THE LONDON NEW SCIENTIST
2 March 1972

P. Marriott, John
CIA 3.03.1
CIA 3.03.2

No break in the code war

Orig under Marriott

The business of intercepting and interpreting the radio transmissions of potential enemies grows steadily more sophisticated, more expensive

John Marriott
is the pen name of a retired RN officer who writes on defence matters for British, European and US periodicals

Last week, senior officers of all NATO nations met for a three day conference at the SHAPE headquarters near Brussels to discuss a subject which is commanding increasing attention—electronic warfare. In the words of General Sir Walter Walker, who has just relinquished the command of NATO's Northern Area, "In a limited aggression situation, the skilled use of electronic warfare by Soviet forces could be an overwhelming factor in deciding the outcome of the battle." Interception of enemy transmissions is one of the key elements in electronic warfare.

When the Second World War began, Britain's own intercept organisation, which had done excellent work during the First World War, had dwindled to practically nothing. However, the principles were well known and it was not long before Britain had established listening posts all over the world. Perhaps because the techniques had not been kept alive, Britain's cyphers were singularly insecure and German intelligence was able to break them with little difficulty. At the same time, British cryptographers were able to read many of the German secret messages —so honours were about even.

By 1943, Britain had built up an efficient intercept organisation, known as the 'Y' service. It consisted of a large number of intercept stations, a direction finding net (directed primarily against the U boats) and a headquarters situated in a stately home at Bletchley Park, Buckinghamshire. The 'Y' service grew apace, and by the end of the war no less than 25 000 persons were employed on this work.

The generic term for the business today is Signal Intelligence (Sigint). This is divided into two halves—Communication Intelligence (Comint) and Electronic Intelligence (Elint). The basis of successful cryptanalysis is to have the maximum possible amount of traffic to work on. Comint organisations, therefore, endeavour to intercept as much enemy signal traffic as possible. This may mean establishing listening stations close to an enemy border (or in the air) to intercept frequencies which travel over line of sight paths such as VHF, UHF and microwave, or in good receiving sites at strategic points around the world to intercept high frequency communications. The listening stations themselves can vary between huge receiving complexes, with perhaps 100 or more receivers together with their associated forest of aerials; a UHF receiver in a jeep or on top of a haystack, and receivers in aircraft or satellites.

The intercepted traffic must, of course, be got back quickly to a central headquarters for immediate analysis. Hence Comint organisations have their own communications [illegible] equipped with their own cyphers. The raw intercepted traffic which has been cyphered-up before transmission is decyphered at the headquarters. Using modern on-line cypher machines, this work is nowhere near as laborious as it sounds.

The traffic arriving at the headquarters is subjected to two processes: traffic analysis and cryptanalysis. The former is a method of gleaning intelligence from the scrutiny of traffic passed, without necessarily knowing its contents, and the latter is actual cypher breaking. The very volume of traffic alone may indicate that something is happening, or about to happen; but apart from this, movements of units can often be deduced simply by the manner in which a signal is routed.

Suppose that a warship, whose call sign is ABC, is heard regularly working a Black Sea shore station. Suddenly she is not heard for two weeks; then she is once again picked up, by another listening post, calling a Vladivostok shore station and thereafter she is heard working this station regularly. Obviously she has moved from the Mediterranean area to eastern Russia. The ship could of course change her call sign, but even then it is sometimes possible to recognise a ship's actual transmitter. Transmitters, like typewriters, often have small characteristics unnoticeable to the human senses but instantly detectable by electronic analysis.

Another useful method of recognising a particular unit, so long as the morse code is still with us, is by "fingerprinting" its operators—most of whom have certain peculiarities, one perhaps making his dashes slightly too short, another hurrying over certain letters and so on. By recording messages and analysing them by means of an oscilloscope it is possible to note these idiosyncracies. This useful give-away is, however, gradually being lost as morse code is replaced by teletype and data transmissions generally.

The unbreakable codes

A modern cypher, working on the one time principle, is virtually unbreakable. The simplest form of "one timing" is to code-up the message from a code book into numbered groups. These groups are then subtracted from (or added to) a recyphering table of similar groups, but the groups so used are never used more than once. This system has now been replaced by machines which do the entire process automatically. In fact, it is possible to type out the message *en clair* and the machine will produce the encyphered version as fast as one can type, the one time recyphering tables being fed into the machine on tape, which is then destroyed to ensure that it is never used again. A refinement is to put the process on-line, with the encyphered version produced on [illegible] a teletype transmitter as it is produced.

What is the situation today? Nobody out-

NEW YORK TIMES
17 AUG 1971

P-Beecher, William
China (Taiwan
CIA 3.03.2

Little Strategic Loss Seen In a Pullout From Taiwan

By WILLIAM BEECHER
Special to The New York Times

WASHINGTON, Aug. 16 — Many United States military planners, looking to the possible results of change in Washington's policy on China, believe that a withdrawal of American forces and installations from Taiwan would not substantially weaken this country's strategic position in the Far East.

Senior military men interviewed here said that while they would rather not see a sudden reduction in forces on the Nationalist-held island, they foresaw no dire consequences if political decisions called for withdrawal as urged by Peking.

Premier Chou En-lai of China, in meetings with visiting journalists and scholars in recent weeks, has insisted that the American military presence must be removed from Taiwan if Washington wants more normal relations with Peking.

High American officials have avoided public comment on the demand. But late last month, Secretary of Defense Melvin R. Laird, when asked about the military value of American forces on Taiwan, answered:

"If we are going to perform adequately and carry forward on the Nixon doctrine of partnership, strength and showing a willingness to negotiate, now is not the time to take unilateral actions in withdrawing or in lessening the credibility of our deterrent."

Advantages Outlined

Nonetheless, military planners are assessing the implications of a force reduction on Taiwan if it should be ordered. In their view, Taiwan currently offers these principal advantages:

¶Excellent repair facilities for tanks and trucks used in Vietnam and a relatively close supply base for the Indochina war.

¶A relatively small headquarters to develop joint contingency plans for the defense of Taiwan under the mutual defense treaty between the Nationalist Government and the United States.

¶Extensive communications-intelligence facilities to eavesdrop on military communications on mainland China.

¶Stores of tactical nuclear weapons for use against China in the event of a major war.

Vietnam Pullouts Cited

On the first factor, military planners say that as the United States continues to reduce its troops and activity in South Vietnam, the need for repair and resupply facilities diminishes.

Of the fewer than 9,000 United States military personnel stationed on Taiwan, about two-thirds are involved in the repair and supply effort. Thirty-three C-130 transports, based at Ching Chuan Kang Air Base, fly regular resupply missions to South Vietnam and Thailand.

The Taiwan Defense Command, which is manned by about 200 Americans from all services, works out contingency plans with Taipei under the 1954 mutual security treaty.

Military sources say that if it becomes necessary to reduce this command to a handful of men, they could be based in the United States Embassy, with the others transferred to Pacific command headquarters in Honolulu. These men could shuttle back and forth to Taipei as direct consultations were required.

The planners say that contingency plans do not include the use of American ground troops in any defense of Taiwain. United States military involvement, should it become necessary, would be primarily those of ships and planes of the Seventh Fleet, together with Air Force planes from the Philippines and Guam.

The Military assistance and Advisory Group, which helps train Nationalist soldiers in using American equipment, numbers 300 to 400 men. This group, too, could be sharply reduced if necessary, officials say.

The United States maintains a substantial eavesdropping and cryptographic effort centered at Shulinko Air Base. While sources are reluctant to discuss this intelligence activity, some have suggested that the information it develops—on such matters as the movement of troops and air units within China—has not been all that valuable.

More useful, they say, has been information on the radar frequencies air defense facilities for use in the event of war. Pentagon sources said this sort of information could be obtained just as easily from electronic intelligence planes and ships operating from international waters and air space.

Overflights Halted

Reconnaissance flights over mainland China were terminated in July to avoid any incident that could interfere with President Nixon's planned visit to China. The most valuable intelligence information, however, comes from reconnaissance satellite missions, which are continuing.

Experts say China has been very skillful in hiding military construction from reconnaissance cameras. Railroad spur lines to missile sites were cleverly camouflaged, they say, that it was difficult to confirm China's first deployment of operational medium-range missiles last summer.

Tactical nuclear weapons, primarily nuclear bombs with about three times the force of those dropped on Hiroshima and Nagasaki, are the most controversial aspect of the American military presence on Taiwan.

Three F-4 fighter-bombers able to carry nuclear bombs are based at Tainan Air Base, on detached duty from the Philippines.

Military planners say that in the unlikely event of a major war with China, Washington would probably not want to use Minuteman or Titan missiles fired from the United States since they would have to pass over Soviet territory on the way to China.

Weapons to Leave Okinawa

The bulk of nuclear weapons that might be employed, they say, are Polaris missiles on submarines in the Pacific, bombs stored aboard Seventh Fleet carriers and tactical nuclear weapons on Guam and in the Philippines, Taiwan and South Korea. Additional weapons on Okinawa are to be removed before the island reverts to Japanese control.

"Taiwan, in effect, is an unsinkable aircraft carrier 100 miles from China," one general said. "We'd like to keep some weapons there."

But he and other military officials acknowledged that if the White House decided otherwise, greater reliance could be placed on B-52 bombers operating from Guam.

NEW REPUBLIC

Code Cracking

The specter has been raised of a massive breach in the nation's communications security as a consequence of the publication by newspapers of top-secret, official documents from the McNamara study of the Vietnam war. Mr. Joseph Alsop, for example, finds that "the quantity of 'plain text' published in the *Times* is already so great that the government cryptographers now consider as compromised all the secret messages sent in the same period over the same types of coding machines."

One can defer to Mr. Alsop's familiarity with confidential information, without accepting his judgment on cryptography. Communications security in the US has progressed considerably since World War II. The old "code wheel" machines, popular at post World War II consulates and for low-level Navy ship messages, invited "cracking" in the traditional sense, because they used the same code base every day. Enough messages and skilled cryptographers could break the system. Today, all secret messages are sent by high-speed equipment, and the code is not breakable. The principle in use is that of the "one-time pad" – used up and destroyed page by page. Secret texts are enciphered with a one-time, random selected code to produce the coded message. It is this that is transmitted. If you have the answer in hand, as Mr. Alsop points out, you could find the original "one time" letters. But it is only good for that one message.

22 JUN 1971

Top Secret: A Former Cryptographer Leaks All

By ALFRED L. MALABRE JR.

The government's effort to stop publication of the Vietnam war documents is based in large part on the fact that the material is classified information. Accordingly, the argument runs, its publication is highly detrimental to U.S. interests. Indeed, there has even been criticism that the published material could enable an enemy to break U.S. codes.

Maybe so.

But pardon a former cryptographer if he experiences a twinge of skepticism about the government arguments. During the early and mid-1950s this writer served as a so-called top secret control officer attached to the staff of the top U.S. naval command for the eastern Atlantic, the Mediterranean and Europe. The job chiefly involved enciphering, deciphering and carefully disseminating classified messages to and from the command.

It was an exciting time—because the command happened to be located in London, which in those days was a wonderfully fascinating and absurdly inexpensive place for a young American naval officer, with his sought-after U.S. dollars, to live. The job itself, however, top secret messages and all, was strictly dullsville. The reason simply was that with one or two rare exceptions, the classified messages flying back and forth between Washington and London and London and other places were trivial, long-winded and generally boring.

For the most part, they would have produced a big yawn on the face of any enemy managing to sneak a peak.

A few illustrations from those London days would hardly jeopardize national security in 1971 and might just shed some light on the current charges against The New York Times and The Washington Post.

Perhaps the most remarkable message, for its insignificance, that springs to mind actually involved The New York Times. The precise phraseology cannot be recalled, but the content will never be forgotten: A notice from Washington to the London command informing it that Mr. Hanson Baldwin, military affairs editor of the Times, was planning a trip to London and elsewhere in the area, and please be nice to him.

Another memorable classified correspondence occurred shortly before a change of command at the London headquarters. There was an exchange of coded messages between the incoming and outgoing admirals (each had four stars) to discuss whether or not they should retain each other's stewards. (These were sailors, black or Filipino, who performed domestic-type work for admirals and other high-ranking officers; the jobs included cleaning shoes, waiting on table, making beds and so on.)

A prime example of the long-winded variety of classified message was a weekly report to Washington, encoded and often classified "secret," yet usually composed wholly of excerpts from local newspapers. Often, a cryptographer would have the task of putting into code an editorial that had appeared three or four days earlier in the Manchester Guardian or London Times. Sometimes the weekly reports to be encoded would run half a dozen single-spaced typewritten pages.

The fondness for classifying messages that involved such things as the abilities of a particular admiral's steward or the travels of Hanson Balwin, it appears on reflection, was not only stupid, making unnecessary work for cryptographers among other things, but also somewhat dangerous.

The danger can be illustrated by recounting events in the message center during the 1956 Suez Canal crisis. Because so many messages were transmitted in code during the heat of the crisis, and therefore required extra time to handle, many reports were not being routed to the proper people in anything like a reasonable period. During the peak of the crisis, when the message flow was extremely heavy, many messages designated for "priority" handling were being deciphered two days after receipt. Some "routine" and "deferred" reports were not handled for more than a week after receipt.

Even some urgent messages were not decoded for many hours. (The highest designation—"flash"—was supposed to be reserved for enemy contact reports and never to be in code on the ground that the urgency would allow no time for cryptographic handling. During the Suez crisis, however, "flash" was frequently used—in code and not involving enemy contact—as a means of trying to ram a report through the traffic jam at the London message center.)

In a year and a half of top-secret message work, handling dozens of classified reports daily, this writer can recall only one message that seemed truly vital. It was a report from sources in Turkey during the early stages of the Suez crisis, when British and French forces were staging at Cyprus. It stated that "unidentified" jet bombers had overflown Turkish airspace, heading toward Cyprus. (A subsequent message reported that the planes had turned around and headed back to the northeast, a maneuver that personnel in the message center at the time felt may have averted World War III.)

The criticism in recent days that the publication of the Vietnam papers may somehow endanger U.S. codes may have validity, but just where that validity lies is difficult to fathom.

Even a decade and a half ago, codes became obsolete daily or involved use of "one time" tapes that only the particular sender and receiver. It is impossible to imagine how the publication of the Vietnam papers could possibly jeopardize such

P Ashworth George W.
CIA 3.03.1
CIA 3.03.2
Soc.4.01.1 New York Times

U.S. security controversy flares

By George W. Ashworth
Staff correspondent of
The Christian Science Monitor

Washington

Disclosure of portions of the Pentagon's war record has raised several security issues that go far beyond the war.

Because the issue is Vietnam, the very controversy of that war and the way it was started has tended to overshadow so far the possible security implications of the disclosures in the New York Times.

But officials here see these potential difficulties:

- Some of the material used was originally encoded, at least several items being sent in very classified and closely held forms. Disclosure of these messages in their uncoded form could serve to help other interested nations decipher other messages of the period that might so far have eluded translation.

Beyond that, the information made available could serve to give a great deal of information about U.S. procedures in cryptography.

- The intelligence material disclosed, while not particularly sensitive now in terms of national security, could serve overseas analysts interested in studying how U.S. intelligence operates, and give better insight into methods, procedures, weaknesses, and strengths.
- Some officials believe that the disclosures tend to weaken expectations by other countries that confidences exchanged with officials of the U.S. will remain respected.
- The disclosures may tend to weaken still further respect by the press for security classifications imposed by the U.S. Government. The present trend, reinforced by the New York Times series, is for media organizations or individuals to be their own arbiters over whether something classified by the U.S. Government should remain privileged.

Although top-secret and secret material is supposed to be closely held and limited only to those with requisite clearances and what is called "need to know," materials of a classified nature have often in the past been shared by government officials with representatives of the news media.

Normally speaking, this practice has largely been carried out at the highest government levels in order to help the press understand various situations more fully. It is usually understood that this material should not be publicly disseminated because of its nature.

However, in the course of the Vietnam war there has been a general loosening of long-standing security practices. More and more, persons who disagree either with the war or with other persons in government have felt more free to release material damaging to those with whom they disagree.

This tendency has been compounded by an increasing government willingness, as many officials see it, to classify excessively. Some of the most mundane material is routinely classified. And it is not uncommon for classifications to be given merely to lend importance. This is particularly true of study papers.

Canadian involvement

As a result, a cloud of classification hangs over a great deal of material of interest to the public and perhaps of no great advantage to any national enemy. It is often said jestingly here that a great deal of classified material is secret only from the American people.

Thus the willingness to classify widely, and the accompanying growth of disrespect for classification, have caused problems for the last administration as well as the current one.

Of particular concern now are American relations with foreign countries in the wake of the New York Times disclosures.

Already the Canadians are having an internal argument over the fact that a Canadian diplomat serving on the International Control Commission carried notes from Washington to Hanoi in 1964.

As one source here put it, "The stories have just about finished the Canadians as intermediaries, as well as weakening their faith in us."

The question of governmental privacy has been raised before by other nations dealing with the United States. Just as there are allied nations that the U.S. will not trust with really important secrets, other nations now are making it very clear that they do not believe the U.S. can be trusted with private matters. This viewpoint has been particularly evident lately in relations with the government of Thailand.

If governments cannot trust each other, relations become both more difficult and more potentially dangerous.

e IA 3.03.2
- Doc. 4.01.1 New York Times

Can Soviets crack it?

U.S. code now in danger

(UPI)—Government officials seem more disturbed about diplomatic and espionage consequences from publication by The New York Times of the secret Vietnam war history than by the facts revealed.

Of particular concern to many officials is the possibility that extensive publication of diplomatic and military cable texts might allow the Soviet Union to crack the code of other U.S. communications transmitted during the early 1960s.

"You may rest assured that no one is reading this series any more closely than the Soviet Embassy," one official said.

Others said the series had produced few surprises.

"If The Times had not printed all those texts," one official said, "very little might have been done. Stories about the study — by themselves — would probably not have caused much reaction."

The Times, however, accompanied the three installments with numerous texts of high-level memos and cables. Many were messages between Washington and Saigon or other U.S. diplmatoic and military outposts in nIdochina.

In each case the sender, receiver and date of the message were given just before the text.

No one knows how many of these messages, transmitted in code, may have been intercepted by the Soviet Union. Security experts at the Pentagon and elsewhere operate on the assumption that any of them might have been intercepted.

They also assume that even the most sophisticated code may be broken by a cryptanalyst who obtains a "plaintext," or decoded version, of messages sent in that code. Once a code pattern is deciphered, other coded messages sent during that period — perhaps to entirely different areas and on entirely different subjects — might be read.

For these reasons, verbatim texts of diplomatic and military messages are almost never released and this is why The Times' printing of the texts generated concern.