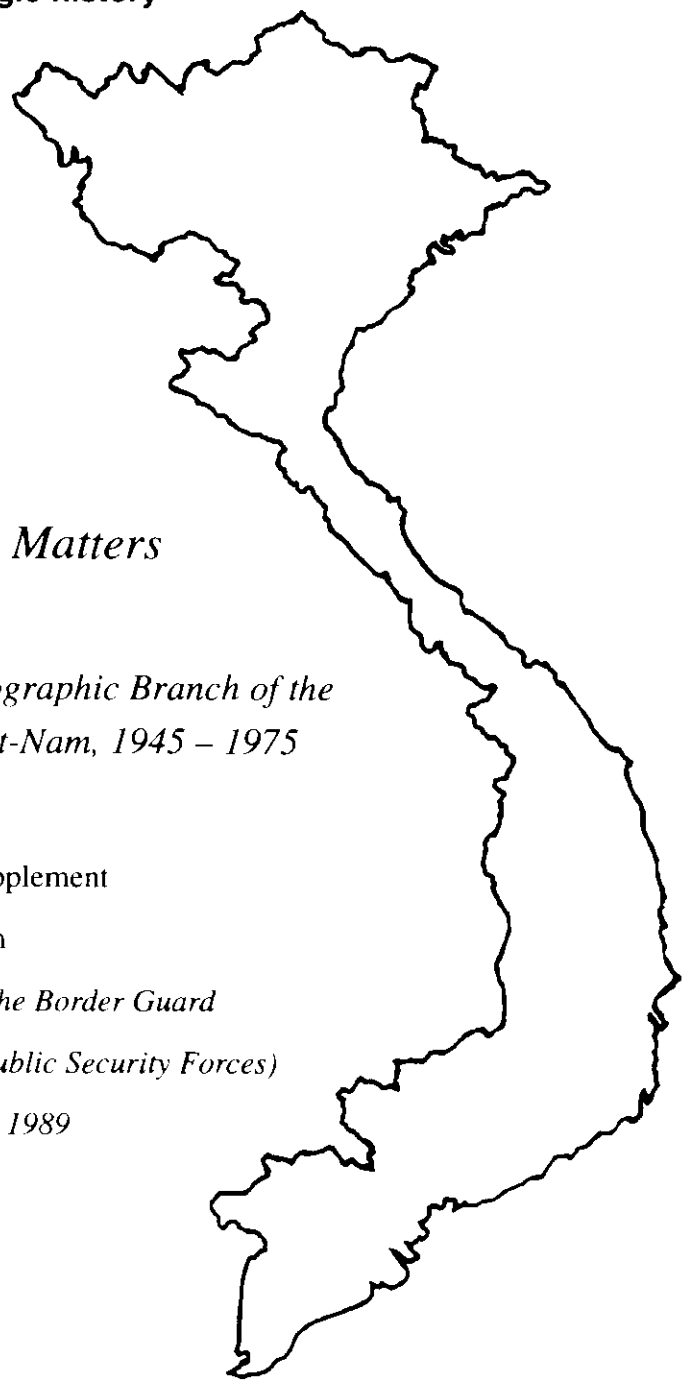
special series
number 5

united states cryptologic history



Essential Matters

A History of the Cryptographic Branch of the People's Army of Viet-Nam, 1945 – 1975

with a supplement

on

Cryptography in the Border Guard

(formerly the Armed Public Security Forces)

1959 – 1989

CCH–E32–94–02

national security agency
central security service

Essential Matters

A History of the Cryptographic Branch of the People's Army of Viet-Nam, 1945–1975

with a supplement

on

Cryptography in the Border Guard
(formerly the Armed Public Security Forces)
1959–1989

UNITED STATES CRYPTOLOGIC HISTORY
SPECIAL SERIES, NUMBER 5

Translated and Edited
by
DAVID W. GADDY

Center for Cryptologic History
National Security Agency
1994

Foreword

The former Democratic Republic of Viet Nam (DRV – now the Socialist Republic of Viet Nam) emerged from revolutionary conspiracy, with roots in native independence movements as well as international communism. Ho Chi Minh – the name itself an alias – led what was originally a small band of revolutionaries in the period between the two world wars. Operating during the Japanese occupation of the 1940s as an underground resistance group (with incidental support from America's OSS) and continuing through the thirty-year struggle to establish the independence of the Democratic Republic of Viet Nam, first against the French, then the noncommunist Republic of Viet Nam, and, finally, the United States and its allies, his followers made secrecy a way of life. The leadership had noms de guerre (Vo Nguyen Giap, for example, was VAN). Given that background, the universal military penchant for abbreviations, acronyms, and nicknames, and a Sino-Vietnamese literary tradition that admired obscurity or hidden meaning, they produced an extraordinarily rich manner of expression, intended only for the initiate. Added to that was cryptography – secret writing – the art and science of codes and ciphers.

Essential Matters is a translation of a 1990 Vietnamese publication, *History of the Cryptographic Branch of the People's Army of Viet Nam, 1945–1975* (Hanoi: People's Army Publishing House). A supplement drawn from the *History of the Cryptographic Branch of the Border Guard, 1959-1989* (Hanoi: The Staff, Border Guard HQ, 1989), an organization originally known as the Armed Public Security Forces, extends the coverage by fourteen years, into the cipher machine era, and provides a natural complement. The Vietnamese of the titles (*co yeu*) literally means vital, essential, important, matters, with a heavy overtone of confidentiality or secrecy, as opposed to the normal Vietnamese word for cryptography, *mat ma*--the original name of this element of the People's Army of Viet Nam (PAVN), once known in the West as the Viet Minh army. (The American reader must bear in mind that "army," as used in the title, PAVN, more closely corresponds to "armed forces" in the United States, for air and sea components are subsumed in the term.) As a result of a decision made at the Eighth Army-wide Cryptographic Conference in February 1951, and in light of the international character assumed by Vietnamese interests in Laos and Cambodia, the euphemism was adopted by the security-conscious Vietnamese. But it was a euphemism that contained within it a reminder of the virtual mania for secrecy that elevated Vietnamese cryptography to such a critical role.

In this translation, both *mat ma* and *co yeu* are rendered as "cryptography." Personnel engaged in this pursuit are presented as "cryptographers," "cryptographic personnel," or even by the less elegant term, "cryppies." Women, as well as men, performed the function. Their organizations are rendered as "cryptographic," "cryptography," or simply "crypto."

Because of a century of French colonial domination in which the Vietnamese language was displaced by French, the generation of revolutionaries – or, at least, the younger ones they recruited--had little scientific knowledge of their own language, especially as a basis for applying cryptography. Learning as they went, by trial and error and precious few

publications, they developed an indigenous cryptography, until, by the early 1950s, men trained in China returned to share the benefits of their learning. Presumably under Chinese influence, the native cipher systems were gradually superseded by enciphered codes. Always conscious of enemy cryptanalytic probing, improvement in maintaining secrecy of message content was a driving concern, adjusting for the educational level of their personnel and the circumstances in which they found themselves, with respect to geography, climate, and equipment.

The evident willingness of Hanoi authorities to break their traditional silence and permit the public reading of this work may be interpreted in several ways: perhaps the rigid protection of all aspects of Vietnamese cryptography has abated, at least for the period covered by these two books, a period that ended nearly two decades ago. Perhaps the techniques described are now passé. And in any event, as time moves on, the anonymous crypto-warriors age and die: for many, this was the last opportunity to see their names in print, and to share in the telling of their unsung role in winning the final victory. In any event, the result is an extraordinary contribution to the history and literature of cryptography. It affords insight into a previously hidden aspect of the military life of a people who, for a few years, held the center stage in world attention. With the passing of that generation, it preserves the names of participants, men and women who once led lives of intentional and enforced obscurity. It tells us of their training and their accomplishments, their hardships and suffering. It tells of the toll they paid – some 500 cryppies paid the supreme sacrifice, nearly 10 percent of those on duty as of 1972. It forms the tradition for the coming generations.

These men and women had created an effective communication security system literally "from scratch." More conversant with French than their native language (which now represented nationalist aspirations), they had to subject their language to the most basic analysis of structure, its specialized military and technical vocabulary, the frequencies of its letters and words, and its rendering for cryptographic and radio transmission purposes. As in other aspects of Vietnamese military life, deprivation was made a virtue: lacking the ability to establish central control over the production and use of cryptomaterials; standards were set and models adopted; then local initiative was encouraged through competition and emulation campaigns. An enemy was thus confronted, not with an Enigma or "Purple" to break, so much as a wide variety of similar cryptosystems, having to be attacked individually, much as was the challenge offered the Allies by Japanese army systems in World War II. (An interesting and instructive companion to the present translation can be found in Edward J. Drea, *MacArthur's ULTRA: Codebreaking and the War Against Japan, 1942–1945* [University Press of Kansas, 1992], which also illustrates the principles of enciphered code.) Production figures, tonnage of materials delivered, and scores attained in cryptographic competition ("Comrade Nguyen Van Hai encrypted x groups in y minutes with an error rate of only z") seem tedious or even silly to the Western reader, until one realizes the importance of such matters in an army using often crudely printed (or even handwritten) manual

cryptosystems, distributed over rugged, distant jungle trails by couriers or man-pack, later to be transmitted by finger or tongue.

In a form reminiscent of the old revolutionary army, lacking ranks and titles, other than "warriors" and "cadre," and with individuality subordinated to "the team," the authorship of this work is identified collectively. The senior of the two officers identified as being responsible for its content, Brigadier General Nguyen Chanh Can, was a graduate of the first formal Vietnamese class in cryptography, September-October 1946, selected to remain at the General Staff Cryptographic Bureau. He may also have been one of the original forty-five-man Vietnamese group sent to China for some six months of training, returning in May 1951, when, as bureau deputy chief, he was concurrently made chief of the Campaign Cryptographic Section of the reorganized Cryptographic Bureau of the General Staff. He headed the Cryptographic Section of the historic Dien Bien Phu campaign (1953-1954), and he figures elsewhere in the text. We can thus assume that the book represents the efforts of both participants and a later generation of researchers, editors, and publishing staff, as presumably is the case with the book drawn upon as a supplement.

At the same time, the book lacks the detailed documentation expected in comparable Western military histories, leaving one to wonder to what extent documentation has been preserved and the extent to which recollections play a major role in this account, making it the basic documentation for the future and, in the process, shaping the traditions and perceptions of coming generations in the speciality.

Finally, and in a departure from conventional orthography, this translation has rendered the Vietnamese letter, "unbarred D," as "Dz," approximating its sound, by contrast with the "barred D," comparable to the "d" sound in English. (This results, for example, in the name of General Van Tien Dung being rendered as Van Tien Dzung, avoiding the unfortunate American tendency to call him "General Dung.")

DAVID W. GADDY

Notes on the Translation

By comparison with the extensive vocabulary of English, its synonyms and its free borrowings from other languages, Vietnamese has a more limited vocabulary to draw upon, but a vocabulary filled with nuance, heightened in the case of communist usage. Strict consistency in translation, while desirable in one sense, would produce a highly repetitive text to the English reader; therefore no effort has been made to ensure consistency when American English seems "richer." The risk is, of course, misinterpretation. An attempt has been made to render certain Vietnamese terminology in equivalent American English, but to avoid "forcing" an interpretation if the precise American equivalent was unknown. This is especially true of technical cryptographic terminology, when a forced meaning could well be a misinterpretation. For example, in normal usage, *tai lieu* would be translated as document or (written) material, but in a cryptographic context, "cryptomaterial" seems warranted. *Luat*, code in Vietnamese, is sometimes rendered as "code," at others as "system," or "cryptosystem," depending upon context.

Certain Vietnamese terminology carries the connotation of echelon (e.g., *tieu ban, ban, phong, cuc, tong cuc*), requiring consistency in translation. Thus the change of a *ban* (section) to a *phong* (bureau) or a *phong* to a *cuc* (directorate) implies bureaucratic growth --elevation and a promotion for the chief. Used in a political or governmental context, *ban* is translated as section. In other instances, inconsistency may seem the rule: "Branch" may be Vietnamese *nganh* or, in military terms, *binh chung*. "Sector," "zone," and "region" may involve the Vietnamese words, *khu, khu vuc, xu* (in the 1940s), *mien* or *vung*. In such cases--and, in general, whenever the Vietnamese appears necessary for comprehension--the original term is given in brackets, as are other interpolations or comments. (By contrast, parentheses are used only as in the original text.)

The book often uses the ellipsis (. . .) in a manner more akin to "etc." or "et al." in our usage. To avoid the misimpression of omission in the translation, "etc." is usually substituted for that practice.

The title "comrade" is so pervasive that it has been abbreviated as "Cde" in the translation. Other abbreviations are standard (e.g., HQ for headquarters, CP for command post, MR for military region), but are spelled out in first instances.

Terminology associated with party and military organizations may also require explanation. "Central" or "Central Party" might well have been rendered in John Le Carré fashion as "The Center," but this has become an accepted way of rendering *Trung uong* or *Trung uong Dang* in English, referring to the headquarters of the Lao Dong Party – or frequently, "the top," in light of the intertwined party-government-military structure French authorities called "parallel hierarchies." Strict consistency is the rule for military organizations, as noted earlier – *Bo tu lenh* is "headquarters," at division, military region, or branch/service level; *Bo chi huy* (an earlier term) and *bo tong tu lenh* are both rendered as High Command (GHQ, in some usage); and *Bo tong tham muu* as General Staff. "*Bo*"

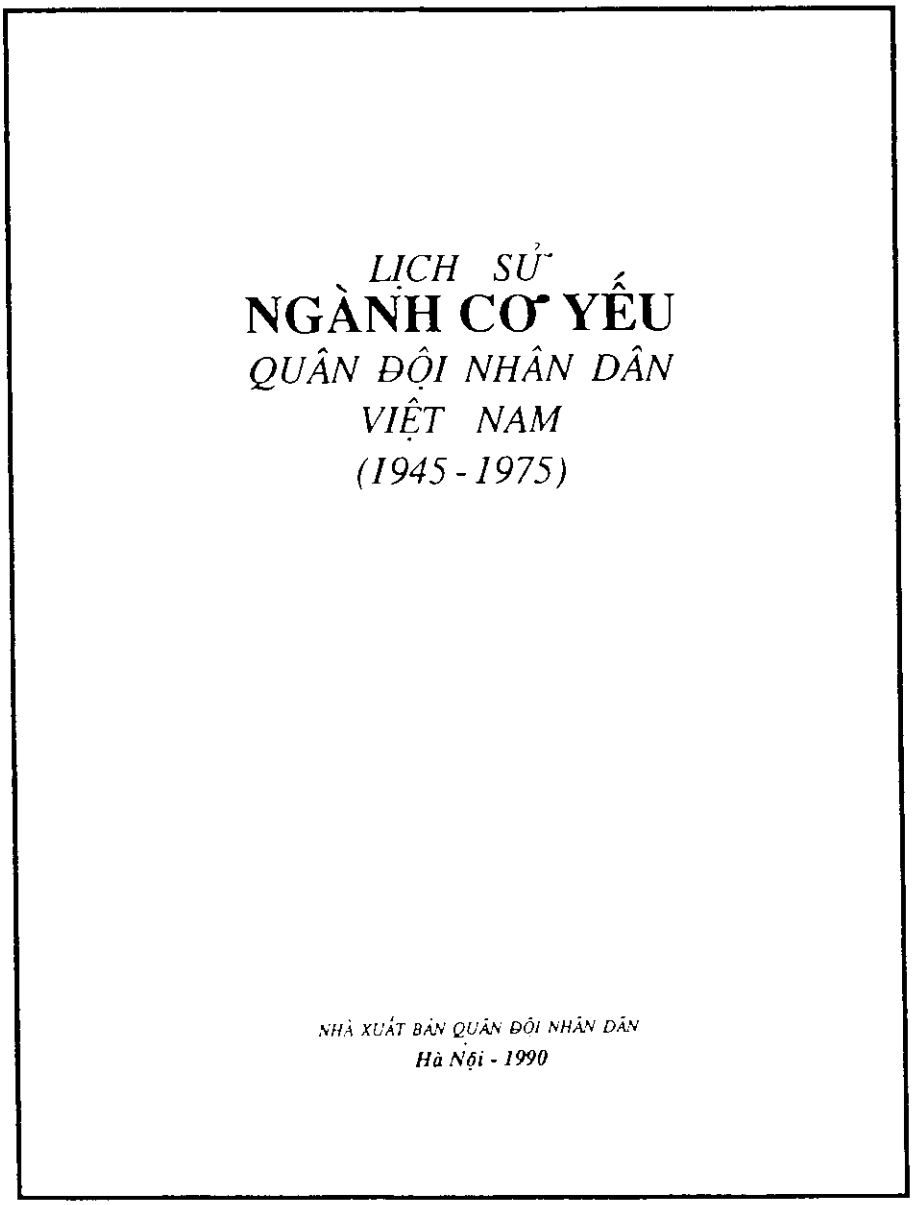
by itself is often used, meaning "the top" for the military structure: is this the High Command or the General Staff? Or might it be the Ministry of National Defense (*Bo Quoc phong*)? Here *bo* is rendered as simply "Headquarters" or "HQ." "Division" has been used to translate both the *dai doan* of the First Indochina War and the postwar *su doan*, the product of "modernization and regularization." On the other hand, the somewhat artificial term, "groupment," has been used for *binh doan*, the forerunner of *quan doan*, "corps," for the Vietnamese used the same term, *binh doan*, for the French "mobile groups" of the First Indochina War, and "group" is the consistent rendering of the Vietnamese *doan*. Military rank tends to be consistent with "normal" American translations, with the exception of Senior General, which is rendered simply as General.

There is a long, if not necessarily honorable, history behind these inconsistencies in English: for some reason, we have always accepted Ho's title as President, notwithstanding the fact that the same term is rendered as Chairman in the case of Mao. Of course, it is rather as Uncle that we find him in the following pages.

DWG

History of the Cryptographic Branch of the People's Army of Viet Nam 1945 – 1975

The Publishing House invites the opinions and criticisms of the readers.



Facsimile of original title page

The History of the PAVN Cryptographic Branch is written to cover the building and activities of the army cryptographic branch from the resistance against French colonialism through the national salvation opposition to America (1945–1975).

Content direction: Brig. Gen. NGUYEN CHANH CAN
Col. PHAM VAN THIEU

Research and Compilation: LE DINH Y
HOANG QUYEN
VU CONG SUU
VU VAN TAN

Manuscript: VU CONG SUU

Ho Chi Minh - "Uncle Ho"

"Cryptography must be secret, swift, and accurate.
Cryptographers must be security conscious and of one mind."

Words of Uncle Ho, with the cadre and students of the 1950 Viet Bac Combat Sector army cryptographic class

"During the decades past, as we fought the aggressor, we knew that, at the most crucial times, our most secret matters would not be leaked out.

"You comrades have participated most importantly in maintaining secrecy, contributing to our common strength in achieving victory.

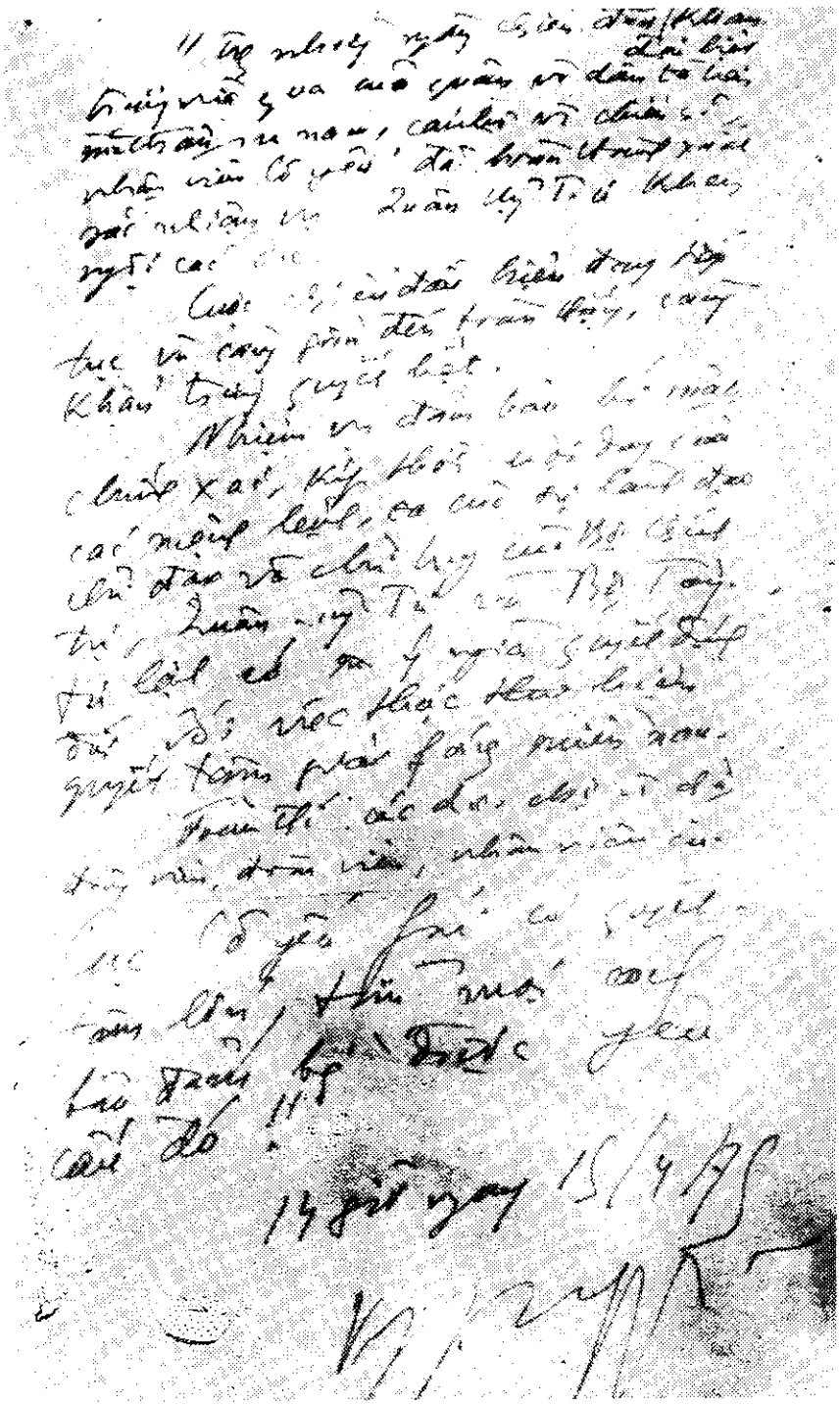
"The cryptographic branch – a most important branch – must bring itself fully up to date; the ranks must be truly pure; the regulation of the task must be very tight."

From the speech by Cde Le Dzuan,
General Secretary, Central Party
Executive Committee, at the 1978
Nationwide Cryptographic Cadre Conference

Comrade Le Dzuan, General Secretary of the Central Party Executive Committee, speaking at the Army-wide Cryptographic Cadre Conference, 1978

General Van Tien Dzung, Central Party Politburo member and
Minister of National Defense, checks out research results in the use of cipher machines (1984)

General Vo Nguyen Giap, Member of the Central Party Politburo and Minister of National Defense,
reads a report message from the front sent back during the Spring 1975 general offensive and uprising



Words of commendation and recollection to the crypto cadre and personnel from General Vo Nguyen Giap, Minister of National Defense

Table of Contents

[Transposed from the end of the original volume]

Chapter One

The Genesis of the Cryptographic Branch of the People's Army of Viet Nam

APPEARANCE OF THE EARLIEST CRYPTOGRAPHIC ORGANIZATIONS AND TECHNIQUES IN THE ARMY

The August Revolution was a success!

On 2 August 1945, in Ba Dinh Square, President Ho Chi Minh solemnly read the Declaration of Independence, giving birth to the Democratic Republic of Viet Nam.

The newly established democratic republican government had to cope with a situation of endless complications. In the South, the French army, hiding behind the British military, landed in Saigon-Cholon, continuing their aggressive plots against our nation. In the North, nearly 200,000 of Chiang Kai-Shek's military came, in the name of the Allied Forces, to disarm the fascist Japanese, and escorted gangs of lackies plotting to overthrow the authority organized by the Viet Minh [Viet Nam Independence League]. Reactionary gangs in the nation took advantage of the people's rising to act to counter and destroy the resistance. The Japanese-French imperialist gangs provoked famine and ran wild.

Faced by the devious plots of enemies both foreign and domestic, together with difficulties in every respect in our homeland after the revolution had just succeeded, the fate of our nation at that moment faced a very dangerous situation, for "money and necessities were hanging on a hair."

In order to confront the enemy's aggressive plots against our nation--in order to protect the incipient authority of the people--the Standing Committee of the Central Party and President Ho Chi Minh proposed some urgent tasks to strengthen authority, counter the French colonialists' aggression, abolish crime, raise the standard of living of the people, and especially to show concern for supplying concrete guidance in building revolutionary armed forces.

On 7 September 1945, President Ho Chi Minh entrusted to Cde Hoang Van Thai responsibility for establishing the General Staff organization. (Cde Vo Nguyen Giap was also present at the occasion). When assigning the task, Uncle said: "Our people have just won their independence, their freedom--all of our nation is starting to build an army of resistance and self-defense to safeguard our independence, our freedom. Pursuant to

collective instructions, the Staff [Bo tham muu] is established to help Central exercise command of the army in our whole nation.

"As the secret organization of the collective--as the nerve center of the army-- the Staff is responsible for military strength, for forging weaponry, for knowing the enemy, in order to defeat every enemy.

"At this time we have no experience--do not yet understand staff work--have many difficulties. But we have to strive to overcome this, studying even as we work. With determination, many difficulties can be worked through. Somehow we must also build a staff branch of our army that is solid and powerful, worthy of the tradition of giving one's mind to forwarding and preserving the nation of the Vietnamese peoples."[1]

On 8 September 1945, Cde Hoang Van Thai sponsored the first meeting of comrades to introduce the organizations of the General Staff, in order to determine and allocate responsibilities.

On 9 September 1945, the Military Communications-Liaison Bureau of the General Staff was officially established, under Cde Hoang Dao Thuy. From a week before, according to instructions from the Central Party Standing Committee and Uncle Ho, Cde Vo Nguyen Giap, Minister of Internal Affairs in the provisional revolutionary government, and concurrently Commander-in-Chief [Tong chi huy] of the revolutionary armed forces, had a personal exchange with Cde Hoang Dao Thuy and handed to him responsibility for preparing to build a military communications-liaison system. This was a responsibility that had to be carried out at once, with no delay, in order to help Central, the government, and the High Command [Bo Tong chi huy] come to grips with the situation and issue timely instructions to the combat sectors [chien khu] and units throughout the nation.

Immediately upon being established, the Communications-Liaison Bureau started to develop the organization of a network [mang luoi] of communications-liaison, and the first task was the early creation of a radio liaison network especially for the army.

With the Central Party concerned with assignment of people and getting equipment, a few of the fellows took it upon themselves to search out old radio stations in French depots, and, after just a short time, an official military radio liaison net was inaugurated, comprising the High Command and General Staff in Hanoi with the combat sectors of Dong Trieu, Viet Bac [Northern Viet Nam, or Tonkin], and Hoa (Binh)-Ninh (Binh)-Thanh (Hoa); the Revolutionary Military Affairs committee of Trung Bo [Central Viet Nam, or Annam]; and the Military Affairs Committees of Thua Thien-Hue and Da Nang. Besides the military liaison network, liaison between the Central radio offices (Hanoi) and those of Trung Bo and Nam Bo [Southern Viet Nam, or Cochin-China] was maintained and shaped, making a liaison network of military postal and radio [service] throughout the nation.

In the first days of the revolutionary regime, the leadership and command comrades, the organizations sending messages and those receiving messages, and the

communications organizations equally felt uncomfortable sending messages over the military radio or via the post offices in plain text, unenciphered. Thus an urgent requirement was to research methods of using cryptography so as to ensure communication security.

Cde Hoang Van Thai personally reviewed and approved the plan to establish the Cryptographic Section [Ban Mat Ma] (not yet called Co Yeu, as it was later) and strongly recommended that Cde Hoang Dao Thuy select good, trustworthy, literate people for the task of cryptography.

On 12 September 1945, the Military Cryptographic Section, the first cryptographic organization of the army, was established, tasked with research, production, and use of cryptographic systems to ensure the secrecy of leadership and command communication of the various echelons of the army going via the various means of communication (principally by radio). This was also the first cryptographic organization of our nation.

The twelfth of September has since been taken as the birthday of the army cryptographic branch.

At the beginning, the Cryptographic Section lay in the Bureau of Communication-Liaison. The working area was a room behind that of Cde Bureau Chief Hoang Dao Thuy in building No. 16 Riquer Street,[2] adjacent to the General Staff organizations.

In accordance with a proposal by Cde Hoang Dao Thuy, Cde Vo Nguyen Giap appointed Cde Ta Quang De,[3] who was working in the Ministry of Internal Affairs, to transfer to the General Staff and assume charge of the cryptographic mission.

Having received the responsibility and concrete recommendations of Cde Hoang Van Thai, and after determining the particulars and mission components, Cde Ta Quang De circumspectly proceeded to select people who could be introduced to the work of cryptography. The "criterion" for selection was based on estimation of a "good, trustworthy person," and an additional condition was "ready-to-go," no family ties, committed to an assignment requiring total reliability. A number of the fellows who were introduced by responsible people to cryptographic work prior to the organization were intellectuals and petty officials, and at the same time Boy Scouts from [troops] such as Dinh Loan. Thuyen, Hoang Quy Quan,[4] also young Miss Bui Thi Loan, a liberation army soldier returned from the combat sector. After a few days, Nguyen Tu Khang, Bach Tuong, Sam, Dich, then Tran Mi Thach in turn were introduced to the work.

After working together a few weeks, the fellows did some brainstorming about many aspects of this new assignment. Prior to this time, the colonialist French gang had not ever instructed Vietnamese people, or entrusted them, in our own cryptographic organizations, so there was no one who thoroughly understood the business. Therefore, the ideas shared by these fellows, together with revolutionary enthusiasm, built up trust on the part of the leadership comrades. Afterwards, in a situation in which people to perform cryptography were lacking in various places and in accordance with arrangements by Cde Hoang Van Thai, Dich went to Combat Sector 4, Thach went up to

Thai Nguyen-Bac Can, and Sam, Khang, and Tuong were placed on a long line from Phuc Yen up to Phu Tho, locales that needed to quickly put down the activities of the [Vietnamese] Nationalist Party and "Viet Cach" [Vietnam Revolutionary] cliques.

Near the end of the year, the Cryptographic Section received two more people: Cde Nguyen Hai Hac, graduate of the Higher Agricultural School, home in Hanoi, and Cde Tung Anh[5] from Quang Ngai, who came at the invitation of the military organization there.

As of this point, people working in the Cryptographic Section were temporaries. Some arriving before, some later, these were the comrades present in the early stage of the formation of the army cryptographic branch. A small, close-knit and affectionate family, united to help each other, with a clear sense of responsibility and personal honor to respond to the requirements of the revolution and the army, these comrades shouldered a tough, essential job, doing the spade work for a technical branch of the PAVN.

Initial feelings of inadequacy passed quickly. With respect to cryptography, it could be said that the resources of the comrades at this stage were simply revolutionary zeal and enthusiasm, together with a book, *The Basic Principles of Cryptography*[6] in French, which had come apart, and some two or three Boy Scout riddle games[7] – this was the level of knowledge at this stage.*

* A variation in the account of the origins of Vietnamese cryptography is contained in Volume 1, 17-18, of the *History of the Communications-Liaison Troops* (Draft) (Hanoi: Communications-Liaison HQ, 1985): "[In the fall of 1945] when they sent out an unenciphered official message, all of the Communications-Liaison Bureau saw it and were uncomfortable. The place that received it also asked why it wasn't encrypted. . . . The chief of the Communications-Liaison Bureau proposed to HQ the establishment of a Cryptographic Section (not yet called 'essential matters'), to be placed in the Communications-Liaison Bureau. Imagine that! Cryptography, placed in the Communications-Liaison Bureau! But that is the truth. We need to say more about this fresh new organization: Beforehand, throughout all of Indochina, the gang of French colonialist rulers would not train and entrust to the Vietnamese employment in their cryptographic organizations. That's understandable. As a result, when we seized power, the two radio liaison centers, north and south, had to generate two reference works for enciphering and deciphering that differed from each other. In Hanoi, when the first messages were sent to Saigon, they requested the recipients to use passages in the classic, Kieu, by Nguyen Dzu as an enciphering-deciphering reference work. In Saigon, they proposed that Hanoi use Mendeleyev's periodic table in order to solve the key and encipher and decipher the messages sent from then on. Thus, it was imperative to have a [or, "one"] cryptographic organization. Not knowing where else to put it, it was properly placed in the Communications-Liaison Bureau.

"On 12 September [1945], the Cryptographic Section was established, subordinate to the Communications-Liaison Bureau.

"Cde Ta Quang De (Ta Quang Dam) and Cde Dinh Loan Thuyen (Hoang Thanh) were invited by the General Staff to undertake the making of cryptosystems. Before the August Revolution, in the scientific games and entertainments of the students and intellectuals in Hanoi, there were many young people–among them Cdes De and Thuyen--who regularly played number and letter games according to set rules, and transformed the numbers and letters to make words and sentences. Now, confronted by the requirements of the revolution--of the army--the comrades readily accepted and got involved with a deep attitude of responsibility. One week later, a cryptographic paper with adequate key was accepted by the General Staff, and the Communications-Liaison Bureau was instructed to quickly develop cryptographic personnel for each radio station."

Ibid., 20: ". . . the troop strength of the Bureau [at this time] (including the bureau chief) was only eight people. . ." [footnote 2:] "8 people, comprising Hoang Dao Thuy, Le Dzung, Vu Han Thang, Ta Quang De, Dinh Loan Thuyen, Nguyen Ai Hac, Do Thanh, and Tran My Thach." -- Tr./Ed.

The comrades divided among themselves going to meet comrades who had experience in covert activities inside and outside our country, seeking to learn from their experience; searching for a few types of [cipher] keys, easy to remember, easy to use; a few methods of writing secret letters; all sorts of text books in the Vietnamese language that could be consulted in research. The comrades regularly said to one another, "Now we've really got to get back to our mother tongue!" Not long before this, every time one spoke up in class it had to be in the language of the French "mother country," and now, how eagerly they were going to work in the Vietnamese tongue! There were young men and women at this time, under the age of twenty, coming to grasp the fact that Vietnamese had many alphabets and knowing which, encountered many, especially in literature. The [cryptographic] concept of "frequency" emerged through the practice of enciphering and deciphering.

At the suggestion and urging of Cde Hoang Dao Thuy, after about a week, Cde Ta Quang De researched a system to use to write and read secret letters.[6] Per instructions from Cde Hoang Van Thai, this cryptographic system was given to a command comrade on the Vinh Yen front to use for liaison. Some days later, Cde Hoang Van Thai gave Cde De a secret letter to encipher for sending to the Vinh Yen front. The content was a short section, but written out to produce a full page. When signing the message form, the comrade chief of the General Staff observed, "First, this way you have to write a lot, use up a lot of time, a lot of paper; second, it's rather difficult to ensure a fit between what's valid and what's false, thus the end is revealed; and, third, it's not handy for message transmission."

From these observations and exchanges with the fellows in the Cryptographic Section, Cde De came up with a different method: a method of enciphering each alphabetical letter--simple in use, a neat, compact chart. In using these systems for monoalphabetic [doc bieu] substitution and transposition, by close observation of a number of cryptograms, the comrades subjected them to detailed scrutiny and saw a number of points arise: Concerning monoalphabetic substitution: the repetition of the plain-cipher values followed a basic form. Some consonants and vowels in the Vietnamese language, represented by two letters, caused the frequency to rise very clearly.

Enciphering by transposition, using a literal key or a digital key: If enciphering by simple letter transposition, then the number of letters of the enciphered message would be equal to the number of letters of the plaintext message. These conditions resulted in cryptography that would not ensure tight secrecy, easily exposed to the eye of an enemy with much experience in cryptanalysis. Each individual arrived at the conclusion that the systems being used would not yet meet the requirement to ensure secrecy, their degree of security was at a rather low level – we had to quickly research different systems to replace them.

Based on experience with monoalphabetic substitution cipher, Cde Ta Quang De discussed with the people in the Section finding a way to change the system and change the key. Above all else, to produce some way that the appearance of the cryptogram was

not dependent upon the appearance of the plaintext message--when our people looked at the cipher text they only saw it in its entirety, whereas clusters of letters differed from others in frequency and quantity. Then, in enciphering, to carry out a key change, a chart or direction change, even right in a message. The concrete method would have to have a composite chart, composed of many contrasting systems, each system with an individual key. After a period of searching and exchanging views within the Section, Cde De came up with a new type of system. The first columnar chart system had succeeded, with Cdes Hoang Van Thai and Hoang Dao Thuy agreeing to introduce its use to replace the systems that had been used for so long. Once the cryptographic systems had been typed up, Cde Hoang Van Thai sent a message to the sector chiefs to select dependable people to come to HQ to receive the system and listen to directions for use. A few days later, Van Tien Dzung came from Chi Ne bringing along a cryptographic cadre, then Le Van Suu from Intersector 4, Vu Hien from Haiphong, Le Quang Hoa, Hoang Minh Thao, et al., and the other units in turn selected cryptographers from their units to receive the system.

According to the principles of this system, each cryptogram had to be changed into a fixed number of columns. Each column had its own key and in order to be certain of ensuring secrecy, each key was fixed for many cryptographic values [ky hieu mat]. At first, many comrades were a bit perplexed, suggesting that use of simple transposition would also ensure secrecy. The comrades in the section had to stand their ground in explaining, and the others finally became truly unanimous. After a period of use, enciphering and deciphering many times, the work became routine. The comrades in the research team continued to realize an additional step, regulating the movement of the cipher strip [viec chuyen bang ma] according to class [theo bac], according to day, etc.

One might say, from forms of "leave out the false, what's left is valid" in order to read secret letters (not yet forms that could properly be called cryptosystems) and monoalphabetic substitution and transposition by pattern, we quickly moved to chart systems using irregularly arranged values with many columns and many keys. These chart systems, given the educational and technical conditions of our society, generally speaking, and our army, specifically, at that time, seemed relatively suitable and achieved a notable level of meeting the requirement to serve guidance and command.

The work came fast and furious, the activity of the Vietnamese Nationalist Party in the provinces of Phu Tho and old Vinh Phuc being reported continuously by message. Then the Nam Bo resistance, the French colonialists hiding behind the British military, swarming into Indochina and attacking and occupying many cities. The endless struggles of great fortitude of our Southern compatriots took place daily. So as to quickly grasp the situation and issue guidance for coping with the enemy and foreign aggressors, the Cryptographic Section, along with the communications-liaison organizations, worked day and night. From the end of September, through October – November 1945, the volume of secret messages increased very rapidly. The matter of telegraphic language frequency posed a need for research into a method of scientific calculation. (Initially, this matter had to be done by guessing, for there was a time-sensitive need to satisfy the most pressing, urgent requirement for the service of command.) The clear part of the cryptographic

system form received concentrated research in construction. Combining experience and research and the use of a columnar system that followed the principle of monoalphabetic substitution with a digital key, with personally searching out and consulting foreign documents in order to apply international principles suitable to the special aspects of Vietnamese telegraphic spelling, Cde Dinh Loan Thuyen and colleagues produced a Vietnamese 676-cell [26x26] chart. The system was constructed according to the method of polyalphabetic [da bieu] substitution encipherment of word components. After completion of the system, it was quickly put into use.

Implementing a directive from the Chief of the General Staff, the Cryptographic Section designated people to convey the system to a number of places lacking the means to receive it. On the first lunar new year's day after the August Revolution, Cde Thuyen was ordered in turn to convey the system and directions for use of the 676-cell chart to the units from Phu Ly to Binh Dinh. Vis-a-vis Nam Bo, that theater of war received concentrated assistance from the whole country: from October 1945, the Cryptographic Section quickly sent cipher models, carried by Cde Hoang Quoc Viet, to be handed over to the Sector [Xu] committee, when the comrade, on behalf of the Standing [Committee] of the Central Party, went down and participated in the opening at the Sector Committee Conference.

A consciousness of the need for constantly changing keys, changing cipher strips, replacing systems dawned early-on among the comrades engaged in cryptography.

One day, around the end of 1945, the Second Bureau [Military Intelligence] sent over to the Cryptographic Section a number of enemy cryptograms. Although knowing nothing about cryptanalysis, the fellows nevertheless took a stab at it. The unexpected result was that the comrades decrypted a third of the cipher messages from a French army unit stationed in Upper Laos exchanging operational matters among themselves by means of a simple substitution system. This resulted in the Second Bureau comrades forming a high opinion of the expertise of the cryptographers. As for us, this small accomplishment in cryptanalysis had the effect of helping our people make up systems, even as it helped them in encrypting messages themselves.

In January 1946, in accordance with instructions from Central, the General Staff organizations were realigned. The cryptographic organization was split off from the Communications-Liaison Bureau. For the political, routine, and administrative aspects, [it would be] directly subordinate to the General Staff secretariat; for speciality professional knowledge that was the essence of its task, directly subordinate to the comrade Chief of the General Staff. The main office of the bureau was moved to No. 26 Hang Bai (a sign in front of the door of the office said "Bureau of Secret Messages"). Crypto elements were also gradually established. In the sectors [khu], the cryptographic organization was called "Department [ty] of Secret Messages," or "Department of Cryptography." In Sector 1, the Department of Secret Messages was organized directly subordinate to the regional command post secretariat, while in the regiments cryptographic teams were directly subordinate to the regimental command section. In sectors 4 and 5, the cryptographic organizations were called

Department of Cryptography, directly subordinate to the secretariat or staff organizations, with cryptographic teams in the regiments.

In March 1946, Cde Ta Quang De became a liaison control officer between the Vietnamese and French sides.[9] Cde Hoang Van Dong became Chief of the Cryptographic Bureau. Research into cryptographic technique was undertaken by Cdes Dinh Loan Thuyen and Hoang Van Dong.

At this time, the 676-cell code chart was improved, fixed strips replaced by movable strips, raising the level of cryptographic security. The content of the chart was added to by compound words [tieng kep] and phrases [doan cau], thus shortening cipher messages. The system received use at once and was brought into play with effect in ensuring communication security between the High Command of the Vietnamese relief troops [Bo Chi huy Tiep phong quan Viet Nam] in Hanoi, with eleven units. Hai Dzuong, Thai Binh, Phu Ly, Nam Dinh, Ninh Binh, Thanh Hoa, Vinh, Dong Hoi, Dong Ha, Hue, and Da Nang dealing with the French army.

At the beginning of 1946, Cde Thuyen received the task of preparing a system to ensure cryptographic liaison between our government's delegation at the Da Lat preparatory conference and the General Staff. Realizing the degree of importance of the matter in our foreign relations struggle with the French, to ensure the secrecy of policy instruction laid down to our delegation by the party and government, Cde Thuyen concentrated all of his efforts into making a system. The good things of the chart form were incorporated into a chart system made solely to serve the Da Lat conference. The leadership comrades also knew that, at this conference, the French side had brought along a guy who was a specialist in cryptanalysis, with equipment to search out our secret information. Having received the first two messages sent back from the Da Lat conference,Cde Thuyen personally broke them out and was flabbergasted: the person enciphering the messages had not conformed closely to the regulations concerning the technique that had been conveyed--the information we were sending could easily be uncovered by the enemy. The Cryptographic Bureau at once suggested to Cde Hoang Van Thai suspending the use of this type of system. During the course of working for the previous half year, Cdes Dam, Thuyen, and Dong were tormented with mixed feelings, principally over whether the cryptography they were using was really tightly ensuring military secrecy or not. After reading some documents that had been received, the comrades knew that those people were still enciphering and deciphering by machine, and especially that they were still using equipment that made it very easy to discover the system and key. Thus they had to be even stricter with themselves, although believing firmly in the sense of loyal service by the young men and women performing cryptography, as far as their country was concerned, the general standard was still low and capacity for carelessness no small matter. The comrades discussed with the young men and women in the section a cryptanalytic test of an enciphered message, setting aside knowledge of system and key, to see if it could be made out. But, although they worked out the system and key, once, when they did not have system and key at hand, no one could make out anything at all. Thus day by day and week by week, continuing this sort of thing, they listened intently and watched for signs of any leaks in secrecy, and they felt reassured.

In April 1946, in order to increase the building and creation of conditions for the cryptographic organization to fulfill its mission in situations that had become more urgent daily, the cryptographic organization of the General Staff was supplemented by comrades Ho Ton Vinh, Hoang Don, Hoang Tuyen, Luong Dzan, Hoang Dzanh Cha--Cde Ho Ton Vinh (alias Hoang Duc Ton) was one of the first three Communist party members in the General Staff organization and was sent to the cryptographic organization as a supplementee. These young men were introduced by leadership and command comrades of high standing.

Along with the building and strengthening of the cryptographic organization at Central, the training of cryptographic cadre to expand the system of cryptography and strengthen the units was fully appreciated. As a matter of urgency, the General Staff cryptographic organization prepared to open a mass class to train cryptographic cadre to supplement the cryptographic organizations at lower echelons. The task of research and compilation of [cryptographic] material to teach in this class was given to Cdes Dinh Loan Thuyen, Hoang Van Dong, and Hoang Dzanh Cha. Although they encountered many difficulties, the comrades diligently consulted, researched, and compiled a quantity of documents concerning the science and techniques of cryptography.

Material compiled by Cdes Hoang Van Dong and Dinh Loan Thuyen first-off comprised basic theoretical content and instruction in the use of cryptographic systems. Cde Hoang Zanh Cha researched and compiled the statistical content concerning Vietnamese language frequency, in order to serve in constructing cryptographic systems. These were also the formative works in the sphere of research into the science of cryptographic technique on the part of the army cryptographic branch.

After preparing sufficient documentary content to cover all aspects, the General Staff decided in September 1946 to open the first class in the army to train cryptographic cadre: it was named "The Hoang Dzieu Class." Sessions took place at No. 7 On Nhu Hau Street (now Nguyen Gia Thieu Street), Hanoi, under Cdes Hoang Van Dong, Hoang Dzanh Cha, and Ho Ton Vinh. Cde Hoang Van Dong was in general charge and bore responsibility for teaching cryptographic principles. Cde Ho Ton Vinh was responsible for political leadership and thought and bore responsibility for teaching political matters. Cde Hoang Dzanh Cha bore responsibility for teaching the methods of researching the frequency of the Vietnamese language and the use of cryptographic systems. Twenty students from the combat sectors and units in Viet Bac, Trung Bo, and the Southern Viet Nam Resistance Committee (in Quang Ngai) were selected to attend the class. Nam Bo, hindered by transportation, was unable to send up people to attend. Before getting into specialized study, the students had to grasp the mission thoroughly, clearly define ideology, and understand the "must-do's and the musn't-do's" of the work of people performing the task of cryptography. Beyond the basic content of the syllabus, the class also received an additional introduction to fundamental knowledge of the cryptology of the world and practiced a number of our forms of cryptography. After more than a month of study, achieving good results, the class came to an end. The students returned to the units, becoming the nucleus of building cryptographic organizations in the combat sectors [chien

khu]. Some comrades were retained to supplement the General Staff cryptographic organization, namely, Nguyen Chanh Can, Hoang Manh Tuan, Vu To, Vu Duc Minh, and Nguyen Van Dzanh (Ho Quang Chinh) – Cde Ngo Vi Thien was sent to supplement Combat Sector 1; Cde Tran Dac Quy to Combat Sector 2; Cde Le Hai to Combat Sector 3; Cde Van An to Combat Sector 4; Cde Dong Tam to Combat Sector 5; Cde Tung Anh to Combat Sector 6, etc.

In May 1946, in order to implement Ministry of National Defense instructions to organize reliable and secure communications-liaison nationwide, the cryptographic organization of the General Staff convened the first cryptographic conference. The conference discussed the tasks of cryptography and secrecy, and the delivery and receipt of cryptographic systems. Comrades in charge of the cryptographic organization in the combat sectors and fronts came to attend (except for cryptographic cadre-in-charge in Sector 5 and Nam Bo, who could not get back to attend). The conference received a visit and teaching from the Cde Chief of the General Staff, Hoang Van Thai. In August 1946, meeting again in the second military cryptographic conference in Hanoi, twenty-five delegates from Trung Ky [Annam] and Bac Ky [Tonkin] attended: the discussion was on cryptographic training. After the conference there was a five-day specialty training course.

Thus, together with resolute research, ingenuity, and expansion of the cryptographic net, having received the concern of the leadership and command cadre, the cryptographic organization urgently strove to train cryptographic cadre and personnel to supplement the units. From the beginning of December 1946, the cryptographic organization in the army had, by turns, organized in the combat sectors, the companies [chi doi], and a number of units, army-wide, participating in "maintaining contact between the combat sectors, an essential condition for unified command," in the spirit of "Chi thi khang chien kien quoc" ("Instructions for Resistance in Founding a Nation"), from the Executive Committee of the Central Party (25 November 1945).

Notwithstanding, during this time we had not yet come out with concrete regulations, so getting and using cryptographic cadre and personnel remained hit or miss. The cryptographic organizations in the sectors were not able to manage the total number of personnel under their authority. The command organizations routinely transferred cryptographic personnel to other assignments, or assigned them work outside the sphere of their technical speciality. This situation worked counter to the ideology of a number of cryptographic cadre and personnel, principally at the regimental and company level. A number of cryptographic personnel had no stomach for the job, and requested direct combat or transfer to some other duty.

SERVING LEADERSHIP AND COMMAND VIS-A-VIS ENEMY ACTIVITY; PREPARING THE ENTIRE NATION TO RESIST AND COUNTER FRENCH COLONIALISM

After the August revolution succeeded in giving birth to a people's democratic nation, under circumstances in which research, ingenuity, and expansion of the cryptographic net competed with providing for the training and development of cadre and personnel and solidly building a system of organization, the army cryptographic organization had to ensure the transmission of the content of leadership, direction, and command of the various echelons through the communication media, responsive to the urgent mission situation of our homeland. The cryptographic organizations from the 16th parallel [Dividing line set for British and Chinese troops entering to disarm the Japanese forces at the end of World War II. Tr./Ed.] up concentrated on serving leadership and command coping with the tricks and schemes and the actions to oppose and destroy or overturn the revolutionary authority on the part of the Chiang bunch and domestic reactionary gangs. The cryptographic organizations in Hanoi, Phuc Yen, Vinh Yen, and Phu Tho ensured the transmission of secret messages directing the struggle, and suppressing subversive acts by the Nguyen Hai Than, Nguyen Tuong Tam, and Vu Hong Khanh gangs; secret message directed provisional political arrangements between the Viet Minh front and the Viet Cach and Viet Quoc.

On 23 September 1945, when the French colonialists, aided by the British, opened fire and occupied Nam Bo, striking and taking over communication centers, the organizations and armed units of Nam Bo overcame obstacles to protect the evacuation of radio stations into bases, ensuring liaison within the region [vung] and with Central.

At 0815 on 25 September 1945, Nam Bo Cryptographic enciphered a message reporting to Central Party and the government concerning the resolution of the Nam Bo Sector Committee [xu uy], determined to resist the French colonialists. At 1010 the same day, the comrades received and deciphered the Central Party instruction agreeing with the resolution of the Sector Committee and the Nam Bo Resistance Committee. The cryptographic units in the South ensured the transmittal of the secret messages of the High Command, instructing the Southern military groups to advance and serve in the resistance struggle against the French in the South.

The task of enciphering and deciphering messages at this period was still elementary, but a first step toward an orderly routine. A number of regulations on enciphering and deciphering were issued, aimed at protecting technical secrets and the content of secret messages. All cryptographic materials had to be reduced to bare bones and constantly kept at the side of the cryptographer. The element enciphering and deciphering messages was to be compartmented by net, and not to express curiosity to know the contents of the work of another, between elements, or between each individual in his special compartment. Ordinarily, messages were transmitted by radio or post. In the beginning, for messages sent by post, the procedure was that the place sending and the place receiving were written in the clear, with the content alternating, some sections clear, some in cipher. If the messages was going by radio, then the sending place, receiving place, and precedence

were written in French. Upon reexamination, these arrangements were seen not to be of value in protecting secrecy, thus gradually redone. Because going and coming was difficult, the replacement of the types of systems in use was not effected at an exact time, nor were new systems distributed in timely fashion.

The situation became more urgent with every passing day. On 19 October 1946 our Party's army-wide military affairs conference resolved clearly that "We must conclude absolutely that, sooner or later, the French will strike us and we absolutely must strike the French." As a result, at the General Staff and the units, the volume of secret messages to encipher and decipher increased daily, with higher precedences.

On 20 November 1946, the French colonialists opened fire, attacking and occupying Hai Phong and Lang Son, increasing the landing of troops at Da Nang, and staging many provocations in Hanoi. The army cryptographic organizations ensured timely encipherment and decipherment of the leadership guidance and command content from Central and the High Command to the theaters, and enciphered and deciphered the situation reports of the theaters to Central. Thus the operational experiences at Hai Phong, Lang Son, Nam Bo,etc., were quickly sent to other regions to study and apply.

On 16 December 1946, the General Staff cryptographic organization was tasked to encipher a message from the Standing Committee of Central Party to the provincial party HQ in the South, with contents as follows: "According to the situation on the French side and the greediness of the colonialists, there is only one global war, protracted, sharp, with difficulties newly resolved for the sovereignty of Viet Nam. The Party guideline is that it is absolutely essential to prepare. We must have good cadre and masses. Fully understand protracted resistance. Somehow victory will come to us."

In accordance with instructions from Cde Hoang Van Thai, the General Staff cryptographic organization reexamined the cryptographic system arrangements in the units and aligned and allocated cadre and personnel prepared and on duty to perform the mission, so as to quickly encipher or decipher instructions and operational orders of the General Staff, going to the combat sectors and the fronts.

Before the French military provocations in Hanoi took place, the General Staff cryptographic organization, along with the General Staff organizations, moved from 26 Hang Bai Street out to Thai Ha Ap (some 200 meters southwest of Dong Da Hill).

On the night of 18 December 1946, the French military command sent a letter of ultimatum to our government, calling for the stripping of weapons of self-defense and the occupation of the Hanoi Office of Public Security.

Implementing a resolution of the Central Party Standing Committee, the High Command [Bo Tong chi huy] issued the order to open fire and uniformly attack the French military on the night of 19 December 1946. From dawn on the 19th, Cdes Hoang Van Dong and Luong Dzan received orders to carry knapsacks and cryptographic systems up to a special place in the sector and work for the chief of the General Staff (at Thai Ha Ap) in order to await orders. And Cde Hoang Van Thai instructed: All cryptographic cadre and

personnel who did not have to go to a sector to work were to stand by and be prepared to receive assignment.

At 0800 on the morning of 19 December, Cde Hoang Van Dong and Cde Luong Dzan received the task of enciphering an immediate message (received with a note and signature of Cde Hoang Van Thai, "need to encipher at once") going to the units, text as follows:

The French aggressors have issued an ultimatum disarming our army, self-defense, and public security. Our government has rejected this ultimatum. Therefore, at the end of 24 hours the French aggressors will definitely open fire. Instructions from Central: All will be prepared!

On the heels of which, this order from the Minister of National Defense/Commander-in-Chief to the entire military:

The motherland is endangered! The hour of combat has arrived!

Per instructions from President Ho and the government, and as Minister of National Defense and Commander in Chief, I order the entirety of the Vietnamese national army [bo doi Ve quoc quan] and self-defense militia [dan quan tu ve], Central-South-North, to the man, to rise up.

You must rush to the front, kill the aggressor, save the nation.

Give your life in battle, to the last drop of blood!

Exterminate the French colonialist gang.

Be resolved to fight!

Vo Nguyen Giap

The two message texts above were speedily encrypted and sent to the combat sectors and fronts.

Immediately thereafter, flash [hoa toc] messages were enciphered and sent to combat sectors 1, 2, 3, 4, 11 and to Da Nang, with the request that they be in the hands of the command comrades of the sectors and fronts prior to 0930 on 19 December 1946 in order to implement the order to open fire and strike the enemy on a coordinated basis on the theaters of war at the precise hour determined, contents as follows:

"The freight will arrive at 1800 hours 21 December 1946. The freight carries the code symbol A + 2 and B-2. Pay attention and meet the freight at the exact time."

Code symbols A + 2 and B-2 were previously established by the General Staff with the sectors. A was the hour, B was the day of the attack. A + 2 was [the stated time,] 1800, plus 2, or 2000 hours. B-2 was [the stated day,] 21 December minus 2, or the 19th.

At 2000 hours on 19 December 1946, at the High Command [Bo Tong chi huy] organization, which had relocated at that time to Chuong My (Ha Dong), Cde Commander-in-Chief [Tong chi huy] Vo Nguyen Giap stood on Chua Tram mountain along the Mai Linh river looking toward Hanoi and waiting for the signal of our guns. The cadre comrades and soldiers of the operations, communication, and cryptographic organizations also burned with impatience, waiting for the results of their service in transmitting command orders to open fire and strike the enemy.

At exactly 2003 on 19 December 1946, electric lights in the sky over Hanoi suddenly went out. Salvos resounded from the fortresses at Lang, Xuan Canh, Xuan Tao, etc., raining down on the heads of the French aggressors in the strongpoints they had set up in the city.

The Cde Commander-in-Chief was quite satisfied with the results of sending the combat orders of Central and the High Command to the units, guaranteeing timeliness, secrecy, and precision in terms of command organization and technical means which were limited.

Keeping pace with the militia of the Hanoi capital, the army and citizens in the large cities and regions, such as Nam Dinh, Vinh, Hue, Da Nang, Bac Giang, Bac Ninh, Hai Dzuong, etc., also opened fire, striking the French aggressor forces. The military cryptographic organizations in these places ensured accurate, secret, and timely encipherment and decipherment of orders and combat instructions from upper echelons.

Thus having taken the step to war, the army cryptographic organizations, from cryptographic organizations of the combat sectors, fronts, and especially the cryptographic organizations of the Capital, Thang Long, Son Tay, Ha Dong, etc., regiments requirements, did a good job of accomplishing their task of ensuring the service of leadership and command in striking the French aggressors, although the units lacked people and technical means. Via the system of cryptography and communications, the Ministry of National Defense, the High Command [Tong tu lenh], and the General Staff were able to grasp the situation in the theaters of war, and leadership, direction, and command from the Central Party and the army were timely, vis-a-vis the regions [dia phuong] and units throughout the entirety of the nation.

Having come through fifteen months of building organization and technique, while having to serve in ensuring the secrecy of the content of leadership and command from the Party and army via the means of communication, although faced by very many difficulties in this initial period, the army cryptographic branch strove upward to do a good job of accomplishing their mission, handed to them by the Party and army. The principal determining factor was the concern shown by the upper echelon leadership cadre, always creating [favorable] conditions and wholeheartedly assisting the army cryptographic organization in building organization, technique, and its job of serving leadership and command. Cdes Pham Van Dong, Vo Nguyen Giap, and Hoang Van Thai, etc., in the first stage of establishing the army cryptographic branch, not only provided concrete guidance concerning the direction of the job, but also personally introduced and assisted in the selection of trustworthy people--personally commented, gave suggestions, sought out documents for the cryptographic organization. After the July-August 1946 Fontainebleau Conference, Cde Pham Van Dong returned, bringing a French book on cryptography, *Le Chiffrement et le dechiffrement*, by Jean Bubois, and passed it to the cryptographic organization for research and reference. Although these accomplishments were only the first step, they demonstrated patriotism, self-reliant will to create technique, and minds

determined to accomplish the mission, on the part of the initial contingent of army cryptographic cadre and personnel.

These results and accomplishments have extreme significance, in that they helped the branch extract lessons from real life experience and participate in the building and combat of the branch.

Notes

1. Based on the 7 September 1945 directive concerning the establishment of the General Staff, Ministry of National Defense (in the History of the General Staff).

2. Now 18 Nguyen Dzu Street, Hanoi

3. Cde Ta Quang De (Ta Quang Dam) is a patriot intellectual who had been a district chief, a scoutmaster in the old Boy Scout movement, and in the student and youth movements before the August revolution. Cde De was given the responsibility of chief secretary of the Communications-Liaison Bureau, especially in charge of cryptography.

4. Thuyen later took the nom de guerre of Hoang Thanh; he was a senior scout in Thanh Hoa, in the troop of which De was scout master. Cde Quan, alias Cde Hoang Van Dong, was chief of the Cryptographic Bureau from the end of 1946.

5. Cde Tung Anh intended to study and become expert, then return to the regional level, but he was retained afterward at the Cryptographic Bureau.

6. Original title, *Elements Cryptographic* (by Capitaine Baudouin). [Reference is evidently to the first, 1939, edition rather than the later, 1946, edition, which reflects the author's rank as major. A copy of this work, inscribed by the author to American cryptologist William F. Friedman, recalling a shared experience in World War I with the U.S. 32nd Infantry Division, is in the Friedman Collection, Marshall Library, Lexington, Virginia. -- Tr./Ed.]

7. The scouting movement of Vietnamese and Indochinese youths and students before the August Revolution involved games such as "Morse Code" and "Maneuver" (a big game). In the "Maneuver" game, the player had to solve secret letters written under the form of a simple cipher.

8. Each letter [piece of correspondence] had a group of digits used to make the cipher key.

9. Subordinate to the relief army newly organized when the French forces entered the North "to guard Japanese POWs," replacing Chiang's forces, who withdrew back home.

Chapter Two

Consolidating and Building Organization and Professional Technique, Meeting Command Leadership Requirements in the First Five Months of the Protracted Resistance (1947–1950)

THE ARMY CRYPTOGRAPHIC BRANCH BUILDS AND SERVES IN COMBAT IN 1947

As 1947 began, war had spread to many places. From the very first years of the resistance against the French colonialists, the MND-High Command and General Staff were settled on expansion of the armed forces and set the course for the activities and tasks of the army cryptographic branch. The resolution of the first Nationwide Conference on Military Affairs, meeting from 12-16 January 1947, put it clearly: ". . . we must pay attention to the immediate training of many cryptographic personnel. Don't constantly shift cryptographic personnel around." In a resolution of the Conference of Sector Chiefs, meeting in Viet Bac in March 1947, under "troop problems," and the objective of "organizing the specialty branches of the troops," is also stated: ". . . we must train personnel and organize communication among the troops by cryptography."

Implementing the resolution of the above conferences and directions of the High Command and the Chief of the General Staff, the army cryptographic branch carried out many means of expanding and correcting the organization and training of cadre and personnel, researching the production of cryptographic systems, and organizing their use in meeting the requirement for command secrecy by cryptographic technique when employing communication media.

In February 1947, with agreement of the High Command, the Cryptographic Bureau organized the third Army-wide Cryptographic Conference, the purpose being to strengthen and ensure liaison on all lines, between Central and the regions, and between the regions and units, with each other. The conference requested the Cryptographic Bureau compile basic theory documents on cryptography to disseminate for cryptographic organizations army-wide.

Implementing the conference's resolution and satisfying the work of "organizing communication by cryptography," in February 1947 the High Command Cryptographic Bureau opened the second Cryptographic Personnel Training Course. Named "Viet Bac," this class opened in the village of Yen Thong, Dinh Hoa district, Thai Nguyen. Room and board for the students and class sessions alike were in the homes of compatriots in the area. The syllabus for this class was more or less that of the first class ("Hoang Dzieu"),

with special attention paid to setting aside more practice periods. Of the more than twenty students in this class, there were a number of female personnel, such as young Miss Kim Chi, Hoang Bao Khanh, Hoang Lan, Nguyen Thi Lien, Le Anh Phuong, etc.

When it moved up to the Viet Bac revolutionary base (early 1947) the Cryptographic Bureau settled, as a matter of urgency, on a place to set up shop, and afterwards continually carried out all aspects of the task of building the branch, requesting upper echelons to supplement with a number of cadre and personnel, and implementing production of the types of cryptographic systems to supply to the units.

As of June 1947, the Cryptographic Bureau set up a party cell comprising comrades Ho Ton Vinh, Hoang Van Dong, Luong Dzan, Vu To, Nguyen Chanh Can, and Hoang Manh Tuan.

On 19 July 1947, President Ho Chi Minh signed a decree concerning the organization of the top-level command organizations of our army, consisting of the High Command and the Ministry of National Defense. According to this organization, the Central cryptographic organization became two cryptographic bureaus: the Ministry of National Defense Cryptographic Bureau, with responsibility for encrypting and decrypting messages serving command and the rear services mission, at the same time researching cryptography and cryptanalysis. The bureau was the charge of comrade Dinh Loan Thuyen. The Cryptographic Bureau of the High Command had responsibility for encrypting and decrypting secret messages of command guidance for army operations, building forces and various other aspects of the task,while at the same time researching and producing cryptographic systems (supplied to units army-wide), training cryptographic cadre and personnel, and research concerning cryptanalysis--Cde Hoang Van Dong was bureau chief. The bureau consisted of these sections: the Research and Training Section, the Clerical Section, and the Encrypting-Decrypting Section. The troop strength of the bureau of this time was sixteen people. Formerly, getting people to come do cryptographic work was usually from the troops – afterward, all of the people were chosen from outside. Because one could not come right out with the conditions and requirements of the task, when they finally saw the strict demands of the task, a number of personnel wanted to get out of enciphering and deciphering, or asked for a change in assignment. Being short of cadre because of supplementing the units, the bureau selected a number of female cadre: the youngsters were industrious in their work, but, when the time came that there was a need to organize cryptographic elements to go and serve on the front, there were difficulties because of the lack of male cadre.

The Encrypting-Decrypting Section only had two teams, one in charge of encrypting and decrypting with the sectors in the South, one with the sectors in the North. The technique of encrypting and decrypting had advanced greatly, compared with the previous year. In the course of a year, the cadre and personnel had become rather well acquainted with the various types of cryptographic materials, and enciphering and deciphering was fast and went without a hitch. By April 1947, outside of the regular liaison points [dau moi], cryptographic liaison nets were opened and expanded with Sector 6, the Southern Resistance Committee, and several sectors in Nam Bo. From the middle of 1947 on, with

hostilities spreading, the cryptographic organizations expanded and liaison by radio was much increased. The cryptographic organizations took care of encryption and decryption to serve leadership and command with a noticeable volume of traffic: Figured from the beginning of the year until September 1947, the total number of secret messages outgoing and incoming at the Cryptographic Bureau approached 2,700 official messages. Especially, during this period, liaison with units in the South was relatively ensured regularly and steadily.

The cryptographic correspondence task became more routine in all of the work of copying messages,sending, receiving, and holding secret messages, incoming and outgoing.

In the sectors, the cryptographic sections were strengthened another notch. The Cryptographic Section's principal mission was the encryption and decryption of secret messages. Besides this, a number of places had entrusted to them the making of cryptographic systems and the training of cryptographic cadre and personnel from their own unit.

From February 1947, the Sector 1 Cryptographic Section implemented consolidation and building of cryptographic organization in the units below regimental echelon: the first stage, consolidating and building cryptographic organizations of battalions subordinate to regiments; the next stage, from the Second Sector Cryptographic Conference (August 1947) until the unification that produced Inter-sector 1 Cryptography, at which stage the cryptographic organizations were extended to a number of companies. When the Sector main force battalions had cryptographic organizations, the Cryptographic Section arranged direct means of liaison with these battalions, but, with the task of researching and producing systems during this period, the Sector Cryptographic Section could then only take care of the regiments, essentially by estimating cryptographic system usage, rather than showing new initiatives, leaving the regiments themselves to see to the cryptographic systems for battalion and company echelons.

The cryptographic organizations in Sector 3 formed a vertical structure in their speciality although the liaison organizations were not expanded and under firm control. The Sector Cryptographic Section organized a cryptographic net down to battalion and a number of essential independent companies. Besides these there were still a number of points in cryptographic liaison, including joint units from the Route 5 Front, provincial Resistance Committees, and local activities of the intelligence and munitions [quan gioi] branches, that needed to organize liaison by military cryptography. The cryptographic teams of the 34th and 42nd regiments regularly kept in liaison with the Sector Command [Bo chi huy Khu] and liaison with a number of battalions (via the means of Communication-Liaison's telephones). Average daily volume of message traffic by cryptography, sector-wide, was 100 official messages. During this time, because of few people, the section chief normally had to assume responsibility for the clerical mission, training, and system research; they almost never had systems in reserve--when it became necessary to organize joint liaison with regiments outside the area of responsibility of the

sector, then there were no systems available to make prompt arrangements (e.g., with the Vinh Phuc and Dong Trieu regiments).

Also in 1947, in Sector 2, although the cryptographic organization had a structure of vertical organization, there was only liaison with one another in the areas of encrypting and decrypting secret messages--there was virtually no exchange of experience, specialty inspection, or the like. At Sector HQ, the Cryptographic Section only had three to four people, because the specialized elements had not yet been set up.

Sectors 2 and 3 opened a class for training in cryptography: the bulk of the content concentrated on practice, but a portion of the remainder followed the syllabus of the HQ training course. Selecting people to go work in cryptography was rather deliberate and careful, and selection was from among educated military personnel, endorsed by the immediate command echelons. Each military person going to work in cryptography had to have sufficient papers, such as personal history, endorsement from immediate commander, obligation to serve and maintain the secrecy of cryptography for the period of two years at the minimum, etc., sent to the Intersector Cryptographic Section.

In 1947, in Sector 4, there was a unified cryptographic organization, sector-wide, but, from the standpoint of horizontal and vertical control, it was still immature--the cryptographic organization had yet to have basic units, especially cryptographic organization in the area temporarily occupied by the enemy. The sector cryptographic organization at this time comprised only three comrades, one of whom was in the HQ Hoang Dzieu class, sent back as an augmentee, but still inexperienced, so the consolidation of the cryptographic organizational structure in Sector 4 encountered many difficulties and expanded slowly, compared to other sectors.

In mid-year 1947, although a structure had been formed, the Sector 5 cryptographic organization was not yet under tight control. The comrades in charge of regimental cryptography were routinely sent off on other tasks. As a result, cryptographic security was not thoroughly maintained. Many of the fellows doing message clerical work did not yet have their act together on outgoing and incoming messages. As for cryptographic systems, they followed, for the most part, the Cryptographic Bureau models with little modification, such as using the Julius Caesar substitution method, afterward adding the Stook [*sic*] system, which was somewhat more advanced.

In March 1947, Sector 5 opened its initial cryptographic course, with about twenty students. Although still lacking in training experience and teaching material, nevertheless the requirement was met to extend the cryptographic organization in the theater of southern and central Trung Bo [Annam]. In order to correct the organization and establish the important parts of the task according to the instructions of the Sector 5 Command, in July 1947 the Cryptographic Section convened a sector-wide cryptographic conference. Problems dealt with at the conference were: correcting the system of organization sector-wide, defining the posting of cryptographic cadre and cryptographic personnel, lessons learned from the task of encrypting and decrypting, etc., doing their bit to help settle the organization and realize the mission of the Sector 5 cryptographic

organizations. Thus by the end of 1947, cryptographic liaison between the Sector HQ and the units was speedier and smoother than before.

In Sector 6, extreme south Trung Bo, three quarters of the area was temporarily occupied by the enemy, and communication was both very difficult and dangerous. The cryptographic organization was lacking in cadre-in-charge--most of them had additional duties. The cryptographic liaison net from Sector down to five regiments (the 80th Regt., Phu Yen; 83rd, Khanh Hoa; 81st, Ninh Thuan; 82nd Binh Thuan; and 79th, Dac Lac) was firmly in hand, but there were still no few difficulties. Seeing that the Sector 6 cryptographic organization had many weak aspects that had to be shored up, in accordance with a May 1947 proposal of the High Command Cryptographic Bureau, HQ decided to appoint Cde Nguyen Van Dzanh (a Cryptographic Bureau Cadre augmenting Sector 5) to go down and take over the Sector 6 Cryptographic Section.

Also from May 1947 the Cryptographic Section was separated from the secretariat and made directly subordinate to the Sector Command [Bo chi huy Khu]. In June 1947, the Sector 6 Cryptographic Section organized a sector-wide cryptographic conference to discuss the matters of improving the organization, replacing cryptographic systems, unified operating procedures, and the organization of a direct cryptographic liaison net with HQ. In August 1947 the Sector Cryptographic Section opened a cryptographic training class, adding to the sector headquarters organizations and a number of independent regiments in the area. With the regiments in the area temporarily occupied by the enemy, the Cryptographic Section drew a number of cryptographic materials from the Hoang Dzieu course to send to the fellows performing cryptography to research and study themselves.

Vis-a-vis the Nam Bo theater--a theater with "no forward area, no rear area"--with dense jungle, honeycombed with canals and streams, and enemy blocking posts, the need for cryptographic organizations had to overcome many obstacles in solving the problems of disseminating cryptographic systems and training cadre and personnel to respond to mission requirements. Conditions did not permit the Nam Bo cryptographic organizations to come up and attend the cryptographic training classes and cryptographic conferences at Central, so the exchange and acceptance of general experiences of the branch were limited. To overcome this limitation, the Cryptographic Bureau issued guidance and professional exchanges by message, and took advantage of leadership and command comrades being posted to Nam Bo to send along a number of models of cryptographic systems. Under the guidance of HQ, Nam Bo, the military cryptographic branch in Nam Bo progressed step by step.

Concurrent with the tasks of building organization, training cadre and personnel, and arranging liaison nets, the army cryptographic branch advanced in research and promulgation of cryptographic technique. Systems were all improved with respect to content and format. Chart systems were constructed more scientifically. The plain content of the chart was enriched, the display clarified and made convenient for encrypting and decrypting. The cipher strip had many columns, the movable horizontal strips had many scrambled rows of cipher letters in order to produce polyalphabetic substitution,

speed up things, and increase security. The seven-column system was enhanced in quantity by the method of using irregularly and in rotation the ten columns in twenty-six random, unrepeated, alphabets, thus changing the appearance of the cipher text to a rather high degree. This type of system was arranged and brought into play in the liaison net between HQ and the sectors, with the designation "Glori-CK."

Initial specialist-task discipline was built with a number of regulations: work "close by" the person in command; when you are working, you must be secretive; you must keep the content of secret messages just as securely as you do your cryptographic systems, etc.

These initial advances in organization, professional technique and routinizing the task demonstrated that the army cryptographic branch was filled with the spirit of the instruction from the Standing Committee of the Central Party: "Frequently change cryptography and the hours of contact of the radio stations; militarize the radio station and cryptographic organizations."[1] This was also the basis for the success of the branch in realizing its mission of maintaining command security by cryptography when we moved into combat to defeat the assault by the French aggressors into the Viet Bac revolutionary base in the fall and winter of 1947.

In October 1947, the French colonialists concentrated a large force, consisting of 20,000 men, forty aircraft,and eighty motorized vehicles, to open a three-directional assault on Viet Bac, aiming to "strike our nerve centers of resistance, wipe out our main force units, [and] have conditions in which they could install puppet authority on the spot."[2]

On 15 October 1947, the Standing Committee of the Central Party issued instructions to demolish the winter offensive by the French aggressors, and, at the same time, proposed the mission and delineated the course of action by the military and people of Viet Bac and our entire nation.

On 27 October, the Cryptographic Bureau cadre and personnel of the High Command conveyed Order No. 132 from the High Command to the sectors and units nationwide: "Strike hard on the Song Lo and Route 4 front; destroy transportation supplying the enemy, set up ambushes on the jungle roads, strike the river routes;constantly harass the enemy bases, encircle and eliminate small positions. Sectors are to strike hard in order to coordinate with Viet Bac."

On its heels was a secret message from the Cde Chief of the General Staff assigning responsibilities to the units as follows:

> "On the Rte 4 front, the 74th Regiment (Sector 1) is in charge of the Cao Bang front, with the Lang Son Regiment (Sector 12) having the mission of striking hard on Route 4 from Lang Son to Dong Khue. The 2nd Battalion of the 350th Regiment of HQ has the mission of striking the enemy on the Lang Son - Vo Nhai Road. The 232rd Battalion of HQ blocks Binh Gia Street. The 80th Battalion of HQ is stationed at Trang Xa, Dinh Ca.

"On the Song Lo front: the 112th Regt (Tuyen Quang), the Sector 10 artillery units, and the 18th Bn of HQ have the mission of striking the enemy transportation on the river and on foot.

"The 72nd Regt and the 19th Bn (Sector 1), the 102nd, and the 160th Bns of HQ have the mission of striking the enemy on the Route 3 front.

"On the Tuyen [Quang]-Thai [Nguyen)] road front, use the 350th Regt of HQ, two regional battalions, and the 103 Bn of HQ (if necessary, these can be augmented with additional mobile forces) . . . ."

The cryptographic organizations throughout the military labored unmindful of day or night, transmitting as a matter of urgency the instructions, orders, and reports, secretly, swiftly, and accurately.

During this same time, implementing instructions from the Chief of the General Staff, the Cryptographic Bureau divided its forces according to the organizations of the High Command and General Staff and prepared to arrange people and means to perform the mission in various directions.

The force to remain behind in Dinh Hoa (besides having to ensure liaison with the light element of the High Command) was responsible for the cryptographic liaison net with the units subordinate to southern Trung Bo and Nam Bo.

The force to accompany the important greater portion of the HQ organization moving up to the new site (Don market, in Bac Can) was responsible for liaison with units in Bac Bo [Tonkin] and Sector 4. At the same time, the Bureau assigned three cryptographic teams to go and serve in three places: one team, under Cde Luong Dzan, to accompany Cde Commander-in-Chief Vo Nguyen Giap personally studying the Route 4 front in order to derive general experiences to direct the other fronts; one team to go with Cde Chief of the General Staff Hoang Van Thai down to direct the preparation of a secure base sector for the Central Party and the government, to block the enemy pushing down toward Chu market, directing the evacuation of workshops and depots around the town of Bac Can, this team being under Cde Hoang Manh Tuan. The third team, under Cde Tran Dien, went to serve alongside the Central Party organizations.

Having to organize many task elements when the cadre and personnel were few, having to organize cryptographic liaison nets over a wide area and to coordinate many units, with cryptographic message volume more than before, still the cryptographic cadre and personnel sensed the significance of the battle, made many efforts that surpassed expectations, realized the encryption and decryption to ensure that the transmission of each order, directive, and report was accurate and timely. In the sectors and fronts combined, the cryptographic organizations also performed their mission well. The army cryptographic branch diligently and efficiently served the leadership and command comrades at all levels, participating in the glorious victory that shattered the French aggressors' attack, guarded the security of the Viet Bac base, kept intact and expanded [our] forces, and held the resistance base of the whole nation.

The army cryptographic branch passed the test and grew another notch, deriving many useful experiences in the mission of combat service, on a far-flung front, responding to the requirement of our army to speed up mobile warfare.

EXPANDING ORGANIZATION - STEPPING UP THE TRAINING OF CADRE AND PERSONNEL

The Fall-Winter victory of 1947 in Viet Bac ushered the resistance of our people into a new stage.

So as to consolidate direction from the Central party and Main Military Committee in the new stage, the Central party determined to strengthen the directing organizations at the various levels, especially the military organizations. On 25 January 1948, the President of the Democratic Republic of Viet-Nam issued a decree organizing and unifying the sectors, to create "intersectors" from north to south: the seven sectors in Bac Bo [Tonkin] merged into three intersectors, intersectors 1, 10, and 3. The four sectors in Trung Bo [Annam] made two intersectors, intersectors 4 and 5. In Nam Bo [Cochin-China], there would be three sectors, 7, 8, and 9, and the Saigon-Cholon Special sector. One element of the main force military was broken up to produce independent companies, armed propaganda units, and volunteer sections for deep penetration into areas occupied by the enemy, to mobilize guerrilla warfare. Consolidated battalions were organized with the mission of mobile operations to sap enemy strength, and create conditions for the spread of guerrilla warfare. The cryptographic task was also realigned, consistent with the organization and command requirements of the High Command, the Intersectors, and the units.

The Intersector Cryptographic Sections were established on the basis of unifying the Sector Cryptographic Sections, while, at the same time, cryptographic organization in lower- level units was also being strengthened, in accordance with the spirit of the 30 January 1948 General Staff instruction: "Organizations must militarize, retaining only the essential elements . . . the troops must be lean and orderly, suitably equipped . . .relying on cadre ability and standards, and our equipment capabilities . . . ."

In order to participate quickly in strengthening the organization of cryptographic activities of HQ and the Intersectors and units, and to meet the requirements of the theaters of war, in April 1948 the Cryptographic Bureau itself opened the third class for training cryptographers. This class took the name the Bong Lau class. Sessions were conducted in the village of Yen Thong, Dinh Hoa district, Thai Nguyen. From northern Trung Bo up, and from units in the High Command, forty-five students were selected to come study--the majority of these being comrades who, although they had worked in cryptography, had never received school training. Cde Hoang Van Dong was in charge, and a number of Cryptographic Bureau cadre were appointed instructors. The classroom was rather tightly organized. The syllabus was improved and at a higher level than previous classes. Besides the part on training in the professional speciality, special emphasis was placed on training in grasping the responsibilities of the mission, and making routine out of the task of organization and cryptographic cadre and personnel at

the various levels. Students researched and practiced making cryptographic systems, researched the frequency of the Vietnamese language, cryptanalytic methods, and principles of security. In the final examination, besides questions about classic cryptographic theory and cryptanalytic practices, each student had to personally produce a code chart [bang luat]. After two months of study, it was essential that the students from units and intersectors return to those units and intersectors. Upon return to their units, the students spread the results of their training. Many comrades were selected to take charge of regimental cryptography or as team chiefs for research and training in the intersector cryptographic sections.

Of this class, three comrades, Nguyen Van Dzuyet, Tran Cong Ta, and Le Nhan, became augmentees for the cryptographic organizations of the Party-Government system.[3]

After their establishment, and, as a matter of immediate attention, the Cryptographic Sections of the intersectors commenced to build organization responsive to mission requirements in accordance with their function.

The Intersector 1 Cryptographic Section came into being in February 1948, comprising the merged Sector 1 and old Sector 12 Cryptographic Sections, quickly settling the organization and consolidation of the Intersector's subordinate cryptographic organizations. Cde Ngo Vi Thien was Section Chief. Most important of the Intersector's cryptographic tasks in 1948 was the organization of cryptography for units subordinate to old Sector 12 and Intersector HQ. The Intersector Cryptographic Section took its structure from elements on the spot, such as those of the former Sector 1. As task requirements and the number of personnel increased, the enciphering-deciphering element was divided into two teams, secretariat and enciphering-deciphering. The dividing of specialized responsibilities in the Section was made clearer, the work of the two teams went deeper into specialization, orderly routine, increased productivity in the task.

The Intersector Cryptographic Section organized many conferences to solve problems of organization, technique, and professional knowledge vis-a-vis cryptography intersector-wide; organized and mobilized emulation movements, raising to a feverish pitch the working atmosphere from Section down to the organization of unit cryptographic. The plan to rectify the organization and expand cryptography to the units was constructed in parallel, with concrete provisions, divided by time periods for realization. At the beginning they concentrated on rectifying the regimental cryptographic organization. Afterward, cryptographic organization was expanded to the battalions and component companies of the regiments. This work met no few difficulties, for cryptographic personnel were insufficient, and a number of unit command comrades had yet to perceive the necessity of expanding cryptographic organization.

With the direction and support of the Intersector Cryptographic Section, the cryptographic organization of the regiments was built single-mindedly, by seeking out ways of realizing the plan. In order to have a sufficient quantity, and to raise the level of cryptographic cadre and personnel for directly subordinate units, all regiments opened training classes in the use of cryptographic technique, averaging ten to fifteen days each.

From February 1948 to January 1949, the regiments opened eight classes, with nearly sixty students.

The Intersector Cryptographic Section also launched an effect to foster cryptographic cadre-in-charge for the units, comprising ten comrades studying for one month. In nearly two years, Intersector Cryptography had held twelve classes for nearly 100 cryptographic students.

Notwithstanding, the mission of developing cryptographic cadre and personnel in Intersector 1 still floundered and was hindered by difficulties: the criteria for selecting people to go work in cryptography initially were boiled down to just one consideration--a cultural level equivalent to the first class, vouched for by the unit command section, but realistically the majority only had a level of elementary education, or second class. And through practice of the mission, Intersector 1 Cryptography still showed weak aspects of hit-or-miss training conditions and no unified program--not yet organized to summarize and publicize specialist lessons learned – not a few of "the cryptographic personnel weren't keen on the cryptographic mission because they'd been pushed into it and saw progress as slow, principally in battalion and company cryptographic."[4] Between an atmosphere of combat seething throughout the army and a breast full of enthusiasm on the part of young people, there were those whose aspiration was to bear arms to kill the aggressor.

The administration of cryptographic cadre and personnel was also initially determined: appointing a regimental-level cryppie as recommended by the Intersector Cryptographic Section and decided upon by the intersector HQ; appointing cryptographic team chiefs under routine orders of Intersector decision. But at regimental level, wishing to propose appointment of battalion and company cryptographic personnel remained extremely difficult, because the majority of the mates had concurrent responsibilities, holding different assignments (the bulk of the cryppies were also company clerks).

Enciphering and deciphering continued as the essential task – serving combat command by means of cryptographic technique in battle. The cryppies accumulated on-the-job experience, avoiding many mistakes in enciphering and deciphering, emulating precise encipherment and decipherment, and seeking out methods of decipherment of messages containing many groups enciphered in error. The emulation drive between units, monitored by the Cryptographic Section, was mobilized beginning August 1948, and pursued monthly, with observations and results communicated to all units, etc., resulting in visible progress in specialization capability on the part of cadre and personnel, generally speaking.

In January 1949, the third Intersector-wide cryptographic conference concluded that the most important task was to strengthen every aspect of Intersector cryptography, with special attention being paid to developing the branch's technique. Responding favorably to the emulation drive mobilized by the branch to produce innovation and improvement in technique, at Intersector [level] a research team was created--one of three essential teams in the Cryptographic Section.

[After] more than three years of building and strengthening the organizational system from Intersector Cryptographic Section down to the unit cryptographic organizations, the Intersector 1 cryptographic organization (and before that the Sector 1 cryptographic) observed themselves:

1. From a tiny organization, careless and casual, until now, the Intersector 1 cryptographic branch has developed into indispensable units and is advancing rapidly on the path of development in order to grow with the national army.

2. The specialist assignment has advanced a great deal, enciphering and deciphering rapidly, and with innovations, having new products, so as to be separated from the cryptographic systems previously in use.

3. [With] personnel from six to seven people, weak in capability, to the present expansion - 100 cryppies, the majority trained. Cryptographic cadre in the units also have adequate capability in the specialty task. As a result, the cryptographic branch has progressed and its capabilities will progress even more as a result of the strenuous emulation effort:

- Rectifying organization sensibly
- Thoroughly grasping and leading the units in the speciality task
- Researching and developing . . .[5]

In Intersector 3 in February 1948, the Cryptographic sections of Sectors 2 and 3 merged to create the Cryptographic Section of Intersector 3. The Intersector 3 Cryptographic section quickly established a system of organization and unification for the entire Intersector. Cryptographic organization of the intersector comprised: at Intersector HQ, the Cryptographic Section, under Comrade Le Hai; Cryptographic Sub-sections at regimental level; cryptographic teams at battalion; and cryptographic sub-teams [tieu to] at company level.

The Intersector Cryptographic Section was an independent section directly subordinate to the Intersector HQ. Troop strength was increased through the merger, building the foundation for organizing Intersector cryptography and quickly firming up the task.

After 1948, following their defeat in Viet Bac, the French aggressors turned their strength to the [Red River] Delta region in a policy of "squeeze and spread the oil slick" to protect this important theater of war.

[As to] serving command in a broad area of responsibility: the Delta is a place of dense population and much property – the enemy made a push to destroy the revolutionary bases and capture cadre and guerrillas, win the people, and plunder the property. The mission of the intersector cryptographic organization was to ensure command secrecy by cryptography via radio, the content being guidance for carrying out the frustration of the enemy's new trick and schemes, striking guerrillas, destroying the puppet administration, serving combat operations--quite a bit of message volume. Each day the Intersector HQ had around 300 official messages outgoing and incoming.[6] With a lot of messages, the principal task for the Section centered on encryption and decryption. The Cryptographic

Section had the mission of directly handling official messages with the bureaus and sections of HQ and also with external organizations (e.g., the Resistance Committees, etc.).

Right from the time of its establishment, Intersector 3 cryptographic become the concern of Intersector HQ, creating conditions from a material [standpoint] while mobilizing the intellect: HQ had instructions concerning the cryptographic task sent to unit command sections. The principal content of the instructions brought up the essentiality of liaison by means of cryptography; selection and appointment; policies toward people performing the cryptographic task, etc.

From mid-year 1948, in the 42nd, 64th, and 34th regiments, cryptographic organization had developed down to the companies, the provincial resistance administrative committees, and the armed propaganda units. The regiments had contact both by radio and wire, thus, between Intersector and regiments, close, solid liaison was assured. If, at the Intersector, the research task was constrained by a volume of cipher messages that had to be gotten out, the comrades in charge of cryptography down at regiment were able to participate constructively in research and to produce systems through their own activity.

The Intersector Cryptographic Section organized a talkfest, a form of specialist activity appropriate to the time, with the object of mutual assistance in the specialty task between the cryptographic organizations of the Intersector, creating circumstances for the unit cryptographic organizations to comprehend and bond tightly, uniting with one another in the assignment, exchanging and supplementing each other's experiences.

By 1949, as a result of changes by the Intersector HQ, the secretariat [van phong] of the HQ was turned into the Clerical Bureau [phong bi thu] of HQ, Intersector 3, the Cryptographic Section becoming one of two principal sections in the Clerical Bureau, managed by the chief clerk as far as administrative matters were concerned, and by the Intersector HQ as far as the specialty task was concerned. Troop strength of the Cryptographic Section was twelve people, as when the Intersector was formed, with a seven-man Encrypting-Decrypting Subsection divided into an encrypting-decrypting liaison element with HQ and an encrypting-decrypting element with the regiments, etc. The clerical subsection had three people copying, receiving, and sending messages and papers. It must be said that the cryptographic teams of the regiments subordinate to the Intersector were developing greatly during this period. Component battalions, companies, and special units engaged in armed propaganda in the enemy areas all could use cryptography. Besides ensuring and arranging cryptographic liaison nets in the military system of the intersector, the Resistance Administrative Committee, the armed propaganda units, and detached guerrillas, liaison nets also had to be open with intelligence, munitions,the provincial units, the Command sections of the fronts, etc. The Intersector, in particular, set up an additional liaison net with the Route 5 front to ensure firm, constant contact.)

The number of liaison points having thus grown, each cadre and person had to look into the work of encrypting and decrypting and constructing new cryptomaterials

adequate to satisfy the immediate need, and that in the short term. Each time Cryptographic had to supply cryptographic materials for radio stations popping up from nowhere was a test of the Intersector cryptographic organization, having to surge to overcome obstacles and accomplish the new mission.

A routine horizontal check of the Intersector branch having taken shape, there had to be a concrete check of subordinate levels. The Intersector Cryptographic Section checked regimental cryptography; regimental cryptographic checked that of the battalions and companies.

In 1949 the Intersector Cryptographic Section held thirteen training classes, both in-service and classroom. Through these classes they created conditions for 75 percent of the total of 130 cryptographic cadre and warriors in the Intersector studying to raise their proficiency.

****

In September 1948, the Intersector 10 Cryptographic Section was set up, after Sector 14 merged with Sector 10. Comrade Ngan Ba Hong was assigned as section chief. The Intersector 10 Cryptographic Section convened an Intersector-wide cryptographic conference to unify and perfect the organization, reorganize the cadre, and replace cryptographic materials.

At the Intersector level, the Cryptographic Section formed three subsections:

- Encryption-decryption Subsection
- Clerical Subsection
- Training and Techniques Research Subsection

Cryptographic organization at regimental level was unified and called the Cryptographic Subsection; at battalion and company, it was the Cryptographic Clerk.

Responsibilities of the Cryptographic Section were determined at the Intersector Cryptographic Conference as ensuring encryption and decryption for the Intersector HQ; building a cryptographic liaison net system for the entire Intersector; supplying cryptographic materials and systems for the independent regiments and battalions; and holding classes for cryptographic cadre and personnel.

Around the end of 1948, the Intersector 10 Cryptographic Section opened a supplemental class for cadre in charge of cryptography in the Intersector, taking the name "Nguyen Van To" for the class, which comprised twenty student comrades. The 148th and Song Lo regiments also held classes to improve cryptographic personnel for battalion and company echelons.

Besides their principal responsibility for encrypting and decrypting, the regimental cryptographic subsections also had a regular responsibility doing a frequency count of the Vietnamese language, in accordance with a work plan and directions from the Intersector Cryptographic Section.

****

After 1948, the cryptographic organizations of Intersector 4 were consolidated and expanded.

At Intersector HQ there was the Cryptographic Section under the HQ secretariat. The Section Chief was Ho Si Bang. The Intersector Cryptographic Section had three teams: clerical, encrypting-decrypting, and research and training. The encrypting-decrypting team had two elements: the element encrypting and decrypting within the sector, and the element encrypting and decrypting external to the sector.

Regiments had cryptographic teams directly under the staff, Command Section, or political commissar. The cryptographic team had around three or four people.

At battalion-level cryptographic, there were two people, and one at company level. In 1948, Intersector cryptographic expanded to the battalions and a number of independent companies.

On the Hue-[Quang] Binh-[Quang] Tri-[Thua] Thien front, there was established a Binh-Tri-Thien Sub-Sector Cryptographic Section, with a liaison net comprising the 101st Regiment, 95th Regiment, with Intersector 4, Intersector 5, and the High Command [Bo Tong Chi Huy].

After the battle of Hoi Mit, because of the compromise of cryptographic techniques of organizations outside of the army, the Intersector [Party] Committee convened an Intersector-wide cryptographic conference to unify and standardize the cryptographic task. A common cryptographic organization was established for the entire Intersector (embracing the cryptographic responsibility of the army, the resistance, public security, intelligence, etc.). This organization had the responsibility to make cryptographic systems to use in the Intersector.

As for the cryptographic organizations in Intersector 5, the High Command augmented cadre to go down and help consolidate and strengthen in various aspects.[7]

Aiming to correct the shortfalls in communication liaison and see to daily improvement for command guidance at the various echelons, according to a proposal from the Sector 5 Cryptographic Section, and with the concurrence of the government representative in the South and that of Sector HQ, on 24 and 25 February 1948, a Southern Trung Bo [southern Annam] cryptographic conference (sponsored by Sector 5) was convened. Attending the conference specially was Cde Pham Van Dong, the government representative, and the gentlemen who headed the secretariat and radio of

the South, the post-telecommunications director of the South, representatives of Sectors 5, 6, and 15 cryptographic, the Resistance Administrative Committee of southern Trung Bo, representative of the Southern Trung Bo Liaison Bureau, etc.

The conference discussed means of consolidating the system of liaison in Southern Trung Bo; the unification of the cryptographic branch in the sectors; alleviating some remaining shortcomings, such as the relationship between the postal and cryptographic branches in the matter of message precedence indicators, etc.

In accordance with the 25 January 1948 decree, as of September 1949 Intersector 5 was officially established, comprising Sectors 5, 6, and 15. At that time the situation with respect to development of the cryptographic organizations was not uniform. The Sector 5 cryptographic organization was relatively routinized and methodical, whereas Sector 6 was still undergoing consolidation and still divided into military cryptography, political cryptography, etc., and Sector 15's cryptographic organization was just taking shape, for Sector 15 was established last. Thus an orderly cryptographic task in Southern Trung Bo had not yet been built through unification, relating tasks between the cryptographic and postal organizations; radio was not yet tight in hand; the sending and receiving of messages was still error-prone and late. Confronted by this situation, the High Command appointed Cde Nguyen Chanh Can, a Cryptographic Bureau cadre, to go down and assist the Intersector cryptographic organizations in straightening itself out and in increasing liaison between the Intersector and HQ.

In Nam Bo, at the end of 1948, Cde Vu To, a cadre of the Cryptographic Bureau, was assigned by the High Command to go down to Nam Bo to "grasp and comprehend thoroughly the cryptographic situation in the sectors and to hand over cryptographic materials,"[8] and to strengthen the organization and the technical cryptographic skills of the units of the Nam Bo theater. To that end, he was appointed chief of the Nam Bo Cryptographic Section, "although a cadre from Central, still quite young."[9] After being strengthened by cadre sent down from the Cryptographic Bureau, the Nam Bo cryptographic organization systematically progressed in its building and expansion. The situation involving the cryptographic task was part and parcel of the general situation of the staff task in 1948, that being "a year in which the staff task had to pay much attention to organization to realize Central's program for expanding guerrilla resistance all over the place, not just in the main theater but beginning to pay attention to the theaters of [Quang] Binh-[Quang] Tri-[Thua] Thien and Sector 5,Nam Bo, Laos, Cambodia, etc. Thus this was a fresh task . . . not yet having satisfied the heavy [original]mission entrusted from above . . . The system of communication liaison with the sectors and provinces was not yet coordinated wide scale, principally with distant theaters."[10]

In order to overcome the difficulty of a situation in which a theater was split up, yet leadership and command had to be assured on a timely basis, in 1949 Sector 8 organized radio station equipment and organized cryptography in the various regiments and battalions, such as the 310th and 925th battalions of the 99thRegiment and in the military intelligence units.

By May 1949, the system of liaison by radio station and cryptography of Sector 9 with the High Command was fully realized.

In July 1949, liaison by cryptography was fully realized directly between Sector 7 and the High Command, rather than through an intermediate station [dai trung gian] (VTG in Quang Ngai), and the matter of ensuring the transmission of the content of command guidance from Central to the sectors in Nam Bo was more accurate and timely.

Also in 1949 the cryptographic organization of the Saigon-Cholon Special Sector came into being to ensure the command requirements of units active within Saigon.

****

Along with the move to develop and improve cryptographic systems, research into building a theory of cryptographic technique and distilling the essence of experience in the use of technique received highest attention. The Cryptographic Bureau began to compile documents to teach theory concerning the science of cryptography and documents to guide in practice. Experience in raising the level of technique use, in searching out erroneously encrypted values [ky hieu] and groups, was compiled to produce widely publicized documents for people directly involved in doing cryptography--compiled by the cryptographic organizations of the Intersectors, the divisions [dai doan], and the General Staff.

At the end of 1948, a set of cryptographic theory documents with the basic essence, a first system, was compiled. The book *Fundamentals of Cryptography* [Mat ma dai cuong],[11] with Cde Hoang Thanh (Cryptographic Bureau cadre) the chief author, was published by the Ministry of National Defense. It comprised five parts and thirteen chapters.

Cde Ta Quang Buu, Minister of National Defense, wrote the foreword of the book. It included this passage: "Although the laws of cryptography are universal laws, each and every nation must comply with the rules of cryptography of that country, which will differ from another country, because language structure differs from one language to another, or, to say it more scientifically, the frequency of letters and 1. Letter groups are not the same in one country as another. Because of this, the science of cryptography in our nation is still in the research stage.""

In the introduction, the author wrote some unvarnished, sincere thoughts: "When you look at our nation, cryptography is a new branch--it was born with the army and it grows up with the army."

The contents of this book initially dealt with fundamental problems of cryptographic theor--brought out principles of encryption, and basic methods of cryptography.

Cde Brigadier General Chief of the General Staff Hoang Van Thai assessed [this book]: "Mr. Hoang Thanh's book, *Fundamentals of Cryptography*, published in late 1948, was most timely, and it greatly aided the military cadre as well as people specializing in

cryptography. Although that book was fundamental, basic, inadequate, compared with today's level and requirements, it helped in no small way those people who needed to use cryptography every day, to have general knowledge of military communications, and it helped people specializing in cryptography to understand methods of applying flexibility and coming up with additional creations."[12]

The book was circulated in command organizations and cryptographic organizations army-wide. The result was to greatly increase the efforts of the Ministry of National Defense and General Staff cryptographic organization.

Also in 1948, the Cryptographic Bureau compiled and promulgated the "Ten Commandments" for the specialty, the first step in laying the foundation for building a system and principles for professional technique for our branch.

At the end of March 1949, on the occasion of summarizing the second "Build the infrastructure, Break the record" emulation, the book *The Use of Cryptosystems* [Cach dung luat mat ma], also authored by Cde Hoang Thanh and published by the Ministry of National Defense, was printed.

The content of the book pointed up the role and importance of cryptography, methods of ensuring secrecy through cryptography, and some essential principles in the use of cryptographic systems.[13]

This was a seminal document, one that fairly well summarized the structure [he thong] and noted the administrative principles in the use of cryptographic systems, because, as the author wrote, "using [cryptographic systems] improperly is like, as it is said, 'moving sand like a sandcrab': You knock yourself out and lose time, but you don't get anywhere."

Cde Hoang Van Thai wrote in the foreword, and for dissemination in the entire branch:

"With a style that is humorous, simple, and colloquial, the author of this volume honestly hopes that, in day-to-day combat, people using cryptographic systems with new experiences and new creations will add on, so that our national cryptography may be enriched."[14]

The book *Fundamentals of Cryptanalysis* [Ma tham dai cuong], compiled by the Cryptographic Bureau in 1949, fell within the plan to compile books on cryptographic deliberations, but not published, however, for it was also a document "to generate sensitivity toward cryptanalysis and help people making cryptographic systems to find ways of avoiding mistakes normally encountered and to progress toward the work of searching out enemy systems."

Relying on the books and study materials in HQ's training classes, in 1948 the Intersector 4 Cryptographic Section compiled and produced a manual used for regimental and battalion cryptographic organizations. It was called *The A.B.C.'s of Cryptography* [Mat ma thuong thuc].

Station MT3 was a mobile station with responsibility for liaison with Intersectors 1 and 10, the High Command, and the Resistance Committees. The Cryptographic Bureau selected two representatives to go take charge and six unit personnel to help out with this station. Although their principal mission was encrypting and decrypting, the fellows at MT3 still participated in the building of cryptographic organization for a number of regiments and battalions within their sector of assignment.

A cryptographic team regularly provided direct service to General Vo Nguyen Giap in liaison with the sectors in circumstances involving Flash [hoa toc] cryptograms, liaison with the Secretariat of the President and government, the Viet Minh Central Executive Committee [Tong bo Viet Minh], and the Intelligence Directorate [Cuc tinh bao]. The team had two comrades, with encrypting and decrypting their essential mission.

At the beginning of 1949, per directive from the MND-High Command, [we were to] "correct troop organization, aim at making branches [nganh] and army branches [binh chung] lean, light, but of adequate numbers, consistent with the requirements of mobile operations. . . correct command mechanisms [bo may chi huy] and the specialty branches [nganh], train cadre and personnel from the standpoint of service, fostering professional specialization, and a number of other matters." The Sixth Army-wide cryptographic conference convened from 20-27 June 1949 in Viet Bac comprised as delegates the cadre in charge of cryptography in units in the North and Intersector 5. (Nam Bo and units in distant theaters were unable to come.)

The Conference reviewed the situation involving the task of the army cryptographic branch from 19December 1946 to May 1949, and went deeply into review of each aspect of the task: building organization,developing cadre and personnel, research into expanding cryptographic technique, and organizing to accomplish the specialty task. Cryptographic organizations from each Intersector reported on their own reviews prior to the conference, in order to exchange training and extract collective experience.

The conference settled on the appropriate duration of training and resolved the direction of the new mission with respect to building an army cryptographic organizational system from top to bottom, unified in thought, organization, and professional technique, in order to have sufficient good outcomes in each mission in the new stage. The conference produced emulation criteria for units in the two years, 1949-50, with respect to development of cadre and personnel, research in the production of cryptographic materials, and emulation to guarantee secrecy, speed, and accuracy in the task of encrypting and decrypting.

In this conference, cryptographic systems researched and produced by the Intersectors and central were likewise reported and presented, aiming at exchange of training and drawing of experience.

The conference was honored to greet the comrade Chief of the General Staff, arriving to visit and speak.Carrying out instructions from the Chief of the General Staff, the conference settled a number of problems:

In 1949, until the beginning of 1950, we launched a series of campaigns in the North: Song Lo (April 1949), Song Thao (May 1949), Le Loi (Hoa Binh, November 1949), Le Hong Phong I (Northwest, February 1950). The Cryptographic Bureau designated cadre and personnel to participate in serving the campaigns and organized liaison nets to ensure campaign command with the left bank and right bank fronts of the Song Da. Cryptographic cadre and personnel of the 174th and 209th regiments, etc., for the first time served command in combined operations, incessantly pursuing and striking the enemy, sometimes on the march, sometimes at work, lacking experience, thus occasionally thrown into a passive mode and at a loss as to what to do. Following the line clearly enunciated at the sixth Central Conference of Cadre, ". . . concentrate cadre, concentrate weapons and means of communication-liaison for units with the mobile strike mission," "tables of organization, training, equipment--all must aim at the objective of carrying out the realization of mobile warfare," the Cryptographic Bureau drew experience promptly and instructed the units in arranging the various types of systems and preparing means of responsiveness to command requirements. The bureau also concentrated research on the improvement of cryptographic systems to respond to the requirements of mobile operations and increased its directives on organizing the cryptography of the main force units in order to adequately perform the mission they had received.

The requirements of the new mission placed upon the army cryptographic branch with respect to such aspects as organization, cadre and personnel, and technique, were large and difficult from the outset. The General Staff plan of assignment for 1949 also laid out concentration of weaponry, cadre, and personnel in the technical specialities for the main force; building of the specialty services from HQ down to Intersectors and main force regiments.

In September 1949, the Cryptographic Bureau opened a training class with the class name, "Dong Thap Muoi," meeting in the village of Dong Dau, Dinh Hoa, Thai Nguyen. Nearly forty students from units in the North went to study. The content of the curriculum was augmented in the areas of politics and the situation involving the new mission. This class had a rather methodical routine for training and close direction, with places to study, live, and work for the students and elements, report cards noting such aspects as morals, capacity for study, and professional technique, and record of merits and demerits of each student. Upon completion of the class, the students received graduation certificates from the Ministry of National Defense (MND).

In 1949, because of the expansion of the resistance, the volume of secret messages of command and direction increased rapidly. On an average, each month the Cryptographic Bureau of the MND/High Command encrypted and decrypted 1,200 official messages. Liaison nets also expanded greatly. System usage from Central to sector was examined. A few systems were a bit difficult to use, with a high degree of complexity, thus seldom used. Besides the stations in contact before, the Cryptographic bureau also developed and kept contact with MT3; MT2; the Song Thao Front, the Hanoi Resistance Committee; the Nam Bo Resistance Committee; HQ of Sectors 7, 8, and 9; and HQ, Nam Bo.