UNCLASSIFIED

DAILY ENTERPRISE

(U) HISTORY TODAY - February 10, 2016

FROM: CCH
Run Date(s): 02/10/2016

(U) **HISTORY'S TRIVIA**:

(U) Cryptologically speaking, what were PLUTO, HIAWATHA, and NOMAD?

(U) **TRIVIA ANSWER**:

(U) One important cryptologic "lesson" of World War II was that machines were the future of the field.

(U) As more and more countries adopted machines to generate cipher, sophisticated devices would be necessary to continue exploiting the communications of target nations. Widespread German use of the ENIGMA machine led to development of the cryptanalytic bombe for Allied exploitation of it. German use of the sophisticated TUNNY machine for enciphering the communications of senior officers led to development and use of COLOSSUS, arguably the world's first operational computer.

(U) The major problem was, despite agreement that machine support for cryptanalysis would be vital, there was no consensus on the type of machines needed.

(U) The U.S. Army and Navy separately began developing computing devices, which resulted in ATLAS and ABNER, two machines that performed various calculations rapidly and could be reprogrammed.

(U) The cryptanalytic bombe had been a comparator, and many felt this was the type of machine needed to tackle the emerging Soviet cryptanalytic problem. The bombe worked by rapidly comparing intercepted German messages with keywords expected to be in a message. When the bombe found a match between a segment of the intercepted text and the keyword, it could determine the setting on the machine used by the Germans and the entire message could be solved.

(U) Another use of a comparator was to compare intercepted messages against each other, looking for similar passages that could provide enough "depth" for a cryptanalyst to solve the system.

(U) While they were developing computers, both the Army and the Navy pursued complex comparators that would operate against machine cryptosystems of the Soviet Union.

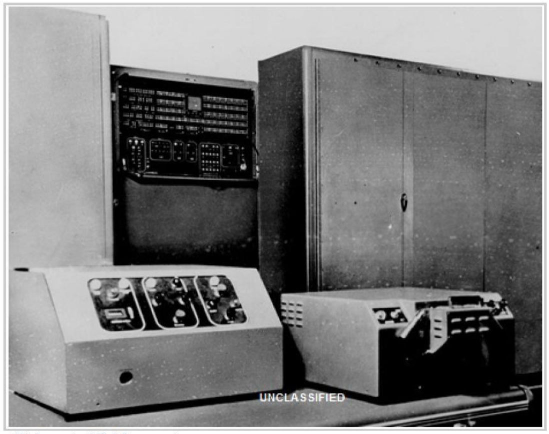
(U) In late 1947 funding -- big money for its time -- was arranged for a "super bombe" nicknamed HIAWATHA to exploit cryptanalytic breakthroughs on a Soviet machine cryptosystem codenamed LONGFELLOW. However, in April 1948 the Soviets, apparently tipped to the U.S.-UK breakthrough, ceased using LONGFELLOW. Plans for HIAWATHA were scrapped. A second electronic device known as PLUTO, which was under development, was finished, but turned to other targets.

(U) The U.S. Army and Navy decided that they needed to concentrate resources on proven types of machines, i.e., comparators, and avoid searching simply for technologic innovation. A history of cryptomachine development in this period put it this way: "The devices did not have to be very intelligent, nor did they have to be multipurpose. But they had to be fast...."

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

[redacted]

(U) One Soviet machine system still seemed vulnerable (the Americans and British called it ALBATROSS), and the services tasked the company ERA in Minnesota to produce a machine capable of searching a day's worth of ALBATROSS intercept in one week. ERA delivered two prototypes, called ROBINs because they performed "round robin" searches. The ROBINs had photoelectric readers that compared characters on punched paper tape at a speed of 5,000 characters a second.



(U) An early ATLAS computer.

(U) Solomon Kullback, one of the Army's senior supervisors of cryptanalysis, wanted 40 ROBINs. The army eventually got 15: they were costly. The ROBINs ran for about five years, but produced little. ALBATROSS was never exploited.

(U) Earl Stone, director of the Armed Forces Security Agency, NSA's predecessor agency, initiated a program to build a computing device 1,000 times faster than existing machines. The device, to be called NOMAD, would use magnetic drums for data storage, and be able to execute some cryptanalytic steps.

(U) AFSA awarded a contract to a major U.S. computer company in 1952. The company's initial plans seemed to promise full achievement of AFSA's requirements. However, the company encountered financial problems and disagreements among members of its engineering department. AFSA (and, later, NSA) did not have any personnel it could dispatch to the company to help oversee the project.

(U) NSA decided it needed to find a way to cancel the contract, and in mid 1954, it announced that delays in NOMAD development put it too far behind in technical capabilities. It concluded the project.

(U) NSA was left with nothing but an expensive prototype machine for all these efforts.

(U) The early development of machine support to cryptologic operations was filled with false starts and confusion. But the experience, despite the problems or, perhaps, because of them, seems to have had a beneficial effect. Within six years of NOMAD's failure, NSA, working with a contractor, would develop a general purpose computer that achieved all its cryptologic goals, and, moreover, served as a prototype for a commercial computer that dominated the market outside government.

(U) The history of early computer development is told in *It Wasn't All MAGIC*, by Dr. Colin B. Burke. Read Burke's CCH cryptologic history here.

(U) To discuss historical topics with interesting folks, visit the Center for Cryptologic History's blog, History Rocks ("go history rocks").

(U) Have a question or comment on *History Today*? Contact us at: DL cch or [redacted]

Information Owner [redacted]
Page Publisher [redacted]
Last Modified: February 8, 2016
Last Reviewed: February 8, 2016

~~DERIVED FROM: NSA/CSSM 1-52, DATED: 20180110, DECLASSIFY ON: 20430110~~
UNCLASSIFIED

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

[redacted]