(U)Before Super-Computers: NSA And Computer Development

(U) At the time of World War I, commercial and government inventors began experimenting with electromechanical machines to encipher and decipher messages. By the outbreak of the Second World War, all major combatants had adopted sophisticated cipher machines for at least a portion of their communications security programs. At the same time, Great Britain and the United States, partners in cryptanalysis, developed machines of increasing power and complexity for solving the cryptosystems of their enemies.

(U) With the knowledge of what machines could make possible in cryptanalysis, Army and Navy personnel adapted and adopted devices of increasing power and capacity during the war. They leased or built machines for compiling and comparing message texts, searching for cribs, or seeking statistical coincidences. Each machine, it seems, also had to have a colorful designator -- DRAGON, COPPERHEAD, RATTLER, MAMBA, DUENNA, MADAME X, SUPERSCRITCHER -- that sometimes signified something about its components or its antecedents.

(U) None of these machines, it should be noted, were computers. They had no memory, and both were "hard-wired" to perform just one task. However, near the end of the war the British cryptologic organization developed a device that many consider the first true computer.

(U) One sophisticated German machine was TUNNY (the Allied codename for it), used by the highest level officials. In 1943, capitalizing on an error by German code clerks, British cryptanalysts solved the system in theory. In practice, however, working individual TUNNY messages required excessive processing time. For rapid exploitation of TUNNY, British engineers invented a device known as COLOSSUS, which had many characteristics now associated with modern computers.

(U) By the end of the war, U.S. Army and Navy cryptologists had considerable experience with special-purpose devices; this experience made clear to both services that rapid data processing would be vital to American cryptology in the future. The challenge was to transfer their hard-won knowledge from special-purpose machines to the design of a general-purpose computer capable of multiple applications.

(U) But American research in data processing faced several challenges in the first years after the war. Budgets dropped, many academicians and technical experts who had entered

the military "for the duration" were now demobilized, and the close "win the war" cooperation between government and industry ended.

(S//SI) In this period of uncertainty, both the Navy and the Army conducted as much in-house research as possible, and contracted as they could with private corporations for development. Despite the hope for a general processing machine, well into the postwar period most cryptanalytic devices were designed to work only against one particular foreign machine. These devices, again like their wartime counterparts, had colorful codenames -- ALCATRAZ, O'MALLEY, WARLOCK, HECATE, SLED.

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

(C) In the summer of 1946, two civilian researchers working for the Navy, Dr. Howard Campaigne and [redacted] attended a conference on computing at the University of Pennsylvania. Participants compared new academic data processors, discussed advances in increasing memory, and shared ideas on programming languages [redacted] report to the Navy in the fall of 1946, prepared in cooperation with Dr. Campaigne, detailed the latest advances in computing and gave examples of how they could be applied in cryptanalysis.

(C) Samuel Snyder, an Army civilian who had been involved with cryptanalytic equipment since the 1930s, read the [redacted] report and was inspired to conduct his own investigation into academic and commercial data processing developments. His findings influenced the Army to invest in computer research in much the same way the [redacted] report had influenced the Navy.

(U) By 1947 both the Army and Navy cryptologic organizations were committed to acquiring general-purpose computers. They had, however, no clear idea which among several competing concepts might work -- if, indeed, any of them would.

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

(C)
(U//FOUO) By late 1950 the Navy and industry working together produced the general-purpose computer ATLAS. This machine, with a cost of nearly [redacted] (triple predevelopment estimates), used 2,700 vacuum tubes and drum memory technology. In addition to the Navy's direct input, considerable work under was done by Engineering Research Associates (ERA), which had begun life as one of the Navy's proprietary companies and had many veterans of Navy cryptanalysis in it. ATLAS would perform well in support of cryptanalysis for a decade.

(U//FOUO) It is believed that the first operational program written for ATLAS was designed to attack isologs in VENONA messages (VENONA was the codename for Soviet World War II espionage communications); the program was written by [redacted] [redacted] a mathematician who had been hired as a Navy civilian in 1946.

(b)(6)
OGA

Navy

(U//FOUO) Once ATLAS went into operation, the Navy's R&D team learned to appreciate

the capabilities it represented, but, even more importantly, they gained an understanding of its limitations and shortcomings. These were the areas in which they would concentrate future research efforts.

(U//~~FOUO~~) Whereas the Navy turned to contractors or proprietary firms for computer research and development, the Army depended primarily on in-house work. Samuel Snyder kept his team kept informed on the latest research at universities, and also at the National Bureau of Standards, which had its own research program. The Army Security Agency engaged in considerable design work for its own computer, but had not begun actual production by the time the Armed Forces Security Agency was founded in May 1949 and many cryptologic research functions were consolidated.

~~(S)~~ In fact, the decision to proceed with production took another year, when the Korean War provided the stimulus. Since conventional means proved too slow to validate U.S. encryption tables for wartime use by American forces, AFSA authorized in-house production of ASA's computer design. The result was ABNER, completed in 1952. Like ATLAS, the machine incorporated innovative features, but had serious limitations, and served as an educational device as much as for designers as for the operators. (The name, by the way, came from a then-popular comic strip, "Li'l Abner," about a powerfully built country bumpkin).

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

(~~TS//SI~~) In addition to the needs of its cryptanalysts, NSA had another pressing problem to which electronic data processing seemed the only solution. Sites around the world were sending [redacted] intercepts to NSA each month in the 1950s; conventional machines were not equal to the task of sorting, standardizing, and routing this tonnage. NSA spent more than [redacted] dollars, working with a contractor, to develop NOMAD, a device that would increase computer memory exponentially to tackle this job. However, for a variety of reasons, including shifting requirements and inadequate monitoring of research, the project failed.

(U//~~FOUO~~) Learning from these deficiencies, subsequent NSA systems incorporated innovative input techniques and storage devices -- drum storage, then tape drives; remote job access; and chip technology. One computer built in the mid-1950s, called SOLO, became the first to replace vacuum tubes with transistors. Special-purpose computers were designed not only for cryptanalysis, but also to generate COMSEC material for protection of U.S. communications.

~~(S)~~ As it became apparent NOMAD was a failure, NSA developed a number of special-purpose devices to perform the data managing and processing NOMAD had been slated to do, some of them made in-house, some by contractors such as IBM. One of the systems, nicknamed BOGART, which had originally been designed to support NOMAD functions, was redesigned to do the whole job. BOGART, which used solid state technology for the

first time, and took advantage of new tape drives for long-term data storage, operated successfully for close to a decade. BOGART also served as the central computer for one of the first remote job entry systems, codenamed ROB ROY.

(TS//SI) In the late 1950s, the highest government levels called for new approaches in the cryptanalytic attack on [redacted] cipher systems; President Eisenhower authorized a number of studies of American intelligence, including SIGINT. One of the studies, chaired by ex-president Herbert Hoover, recommended an all-out attack on [redacted] ciphers similar to the project that had developed the atomic bomb.

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

(TS//SI) Some felt, however, that NSA was not taking advantage of the latest scientific thinking and advocated the creation of an outside group to research advanced methods of cryptanalysis. To help forestall any movement to break NSA apart, the DIRNSA, General Ralph Canine, brought in Howard Engstrom to lead the Agency's research efforts. Engstrom had directed the Navy's wartime cryptanalytic R&D, and had worked in private industry in the decade since, giving him a solid grasp of the problems and possibilities in both worlds. (As an aside, this recommendation for a cryptologic "think tank" resulted in the creation of [redacted]).

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

(TS//SI) Engstrom collated ideas from NSA scientists and cryptanalysts regarding long-term research into super-fast computers and research into [redacted] cryptosystems. These suggestions, which called for work both inside and outside the fence, coalesced into a proposal that came to be known as "Project FREEHAND." A subsidiary effort to develop hardware became known as "Project LIGHTNING." General Canine, who in 1956 was facing retirement, wanted the plan begun before he left.

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

(TS//SI) General Canine convinced President Eisenhower's science advisors to support the research outside NSA, but, in light of failures such as NOMAD, they were reluctant to agree to fund in-house work. Canine put pressure on NSA's own Science Board to prepare a plan acceptable to the government's highest levels. Working their individual high-level contacts, General Canine and Howard Engstrom obtained promises of funding for FREEHAND and LIGHTNING; Engstrom took the lead in advocating these projects when Ralph Canine retired.

(TS//SI) President Eisenhower approved Project LIGHTNING in a meeting with General John Samford, the new DIRNSA, giving a powerful boost to the project. Engstrom believed that with an adequate budget and a genuine "free hand," NSA could create a new generation of super-fast computers, perhaps tripling processing speed at a stroke [redacted] To manage LIGHTNING, he chose Howard Campaigne, the data processing pioneer. NSA went to three major contractors for research on the latest technologies, with other commercial firms and some universities taking smaller aspects of the overall research plan.

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

(C) At this same time LIGHTNING started, the IBM Corporation proposed a parallel research track known as HARVEST, an outgrowth of work already in progress for NSA and other government customers. Although Howard Engstrom -- now NSA's deputy director -- and Sam Snyder, another computer pioneer, opposed the concept, arguing that the technology involved was not as advanced as needed, and that funding HARVEST would interfere with Project FREEHAND, General Samford approved the proposal.

(TS) HARVEST came in at a higher cost than projected, proved to be a difficult system to use, and had slower processing speed than planned. However, NSA personnel wrote innovative programs for it that extended its applications, although it never achieved their goal of multiprogramming. As with earlier systems, its development and use turned out to be good experiences for those who went on to the next generation of equipment. HARVEST itself remained in service from 1962 to 1976, a long span of use for a computer system.

(S//SI) No machine resulted directly from Project FREEHAND. But the knowledge gained from the research was applied for years to development of computing systems.

(S//SI) From the mid-1960s, NSA began purchasing commercially developed computers in addition to building its own. Agency programmers often wrote specialized software that extended the cryptologic capabilities of COTS systems. By the late 1960s, it is likely that NSA, with about [redacted] of equipment, had the largest collection of advanced computers in the United States, and probably in the world. (b)(3)-P.L. 86-36

(S//SI) NSA organized its computers in complexes, according to the type of processing performed. By the early 1970s, the Agency was moving into the era of the supercomputer with the purchase of the CDC 6600. One CDC employee, Seymour Cray, left to form his own company in 1972 and began designing supercomputers. NSA purchased the first, CRAY I, in 1976.

(U//FOUO) The development of computers for cryptologic applications did not happen smoothly or directly. NSA research focused on specific problems and how to solve them, not abstract theory, and there were many failures and false starts as well as successes. However, each new machine gave enhanced capabilities to NSA's analysts and excellent learning experience to those involved in research. It should also be pointed out that even if NSA's computers did not achieve the Agency's own high goals, they frequently were well in advance of data processing equipment anywhere else.

FOR FURTHER READING:

(U) Colin B. Burke, *It Wasn't All MAGIC: The Early Struggle to Automate Cryptanalysis, 1930s-1960s* (CCH: 2002).

(U) Thomas R. Johnson, *American Cryptology in the Cold War* (CCH: 1995-1999)

Almanac 50th Anniversary Series

Content Owner: Feedback
Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days