NYTimes JUN 22 1973

Embassy Burglaries? Old Hat

By David Kahn

OXFORD, England—Breaking into embassies, as a White House official urged doing in papers leaked recently, is not new.

During World War II, Great Britain slipped a safecracker into the Vichy French Embassy in Washington with the help of an attaché there. He removed the French naval code and passed it to an accomplice who photostated it. Within hours it was back in the embassy safe, and the British used it to keep tabs on the movement —or nonmovement—of the French fleet before the 1942 North African invasion.

The White House official, Tom Huston, President Nixon's assistant for internal espionage, revealed American activities in the leaked papers, which dated from 1970:

"The F.B.I., in Mr. [J. Edgar] Hoover's younger days, used to conduct such operations with great success and with no exposure. The information secured was invaluable." Whatever modern burglaries take place are alleged to do so in Eastern Europe, where such crudity is rather more acceptable, against the embassies of the developing nations, who do not have the sophistication to defend against them.

For though embassy break-ins are not new, they are relatively rare. Diplomatic gossip seldom mentions them. Even the Nazis seem to have generally eschewed them. A wide reading of their intelligence archives, a thorough acquaintance with the literature on their espionage and extensive interviewing shows only one case. After several failures, a bug planted in a sofa pillow of an American Embassy finally produced intelligible discourse. But it lasted only a short time before war ended it.

One reason for this rarity is that the risks, both moral and practical, are too great. An embassy burglary shatters tradition and treaty. The ancient world regarded the person of a diplomat as legally invulnerable: *"Sacra sunt corpora legatorum,"* wrote Varro. States extended this immunity to the residences and offices of the diplomats when permanent diplomacy evolved during the Italian Renaissance. And the Vienna Convention on Diplomatic Relations reaffirmed in 1961: "The premises of the mission shall be inviolate. The agents of the receiving state may not enter them, except with the consent of the head of mission."

Furthermore, burglaries can backfire. In 1943, the Office of Strategic Services, the American wartime spy agency, searched the Japanese Embassy in Portugal. "As a result the entire military attaché Japanese code all over the world was changed," wrote Army Chief of Staff George C. Marshall, "and though this occurred over a year ago, we have not yet been able to break the new code and have thus lost this invaluable source of information."

The other reason for the rarity of break-ins is that different means produce the same results without these risks. One such means is espionage. The Italians obtained the American "black" code in 1941 not by entering and cracking a safe but by getting a copy from an Italian Embassy employe. Another means has long been codebreaking. This is desk work, easy to keep secret, and governments can construe §485-7 of the Radio Regulations of the International Telecommunications Union as at least not prohibiting communications intelligence.

Starting in World War II, and lasting until five or ten years ago, the interception and surreptitious reading of foreign messages produced the most and the best secret intelligence that major nations obtained on others. The cipher machines and codebooks of those days could not withstand concentrated attack if they had encrypted a heavy volume of text. Codebreaking led to the American victory at Midway, the mid-air assassination of Admiral Isoruku Yamamoto, and the winning of the Battle of the Atlantic.

Of course, even then the one-time pad or tape, the one absolutely unbreakable system, preserved the most important secrets of the most sophisticated nations. Nobody read Russian diplomatic messages after 1933, when the Soviet Union introduced that system. But administrative, distributive and financial problems greatly restrict the system's use. Consequently, many nations fell back on other systems, often those of World War II. Though more practical for heavy network communication, they could be—and were—broken.

One of the most successful codebreaking organizations of those postwar years was the National Security Agency. It and its armed forces affiliates grew to 100,000 persons, assembled more computers in one place than any other institution, and read the secret messages of dozens of nations. It drew the gratitude of at least one American ambassador to the United Nations and saw one of its cryptanalysts decorated by a President in person.

But cryptology has advanced, in the last decade or so, to systems that, though not unbreakable in the absolute, are unbreakable in practice. They consist essentially of mathematical programs for computer-like cipher machines. They engender so many possibilities that, even given torrents of intercepts, and scores of computers to batter them with, cryptanalysts could not reach a solution for thousands of years. Moreover, the formulas are so constructed that even if the cryptanalyst has the ideal situation—the original plain text of one of the foreign cryptograms—he cannot recreate the formula by comparing the two and then use it to crack the next message that comes along.

Electronic machines embodying these techniques replaced machines from World War II in the State Department shortly after the Cuban missile crisis. Other rich countries have also begun to use such devices. But poor countries still have not. Consequently, the N.S.A. can no longer solve the high-level messages of the major powers—it has carloads of intercepts of them on sidings at its headquarters at Fort Meade, Md.—but only those of the third- and fourth-rate powers. Their messages, however, seldom provide insights into plans seriously affecting the United States.

Hence Mr. Huston's suggestion to break into embassies: "It is possible by this technique to secure the material with which the N.S.A. can break foreign cryptographic codes. We spend millions of dollars attempting to break these codes by machines. One surreptitious entry can do the job successfully at no dollar cost."

Things are probably not as simple as Mr. Huston envisages. In the nineteen-forties, the Soviet Embassy in Ottawa kept its cryptographic keys in a sealed bag that was placed each night inside a steel safe that was within an eight-room suite, closed by double steel doors and with iron bars and steel shutters on the white-opaqued windows, that was on the second floor of a separate wing of the brick embassy building, which was surrounded by a fence. Today electronic locks and supersonic burglar alarms increase the burglar's problems.

Moreover, once inside, he would find it much harder to obtain information about the cipher system. Codebooks could be photographed. Today's cipher secrets reside in electronic circuits, some of them integrated on a pinhead, some embodied in printed-circuit boards with up to fifteen layers.

The result is that, outside of betrayal, it seems almost impossible to read the secret messages of the major nations, even if the United States wanted to run the moral and practical risks of Mr. Huston's proposals.

David Kahn, author of "The Codebreakers," is a Senior Associate Member at St. Antony's College, Oxford, England.