Growing Up With Computers at NSA

A Panel Discussion

Panel members: JOSEPH EACHUS, ROBERT L. HAGEDORN, WALTER W. JACOBS, [redacted] SAMUEL S. SNYDER; Moderator, HOWARD H. CAMPAIGNE

(b)(3)-P.L. 86-36

~~Top Secret Umbra~~

The major and significant events in the history of computers at NSA are highlighted, beginning with punched card equipment and progressing to the most complex of today's computer facilities. The scope of the discussion includes the NSA problems addressed with each system of equipment, the successes achieved, the difficulties encountered, and the improvements desired in future computers. Panel members speak from their own personal experiences, pointing up the colorful and human side of computer developments at NSA. Devices covered include ATLAS I, ATLAS II, ABNER, BOGART, SILO, HARVEST, LIGHTNING, CXCO, [redacted] UNIVAC, RAYTHEON, EDVAC, [redacted] ALWAC, Sperry Rand 490 and 494, [redacted] and TRACTOR, [redacted] and [redacted]

FRANK C. AUSTIN, Introduction of Panel Members:

In spite of what I said about not spending a lot of time on reminiscing and boasting about past accomplishments, we will start that way. The topic is "Growing Up with Computers at NSA," and it brings together a number of the NSA officials, past and present, who fathered—and, I suppose, in some cases mothered—our present computer complex.

First I would like to introduce the man whose idea of a session honoring the computer development here led to this symposium. He worked here at NSA for twenty-eight years, at NSA and its predecessor agencies. From 1964–1966 he directed the Library of Congress automation program. From 1967–70 he was with the Research Analysis Corporation as an information system consultant, and he now serves us as an information systems consultant in a Production organization—Mr. Samuel S. Snyder.

Next, a member of the NSA Scientific Advisory Board. Formerly he was Assistant Chief, Development, at NSA. Before that he was in the Navy. His present position is Director of Advanced Development, Honeywell, Inc. He holds a consultant's appointment with the Institute for Defense Analysis—Dr. Joseph J. Eachus.

Our next panel member saw military service at Arlington Hall and Bletchley Park during the war. He was Deputy Chief of the Computation Division, Headquarters, United States Air Force, 1951–1957; a senior mathematician here at NSA from 1957 to 1960; Deputy Chief of R4 and Chief of C4. He was at IDA from 1963 to 1964. He was Commandant of the National Cryptologic School from 1966 to 1969, when he retired from NSA. He is now Chairman of the Mathematics and Statistics Department at American University—Dr. Walter W. Jacobs.

Next, the Chief of the Office of Applications Engineering in the R & D Organization: He has been with the Agency in a military and civilian capacity since 1943. During his tenure with the Agency his office has made major contributions to the development of many special-purpose equipments and general-purpose computers, such as SOLO and BOGART. Many equipments already in use often require major design changes and refurbishments in order to solve new problems. All such modifications are the responsibility of his office—[redacted]

(b)(3)-P.L. 86-36

Next, the Chief of Production Group C: [redacted] (b)(6) when he entered the Army. He was assigned to the forerunner of the Army Security Agency and was placed in charge of high-level cipher machine problems. Since then he has held many positions of responsibility within the Production Organization, directing our efforts in computer processing and cryptologic research. He has also designed and supervised the development of many of the special-purpose equipments used at the Agency and is at present Chief of Production Group C— [redacted] (b)(3)-P.L. 86-36

Next, the Chief of Computer Operations, C7. He saw military service with the Navy cryptologic organization during World War II. He was cryptanalyst on a variety of problems from 1946 to 1954 and from 1954 to 1960 he was a systems analyst in computer assignments. From 1961 to 1966 he was Chief of Computer Applications, and since 1966 has been Chief of Computer Operations - Mr. Robert L. Hagedorn.

Finally, a man who has been a leading mathematician since 1933; Assistant Professor of Mathematics at the University of Minnesota; in the Navy from 1942 to 1946. He was a mathematician with the Navy Department from 1946 to 1949 and Assistant Chief of Research at NSA from 1950 to 1957. He was then Chief of Research from 1957 until he retired in 1970. He is currently Professor of Mathematics at Slippery Rock State College. He has kindly consented to act as the Moderator of the panel in Dr. Tordella's absence—Dr. Howard H. Campaigne.

DR. CAMPAIGNE:

Within the defense establishment, NSA has always been considered a young agency. If one can say that we were born in 1949, when unification of the armed forces took place, then we are just past 21 years old. In fact, we are reaching maturity along with the computer industry, which also had its beginnings about that time. It is therefore fitting that this symposium include a session whose principal focus is history.

NSA has probably done more than any other single organization, government or private, to pioneer and support computer research. Just to recite a list of our computer names recalls a succession of computer "firsts." Remember ATLAS, ABNER, BOGART, SOLO, and finally HARVEST? We had the first transistorized computer in the world, and the first remote multi-terminal computer. We were also responsible for component and device research, tape and memory developments, e.g., cryotrons, thin films, and for the design of high speed circuitry, notably LIGHTNING. And of course, we have made a big investment in programming language research.

Now NSA is like a grown-up agency, and the computer field is also approaching maturity. It is now just 21 years since ATLAS I was installed, and some of our people who helped contribute both to the Agency's development and to computer development are with us today. I will be calling on them to tell about those days. But first, let's start with some recollections about machine operations at NSA's predecessor agencies before computers burst on the scene. The display at the rear of the stage illustrates a span of time from an era of exclusively manual operations through three or four computer generations. At the same time, I'm sure it will help make us aware how much change has taken place within one human generation.

Let me take a few minutes to examine the extent of these changes, in terms of the effect on the way we do our daily business. In the early days, intercepted traffic, totaling a few thousand groups per day, came by mail and the handful of analysts and clerks performed everything manually. The "daily bulletin" which went to higher authority consisted of translations of the cream of diplomatic and naval messages of only one target country. From that time to the present, we have seen machines grow in speed to exceed human capabilities by factors in the millions, yet the scope of our assignments has expanded even more rapidly. Only in a few isolated situations has there been an effective reduction in numbers of people, due to introduction of machines. Rather, we have multiplied and enriched the number and kinds of jobs we can tackle. A little later in the program, we will hear about some of the ways computers and other machines are helping to do this.

The real beginning of modern U.S. cryptology was in 1929, with establishment of two small offices, in the War Department and Navy Department. The Navy office, known as the Code and Signal Section, early felt the need for machine help in attacking certain Japanese systems. By the fall of 1931, a few punched card machines were obtained on loan from another part of the Navy Department. In 1935, the War Department's Signal Intelligence Section obtained the use of a few pieces of punched card equipment on loan from the Civilian Conservation Corps. Mr. Friedman soon succeeded in convincing the Chief Signal Officer that IBM equipment was essential for his cryptographic efforts, and he set up a separate machine room for the initial four machines that made up the S.I.S. "machine section" for the next few years. Mr. Sam Snyder was among those early staff members who taught themselves to use IBM equipment for crypt purposes. He is here today to recall some of his early experiences.

MR. SNYDER:

Dr. Campaigne's reference to the War Department and Navy Department first uses of punched card equipment in cryptology certainly brings back a flood of memories of an interesting period in Agency history. Since my connection began on the War Department side, my personal reminiscences concern incidents in that particular Agency predecessor.

The Signal Intelligence Section in the War Department numbered seven people in 1935, when Mr. Friedman was able to obtain the use of a few pieces of punched card machine. By this time the S.I.S. was regularly reading several Japanese diplomatic systems and also was responsible for producing the U.S. Army's codes and ciphers. As you can imagine, with a staff of this small size, and using manual techniques only, this is quite impressive. It was the responsibility to produce new codes, by the way, which was Mr. Friedman's principal justification for requesting money for punched card equipment rental. When the original request was denied, Mr. Friedman finally was able to get the use of a small group of machines that the Civilian Conservation Corps no longer needed.

You may be amused by one of the stories about the use of punched card machines for code compilation. To produce a new edition of the code, one deck of cards containing the code groups, would be passed through the reproducer to copy the code groups from the second deck to the first. But before doing this, it would be necessary, for each new edition, to rearrange one of the decks of cards in random order. And the most natural way to randomize a large group of cards is—you guessed it—to throw the cards up in the air, and pick them off the floor. On one of these code production jobs the pass through the reproducer showed the code deck to be one card short. The missing card couldn't be accounted for until some time later, when one card was found stuck in a crack over a doorway!

By the time I came to the S.I.S. in August 1936 the section had grown to 9 people—I was number 10. My time was divided between training in cryptography and cryptanalysis, clerical work in support of just about everyone else, and learning to operate the punch card machines. We were using the IBM equipment, by this time in cryptanalytic support as well as code compilation. We made analyses of various language samples, listings of message beginnings and endings, pattern studies, and most important, text indexes showing frequencies and contextual information. Each analyst typically prepared his own material, wired tabulator and reproducer plugboards, and operated the machines. Every job was different, and each analyst had his own way of running the machines. Mr. Friedman soon realized that things in the machine room were becoming chaotic, and took steps to correct the situation. He asked Larry Clark to begin work on a series of written machine procedures, and asked me to take full-time responsibility for machine room operation.

We worked together to begin standardizing procedures and to refine the techniques for preparing indexes. Things in the machine room soon became more systematic, and by the fall of 1939 we hired two key-punch operators, and in December 1939 our first IBM professional, Mr. Ulrich Kropfl.

Although at the time I didn't appreciate working in the machine room, as I felt it took me away from a career as a "cryppie," I am grateful for this early exposure to IBM principles, and the chance to participate in some pioneering developments. Undoubtedly the outstanding product of that experience was our method for producing indexes, for "Key-Word in Context."

In those first three or four years, the use of punched-card equipment contributed immensely to our success in breaking into the Japanese Red and Purple machine ciphers, as well as several other systems, including the famous J-19 transposed code system. It was in connection with J-19 that we built what must have been the first special-purpose cryptologic attachment to the IBM tabulator. In the spring of 1941 we had begun using the IBM tabulator to print out [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

With the outbreak of World War II the Agency expanded rapidly, and because of great problem pressures, the IBM installation grew as well. A number of attachments to the punched-card machines were built, which facilitated such operations as deciphering, decoding, and calculating. By the end of World War II the Machine Branch had over 1200 people and about 400 machines.

DR. CAMPAIGNE:

Thank you, Sam. It would be out of the question to attempt an exhaustive chronicling of all the machine applications in cryptology that followed from these beginnings. This would fill many volumes, and indeed you may have been exposed to many of these stories by reading the *NSA Technical Journal* and other publications. Since we were still in the pre-computer era during the war, the closest thing to the computer as far as generality is concerned was the punched card installation. That is, one could use the same complement of equipment for a great variety of problems by suitable combinations of equipment, pluggings, and procedures.

Another useful series of machines which were developed during World War II by IBM, with guidance and direction from Capt. Skinner and other Navy officers, was the CXCO equipment. These machines combined electric typewriters with teletype tape readers and punches, relay gates, and plugboards to produce a remarkably useful series of devices numbering in the hundreds. But many problems demanded far greater power and speed than could be obtained using punched card methods or CXCO equipment. Many special-purpose machines were built, in some cases specialized as to a particular problem; in other cases machines were specialized as to function, such as for comparing, or counting. Dr. Joseph Eachus is here today to tell about some of these.

DR. EACHUS:

The era of which I speak is one preceding that of the concept of the stored program computer, but beyond the largely electro-mechanical devices of which Sam spoke. There were in particular two electronic devices that came into play—the vacuum tube and the photo cell. These could react substantially faster than could the relay; so we made progress. There were in this period a number of machine aids to cryptanalysts. With some of them the ingenuity was within the device itself, and relatively simple care and feeding was necessary, and in others the ingenuity had to be supplied entirely by the cryptanalyst in determining what to give it. The device, called [redacted] is an example. The input was a five-level paper tape with a photo cell reader. You ran two tapes against one another and did lots and lots of counting, but it was a matter of the ingenuity of the cryptanalyst to decide what counting to do and what positions of the paper tapes would produce useful results. A digraph counter was perhaps the least sophisticated in concept to anything around. You put one paper tape in one reader and one in another and it would count the digraphs, and there was a line

(b)(3)-P.L. 86-36

printer. This really did things surprisingly fast and it was just as well because it cost an immense amount of money in those days.

(b)(3)-P.L. 86-36

[redacted] brings in another device, the magnetic tape drum, for storage. It did the same general type of thing as [redacted] that is, compare two streams of data. But here we have the data stored on magnetic drums and could process one stream with respect to another and do somewhat more sophisticated counting. I recall that it was somewhat temperature sensitive, and when the air conditioning fluctuated a bit the signals might degrade to where they became unreadable. We attempted at one time to stabilize a little bit more by putting a light bulb in a thermostat inside the box the drum lived in, and we found we didn't do so well, as the temperature swings were even greater than they were with the air conditioning; so we had to take that out in a hurry. The physical size of the drum was roughly the diameter of a bicycle wheel, and the axial length was a foot or more. The recording density on the drum was 8 pulses per inch. I think things have improved since then.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

(b)(3)-P.L. 86-36

[redacted] is in the class of machines that worked on code depths. It was a matter of [redacted] This is the sort of thing we had before the basic idea of a stored-program machine. We also had a couple of types of devices during this period. One class was a device that used photographic film to carry information. One could

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

juxtapose two films and move one and look [redacted] by maximum amount of light. This was a great deal faster than some other devices, although the precision of measurement, the photo cell, measuring the amount of light was far inferior to the digital counting that was done by other devices; however, if you could overcome this with a stronger hit situation, then you were ahead by having the photo device. As the technology in the photo devices improved, we went to another one where, in addition to having either clear film or black film, one of the films could take advantage of the gray scale of photographic film and get [redacted] through. This particular one required a matched pair of photo-multiplier tubes, and they did not come in matched pairs. What we did was buy a box of one hundred photo-multipliers and then hunt for a few pairs that would match among them.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Another class of machine is the type that used punched paper tape, rather wide 70mm paper tape with quite small holes punched in it, that would run two tapes against one another and do accounting in that fashion. This is very much the type of thing where it depended strictly on the ingenuity of the cryptanalyst to determine whether or not it ever did anything useful. It did in fact do a great deal of useful work.

Dr. CAMPAIGNE:

Thank you, Joe. Dr. Eachus, after a most productive period at NSA, has been with the Honeywell Corporation since 1956, pursuing more of his innovative projects.

The real beginning of the modern computer era might be considered to have taken place at the Moore School of Electrical Engineering, University of Pennsylvania, in the summer of 1946. At that time, a series of lectures was presented by outstanding mathematicians and engineers who had been identified with ENIAC, the electronic computer just delivered to Army's Bureau of Ordnance. ENIAC was large, it was fast, but it was not flexible, primarily because problem setup had to be done by cable interconnection. The leading scientists who presented the lecture series at Moore School, including John Von Neumann, J. Presper Eckert, John Mauchly, and others,

presented among other things their proposals for a new computer logic, which became the basis for all general-purpose electronic digital computers built since that time.

That historic summer lecture series was attended by only 28 representatives of government agencies and private organizations. Among the attendees was a young mathematician from our Navy predecessor agency, LCDR James Pendergrass. Jim Pendergrass was convinced by what he heard at Moore School that this new breed of machines was so versatile that a machine of this type should be obtained without delay for use in cryptologic work. In October 1946 he issued a report titled "The Cryptanalytic Use of High-Speed Digital Computing Machines," which stands as a milestone in cryptologic machine developments. His report included detailed programs for performing several of our most sophisticated cryptanalytic operations. He stated what at that time seemed like heresy: "... a computer could do everything that any analytic machine in Building 4 can do, and do a good percentage of the problems more rapidly." Now, for those of you not familiar with the Naval Security Station of that time, that building housed almost all the special-purpose machines being used, such as those just described by Dr. Eachus. And so Jim, George Kramer and I sat down to program some cryptanalytic operations. Out of this effort arose a paper that Jim Pendergrass published and distributed in October 1946, in which he showed by programming what a computer could do and that cryptanalysis could be done. A month or so later he did some more sophisticated operations and oddly enough the cryptanalytic operations we considered the most sophisticated at that time were some of those which were the easiest done on a computer. This convinced us that it could be done. We started Project 13, which was contracted to ERA in St. Paul. At about the same time, the people at Arlington Hall were also interested in this effort and they already had a contract with the Bureau of Standards to build a duplicate of the computer that Bureau of Standards had started (SEAC). So the cryptologic community had two computer projects underway. Project 13 turned out to be ATLAS and SEAC turned out to be ABNER. The people at Arlington Hall had cause a little later to be unhappy with the Bureau of Standards because their progress was so slow. The people at Arlington Hall turned to and soon surpassed the Bureau of Standards.

ATLAS began to work in January 1951 and that was very shortly after the UNIVAC machine was first delivered, but the commercial UNIVAC was a decimal machine which for our purposes made it almost unusable although it was mechanically a very good device. The present day computers are more nearly like ATLAS I than they were like UNIVAC. ATLAS I was forty feet long, 7 feet high, 2 feet thick, and had a drum which was the only kind of memory we had at the time. This meant if you wanted random access you had to wait an average of 17 milli-seconds for your next instruction or next data. By some very ingenuious modifications we were able to cut the average time by a factor of about 10. In fact we could cut it by a considerably bigger factor, but every time you had to have a random access you had this 17 millisecond delay. Unfortunately the input and output were through the quotient register, which meant it was absolutely impossible to do any overlapping, and, since its input was from CXCO equipment through punched paper tape, you could see you could put in only a few bits per second. It was quite slow.

ATLAS was in the process of being built for 3 years, perhaps somewhat over three years. We had all these ideas. We had programs written out in machine language in great detail without the slightest idea what was wrong with them; and of course there must have been hundreds of things wrong with them. Experienced programmers know how those things go. So we devised a relay analog called ABEL which was logically precisely the same as ATLAS but was built with relays and had the advantage that one could assemble it in a much more reasonable time, 4-5 months. We were then able to try out programs. Now as a device it wasn't much good to do any cryptanalysis on; it was too slow. But as a device for checking out programs it was invaluable and it was useful to the engineers too because they could use it and see how the electronic device should work. Once ATLAS was delivered, ABEL became much less used. It became completely obsolete and we gave the device to George Washington University who used it for quite a long time and then gave it to Albert Einstein High School. The last I heard, it was still in operation at the High School.

While we were waiting for ATLAS I we did a lot of reading and following of what was going on in the outer world. Everyone was learning about computers, and we were learning; so we had many ideas—mostly Joe Eachus' ideas—about how to improve the computer. We developed ATLAS II with a longer word, a 36-bit word. We incorporated William's tubes memories, which is an electronic memory and about 1000 times faster than our drum on ATLAS I. It was marketed commercially as the 1103; ATLAS I was also marketed commercially by ERA under the number 1101, which is binary 13. Oddly enough the entire industry caught on to that fact. They just announced it 1101 and didn't say why, but conjecture quickly sprung up that this was number 13 and they watched with great interest what the next number would be, and the conjecture was verified. That covers the ATLAS period. The ABNER of course was delivered and it had a different kind of memory, the sonic delay line, as SEAC had, and this type of memory enabled them to do a lot of fancy logic. ABNER had a considerable number of facilities which Sam can tell us about.

MR. SNYDER:

At the Army Security Agency, our computer activity began in late 1946 when we received a copy of Jim Pendergrass's report on the cryptanalytic use of computing machines. After our first favorable reaction, the recommended course of action was to learn about the several computer projects being pursued at the time and evaluate them by doing actual experimental programming of representative crypt problems. During the next few months we visited the Institute for advanced Study at Princeton, the Raytheon Corporation, Eckert-Mauchly Computer Company, Prudential Insurance Company, and Evans Signal Laboratories in New Jersey. We also attended many meetings at the Bureau of Standards, where much of the technical supervision was done on behalf of the Navy Department and the Bureau of the Census. Our programming of crypt problems was done using several of the "paper computers," including ATLAS, UNIVAC, RAYTHEON, and EDVAC. The outcome of these programming experiments was a report favoring a four-address computer of the EDVAC type over the one-address machines, like ATLAS or UNIVAC.

About the same time that we were investigating ways to order a computer, the Bureau of Standards decided to design and build a machine for their own experimentation, and they also chose a design idea based on EDVAC four-address logic. We approached the Bureau and tried to interest them in building a computer for use at the same time. They couldn't undertake such a commitment, but did agree to develop the engineering design for us and to assist our engineers if we would build our own. Thus began a series of meetings at which our engineers obtained fundamentals of computer logic and serial circuitry based on the EDVAC computer being built by Moore School of Electrical Engineering at the University of Pennsylvania. Also, the Bureau contracted for Raytheon magnetic tape drives and for the mercury-delay-line memory to be built for both machines by Technitrol Corporation.

After a few months, it became evident that the Bureau of Standards was totally absorbed in pushing through construction of their own machine, SEAC, and that our computer design job would have to wait. Also, our engineers, working closely with our programmers, were already going ahead with logical design of our machine, which we called ABNER. It was therefore decided that we shouldn't wait any longer, but should go ahead with ABNER construction.

While construction was underway, our programmers were doing much experimental programming of typical crypt jobs. We became convinced that many of these functions were clumsy to implement using standard elementary computer commands, and decided to play with the kinds of special crypt instructions that ought to be available in a future improved computer. Although they were busy building ABNER, our engineers took a keen interest in helping perfect such an "ideal" code of orders. Furthermore, even though ABNER was about half built by this time, it was proposed that these new features be built into ABNER, since the increase in cost and time would be relatively slight. In addition to the extra effort to perfect an expanded set of sophisticated analytic instructions, we also put great emphasis on extremely flexible input-output features. These included input and output capability by punched cards, punched paper tape, or magnetic tape simultaneously with computation, and ability to convert among these while computing.

ABNER's complete instruction code consisted of 31 instructions, 15 of which were special analytic orders. The most sophisticated instruction was the "Swish," so-called because it "swished" two streams of characters past comparison and counting units, delivered a count of hits, and offset one stream against the other before performing another "swish." As a matter of fact, this instruction was the prototype for the HARVEST Streaming Unit, which came ten years later. ABNER was completely checked out in April 1952. Some time before, a contract had been let for construction of a second ABNER, and it was delivered in April 1955.

Both ABNERs were used successfully on complex analytic jobs for several years. The first machine was dismantled in January 1958 because it would not pay to move it to Fort Meade; the second ABNER was retired from active service in 1960. Neither machine performed as reliably as ATLAS and later commercial computers, mainly because serial circuitry required careful maintenance and complex instrumentation, and also because of difficulty in training maintenance engineers; however, much valuable experience was gained, both on the engineering and on the programming side, which profoundly affected later developments.

The thing that may occur to you at the moment is what was life like for the people who were using these devices during this period. Bob Hagedorn is here to tell you about this aspect of computer history.

MR. HAGEDORN:

It might be worthwhile at this time to review with you the relationship that existed during this period between those engaged in computer development and those engaged in other disciplines of the COMINT effort.

Since this is the first symposium of this kind, there obviously were no such symposiums or other organized means of dissemination of this information; training classes and literature on this subject were almost nonexistent. So the general worker population, who represented the potential users, remained, for the most part, completely ignorant of computer developments and the capabilities that computers offered. This is in contrast to the relationship that exists today where the users are proficient in programming and often manage their operations from remote terminals physically located in the user areas.

Therefore, during the early fifties the initial use of computers was limited to a relatively small number of very talented mathematicians, engineers and cryptanalysts, who in addition to selecting the applications also designed and wrote the programs. I might add that in most cases they also evaluated and used the results towards problem solution.

The first applications were restricted to mathematical approaches to crypt problems. This was due both to the backgrounds of the individuals involved and to the limitation of the early computers which were not well suited to handling large volumes of input or output.

Between the early or mid-fifties, the occupation of a computer programmer became established, and many of these individuals came from the ranks of EAM and special-purpose equipment operators and methods personnel (methods personnel designed procedures—they are now called systems analysts). This group supplemented the early group of pioneers and began attacking the many Agency problems that were amendable to computer processing. Most of the early applications were conversion of hand techniques, EAM or special-purpose equipment problems.

I recall a few examples of some early programs written for the ABNER and ATLAS I computers during the early fifties: (b)(3)-P.L. 86-36

[redacted] —ABNER
[redacted] ATLAS

[redacted] approach was developed from a manual process, whereas [redacted] (b)(3)-P.L. 86-36

As you can see, the general work force or eventual users of computer products played a very passive role in the development of the early applications. The user was for the most part not only totally ignorant of how the computer functioned, but was also ignorant of the capabilities of the computer. There was even some concern that these devices would create unemployment. Among

others more cynical—these devices were where you forwarded your data and never got your results back—there were, of course, advantages and disadvantages to a user population of this nature. Since they had never heard of "real time" or "on line," they readily accepted a 3-to-4-day turnaround time.

This separation between the technical source and the program design, however, often produced elegant programs long after the SIGINT problem had changed, and it wasn't long before the "Machine Room" began recruiting personnel with knowledge of the user disciplines.

Today, twenty-plus years after the first computer became operational, we must have at least two thousand users who are familiar both with programming techniques and with their primary profession.

After our first few computers became operational, the commercial computers came on the market. NSA was one of the earliest to use IBM's first practical electronic computer, the Defense Calculator, better known as the Type 701. This was followed by a succession of other commercial computers. But NSA's R&D Organization continued to investigate better machine organizations and to refine engineering techniques. In fact, as I have said, NSA's sponsorship of computer researches led the world, and resulted in delivery of development models of machines which became in some cases forerunners of commercial successes. [redacted] as head of the R&D shops where much of this computer development took place, can tell about these from first-hand experience.

[redacted] (b)(3)-P.L. 86-36

I don't know—as I look at some of these pictures of the past I'm convinced we had more guts in those days than we had sense. As some may recall, they took hundreds of tubes and took a lot of floor space. We were getting to where we couldn't afford Potomac Electric Power Co. for heat and air conditioning. So in 1954 we started to develop, as a result of pressure from users, hardware systems with increases in speed and a decrease in size. We signed a contract with UNIVAC to develop a machine to do away with a lot of the tubes, reduce the heat, power, and size and to increase the reliability—that was the start of BOGART computers. It started out as a 7-bit, character machine, and by the time we got it finished we had it up to 24 bits. This computer turned out to be a real work horse. I don't think anything came into this Agency that didn't go through BOGART.

It was about this time that the analysts, PROD Group, and R&D got together to discuss the many problems with magnetic tapes—the old Raytheon magnetic tapes that we tried on ABNER and ATLAS resulted in many gripes on the input-output—so what's new today? At that time, we decided to install the IBM bus (the 705 bus system) on the BOGART machines.

(b)(3)-P.L. 86-36 Well, you think documentation is bad now; it didn't exist in those days. We had a couple of young engineers, by the name of [redacted] whom I sent to IBM and they worked up there with the design engineers so that we could turn over a package to Sperry Rand—Sperry Rand is now UNIVAC—to make sure that the wires that showed at a certain point on a plug went there. When we were trying in a lot of companies' different equipment you can bet we had all kinds of fun being caught between two companies. Everyone pointed the finger at the other person, but nevertheless the system actually worked. I believe the BOGART console was about 8 feet compared to the ATLAS computers which were at least forty feet, and this was about the same size computer in processing power. This was the start of the miniaturization. I might point out that many of the individuals who worked on this machine left this company and formed what is now called Control Data Corporation.

In 1955 General Canine jumped on R&D and said he wanted a solid state device. He wanted the best computer in the world and he said it a little more strongly than that. And we did some investigation early in 1955 on solid state technology. We let a contract with PHILCO and that machine got delivered in March of 58. Like everything else you have all kinds of trouble with the first ones. We had trouble with the memory, power supply, cold solder joints, and anything you can name—we had it. We got the thing to work though and it was finally used by the C Organization as a training aid. And one of the things that was always interesting, General Canine picked on me everytime he saw me. He said, "Dammit [redacted] you built the best, most modern computer

(b)(3)-P.L. 86-36

in the world, and you have a horse and buggy input-output on it. Well, the thing of it was, PHILCO wasn't too good on input-output, and I didn't feel we wanted to educate them on tapes; so we put some tapes on it after we got it here in the building. General Canine wanted the best one in the country and the main reason was that he was thinking ahead to the time that we were going to have multiple copies like 50 or so spread around the Agency.

About this same time, the 1954—1956 era, we were also trying to see if you could operate computers from remote stations, and we had a computer called ALWAC—this was another disc machine—but we did put four remote stations on it. It was at Arlington Hall, and some of them were at least 1000 feet from the station and each one had its input-output paper tape keyboard. One of the things we did learn out of this experiment was that we caused limited remote station use. The machine would step around so that one station couldn't hog the machine all day, and each station was limited to 15 minutes. Probably one of the good things about it was that there was no administrative control or record keeping on this one. And there were a lot of useful jobs performed using this type of technique where analysts could actually improve their program so that they had a 15 minutes turnaround time. In this case I guess it turned out to be an hour with four 15-minute stations. This thing was called ALWAC and it was received so well in the Agency that we turned the fifth BOGART into a remote station, and it had four or five stations—that was put into this building. It was quite an improvement over the old ALWAC. The thing had tapes and a drum; you could input-output, not knowing your interrupts, and so forth, So in 1962 the Prod Organization let out specifications for a system called RYE to four or five companies. Sperry Rand was the winner of this with a Sperry Rand 490 machine. Now this thing has been updated into a 494 system. That's about all I want to say about the thing. I might point out for those who are interested in history, that Sam Snyder has prepared a book, written in 1964, that describes all these machines.

DR. CAMPAIGNE:

It's too bad we can't give Charlie all the time he needs. He could tell us about many more interesting applications.

In many ways, our HARVEST qualifies as the most sophisticated computer ever built. In logic features, it is certainly the most advanced in the crypt community. We have just passed the 10th anniversary since its delivery to NSA, and it continues to perform powerfully; in fact, I am told better than ever, because we are still learning more and more about how to use it. In 1955, when IBM proposed to this Agency and to the Atomic Energy Commission the construction of a "10-megacycle computer," we insisted that we needed not only a 10-fold speed increase but also specialized logic and large-volume data-handling features. The result was an advanced computer suitable for both AEC and NSA, and, for this Agency, attachments to accomplish these two additional requirements. The logic attachments, sometimes nicknamed the [redacted] and the TRACTOR tapehandling system are what make HARVEST unique. Besides the unusual hardware which is certainly involved, the problem of programming such a complex system demanded an exceptional investment of money and talent. Dr. Walter Jacobs, another recent retiree and currently Chairman of the Mathematics and Statistics Department at American University, had a hand in much of the planning for HARVEST operation, and will discuss some of these problems.

(b)(3)-P.L. 86-36

DR. JACOBS:

I'm going to resist the temptation to reminisce and to talk too much about the hardware. I'd rather spend the time drawing some lessons from the HARVEST experiment. HARVEST, by the way, is the only thing that's been talked about that's still around. In fact last week we had a 10-year birthday party for HARVEST and in the rosy glow of admiring a highly successful accomplishment I felt a little out of place remembering some of the frustrations that were encountered in the process of making this thing work. But briefly, HARVEST was started as a development idea about 15 years ago. It was designed to push the frontiers of computer technology, both hardware and soft-

(b)(3)-P.L. 86-36

ware, to the limit. We built a general-purpose computer which was not only substantially faster than anything else that was then on the drawing board, but also had a [redacted] that was designed to do special Agency work. We also built the TRACTOR System and then, recognizing the complexity of this for the user, we undertook to design a software package to go with this, which was again pushing the frontiers of the art. It was the first really substantial operating system. This also involved the development of a special Agency computer language, ALPHA, which is still in use and is being replaced by a better more up-to-date language called BETA. We called it ALPHA to indicate that it was going to be the first of a line of improvable languages. And then we had a job request language, a high-level language, in which you simply had to ask for a sort, let's say of a particular file, or you operated with instructions at that level. All of these things were new, and I remember beating on Sullivan Campbell because it was taking a long time to produce these things and he just said, "We don't know *how*, we are *learning*." It took a while.

Now something about the HARVEST System. We had the STRETCH computer, which was the first third-generation computer, and it was the computer that developed the third-generation technology. We had a streaming unit which was designed to operate on large masses of data, and a TRACTOR tape unit which provided the availability of a large tape memory under program control for rapid call-up processing. We had a number of tape units and a peripheral processing system. At that time we used two 1401's.

I want to say a little about the history and the lessons that can be drawn from HARVEST. We had a five-year R/D project. Then HARVEST was installed; the ribbon was cut almost exactly 10 years ago. And it began a five-year shakedown period to prove that this thing was a good idea. I had only about a year and a half of this. By the time I turned it over to Arthur Levenson I think we were up to 15% utilization, productive work, out of the total time it was in operation, and it took 3½ more years to get that up to the point where we could sit back and say this thing has been worthwhile. This kind of cost, the shakedown cost, is one of the costs that sort of gets forgotten in starting a massive new program, which, like everything else the Agency does, has to push the frontiers of technology beyond the point that is reasonable to attempt. On the other hand, if we don't try something that is really hard, it isn't worth the effort. We might just as well sit back and let the technology develop at its own rate. So you have these tremendous costs, the manpower input and the headaches that go into proving that one of these new ideas is worthwhile. But there are important gains that come from this kind of investment. I think there are two gains in particular that are worth recognizing. In the first place, pushing the frontier speeds up the pace of technological advance so that the Agency benefits that way as well. Without the HARVEST program, the third generation of computers would have taken a lot longer to come about. And the software advances that are so important in making the computer conveniently accessible to users, who don't really know much about what goes on down in the basement, again were a part of this particular development. The other benefit that comes out of wrestling with this advanced technology is expertise. Many people today are holding important positions with the Agency because of their broad as well as detailed knowledge, people who learned the hard way by taking something that never should have been tried, it seemed then, and proving that it could be made to work. I think there are lessons like this still to be faced and perhaps even now the Agency is involved in the same kind of thing with [redacted]

(b)(3)-P.L. 86-36

DR. CAMPAIGNE:

Our data-handling problems continue to multiply in number and volume and in complexity. And, tied more and more intimately with processing problems are our communications links. At several points in the processing cycle, such as the raw data input point, the intermediate levels, and at the delivery of the finished product, we must be able to receive, identify, and deliver data without delays due to conversion or other problems. To provide for this requires extraordinary memory capacities, standardization arrangements, and stringent controls. [redacted] who pioneered much of the special-purpose equipment development and who is currently the Chief of the C Organization, will tell how his plans for the future take these problems into account.

(b)(3)-P.L. 86-36

[redacted] (b)(3)-P.L. 86-36

We find ourselves today in the position of beginning to be a factory. To some it is not as much fun when you don't see the data. I think one of the biggest developments was when the target countries began to use teletype equipment and began to send their data electrically. We thought at one time that we would have a mile and a half of cards, and that we would have the whole building filled with key punch operators to punch all the data; but fortunately the target countries began to be our key punch operators, which led to our being able to forward this data electrically. We are currently handling by electrical circuits some [redacted] per day which come directly into the building and are handled automatically. This will be expanded shortly to abou[redacted] a day. This comes about because each intercept operator is now a key punch operator; as he hits his keyboard he produces an electrically forwardable signal which is sent to NSA and processed by computers. The feedback goes via reverse route such that in effect we are no longer a nice working team; we're a factory. Much of this data is never seen by any particular person. In some cases, the results go back within less than a minute, having really never been seen by an individual. That doesn't mean that much analytic work doesn't go into the preparation of the data.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

In addition to the electrical data coming in at the rate of [redacted] a day, much more that arrives on magnetic tape at the rate of a factor 10 times as great (such as telemetry and similar types of signals) has to have some place to reside. Projecting from our current tape library, which is now 150,000 tapes, we soon discovered that with this growth rate the building would soon be full of mag tapes. In 1965 we started on the [redacted] project, an extension of the TRACTOR concept on HARVEST in which we hope to put all of our magnetic tapes and data on line under program control of a computer. As Dr. Jacobs said, this is quite a project in itself, and perhaps will be as difficult to come about as HARVEST. This particular system will be available to all third-generation computer systems. We expect [redacted] to have the storage capacity of something on the order of [redacted] on line. If you do a bit of figuring, that is a few more miles of punched cards than a mile and a half. As pointed out by previous speakers, users are no longer content with a five-hour turnaround time. Much of our work comes from overseas via communications links on line through the computers, is processed and is sent back [redacted] We are presently processing on one of our systems some 15,000 different jobs a day, many of which are completed in under five minutes. This system not only supplies intelligence feedback; it also supplies data from large files for research by various analysts. Our automation plan for the 1975–80 time period calls for all systems to be connected electrically. The input will be from three sources: manual preparation thru a keyboard, where the data is collected and controlled in a system known as [redacted] Our [redacted] system interfaces all the communications lines with the digital computers called [redacted] which is our interface with the analog world. We envision the latter two systems to be able to handle [redacted] input of communications signals from the air and enter them directly into our computer complex. We have a mass of computers in the basement which will simply be on line to a large population of users. The data will flow through the system and be available to all qualified users. I like to think of it in terms of a person working on a particular cipher system. He arrives in the building at eight o'clock in the morning and goes to a remote terminal connected to [redacted] and 29 messages appear on the screen of this cathode-ray tube. He decides what he needs to do with each message to get plain text and then he goes home.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36