MEMO ROUTING SLIP

NE[illegible] USE FOR APPROVALS, DISAPPROVALS, [illegible]CURRENCES, OR SIMILAR ACTIONS

	NAME OR TITLE	INITIALS	DATE	
1	1. Costanza	JVC		CIRCULATE
	ORGANIZATION AND LOCATION 2. Breach		2 Dec	COORDINATION
2	3. Bernard			FILE
	4. Egelanian	WE		INFORMATION
3	5. Douglass 7. Yates	WJD		NECESSARY ACTION
	Return to MPRO-4			NOTE AND RETURN
4	for file.			SEE ME
				SIGNATURE

SECRET

REMARKS

MACH 1
HARVEST

SECRET

FROM NAME OR TITLE	DATE
ORGANIZATION AND LOCATION	TELEPHONE

DD FORM 1 FEB 50 95 Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used.

16—43437-4 GPO

SECRET

DEC 1957

HARVEST
IN PERSPECTIVE

SUMMARY HARVEST is the name of a general-purpose computer. The operating characteristics of HARVEST were developed especially for NSA by the IBM Corporation under the provisions of NSA project RANCHO. HARVEST, as now proposed, will be completed in 1960-1 and is expected to cost approximately thirteen million dollars. The processing capability of HARVEST, as evaluated by NSA, is considered equal to one hundred of the best computers now available. On the basis of machine-processing trends, this paper concludes that HARVEST is an essential and economical step in the continued progress of NSA.

EXPANDING ROLE OF MACHINES As a result of the growing complexity of COMINT, the machine-processing effort has undergone a continuous expansion. In effect, the expanding role of machines has a four dimensional aspect: quantity, sophistication, scope, and timeliness. Although the quantity of data that is machine processed has increased significantly, the biggest challenge has come from the increasing complexity of the cryptanalytic problems. A more sophisticated processing system has been a constant demand. At the same time, as a result of the increase in complexity and greater need for timely processing, it has been necessary to extend the scope of machine processing. Expanding into areas formerly satisfied by manual methods, the enlarging scope of the machine effort sometimes encompasses clerical operations and othertimes reaches into the more difficult domain of analysis and decision processes.

Example of Improvement in Machine Process The improvement that has taken place in machine processing can be more readily appreciated from the use of an example. A popular, commercial cipher-machine manufactured by Hagelin of Sweden will be used as the cryptanalytic illustration. In order to avoid a detailed technical discussion, let it be stated that among the many techniques presently used to cryptanalytically attack the Hagelin machine there are a number that can be grouped and considered as two types of techniques. It should be emphasized, however, that cryptanalytic techniques are not normally interchangeable; each technique depends on the presence of certain favorable factors. In the case of the two types selected for this illustration, the application is also limited to those cases where the preliminary phases of the analysis have been successful. The evolution of these two types is graphically shown in Figure 1.

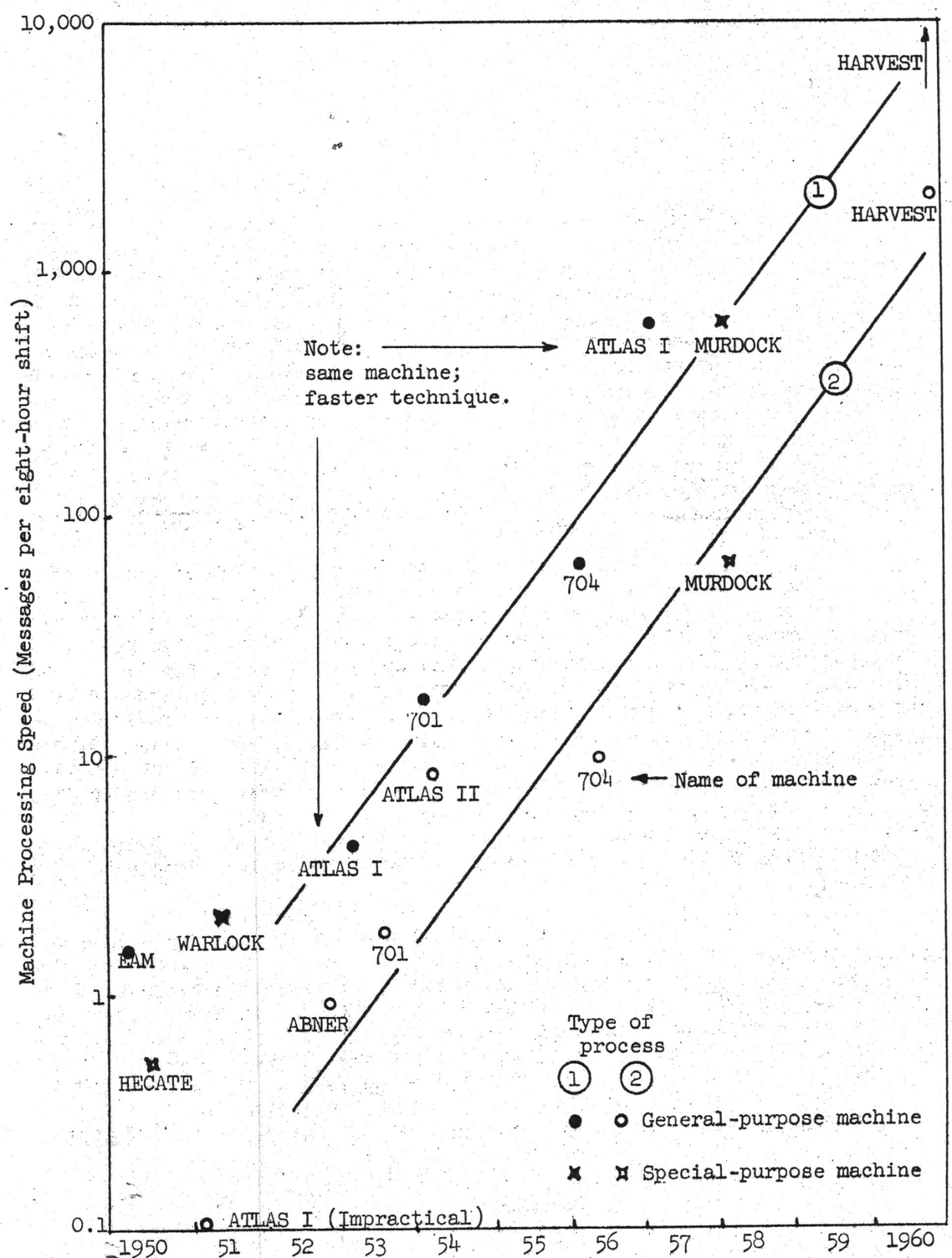

Figure 1. Improvement in Two Types of Machine Processes

SECRET

Although the graphs of this example adequately show the improvements that have been made in processing speeds, the picture is incomplete in several respects. The graphs do not show how the total time of analysis has been reduced--only the machine time--nor do they show the increase in sophistication and corresponding improvement in the probability of success. For example, in 1950, Type No. 1 used about six hours of EAM processing (IBM electric accounting machines), but the intervening manual analysis often extended the total time of the process to a week. Later developments of this technique have gradually strengthened the process, eliminating the need for intervention by the cryptanalysts.

Relationship of Machine and Technique As evident in the foregoing discussion, the machine and technique are complementary factors in the total machine process. Each contributes to the success of the process. Theoretically, a machine with sufficient speed and capacity can find the desired solution by crudely trying all combinations of the problem parameters (brute-force method); conversely, a much inferior machine may find the same solution using a more sophisticated technique. In a practical situation, however, it is usually a case for the best machine and the best technique available. Machines are rarely fast enough for brute-force analysis, and in spite of progress in the development of better methods, many analytic techniques involving exhaustive trials are limited by the speed of the machine, Consequently, in many cases, faster and better machines are the only known method for increasing the chances of cryptanalytic success.

Increasing Complexity of Cryptanalysis Before the discussion concentrates on machines, another aspect of the example will be considered; lest the significant improvements shown in the machine processes give a false sense of confidence. The users of the Hagelin cipher-machine have likewise made improvements. The two graphs on Figure 2 attempt to separate the naive users of the Hagelin device from the more sophisticated users. As shown by the graphs, the cryptanalytic success with communications of the naive user is increasing in proportion to the improvements illustrated in the machine processing; whereas the increasing sophistication of the other users has offset the machine-processing improvements. In other words, the dynamic nature of the problem demands an equally aggressive improvement in the cryptanalytic tools.

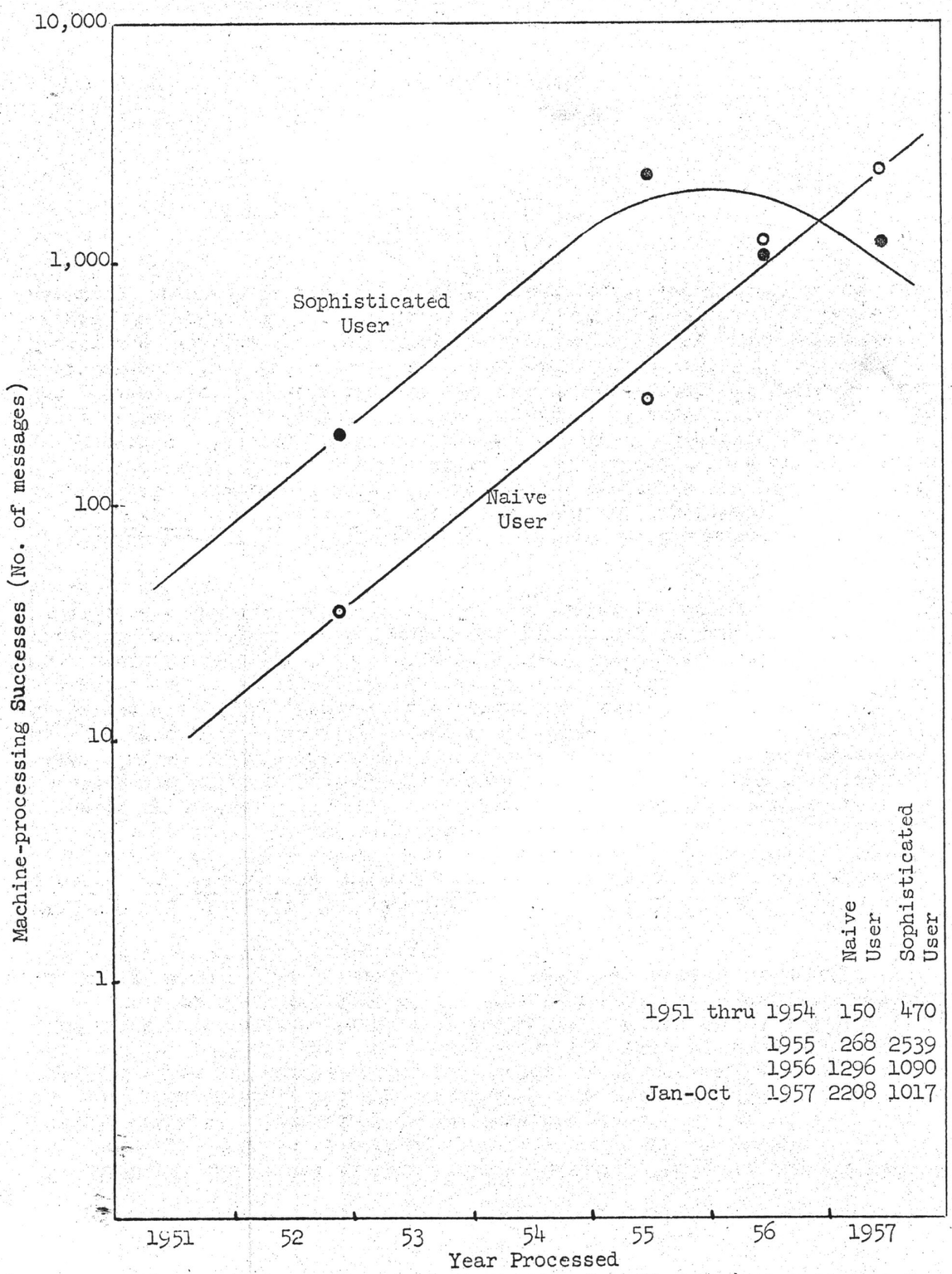

Figure 2. Hagelin Successes from Machine Processing

~~SECRET~~

COMPUTER CAPABILITY TRENDS IN NSA

Recognizing the increasingly important contribution of machines to COMINT, particularly the general-purpose computer, it would be helpful in appraising HARVEST to see what trends have been established in NSA with respect to the general-purpose computer. The use of computers for COMINT dates back to 1950 when the Agency placed into operation a product of its own R/D program--the ATLAS I computer, forerunner of the present Univac Scientific Computers. Since that time, the acquisition of commercial computers and additional R/D developments have steadily enlarged the computing capacity of NSA. The time schedule for these acquisitions is shown graphically in Figure 3.

Processing Capability Index	Name of Computer	Period of Operation: 1951	52	53	54	55	56	57	58	59	60	61	62	1963
100.0	HARVEST													
1.5	709													
1.2	704-3(32K)													
1.0	704-2													
1.0	704-1													
0.2	701													
1.2	705-5													
1.2	705-4													
1.2	705-3													
1.2	705-2													
1.2	705-1													
0.25	702													
0.75	BOGART-5													
0.75	BOGART-4													
0.75	BOGART-3													
0.75	BOGART-2													
0.75	BOGART-1													
0.35	ATLAS II-2													
0.35	ATLAS II-1													
0.5	ABNER-2													
0.25	ABNER-1													
0.035	ATLAS I-2													
0.2	(modified)													
0.035	ATLAS I-1													
0.2	(modified)													

Figure 3. Schedule of NSA Large-Scale, General-Purpose Computers

~~SECRET~~

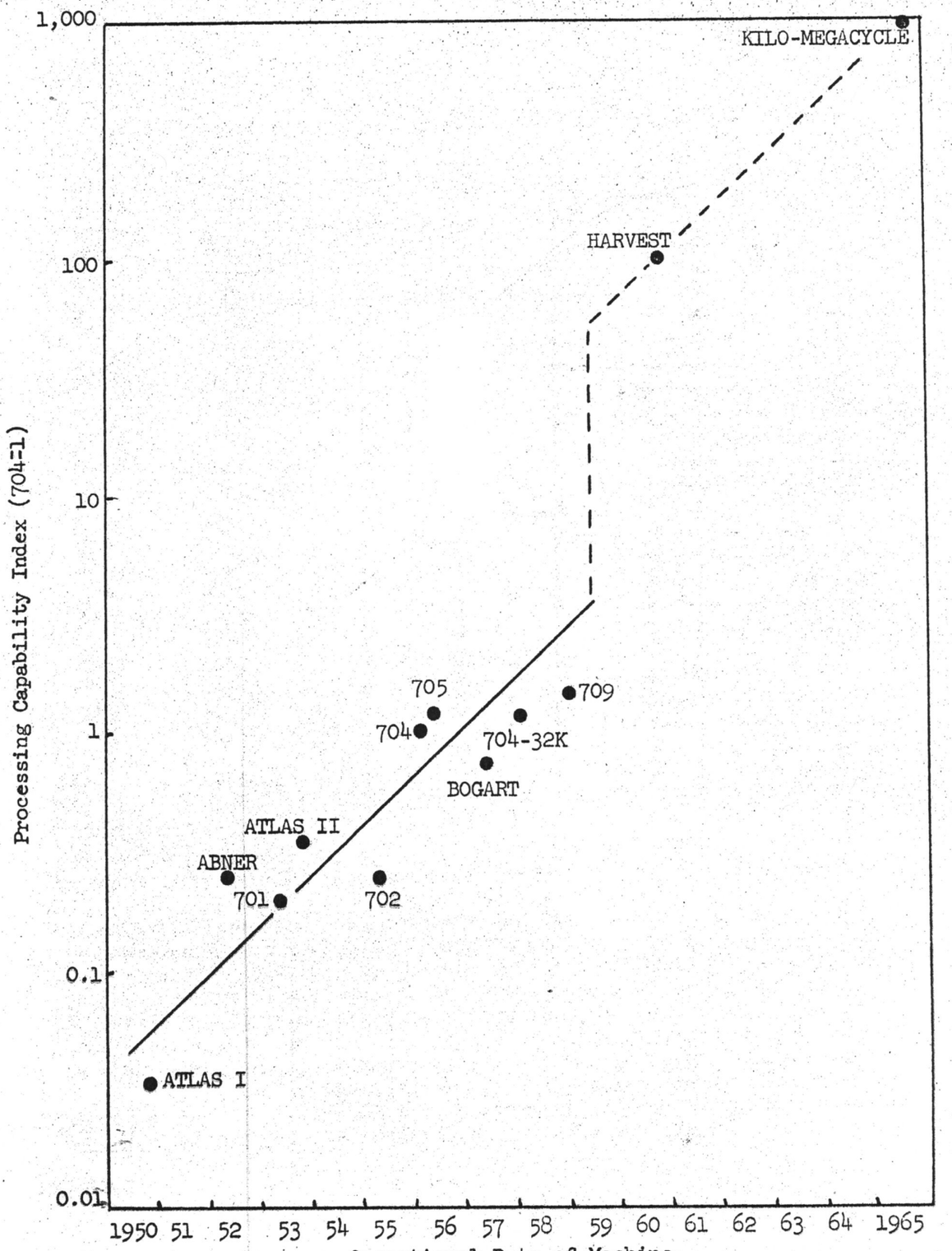

Figure 4. State-of-the-art; NSA Computers

~~SECRET~~

Processing Capability Index What has been the effective increase in the total computing capacity of the Agency as the number and types of NSA computers have increased? Computers differ in capability, so it becomes necessary to find a common yardstick for measuring their processing capability. Although precise comparisons can be made between computers on the basis of, for example, internal processing speed, memory capacity, and output recording; there are also many valuable features peculiar to particular machines that cannot be directly compared. In addition, intangible factors and considerations such as operation reliability, programming efficiency, and manufacturer's assistance tend to confuse the picture. The type of problem processed and the manner in which the equipment is managed must also be considered. Consequently, a complete evaluation of a computer's worth or capability is inflected by many subjective judgments. For the purpose of this paper, the EDPM-704 has been selected as the unit of measurement for rating all of the large-scale, general-purpose computers used by NSA, and this rating will be known as the Processing Capability Index.

State-of-the-art If the Processing Capability Index for each large-scale computer used by the Agency is plotted in relation to the operational date of each computer, a state-of-the-art trend for NSA computers may be observed. This trend is shown on Figure 4. The trend shows that to date there has been a steady improvement in the type of computer used by NSA, and on the basis of this analysis, HARVEST may be considered a break-through in the art of COMINT computers. As a matter of speculation, the trend is extended, and a kilo-megacycle computer (ten times HARVEST) is shown at a point where it might hopefully appear.

Total Computer Capability Although the previous figure shows that NSA has been steadily improving the type of computer it employs, this advance has not been sufficient to meet its processing demands. The Agency has therefore met its computer requirement with multiple copies as well as better types. The total build-up of computer capability in NSA can be shown graphically by using the schedule of computer acquisitions, previously shown in Figure 3, and applying the Processing Capability Index. The results are shown in Figure 5. The trend of this graph is significant from two aspects: the almost linear nature of the trend and the steep slope of the trend. The consistent nature of the trend tends to support the assumption that the demand for computers will continue at the present rate; in which case, the trend indicates a demand for a computer capability equivalent to HARVEST at a time corresponding to the anticipated completion of HARVEST. And again speculating with regard to a kilo-megacycle computer, the graph indicates a requirement for the capability of a kilo-megacycle computer at a time previously selected for this computer on the state-of-the-art graph.

~~SECRET~~

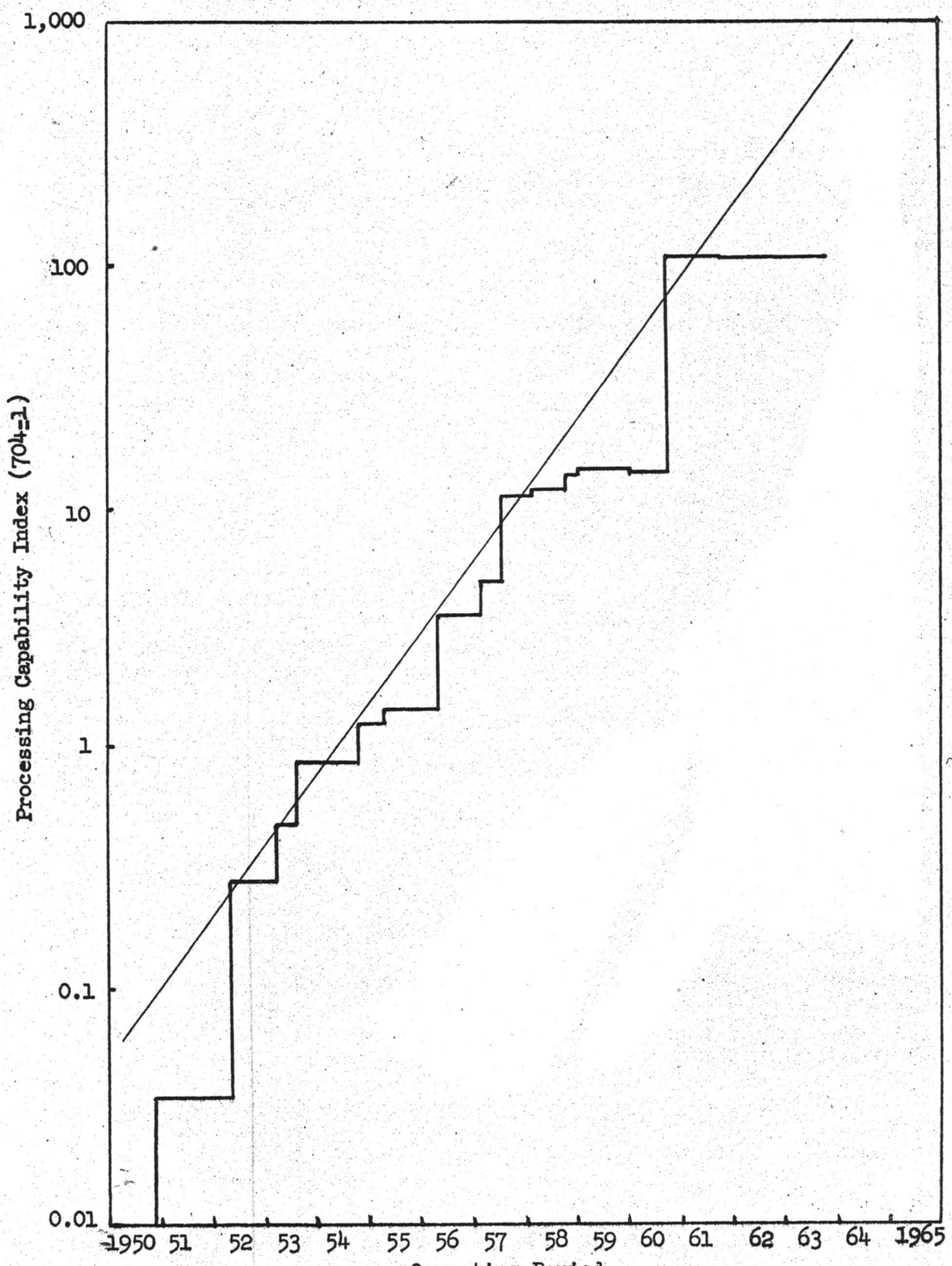

Figure 5. Total Computer Capability

~~SECRET~~

~~SECRET~~

COST At approximately thirteen million dollars, HARVEST will cost as much as eight EDPM-704 computers. Although the choice seems obvious--since HARVEST is rated as one hundred times more capable than the EDPM-704--it is interesting to see what trends have been established for processing-capability per dollar-cost. The processing-capability-per-dollar-cost ratio will be computed for each NSA computer as follows:

$$\frac{\text{(Processing Capability Index of Computer X) times (Purchase Price of EDPM-704)}}{\text{(Purchase Price or R/D Cost of Computer X)}}$$

The purchase price of the 704 computer is used as a multiplier in order to again use the 704 as a basis for comparison. The resulting capability-cost trend for NSA computers in Figure 6 indicates that NSA has been steadily receiving proportionally more for the dollars it has spent on computers. In this respect, HARVEST occupies a favorable position in the general trend.

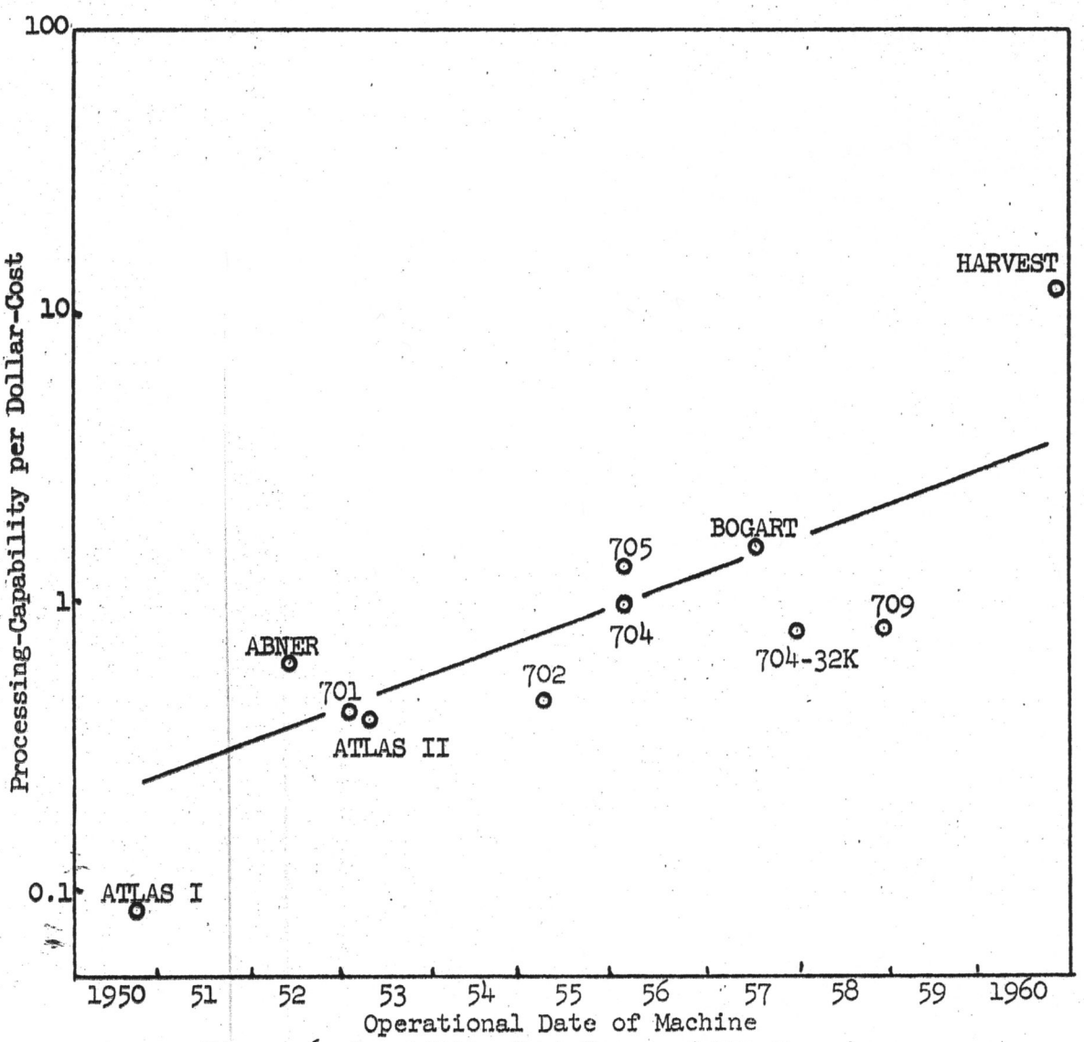

Figure 6. Capability-Cost Trend of NSA Computers

~~SECRET~~

CONCLUSION In terms of present day computers, HARVEST stands out like a giant. Viewed from the perspective of long-range trends, however, the expanding role of machines and the increasing complexity of cryptanalysis brings HARVEST into focus. By the time HARVEST is fully operational, it can be expected that the requirements for machine processing will completely tax the capability of HARVEST. There is, of course, the possibility that commercial equipment will develop to a position in the state-of-the-art comparable to HARVEST. However, the special cryptanalytic features peculiar to HARVEST give it a decided advantage over a machine designed for commercial applications. This advantage, estimated to make HARVEST ten times more effective than a commercial version, and the earlier availability of HARVEST more than offsets the development expense incurred by HARVEST.