Supplement

Cryptography in the Armed Public Security Forces, 1959 - 1989

The Armed Public Security Forces – a sort of State police, border and coastal guard, and internal security force, distinguished from the PAVN by green, as opposed to red, collar tabs or shoulder boards – were formed in March 1959 in accordance with Politburo Decision 58 of November 1958 (HQ, Border Guard Troops, History of the Border Guard Troops, Vol 1, 1959-1979. *Hanoi: People's Public Security Publishing House, 1990, 15). Shifting from its parent ministry (which had had its name changed to Internal Affairs) to the ministry of National Defense, and finally back to the Ministry of the Internal Affairs in subordination, they were initially (1959) issued a reserve PAVN cryptosystem to commence operations. In a 1989 publication* (Socialist Republic of Viet-Nam, Armed Public Security Forces Staff, History of the Border Guard Cryptography, 1959–1989 (Draft). *[Hanoi:]Border Guard Headquarters, 1989) appears an account that naturally complements the preceding history of PAVN cryptography and moves the account into the cryptomachine era. The following excerpts span the thirty-year period of APSF/border guard cryptography history to 1989.*

****

"One of the most important tasks of the Forces' Cryptography at this time [i.e., at the outset, in 1959] was the urgent research and compilation of a code for the Armed Public Security [APS] in order to replace the DzB2 [Vietnamese DB2] code. The DzB2 code was an army cryptographic reserve [zu bi] type of code, supplied to APS Cryptography by the Cryptographic Bureau (General Staff) for temporary use in making contact during the time in which the Forces were newly established. The content of this type of code was not appropriate to the nature, mission, and sphere of activity of the APS; moreover, it was used all over the entire North – capacity was limited; timeliness could not be ensured.

"From mid-1959, the Cryptographic Section sent up to the Central Cryptographic Section a plan to compile a new code dictionary; at the same time, they instructed cryptography of the units to participate in a study of the frequency of words in messages. This approach was aimed at compiling code content consistent with the nature and activity of each unit, thereby producing high results in usage. . ." [p. 23]

"With high resolve and firm perseverance in the research, by February 1960 APS Cryptography had produced the first type of code for the Forces, designated 'Code T90'.

"The T90 code was constructed for superencipherment with cryptographic key having a reliable level of ensuring secrecy, belonging to the KTB4 type of technique. The use of

code T90 was very handy, easy to manipulate, productive in encryption, and twice as fast in decryption, compared with the DzB2 system.

"After the Central Cryptographic Section finished printing the T90 code by April 1960, APS Cryptography officially brought it into use throughout the liaison network of the Forces, and terminated the use of the DzB2 code." [23–24]

[In 1962, following Central Cryptographic Section directives to continue to improve cryptographic security, APS Cryptography coordinated with the Central Cryptographic Section to produce], "along the lines of code T90, codes type VQ1, VQ2, VQ3, VQ4, and VQ5 . . . and arranged to use them on the Vietnamese-Chinese and Vietnamese-Laotian border nets." [39]

"Effective from January 1966, the [APS] Cryptographic *Section* was elevated to become the Cryptographic *Bureau* (Decision 113/QD-CA, 18 January 1966)." [64n]

"[In 1968,] per instructions from the Ministry of Public Security, HQ, APS directed the Nghe An APS Command Section to cross over and coordinate with and assist our Laotian friends in that area of responsibility (the designator of the area of responsibility was K5) . . . A cryptographic team comprising Master Sergeant Pham Xuan Hop and Dang Van Thong was ordered to move out with the command organization cadre group from the province, going over to the K5 area of responsibility. The cryptographic team took the designator DX5." [71] "A cryptographic team from the Ha Tinh APS (with the designator DX6) was active along with a provincial reconnaissance subunit in the Na Muong sector." [72]

CHANGING OVER TO THE USE OF THE NEW TECHNIQUE THROUGHOUT THE FORCES, RAISING THE LEVEL OF SECURITY OF COMMUNICATION CONTENT THROUGH CRYPTOGRAPHIC TECHNIQUE

"Schemes to destroy the Vietnamese revolution were carried out: The intelligence organizations, especially technical intelligence, concerned with the discovery of the contents of communications through cryptographic techniques, held the most important position. They said that 'information of the greatest importance, and latest and most reliable, is information obtained through the process of cryptanalysis.' Thus America's technical intelligence organizations had built a gigantic system for collecting information and cryptanalysis. This system was comprised of centers and bases positioned in many spots, all over the South, Laos, and Thailand, and on ships along the coast. They carried out deadly radio reconnaissance activities, using types of search-and-measurement equipments, pinpointing the locations of our transmitting and receiving stations, using transmitters, metal, etc., to jam, or for airplanes to shell and bomb. They collected our encrypted messages; they used the most modern and sophisticated equipment in order to search out the secret contents. Together with a large amount of modern equipment, hundreds of scientists and American professional technical specialists, the puppets [i.e.,

the forces of the Republic of Viet Nam in the South] were mobilized and used for the above objectives.

"In parallel with this activity, they sought to infiltrate into the cryptographic organizations to pilfer secrets, to buy out and win over or pressure cryptographic personnel to serve their ends.

"The more cunning the enemy's designs, the more we had to be vigilant, to raise the level of secrecy protection of our technique. The approach, 'mobilize to get a step ahead of the enemy,' in this arena immediately became the dominant direction of the Vietnamese cryptographic branch.

"Starting right out in 1964, the Central Cryptographic Section decided to carry out research on new technique.

"In 1966, the Central Party Secretariat issued Instruction No. 129/CT-TU (6 June) concerning the matter of 'Increasing the Preservation of Secrecy in the Radio Communication-Liaison Task of the Party and the Nation,' and the Prime Minister issued Instruction No. 96-TTg (6 June) defining 'Preservation of Secrecy in the Use of Telegrams.' [See above, p. 123]

"In 1967, after a time of consolidation, the ranks of scientific cadre researched and prepared. The Central Cryptographic Section decided that we must 'change over by positive steps to the use of technique KTB5 to replace KTB4 throughout the nation, in order to heighten the degree of secrecy protection of cryptographic technique. At the same time, expand the area of experimentation in KTC technique in a number of major liaison nets and make basic preparation to go into the total use of KTC.'

"At the end of 1967, thoroughly grasping the decision of the Central Cryptographic Section, the APS Cryptographic Bureau constructed a plan to implement the switchover to the new technique. The Party committee and commander of the Staff Directorate issued concrete guidance for each step of the implementation,with the requirements: positively, urgently, firmly by each step, changing to good technique means ensuring guidance and command requirements of the various echelons in every situation.

"At the beginning of 1968, the Staff Directorate opened a training class in technique KTB5 for cadre in charge of cryptography in the sectors, cities, provinces, and directly subordinate units, in order to thoroughly grasp the line of spreading the technique of the Vietnamese cryptographic branch and the requirements involved in the process of preparation and implementation of the changeover to the new technique.

"After training at HQ and returning, the units promptly organized short training classes for cryptographic cadre and personnel.

"In wartime conditions, with rank and file scattered over border posts, implementation of the plan encountered many difficulties. All of the provinces had to organize two to three training classes, with rotational replacements for those going to the provincial headquarters to study: they had to ensure both people for the continuing task and the

plan's provision that 100 percent of the troop strength of the units would have completed study of the new technique. By October 1968, cryptography throughout the entire Forces had accomplished the training classes.

"At the same time it was guiding the units in implementing organization to develop the plan, the Cryptographic Bureau was researching and completing the compilation of the KTB type of cryptographic codebooks [lit., "dictionary codes," or "code dictionaries"], so as to have them so the nets could quickly put them into use.

"In December 1968, APS Cryptography in Thanh Hoa, Nghe An, Ha Tinh, Quang Binh, and Vinh Linh developed the use of the KTB5 technique comprehensively throughout their system of cryptographic technique. At the beginning of 1969, the development had expanded to the provinces of Quang Ninh, Hai Phong, Son La,and Lao Cai, and the internal net of the Viet Bac Sector.

"In October 1969, Lai Chau was the last unit of the Forces to change from the use of Technique KTB4. This was also the point in time that marked the conclusion of changing over to technique KTB5 in the entire cryptographic technique system of the APS.

"In order to promptly achieve productivity and quality in the use of KTB5 to attain the level of proficiency throughout the entire system of organization, Forces' Cryptography set up a 'burst of emulation study, study closely aligned with the real-world assignment'. After only a bit more than two months of being roused, many code clerks achieved high quality and productivity. Units with good study movements were Lai Chau, Nghe An, Ha Tinh, Vinh Linh, and the Encrypting-Decrypting Section of the Cryptographic Bureau.

"The changeover to the use of technique KTB5 marked a new stage in Vietnamese cryptographic technique. But not stopping there, the Central Cryptographic Section--after implementing research on technique KTC--decided to expand the experimental use of this type on a number of important liaison nets.

"In September 1969, the military regions and services in the North, Military Region Tri-Thien, Military Region 5, and HQ of the South began to test the use of KTC in contact with the Cryptographic Directorate of the General Staff. The APSF cryptographic system [he thong] was one of those under Central Cryptographic Section guidance in the experimental implementation of the use at a number of points. Preparing for this plan, at the end of 1967, APS Crypto assigned four comrades, Nguyen Van Mui, Ngo Quoc Bo, Nguyen Van Ba, and Nguyen Quoc An, to go study the use of technique KTC at the Central Cryptographic School.

"The Central Cryptographic Section handed over to APS Crypto KTC-type codebooks to research and compile, then to send up to the Section for printing--the Section would supply the types of crypto key.

"In accordance with guidance from the Central Cryptographic Section, Forces' Cryptography was to try out contact with KTC3 first, concentrated in three nets--Sector 4, Sector Viet Bac, and the coastal net. Based on the real-world situation, the Section sent along guidance: vis-a-vis the APS cryptographic system, immediately thereafter, change

over to the KTC5 technique and prepare at once the rank and file of cadre and personnel to accept the new technique.

"Changing to the use of KTC5 posed numerous difficulties, requiring simultaneous resolution between people and technique. At that time the rank and file of Forces' cryptographic cadre and personnel had many comrades of advanced age, physically weak, with a cultural level not past second grade. This was the contradiction between the real-world capacity and the requirements of the technique.

"On 1 October 1970, the Staff Directorate sent a report from Comrade Minister Tran Quoc Hoan and the HQ concerning the situation of the Forces' cryptographic organization and cryptographic technique to solicit opinions and guidance. The minister instructed: 'We need to prepare a cryptographic force to guarantee the political standard, be in good health, have a third-level cultural standard--tenth is best--then organize to use KTC5'.

"Implementing the instruction from the comrade minister, on 13 November 1970 HQ issued guidance to the related directorates subordinate to the organizations of HQ and the provincial command sections: 'We must reexamine the number of cadre and warriors performing the cryptographic task, aiming at selecting comrades with sufficient standards consistent with conditions of employment of the new technique. Besides the matter of trustworthiness with respect to politics, they need to be in good health, have long service, have a cultural level of class six up--these numbers to be selected to go for refresher in the new technique for use on liaison nets from sector, city, and province with HQ. Afterward, we want to directly augment culture to the third level in order to build better conditions for the use of the new technique. In addition, those comrades lacking good health for long service need research to shift to other assignments in the Forces. We need to enroll sufficient numbers for training in the use of the new technique, with the standard being, Party members of the Vietnamese Lao Dong Party, from the working class, guaranteed to be trustworthy politically, in good health, with a cultural level three'.[1]

"Implementing the instruction, the Staff Directorate had a concrete plan to develop the related-task aspects for the entire Forces, in order to attain the requirement of changing technique.

"In March 1971, twenty-one unit cryptography comrades were selected for refresher in KTC5 at the Central Cryptographic School. After these comrades had studied and returned, the Cryptographic Bureau opened two supplemental classes in the use of KTC5 for seventy-three cadre and personnel (the first class, three months; the second class, six months). Along with instruction at the school and consolidated supplemental [training], a number of units had in-place supplemental training themselves for eleven other comrades.

"Tied right in with the organization task, the Cryptographic Bureau, as a matter of urgency, researched and compiled KTC5-type code books in accordance with guidance from the Central Cryptographic Section. A team of technique research cadre from the Bureau applied the methods, compared the sample code, and picked out from secret messages the vocabulary content of the Forces during this time, while at the same time they guided those in charge of cryptography in the units in becoming directly involved in

'frequency counting'. As a result of close guidance, cryptography in the units made concrete plans, set norms, and made allocations for each of their cadre and personnel to go deeply into research, to collect, and to sort out findings.

"After a year of diligent implementation, up to the end of 1970, the units belonging to the former Sector 4, Haiphong, Quang Ninh, Lai Chau, Son La, and Viet Bac Sector HQ in turn sent the Cryptographic Bureau thousands of 'plain elements' of high frequency from the secret message vocabulary of each unit.

"On the basis of contributions from unit cadre and personnel, the Bureau research team proceeded to analyze, select, and compile seven types of KTC5 codebooks--seventy sets of the least, 120 sets of the greatest. This quantity was sufficient to replace the entirety of the KTB5 code and set aside a reserve, against the prospect of having to replace a code while in use.

"In December 1971, after receiving more than five tons of professional means and the KTC5 cryptomaterials from the Central Cryptographic Section, the Cryptographic Bureau completed allocation to the liaison nets between HQ and the sectors, cities, and provinces.

"In order to ensure tight control from the very outset, the Cryptographic Bureau directed test contact over the net between HQ and the sectors, cities, and provinces. The Message Encryption-Decryption Section (Cryptographic Bureau) picked places for experimental guidance, and publicized to all units throughout the Forces the experience they derived." [75-81]

By 20 July 1972 the net from HQ with the sectors, cities, and provinces used entirely KTC5. [82]

By August 1972, all border posts, coastal defense, islands. [Ibid.]

On 30 October 1972, all were using KTC5 - KTB5 was out. [Ibid.]

"In parallel with the building of organization and service to the steerage and command of the forces, following the aim of developing the cryptographic technique of the security branch's cryptography and the aim of building the cryptographic technique of the APS, at this time it was clearly stated: 'Research into the improvement of technique goes hand in hand with change to new equipment, by steps introducing cipher machine technique into the service of the Forces' steerage and command, aiming at increasing the speed of cryptographic transmission'.[2]

"The realization of this objective had fundamental benefits. At the end of 1977/beginning of 1978, the Cryptographic Directorate of the Ministry of Internal Affairs [the Ministry of Public Security having become the Ministry of Internal Affairs in 1976] issued for APS, twenty-three sets of M111 cipher machines and two sets of 1Bautomatic teleprinter cipher machines [bo may ma truyen chu tu dong].

"This was the beginning of the development of modern technical equipment in the cryptographic technique system of the APS, creating step by step the capacity to use

mechanical means of encrypting and decrypting at the primary CPs of the provinces and cities throughout the entire Force.

"The introduction of cipher machines into use in the units brought practical results, cutting short the time required for transmitting information, reducing the mental labor for the cadre and personnel directly involved in the use of the technique.

"The development of technique was closely connected to the development of the ranks of cadre to administer with a corresponding degree of professional steerage, to develop symmetry and synchronicity between man and technique – this was a long-term, fundamental measure, with respect to the Forces' cryptography. Therefore, immediately in 1977, the Forces assigned five cadre to go and perform the cryptographic task in the units and to be developed in the schools of higher education; at the same time, enrolling twenty-eight other comrades for development in a short course at the Border Guard Officers' School (Son Tay). Once their studies were finished in the general curriculum of the Officers' School, they were transferred to the 12th Battalion (at Xuan Mai, Ha Son Binh), where they further studied the content of the administrative task, guidance in the use of cryptographic technique by the APS cryptographic at provincial and city level, and basic knowledge with respect to the science of modern cryptographic technique." [103–104]

[Tracing the years, 1975-1979, with two wars, one in Cambodia and one with China, both of which involved the APSF:] "With 122 cryptographic organizations and 295 cadre and personnel (1974), by 1979 that had grown to 278 organizations and more than 500 cadre and personnel. The system of cryptographic technique [had gone from] using entirely manual methods until, by 1979, one third of the cryptographic organizations at provincial and municipal level were equipped with cipher machines." [145]

[10 October 1979, APSF was transferred from the Ministry of Internal Affairs (formerly the Ministry of Public Security) to the Ministry of National Defense and renamed the Border Guard Troops.] [148]

"The total number of cryptographic [units] as border guard troops, army-wide, was 280 units with cryptographic organizations, including two HQ CPs; thirty-one provinces and cities; thirteen regiments and regimental equivalents; twenty-four subsectors, battalions, and mobile companies subordinate to the provinces; and 186 border posts." . . . "The number of cryptographic cadre and personnel in the entire force at that time was 647 people." . . . "Vis-a-vis the system of technique: the various types of cryptographic materials, cipher machine equipment,and professional means were also transferred along with the organizational system." [149]

"As of May 1987, the synchronous teleprinter line [or circuit: duong tryen chu dong bo] between cryptography's cipher machines (TN-75) with the communications van (R-140-M) was officially active at the two HQ CPs (in Hanoi) and (Ho Chi Minh City), assisting in resolving in a fundamental way the volume of secret communications transmitted between these two CPs." [164]

". . . On 3 August 1988,. the two ministries, National Defense and Internal Affairs, proceeded to transfer the Border Guard Troops from the Ministry of National Defense [back] to the Ministry of Internal Affairs." [Ibid.]

"Along with the transferal of the organization of the forces, on 25 August 1988 the Army Cryptographic Directorate officially transferred the system of cryptographic organization and the system of cryptographic technique of the Border Guard Troops over to the Cryptographic Directorate of the Ministry of Internal Affairs for administration and professional guidance." [Ibid.]

[On 3 March 1989, the Border Guard Troops celebrated their thirtieth anniversary, 3 March 1959– 3March 1989.]

Notes

1. Instruction No. 24/CT-CY, 13 November 1970, signed by Brigadier General Pham Kiet, Commander and Political Commissar of the Forces.

2. "Aims for the APS Cryptographic Task, 1977."