Science and Cryptology

BY HOWARD T. ENGSTROM

~~Secret~~

The address at the first meeting of the NSA Crypto-Mathematics Institute.

Ladies and Gentlemen: I hope that my address to you this morning, if it can be called an address, will not be considered as an example of your future proceedings. I am unprepared. Now that I have become a manager, I have given up such childish things as working, particularly in the technical area. I might say it is with considerable regret that I have given up these very fascinating things. The establishment of the Crypto-Mathematics Institute is a great step forward in the progress of the National Security Agency. The address that I shall attempt to give you this morning will not be marked by examples of scholarship and accuracy. In fact, any remarks I make are subject to future revision, since I have not had the time to verify certain dates and facts.

I've chosen as my subject "Science and Cryptology." Of course, a natural way to begin a discussion of this sort is to attempt to define the terms. I have spent a little time during the last few days looking for a good definition of science but, unfortunately, I haven't been able to find one. It is a rather complex concept. It has something to do with observation versus authority. It has something to do with knowledge of natural laws versus superstition. Mr. Bertrand Russell states that modern science is about three hundred years old. I think we all understand approximately what science is and the impossibility of giving a definition of it in a few sentences. On the other hand, one might ask what is cryptology? Cryptology really is older than science in the modern definition. Certainly it existed at the time of Caesar and before. It has essentially two parts to it, as you all know; one is the concealment of your meaning from a possible enemy and the other is unraveling the meaning concealed in such a message or such a writing. I believe that the impact of science on cryptology probably started in this century. I suppose one can blame a great deal of our troubles on Marconi, or go further back to Hertz and perhaps even to Maxwell and Faraday, who discovered the natural laws that enable us to convey meaning through electromagnetic phenomena. Marconi and the radio came in in the early 1900s, perhaps 1910–1914. They made the problem of the cryptologist somewhat more complicated, in

Approved for Release by NSA on 01-07-2008, FOIA Case # 51551

that he no longer had a piece of paper delivered to him which contained some meaning, but had to plumb the depths of the atmosphere to extract his raw material. Many other things which had an impact on cryptology and might be called scientific, happened in this century. For example, in the early twenties, one of the achievements was the invention of the flip-flop circuit. Two men, Jordan and Eccles, in 1919 got out a patent on a circuit involving two vacuum tubes. This circuit had the remarkable property of having two states which could be changed just as you turn off and on an electric light, and this could be done in a matter of microseconds. Here is an example of fairly pure science. What use can be made of such a device triggered by electronic pulses at microsecond rates? Electronic counters making use of the Jordan-Eccles flip-flop circuits were developed to considerable perfection in the thirties and used in the study of cosmic ray phenomena.

Things happened in the field of cryptology during this period of which perhaps the most significant was the introduction of the wired wheel, which you are all familiar with. In the early twenties, an old gentleman named Hebern from California came to the Navy Department with some drawings on a piece of wrapping paper indicating the original form of a wired-rotor device for use in encipherment. During the twenties and the thirties, the use of wired-wheel machines extended considerably and in World War II, of course, they were a principal means of encipherment. Now, through the introduction of wired wheels in cryptography, the necessity for the use of advanced techniques in solving some of these devices became evident. When I came into the Navy in 1941, I was presented with problems involving the solution of a German cipher machine which was based upon the wired-wheel concept. This required the application of very high-speed techniques. During World War II, we built approximately 150 large-scale electronic devices, including electronic counters, to solve the cryptanalytic problems imposed upon us by the use of wired-wheel machines. I might say that our successes were considerable. The tantalizing thing about the situation in 1941 and 1942, particularly in the Battle of the Atlantic, was that although we knew how to solve the problem, principally from researches carried out by the British, a tremendous amount of equipment was required. It took us two years to get this equipment into operation, and during this period, of course, the number of sinkings in the Atlantic was enormous. We were struggling to create something in the development sense and in the production sense, that would solve problems which we knew very well how to do. On the cryptanalytic side, the problems in World War II were extremely challenging, and we developed a number of original cryptanalytic methods based upon the capability of performing operations at these very high speeds. We

explored many methods of handling these problems. [redacted] Many physical scientific ways of doing the job were explored. We had a great deal of work at the Eastman Kodak Company in which recording was done with spots on film, and scanning by optical means; we did the digital work principally at the National Cash Register Company; we put forth every effort to explore all possible means of solving these cipher problems.

It was not only in this area that science had an impact on our successes in World War II; we also became increasingly conscious of the problems of propagation. In 1942, the British sent over a delegation who were quite disturbed at our lack of knowledge of the upper atmosphere, the "E" layers and the "F" layers and the phenomenon of ionic reflection. Admiral Redman, who was then Chief of Naval Communications, commissioned me to form some sort of organization to explore these phenomena. I managed to get started an organization called the Inter-Service Ionospheric Laboratory, which has since become the Central Propagation Laboratory at the Bureau of Standards, where phenomena of propagation through the upper atmosphere are studied. Sounding stations in many places were established in order to determine the heights of various layers, the maximum usable frequencies, the optimum assignments of our intercept positions—the problems became quite intricate. We studied such problems as identification, [redacted] problems of direction-finding, which are still with us, and location of transmitters through various means of detecting phase differences,—times of arrival. In other words, the problem of cryptology in World War II involved not merely a matter of reading some ciphers on a printed page, but had become an extremely scientific matter of extracting information from the atmosphere around us by the use of all possible scientific means available. At the end of World War II, everyone appreciated the necessity for the application of modern science to NSA problems.

In the late forties, NSA established the Scientific Advisory Board. The best scientists in the country have been called to see if they could help us and suggest ways of analyzing some of our complex problems. We were extremely fortunate, for example, in having a person like John von Neumann, who was considered one of the outstanding mathematicians of his time, as a member of our Scientific Advisory Board, and I could mention many more names of outstanding individuals in Science who have examined our problems. We have ourselves been searching for new scientific methods of attack. A project was started at the University of California at Los Angeles, in an organization

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

called SCAMP, in which for three months each summer a group of outstanding mathematicians get together to consider our problems in the broad sense. [redacted] The mathematical advisory panel of the Scientific Advisory Board has examined our work. They have said that, to their knowledge, there exists no discipline in mathematics having a potential application to our problems that has not been explored, and explored in an extremely efficient way. [redacted]

We have tried to apply many disciplines of mathematics to our field. It seems fairly elementary that the science of group theory should be applicable in our business, which is concerned a great deal with permutations, which certainly form a group, but the efforts to apply group theory to our problems have not been particularly fruitful. Group theory does not seem to contain the key to the things that we want to do.

Another thing that has happened to us in the period since 1946 is the tremendous development of the communications art; the problems of searching for and extracting from the ether the things that we are interested in are becoming extremely difficult. We are faced with problems of speech encipherment, facsimile encipherment, television privacy, IFF, and data links for the control of aircraft. These many new forms of communication mean that it is essential to maintain a very forward scientific posture. We have tried to see whether there are any implications of the Information Theory as developed by Nyquist and Shannon which will assist us in our attempts to find meaning in these various transmissions. The problems of communications intelligence and those of what we call electronic intelligence, or ELINT, are becoming more and more merged. The distinction between what communications and what control signals are grows increasingly fuzzy.

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

With these remarks, I hope that I have succeeded in establishing some relationship between the progress of science and the problems of cryptology, both in the cryptographic and the cryptanalytic sense. NSA can be rightly proud of its position in stimulating research toward its mission. We had a considerable part to play in the development of the modern internally controlled calculators, the large-scale digital computers. I think the first large-scale digital computer in operation was the 1101, which was essentially designed by NSA people. They played a tremendous role in the development of these large-scale computing devices. Now also in the last years we can be justly proud that we have stimulated people like [redacted] who have pioneered in the low temperature cryotron in connection with digital computers. We pioneered through one of our people, [redacted] the work in deposition of films by evaporation for use in the magnetic memories. NSA has played a central role in many of these basic researches in computation. Now, the question always arises in connection with budgets and money: is it necessary for NSA to sponsor this basic research? Why can't institutes like the National Science Foundation, the Office of Naval Research, and so on, take care of this fundamental progress in science which is necessary to us? Why do we have to spend our money for this sort of thing? In fact, when I first arrived here, I got into trouble with the Bureau of the Budget because R/D had been spending some of its money in support of solid propellants for rockets, and this seemed to be a bit far-fetched. The reasons for it were principally good, and our interest in the upper atmosphere was such that we wanted to get some instruments up there to see how things are. However, I couldn't establish the justification for NSA's supporting work in solid propellants—we must stick more closely to our own last.

Now we are definitely supporting certain things in the way of basic research. The needs of NSA in high-speed computing are unique. As a result, we have established a project called LIGHTNING in which we are exploring the possibilities of computation [redacted] I might say that we are doing this in a rather free-hand manner at the moment. We have three major companies engaged in the field: RCA, IBM, and Sperry-Rand, who are going their independent ways. We feel that we should let them go for a year or eighteen months and then see if we can figure out which is the most promising approach and try to head the work in that direction. The Laboratory for Electronics at M. I. T., under Professor Wiesner, is participating to a smaller extent in this program, as is Philco with its work in connection with special transistor devices. The work in

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

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

connection with the ~~LIGHTNING~~ project [redacted] A year ago, we were highly skeptical as to whether speeds of this order of magnitude could be achieved. Now, I should say, it looks quite possible that at the end of the five-year program we shall indeed be able to construct computers that operate with this speed. We are now doing another thing to promote the application of science to cryptology. We have recently had a committee looking over our work, reporting to President Eisenhower, under [redacted] of the Bell Laboratories. The first recommendation that [redacted] made in his report was that there be established an Institute outside of NSA devoted to basic research problems; an Institute with an academic atmosphere which would not be subject to the tremendous pressures to which you all are subject—pressures to solve immediate problems as against thinking about the long-range future of the art. A report has been submitted to the President, who said by all means to set up such an Institute. We are now in the process of doing so. I can't tell you where it will be, but we shall establish something of a basic research nature. I hope in the next few months to be able to report that this has been achieved.

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

I trust that I have been able to convey to some small degree the impact of science on cryptology. There are people—and very distinguished people—who still feel that cryptology is an art. I think it is an art, but I don't see how the results in the modern type of security of communications and electronic dissemination can be achieved without drawing upon the tremendous accomplishments of modern physical and mathematical science.

I might say in closing that I came back from industry partly with the idea that perhaps I could contribute something to the Agency, but I think the principal reason was that I have never worked with such a stimulating group of people as I find in NSA.