

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

(U) Vietnam: A SIGINT Paradox (Part I)

(U) The American cryptologic experience with the Vietnam problem demonstrated the complexities of producing SIGINT. Both time and analysis are required to produce SIGINT. There are numerous examples in cryptologic history that demonstrate that the accumulation of knowledge gained through traffic analysis, cryptanalysis, and language analysis and translation should make it easier to produce SIGINT. However, the Vietnam experience demonstrated that study and preparation do not automatically lead to success.

~~(S//SI-REL)~~ SIGINT failures have occurred because we were unprepared for unexpected crises. However, this was not the case in Vietnam. As American involvement in the Vietnam War began to increase during the 1960s, NSA had a distinct advantage compared to the rest of the intelligence community. NSA had been studying Viet Minh (predecessor of Viet Cong and North Vietnamese) cryptology throughout the 1950s. We had both experienced personnel who worked on the problem and extensive knowledge of North Vietnamese cryptanalytic techniques. We recognized that the North Vietnamese were cunning, imaginative cryptographers.

(U) The first part of this two-part article will focus on the 1950s. What did we know about North Vietnamese COMINT capabilities? This article will also demonstrate the cryptographic talents of the Viet Minh and their communist successors. Part II will focus on one explanation of why NSA lost its advantage.

The 1950s: A Decade of Cryptanalytic Study

(U) To appreciate NSA's activities on the Vietnam problem during the 1950s, it is necessary to look at the historical setting. Vietnam has a long history of opposition to dominance by colonial powers. In May 1941 Ho Chi Minh established the Viet Nam Doc Lap Dong Minh, or Viet Minh (The League for Vietnamese Independence) to formalize this resistance. At the end of the war, on 2 September 1945, Ho declared the independence of Vietnam and announced the formation of the Democratic Republic of Vietnam. With the Allies' permission, France reclaimed its colonial hold over Vietnam. Ho reacted by warning the French prime minister, Georges Bidault, in a meeting on 14 September 1946, that "If we must fight, we will fight. You will kill ten of our men, and we will kill one of

yours. Yet, in the end, it is you who will tire.”

(U) After a war which lasted approximately nine years, the French were defeated at Dien Bien Phu and forced to come to terms. However, what the Viet Minh won on the battlefield was taken from them at the Geneva peace conference. The Geneva Accords divided Vietnam at the seventeenth parallel into North Vietnam and South Vietnam. With that division in place, the accords imposed a cease-fire and provided for the withdrawal of French forces from North Vietnam and of Viet Minh forces from South Vietnam within the next three hundred days. New foreign troop placements were prohibited throughout Vietnam, and both the French and the Viet Minh were to withdraw their troops from Laos and Cambodia. Finally, the accords provided for free elections in 1956, with the goal of reunifying the two Vietnams.

(U) South Vietnam did not sign the accords. To preserve his regime, Ngo Dinh Diem, the head of the South Vietnamese government, used this failure to sign the accords as an excuse to cancel the 1956 elections. North Vietnam, on the other hand, remained determined to achieve a united country.

~~(S//SI//REL)~~ NSA certainly had a long history of working the Vietnam problem, although it is difficult to pinpoint the exact date when American cryptologists began to work the problem. According to legend, a navy officer first translated Vietnamese traffic in 1949, during the days of the Armed Forces Security Agency, the predecessor to NSA. After the French-Indochina war ended in 1954, NSA analysts did a retrospective study on old communist traffic. David W. Gaddy, a cryptolinguist who was hired in 1953, reported that he worked on Vietnamese traffic that dated back to 1951. Dr. “Tony” D. Vang Ly, the first native Vietnamese instructor, began teaching Vietnamese to Agency students in 1952.

(U) Vietnamese was a difficult language for NSA students to master. Vietnamese is a tonal (with six tones), monosyllabic language. Moreover, Westerners have to learn a new alphabet consisting of 27 consonants and 12 vowels. The task of mastering this language was particularly difficult in the early 1950s, because there were no Vietnamese-English dictionaries. NSA linguists had to look up a word in a Vietnamese-French dictionary, then consult a French-English dictionary to finish the translation of the Vietnamese word.

(U) Gaddy further explained: “Despite the excellent instruction provided at the NSA school, linguists really had to learn their trade from on-the-job training. Native instructors lacked clearances, so they were never told what jobs we performed. They could not tailor our instruction to job requirements. NSA told the instructors to emphasize reading over pronunciation, which made it difficult to really learn a tonal language.”

(U) Cryptolinguists faced additional challenges. Vietnamese cannot be transmitted by using standard international morse code because of its peculiar letters and the use of accent

marks. The cryptolinguist had to learn the system created by the Vietnamese to express these features in morse before tackling an actual translation. For instance, the vowels u and o appear as simple letters or with hooks. To indicate the use of the letter u with a hook, the Vietnamese operator sent the letters uw. W does not exist in the Vietnamese alphabet so it was available for special assignment. Since uo with hooks is a frequent letter combination in Vietnamese words, the morse operator used the shortcut wow rather than uwow in morse to indicate these hooked letters. Such a system made on- the-job training essential.

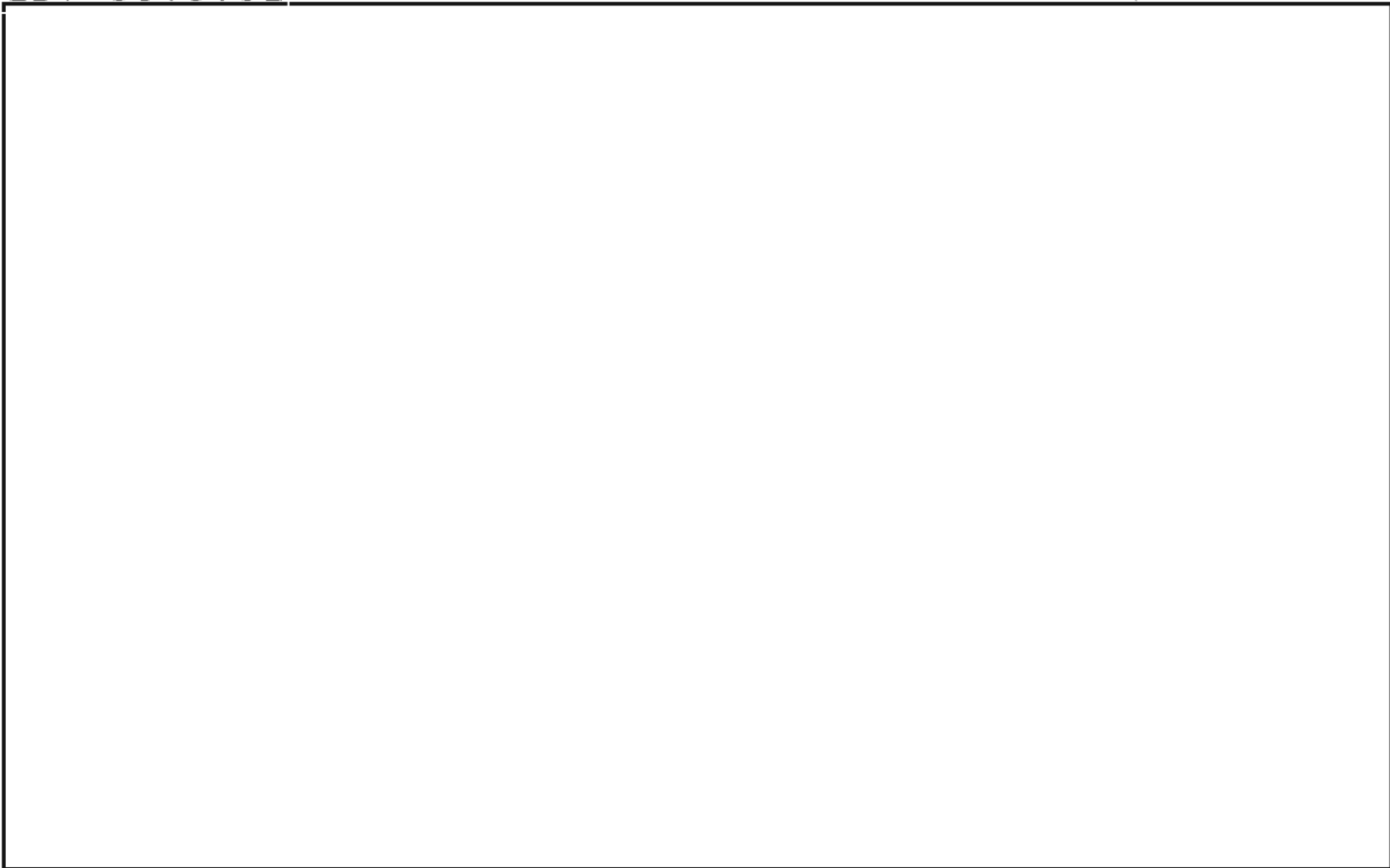
~~(S//SI-REL)~~ During the 1950s, the Viet Minh communications became more sophisticated. Early in the decade, the Viet Minh operated as if they were in the 1930s and 1940s. These communists were bands of guerrillas who were forced to use old equipment from World Wars I and II. Americans reading Viet Minh traffic saw references to German 88 antiaircraft terminology. Gaddy recalled: "During the Dien Bien Phu campaign (1953-54), their traffic had lots of references to howitzers. By this time, there was only one company left in the U.S. that continued to make howitzers. Fortunately, we found them in Fort Carson, Nevada. This company was able to help us with the terminology that we saw in our traffic."

~~(S//SI-REL)~~ By 1957-58, the North Vietnamese were transformed from a poorly equipped guerrilla organization to a regular, standardized military establishment. These changes became apparent through COMINT, which now contained references to military rank and terminology for rockets and missiles.

EO 1.4.(c)

~~(S//SI-REL)~~ Gaddy reported a similar growing sophistication in cryptography: "Through cryptographic changes, NSA analysts suspected that the Viet Minh were being trained in cryptography by the Chinese. They saw greater communication security and the use of more sophisticated techniques in code construction." This suspicion was confirmed by the North Vietnamese in their publication *Essential Matters*, which was translated into English in 1990 (and which is available from the Center for Cryptologic History). The North Vietnamese revealed that the first group of cryptographers studied in China as early as 1950-51. They left in 1950, studied for six months, and returned home in May 1951.





~~(S//SI-REL)~~ By 1959 North Vietnam had organized a unit called Group 559, to begin work on refurbishing the southern infiltration route, popularly known as the Ho Chi Minh Trail. The Ho Chi Minh Trail ran from North Vietnam through the Laotian panhandle into South Vietnam. Later in 1959 the North Vietnamese also organized Group 759 to find ways to supply their southern forces. The extent of this supply and resupply effort was known through COMINT. As Gaddy pointed out, “the depth of our knowledge was evident from activity by the State Department, [which] attempted to acquaint the public with the magnitude of this problem by publishing a white paper entitled 'A Threat to Peace: North Vietnam's Effort to Conquer South Vietnam', in December 1961. This paper was based on previously classified COMINT.”

(U) In 1961, as American advisers began to provide assistance to South Vietnam, NSA analysts knew that our opponents were good at the cryptologic trade and maintained a healthy respect for the cryptologic abilities of the North Vietnamese.

[(U//FOUO) Sharon A. Maneki, Center for Cryptologic History, 972-2893s, samanek]

Content Owner: Feedback

Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR and NZL//X1

~~DERIVED FROM: NSA/CSS MANUAL 123-2~~
~~DATED: 24 Feb 1998~~
DECLASSIFY ON: X1