DISPOSITION FORM

SECURITY CLASSIFICATION (If any)

~~CONFIDENTIAL~~

FILE NO

SUBJECT Open source mention of use of electronic computers in cryptography

TO SEC
Attn: Mr. Lanham

FROM PROD-0411

DATE 8 October 1957 COMMEN

H Levenson B578/R1141

1. In re your request for previous mentions in open source material of the use of electronic computers in cryptography, the following items are submitted.

An article appearing in U.S. News and World Report, 22 October 1954, p. 12, discusses former NSA employee, Joseph S. Petersen, Jr., and the agency for which he worked. It mentions that "a major job of the agency that employed Mr. Petersen for 13 years is to break foreign codes, a job in which it uses electronic 'brain' devices."

Mr. John Kobler, writing in Colliers, 28 October 1950, p. 48, on the subject of cryptography, states that "there is a possibility that the electronic principles of our giant mathematical calculators can be adapted to cryptography."

S/S FRANCIS A RUPP
Chief, PROD-0411

Declassified and approved for release by NSA on 09-25-2013 pursuant to E.O. 13526

REF ID:A40399

~~CONFIDENTIAL~~

Open source mention of use of electronic computers in cryptography

PROD-0411 8 October 1957

H Levenson B578/R4141

SEC

Attn: Mr. Lanham

1. In re your request for previous mentions in open source material of the use of electronic computers in cryptography, the following items are submitted.

An article appearing in U.S. News and World Report, 22 October 1954, p. 12, discusses former NSA employee, Joseph S. Petersen, Jr., and the agency for which he worked. It mentions that "a major job of the agency that employed Mr. Petersen for 13 years is to break foreign codes, a job in which it uses electronic 'brain' devices."

Mr. John Kobler, writing in Colliers, 28 October 1950, p. 48, on the subject of cryptography, states that "there is a possibility that the electronic principles of our giant mathematical calculators can be adapted to cryptography."

S/S FRANCIS A RUPP
Chief, PROD-0411

Incl II

REF ID:A40399

Giant Brains Enter Secret Coding World

By North American Newspaper Alliance

WASHINGTON—Giant machines have moved into the secret military world of codes and ciphers. The electronic brains can turn a message into gibberish as fast as a man can type.

At the receiving end another machine can ungarble the secret message as fast as it can print.

And chances that the enemy will be able to figure out the message in time to use the information are slight—unless some human has goofed.

But humans are humans.

An expert in the field says:

"There can be devised a theoretical machine system that can be mathematically demonstrated as unbreakable—a system with such an incredible order of complexity that there is never a repeat in it."

By a "repeat" the expert means that the same signal is used more than once to stand for the same word or letter in the message.

Machines Offer Time

But the machines have not fundamentally changed what the experts call the art of cryptography (putting message in codes or ciphers) or of cryptanalysis (breaking codes and ciphers). Says one:

"What the machines give us is time and an extremely high number of variables approaching infinity."

The complexity of the machine systems means that no such system can be broken by a potential enemy that does not have machines. But the electronic theory behind the units is common knowledge and everybody who is anybody now has machines.

As one expert put it:

"In this field the offense and defense stay about equal. Five hundred years ago it was pencils against pencils; now, it's machines against machines."

Always Human Error

How are cryptographic systems ever broken?

One method is to jump on a human error.

Example: The Secretary of State hands a diplomatic note to the ambassador of the land of Poo. He sends it to his home government in code rather than 'in the clear." The cryptanalyst has the original text. By comparing it with the gibberish sent by the ambassador he can break the system.

Another example: The operator of a machine system is ordered at intervals to "pull a switch" that changes the system. If he forgets, the monitoring enemy may get some repeats. That gives him messages to decipher in what the experts call "depth." With the help of the machines the system can then be broken.

Playing It Cool on Boardv

REF ID:A40399

~~CONFIDENTIAL~~

NATIONAL SECURITY AGENCY
Washington 25, D.C.

TITLE: "Giant Brains Enter Secret Coding World"		Character of Case Possible Compromise of Classified Information
Report made at Washington, D.C.	Period Covered 4,7,9,10 Oct 57	Report Made by Thomas T. Lanman

Synopsis

An article entitled "Giant Brains Enter Secret Coding World" appeared in the 20 Sep 57 European edition of the Stars and Stripes. The Agency was informed by message from Europe by William F. Friedman. Inquiry reflected article was written by David L. BARNETT, syndicated columnist with the North American Newspaper Alliance, Washington, D.C. Evaluation by PROD-03 and PROD-0441 reflected that the information appearing in the article is within the public domain and would not be classified. Special Operations Division, SEC, contemplates no further inquiry in this matter.

Distribution: Routing: SEC-1 OCC	Incls: Copy of Art. (dup) 20 Sep 57 D/F from PROD-0441 dtd 8 Oct 57 Copy of deletions by Stars and Stripes.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

"Giant Brains Enter Secret Coding World"
Stars and Stripes, European Edition

An inquiry was conducted regarding an article entitled "Giant Brains Enter Secret Coding World" which appeared on the 20 Sep 57 European edition of the Stars and Stripes, to determine who wrote the article, the writers source (s) and/or the disclosure of classified information. A reproduced copy of the article is attached to this report as inclosure (1).

On 7 Oct 57, a copy of the article was transmitted to Francis A. RUPP, Chief PROD-044l, for an official evaluation of the information contained in the articles. RUPP advised that similar information has appeared in the public press. RUPP stated that it is his opinion the information contained in the article is within the public domain, and therefore would not be classified. A D/F from PROD-044l dated 8 Oct 57, subject: Open source mention of use of electronic computers in cryptography, citing publication of articles relative to the article appearing in the Stars and Stripes, is attached as inclosure (2). Dr. Robert H. SHAW, Chief PROD-03, concurred with RUPP on the evaluation of the information contained in the newspaper article.

On 9 Oct 57, Ned AXTELL Jr., Chief CERF-11, was interviewed. AXTELL advised that CERF-11 received a request from the Adjutant General (AG) on or about 18 Sep 57, for a copy of the 20 Sep 57 European edition of the Stars and Stripes. AXTELL stated that William F. FRIEDMAN sent a message from Europe to H. C. BARLOW, R/D Consultant, mentioning the Stars and Stripes article and that AG requested the paper when the message came through AG. AXTELL stated that CREF-11 also received a request for the paper from BARLOW. AXTELL advised they obtained a copy of the 20 Sep 57 edition from the G2, Pentagon, and forwarded reproductions of the article to the AG and BARLOW.

AXTELL advised that Hohn NICHOLLS, CERF-11, Liaison Representative to the Navy and State Departments, contacted the North American Newspaper Alliance (NANA), Room 900, National Press Building, and was informed that the article appearing in the Stars and Stripes does not appear in its entirety. The NANA provided NICHOLLS with that part of the article deleted from the Stars and Stripes edition. The deletion was three paragraphs, a line ("The information was supplied by top Government code experts, whose names cannot be divulged"), and the name of the writer, David L. BARNETT, a syndicated columnist with NANA. A copy of this information is attached to this report as inclosure (3). AXTELL advised a check of the Washington area telephone book reflected that David L. BARNETT is listed as residing at 306 Beachwood Road, Alexandria, Va., telephone number SO 5-6566 and also as a correspondent with offices in the National Press Building, telephone number ME 8-6860. AXTELL stated it is not known if this article has appeared in any other publication.

~~CONFIDENTIAL~~

CONFIDENTIAL

On 9 Oct 57, John NICHOLLS, CERF-11, who obtained the informations from NANA, was interviewed. NICHOLLS advised he went to BARNETT's office to attempt to gain further information regarding BARNETT's sources. NICHOLLS said BARNETT was not in the office but called while he was there. He said he talked to BARNETT on the telephone, representing himself as a member of a Cryptogram Club who was interested in obtaining speakers for the club meetings, and asked if BARNETT could put him in contact with the "government experts" mentioned in the article. NICHOLLS advised that BARNETT cut the conversation short stating that he (BARNETT) could not divulge the names of his sources.

Special Operations Division, SEC, contemplates no further investigation in this matter.

CLOSED

CONFIDENTIAL

By David L. Barnett
The information was supplied by top Government code experts, whose names cannot be devulged.

Another method in what the experts call an "exhaustion attack". Each element in the original language in which the clear message was written. The machines can make millions of such comparisons until the cryptogram makes sense. By that time, the sender has "pulled a switch" and the process starts all over again.

In other cases, fake messages are used. Suppose an enemy is informing its forces of the disposition of ships around some place that in code they call "Jimmy". The cryptographers think "Jimmy" might be the code name for Hawaii but are not sure. So a fake message is put out about the dispatch of a battleship to Hawaii. Sure enough, the enemy informs its forces of the dispatch the dispatch of a battle ship to "Jimmy." The cryprographers then knew "Jimmy" is Hawaii.

Sometimes, the experience and intuition of cryptographers does the job. As one expert put it:

"I have seen people look at a stream of numbers and say, 'I bet that is a five digit cipher run on a multiplex.' So we try it on the Multiplex - which is one type of machine - and by gosh, that's exactly what it is."

Incl III