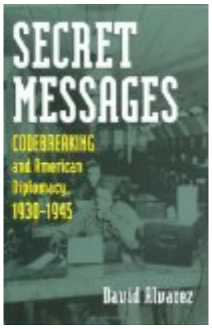
H-Net Reviews
in the Humanities & Social Sciences

David Alvarez. *Secret Messages: Codebreaking and American Diplomacy 1930-1945.* Lawrence, Kansas: University Press of Kansas, 2000. xi + 292 pp. $35.00, cloth, ISBN 978-0-7006-1013-6.



Reviewed by John E. Haynes

Published on H-Diplo (June, 2000)

David Alvarez's ***Secret Message*** is a badly needed history of the origins of modern American signals intelligence. America's National Security Agency (NSA) has a budget said to match that of the CIA, possesses some of world's most advanced computers, and employs some of the nation's most skilled linguists, scientists, and mathematicians because for more than fifty years American policy makers have wanted and used its product. Broken codes are no more a faultless source of information than any other, but any sophisticated policy maker seeks information from a variety of sources and checks one against another when making a judgment. And both American and other policy makers have come to value signals intelligence as one of the sources that they would be foolish to exclude from their judgment. Many historians, however, have excluded it from theirs. Partly this is due to ignorance, and Alvarez is an excellent way to end that situation.

While one can find institutional continuities in cryptanalytic intelligence activities in some European states going back hundreds of years, American involvement with such matters has been episodic until well into this century. From the American revolution onward, Americans have hastily pulled together people and mechanisms to break codes under the press of war, but once peace came, the wartime arrangements dissolved. When the next emergency occurred, the Americans started over, if not from point zero, then close to it because no institutions had carried on what had been learned. This deficiency grew progressively serious as the increase in potential intelligence value of intercepted messages grew over time as more and more diplomatic and military communications were electronic, first telegraph and then radio, with much greater opportunity for interception.

NSA began with that sort of cycle. So ill-prepared was the American Army to deal with signals intelligence in World War I that it initially accepted the offer of George Fabyan, a rich and somewhat eccentric patriotic businessmen, that the cipher department of his private research laboratory take on much of the government's code breaking work and the training of Army officers in cryptology. Fabyan had earlier established his cipher department (an excellent one) in order to examine Shakespeare's plays for evidence that they had actually been authored by Francis Bacon. The Army soon established its own cipher bureau under Herbert Yardley, a State Department code clerk who had taught himself codebreaking. When the war ended, most of the government's code breaking operations ended, but in a partial break in the cycle, Yardley's bureau, although drastically cut back, continued to operate with small subsidies from both the Army and the State Department. Yardley's bureau had some successes, notably the deciphering of Japanese diplomatic cables, which provided Secretary of State Hughes insights into the Japanese negotiating strategy at the 1921 Washington Conference on the Limitation of Armaments. But the bureau's small size and limited support from other agencies, which failed to provide the vital raw material of intercepted messages, starved it. Its productivity shrank, and it was already moribund when Secretary of State Stimson, who thought diplomatic code breaking unethical, cut off State Department funding in 1929.

With Yardley's bureau dead, the Army decided to establish its own cryptologic agency, initially called the Signals Intelligence Service (SIS). And once more the cycle started over, not from point zero, but close. The Army picked up the files but none of the personnel of Yardley's old Cipher Bureau and instead turned to William Friedman, a product of Fabyan's private cipher laboratory who had spent the 1920s working on cryptography (making codes) for the U.S. Army rather than breaking codes (cryptanalysis). The SIS got under way in 1930 with a staff of seven, of which only one, Friedman himself, had a background in cryptology. The rest of the staff consisted of four former high school teachers, a stenographer and a gardener. The cipher bureaus of first rate and second rate European powers in the 1930s were all larger and technically more sophisticated than the tiny SIS. Yet by the end of World War II the SIS employed many thousands of linguists, intercept technicians, radio and electronic scientists and engineers, code clerks, cryptologists, and cryptanalysts and was regularly reading tens of thousands of ciphered Japanese and German radio messages, chiefly military but some diplomatic as well, that were fed into the American intelligence system.

The history of how Friedman and his half-dozen amateurs first taught themselves cryptanalysis and then taught thousands of others and how the SIS in time became the world's premier code breaking agency is the heart of Alvarez's book. It demonstrates the enormous technical and human resources the United States could bring to bear on a problem if it had reason to mobilize those resources, and given the haste with which it was done, the remarkable skill of the mobilization. There was a good deal of interservice rivalry with code breaking offices of the Navy, the FBI, and others, but the resultant wasted assets and duplicated effort, which might have had disastrous results for a nation with limited technical resources, produced only a regrettable inefficiency largely compensated for by the tremendous resources thrown at the problem. It is also a story of a highly fruitful cooperative relationship SIS forged with Britain's Government Code and Cipher School, hitherto the world's leading code breaking bureau, a relationship only possible due to the congruence of American and British policies and interests. Organization history can be deadly dull, but Alvarez's thoroughly researched and well documented study relates that of the SIS in an engaging manner. Even more given to the MEGO problem are attempts to explain to non-specialists how codes and ciphers are constructed and how they are broken. Alvarez provides as part of his narrative an introduction of cryptanalysis that is understandable and will help non-specialists to have some feel for the esoteric language and daunting intellectual challenges that one faces when dealing with code breaking.

Alvarez notes that in 1996 NSA transferred 1.3 million pages of 1914-1945 cryptologic materials to the National Archives, and this in addition to significant earlier transfers. We now know that signals code breaking was not only an important element in intelligence activities in World War II, but played a vital role in several of the key actions of the war, particularly the battle of Midway in the Pacific and the Anglo-American defeat of the Nazi U-boat offensive in the Atlantic. American success against German and Japanese military communications has been discussed in detail in other works, and Alvarez in this book provides the first comprehensive survey of SIS attacks on diplomatic communications, not only that of Germany and Japan but of many neutral and allied powers as well. A few historians have made use of these deciphered diplomatic messages, but Alvarez shows that there is a very great deal left to be done.

We know far fewer of the details, but there are indications that the importance of signals intelligence to American policy makers increased during the long Cold War. And here the old cycle was thoroughly broken. At the end of World War II, the SIS was not disbanded and its skilled personnel scattered and institutional knowledge lost. While it underwent an initial down sizing, the quick rise of international tensions and the need for reliable intelligence in the uncertain diplomacy and murky international politics of the Cold War quickly led policy makers to rejuvenate the agency, merge other code breaking offices into it, and in the 1950s remove it from direct military control and transform it into the National Security Agency we know today. Lamentably, most Cold War signals intelligence remains classified, but some is becoming public and the volume should grow over time. As historians avail themselves of this new resource, their ability to evaluate its worth and to spot evidence that signals intelligence has influenced policy will be enhanced if they understand the organization context and process that produced the intercepted and deciphered intelligence. David Alvarez's ***Secret Messages: Codebreaking and American Diplomacy, 1930-1945*** is an excellent introduction to that needed background.

If there is additional discussion of this review, you may access it through the network, at https://networks.h-net.org/h-diplo

Citation: John E. Haynes. Review of Alvarez, David. ***Secret Messages: Codebreaking and American Diplomacy 1930-1945***. H-Diplo, H-Net Reviews. June, 2000.

URL: https://www.h-net.org/reviews/showrev.php?id=4223