNNY

This example of the German teleprinter-related encryption device used in WWII that provoked the development of the COLOSSUS computer system is on display in the National Cryptologic Museum. (photo by J.V. Boone)

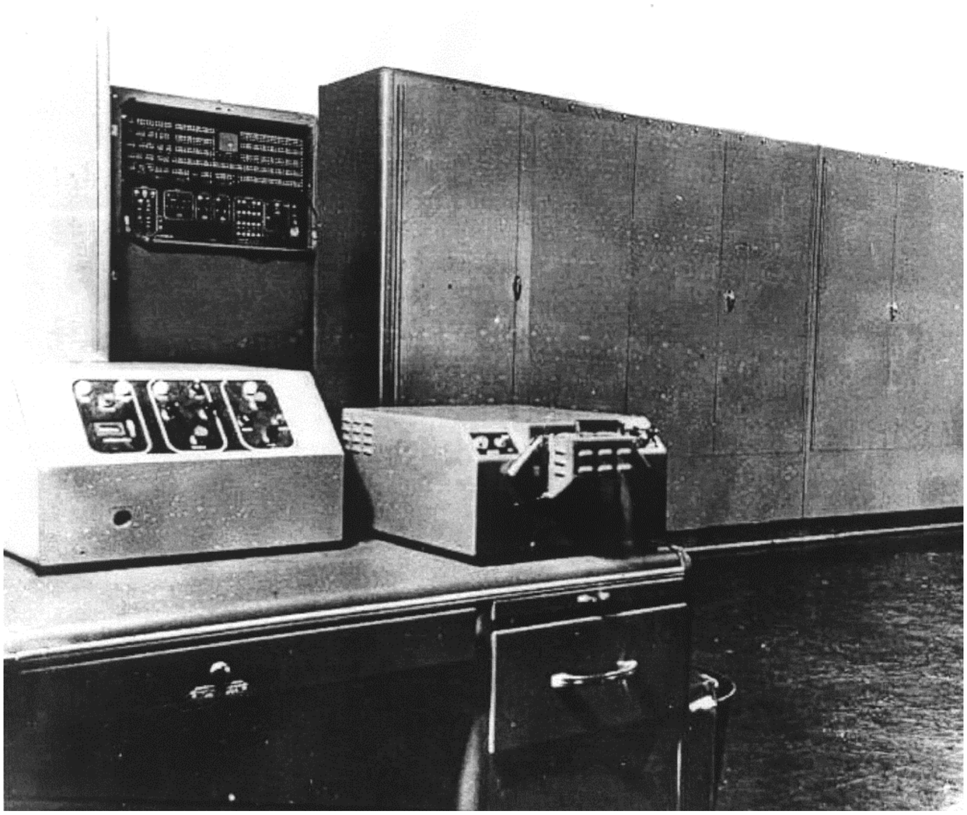


Figure Two

ATLAS

This is an ATLAS installation, ca 1954. While this photograph does not show any of the technical detail, it does serve to show that they were formidable systems. Each ATLAS used over 2500 vacuum tubes and the cabinet complex was over twenty feet long. (Photo courtesy of the Center for Cryptologic History, NSA)

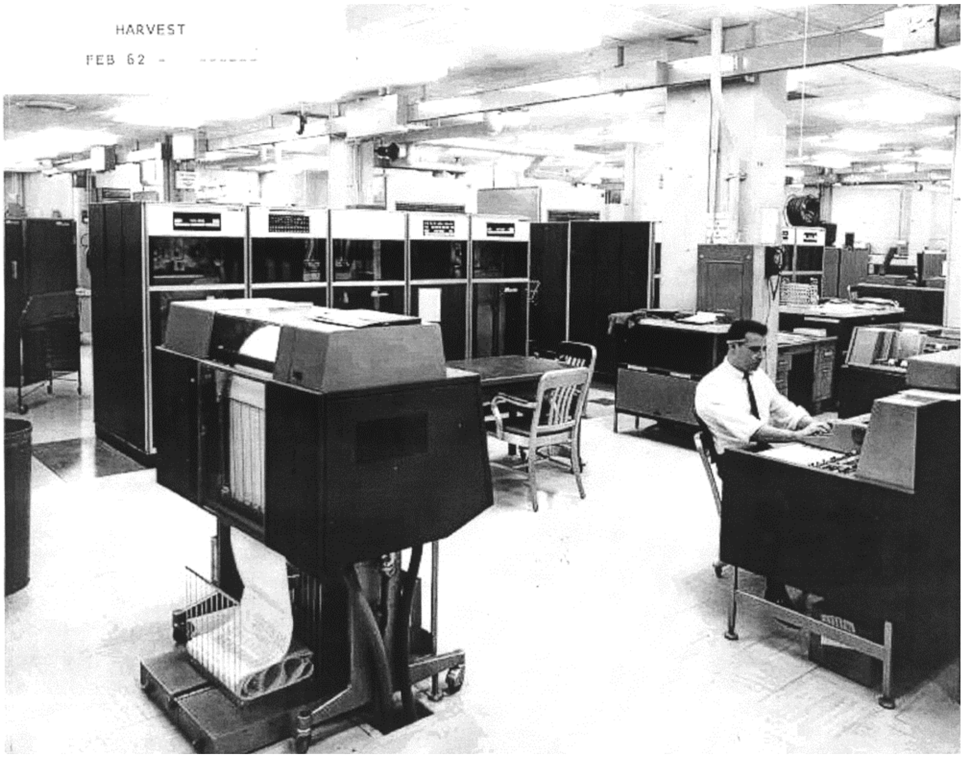


Figure Three
HARVEST

A view of the HARVEST operating area , February 1962. Although this staged photograph shows a rather sterile scene, in actual operation this system was at the center of a very busy operations area. The mechanical actions of the unique magnetic tape drives gave this area its own dynamic personality. (Photo courtesy of the Center for Cryptologic History, NSA)

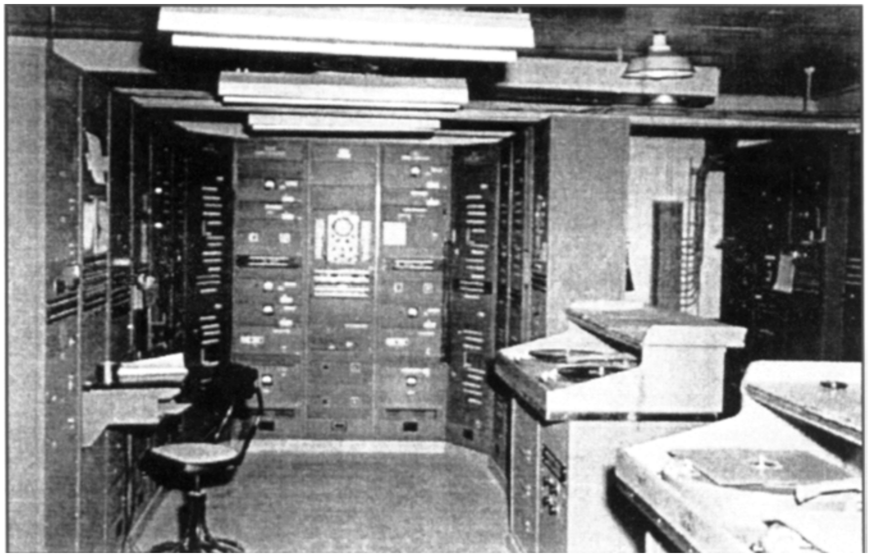
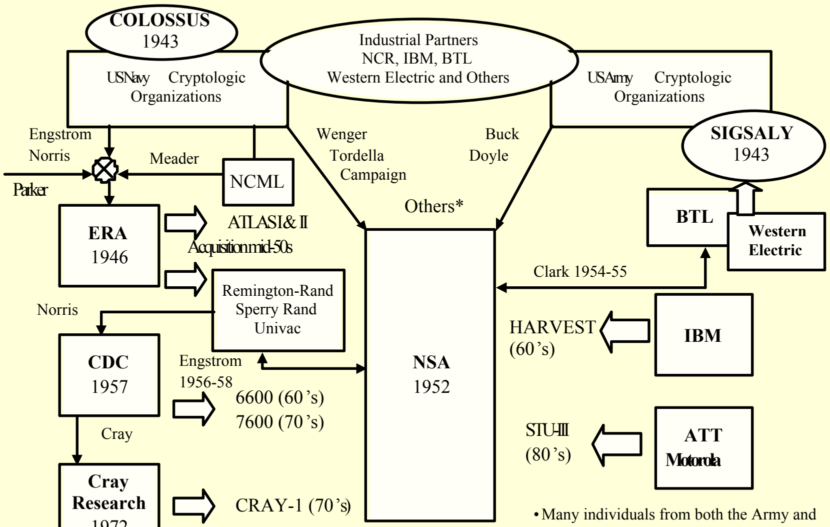


Figure Four
SIGSALY

A 1940’s era SIGSALY installation. This photograph conveys the complexity and size of the system. The phonograph turntables on the right of the picture supplied the cryptographic key for system operations. An associated HF radio system, not shown, was used for transmission and receiving the complex signal and for supplying an international time signal. There were on the order of 40 racks of equipment in each system. (Photo courtesy of the Center for Cryptologic History, NSA)

Figure 5
Some of the Key Individuals, Organizations and Products with WWII Cryptologic Connections



• Many individuals from both the Army and Navy formed the core of NSA in the 1950’s

References and Notes

[1] An excellent summary of the COLOSSUS story is contained in the paper by Anthony E. Sale, "*The Colossus of Bletchley Park-The German Cipher System*", published in the book, *The First Computers, History and Architectures*, Raul Rojas and Ulf Hashagen, eds., the MIT Press, Cambridge, MA, 2000, p 351-364.

[2] See John Hendry, "*Innovating for Failure: Government Policy and the Early British Computer Industry*", The MIT Press, Cambridge, MA 1990. This volume records an extensive analysis of post-WWII events in both the U.K. and the U.S. The analysis is thoughtful and detailed.

[3] For a brief and readable account of the development of the BOMBE, see Jenifer Wilcox, "*Solving The Enigma: History of the Cryptanalytic Bombe*", Center for Cryptologic History, National Security Agency, 2002.

[4] For a complete description of this program and its aftermath, see Scott McCartney, "*Eniac: Triumphs and Tragedies of the World's First Computer*", Berkley Books, N.Y.. NY. 1999.

[5] This, and other sequence information was obtained by telephone interview with CAPT Pendergrass on 22 January 2004.

[6] A much more complete description of the complex story surrounding the founding of ERA is contained in Erwin Tomash and Arnold Cohen, "*The Birth of an ERA: Engineering Research Associates, Inc.1946-1955*", *Annals of the History of Computing* Vol.1, No. 2, October 1979, American Federation of Information Processing Societies.

[7] This report was completed and with the support of the Of fice 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, p v. This book is very valuable for historical research today because its extensive references and bibliography contain a virtual roadmap to all relevant work in the 1930-1950 time frame.

[8] 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 backgound and context for this paper, Audrey and William Boenning, two of the earliest employees of ERA, were interviewed in March of 2004.

[9] The National Security Agency was formed by executive direction via National Security Council Intelligence Directive (NSCID) No. 9 on 24 October 1952. It absorbed most of the technical cryptologic development activities of the WWII Army and Navy organizations.

[10] He continued to serve in an advisory capacity to NSA until his death in 1962

[11] 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*", the MIT Press Cambridge, MA, 1991.

[12] Some of this general story sequence is also reported in James Bamford, "*The Puzzle Pallace*", Houghton Mifflin, Co., Boston, Massachusetts, 1982.

[13] Much of this section has been extracted from the booklet by J.V. Boone and R.R. Peterson, "*The Start of the Digital Revolution: SIGSALY, Secure Digital Voice Communications in World War II*", Center for Cryptologic History, National Security Agency, 2000.

[14] William R. Bennett, "*Secret Telephony as a Historical Example of Spread-Spectrum Communications,*" IEEE Transactions on Communicatons, Vol. COM-31, No. 1. January 1983.

[15] David Kahn, "*Cryptology and the Origins of Spread Spectrum*", IEEE Spectrum, September 1984.

[16] This material was recovered in the National Archives by Donald E. Mehl who has privately published a detailed description of SIGSALY . His work is entitled "*The Green Hornet...America's Unbreakable Code for Secret Telephony.*" Copies are available from Mr. Mehl and are in the library of the National Cryptologic Museum.

[17] From Atsushi Akera and Frederik Nebeker, "*From O to 1,"* Oxford University Press, N.Y., NY, 2002, p20.