SIGINT Goes to War

THOMAS R. JOHNSON

Doctrine is not NSA's strong suit. We are much better at execution than at philosophy. The following paper, an extract of one originally presented at the October 1993 Cryptologic History Symposium, comments on cryptology's doctrinal difficulties relating to a specific type of activity – wartime SIGINT. It illustrates the problems that lack of doctrinal focus sometimes creates when the cryptologic system must make a transition.

Some thirty years ago, I arrived at Goodfellow AFB to be trained in what I thought was surely police work. This appeared to me to be a strange assignment selection, since I had requested "intelligence," but had instead been assigned to "security." Once I started classes, however, it began to dawn on me that they were not training me to be a cop after all.

Our introductory week covered SIGINT doctrine. One of the first things we were taught was that SIGINT, this new discipline that we had just been cleared for, was strictly a peacetime profession. While the rest of the defense establishment played games in the sand and waited for the balloon to go up, we were on the front lines, and we would tell everyone else when the balloon would go up. Our powerful position in the defense establishment was underlined by our instructor's assertion that we would have a red phone on our desk connecting us to the White House. The president was on the other end, and he was waiting to hear from us about the possibility of immediate nuclear war. This framed our job in a uniquely peacetime context, and I came to think of it as such. Then some wag from the back of the room asked, "Do we have a job during wartime?" The instructor had a ready answer for that one. No, we just crawled under our desks and hoped the bombs wouldn't fall on us. When war began, our jobs were at an end.

I learned in later years that that had been a wrong answer. Although our training had been generally good, it was not unadorned by misinformation, the red desk phone story having been one such example.

The combat forces operate in wartime, but have problems adjusting to peacetime. SIGINT has had the opposite problem – we operate in peacetime, but have problems adjusting to a wartime environment. Moreover, wartime confronts us with serious problems relating to SIGINT centralization, control of resources, tasking authority and a host of other knotty (naughty?) problems. It exposes all the system's fault lines.

How, indeed, does SIGINT go to war? What changes do we make? How is our business different in combat? And how do we tailor our system in peacetime to meet wartime conditions? These and other questions form a central dilemma of our business – how do we go to war?

My field is not World War II, but I will begin there because it (the war) is where one must begin in order to describe the postwar world.

In 1940 there was no central control of COMINT. The Army and the Navy cryptologic organizations were rivals without a referee, and went their own separate ways, either oblivious to, or in direct competition with, each other. Mechanisms for conflict resolution were rudimentary and hastily contrived. Lack of centralized control of the SIGINT system was, then, one problem that emerged during the war.

Of the two services, the Navy was the more prepared for conflict because it already had an extensive system of overseas intercept sites, including stations in the Philippines, Hawaii, Guam, Winter Harbor, Bainbridge Island, San Juan, Cheltenham (Maryland), and several other locations. Moreover, the Navy had natural mobile field sites in the form of their larger capital ships, and had been placing COMINT intercept organizations on board for a number of years. So the Navy was relatively prepared for war, and OP-20-G (the Navy COMINT organization) slipped naturally into its wartime role.

Within the Navy structure itself, however, were buried the seeds of later conflict. The system was unitary in the sense that all naval COMINT assets were under the Chief of Naval Operations. However, Naval Communications controlled the intercept sites, the theater commander gave operational orders, and OP-20-G in Washington lent technical direction to the worldwide effort. This produced occasional flair-ups as OP-20-G tried to rein in maverick field organizations. The most famous incident was the firing of Joseph Rochefort in 1942. Rochefort commanded the unit on Hawaii, and worked directly for Admiral Layton, Nimitz's intelligence chief. But OP-20-G issued technical directions and made field assignments. When Rochefort ran afoul of OP-20-G, he was relieved, Nimitz notwithstanding. Nonetheless, the conflicts were generally muted – partly by the overwhelming effort required to prosecute the war, which left precious few energies remaining for internecine conflicts, and partly by the absence of an organization external to the Navy contending for control. At least all the players in the game wore the same color of shirt.

The Navy's unique method of managing afloat detachments gave all power to the senior naval officer aboard, unencumbered by any sort of central control. This system has continued to this day.

For many reasons, the Army COMINT organization required more changes to be ready for war. Signal Intelligence Service had, in December 1941, only seven intercept sites, and some of those were in the wrong places, targetted toward the wrong opponent. The Army COMINT organization (SIS at the start of the war) was strategically oriented, worked primarily against Japanese diplomatic traffic, produced little of tactical interest, and had virtually no tactical assets such as mobile field sites. During the war SIS quickly built up

a mobile, tactical capability, with some forty radio intelligence companies and signal companies supporting forces in the field. SIS headquarters at Arlington Hall did central processing and reporting, specializing on difficult-to-solve cipher traffic, leaving to the tactical units (often called "Y Service" after the British usage) the exploitation of lower-level communications.

The Army was burdened with the same bureaucratic conflict between intelligence and communications for control of intercept units as was the Navy. SIS reported to the Signal Corps, the information that SIS produced was worked in Military Intelligence, and the tactical units, once deployed, worked for the local commander. Stresses developed within the system, the most notable being a nasty fight between General MacArthur and the War Department over the control of Special Security Officers (SSOs) in the Southwest Pacific Theater. But because of a lack of centralized control of COMINT, the doctrinal stresses that built up during Vietnam between a central COMINT organization and the JCS did not exist during World War II.

With the disarmament of 1945, the SIGINT system wasted. As the SIGINT folks circled the wagons, they strove desperately to maintain their basic capability to decrypt crypt systems centrally. The tactical assets accumulated during World War II languished. By the time of the North Korean invasion of South Korea, our tactical system had to be reconstructed – doctrinally, monetarily, and by the acquisition of personnel.

The SIGINT system was caught flatfooted by the Korean War. In June of 1950 the Army Security Agency (ASA) and the U.S. Air Force Security Service (USAFSS) were engaged in establishing a system [redacted] targetted against the Soviet Union. It was not easy to divert these assets to the Korean problem because they lacked target expertise, technical competence and linguists. Even more difficult was the need to once again field mobile SIGINT units to give direct support to 8th Army and 5th Air Force on the Korean peninsula. They both engaged in a scramble to find vans and trucks, to unbolt receivers and recorders from racks at fixed sites, and to position them in Korea in hopes of intercepting something of value. Both services struggled throughout the war with these problems of technical and physical resources, with generally indifferent success. Although we succeeded in situation-oriented direct support like the Cho Do Island warning operation, and Army low-level voice intercept (LLVI) teams [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

The year before the Korean War, the Defense Department created the Armed Forces Security Agency (AFSA), the first real attempt at central control of COMINT. AFSA achieved some notable technical successes against great odds. But AFSA's organizational problems were insurmountable. Each service (there were now three of them) clung tenaciously to its COMINT resources, especially those in the combat zone, and AFSA made no progress in centralization. The AFSA experience during the Korean War did, however,

highlight the doctrinal difficulty of centralization and control, and led to a thorough reexamination of the COMINT structure. The creation of NSA in 1952 occurred too late in the war to significantly affect resources in the combat theater. The doctrinal conflict remained dormant throughout the 1950s, and reappeared with a vengeance during Vietnam.

Following the unfortunate experience in Korea, America retreated into its strategic Fortress America defense posture. The new way of doing business was reflected in NSC-162/3, the doctrine of massive strategic nuclear retaliation. The Soviet strategic nuclear forces became the overriding priority. Theater and localized conflicts were simply assumed away, and we became almost totally preoccupied with the Soviet nuclear threat.

(b)(1)
(b)(3)-P.L. 86-36

Within the SIGINT system this meant focusing our efforts on Soviet nuclear weapons and their delivery capabilities. We optimized our intercept system to the strategic target, building huge antenna systems like the FLR-9. [redacted] USAFSS built the GLR-1, which, [redacted] was so expensive that NSA became involved to head off future projects of such magnitude. FLR-9s and GLR-1s just weren't anything like the tents and trailers we had used in World War II and Korea. Big, immovable intercept sites became the order of the day, and Air Force Security Service fell completely into the trap. Beginning with a system in which each intercept site was called a Radio Squadron Mobile, Security Service quickly became the least mobile of all the Service Cryptologic Agencies. The command even took over the management of its own bases, rather than becoming a small tenant unit at someone else's base; at the height of its power, USAFSS operated eight bases of its own. The command installed five FLR-9s around the world, and was the host base at all of them except one [redacted] The Army maintained its mobility to a greater extent, but ultimately succumbed to the seduction of the super-site and built two FLR-9s of its own. The Navy stayed more tactical than the other two services, even though it put lots of money into the FRD-10, a smaller version of the Wullenweber antenna. The program of afloat detachments remained vibrant throughout. Moreover, the Navy steadfastly refused to relinquish any sort of national (read NSA) control of its tactical assets. While we poured money into the super-site program, we skimped on the tactical system. As the years passed, we almost forgot how to do the wartime mission.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

In sum, we relied during the Eisenhower years on a defense doctrine which placed emphasis on the strategic system, to the detriment of tactical forces. This saved money and balanced the federal budget, but left us unprepared to fight wars. The SIGINT system of the time simply reflected the national priorities.

Vietnam was one long, agonizing struggle to reconstruct a tactical SIGINT system so that it would work. It didn't start in 1964, of course, but earlier, when the Kennedy administration began reexamining the assumptions which undergirded NSA-162/3. The result was the doctrine of limited war and graduated response, embodied in MC 14/3. But it took years for the SIGINT system to find the appropriate and effective response mechanisms, and in some cases we had to call back the Korean War vets. In other cases we

had to invent new techniques, like Airborne Radio Direction Finding (ARDF), to help us fight a war which was, to a greater degree than any previous war, a guerrilla action.

Every war has seen a struggle for the control of SIGINT resources. In a real sense this has been another manifestation of our doctrinal difficulties. This has occurred most basically in the attempt of the field commander to operationally control theater resources. Whenever you put a SIGINT asset, be it a field processing center, a major field site, a SIGINT aircraft, or a collection van, in a war zone, the tactical commander will want it, and this will produce a fight for control.

With the creation of NSA in 1952, the struggle for control became inevitable. SIGINT resources in a war zone belonged to DIRNSA, and this violated the basic precept of unity of command. There was a resource that the theater commander did not control, and in order to effectively prosecute a war, all theater commanders believe they must control all military assets in their zone of command. This must happen, they believe, in order to insure rapid and complete response.

But unity of command in the theater violated SIGINT unity of command. The way NSA looked at it, the field commander did not have the technical expertise to effectively employ the resources, and would just bungle the job. All SIGINT assets fit into a worldwide system, which must be kept whole in order to function properly. DIRNSA could support the field commander better from Washington than fragmented SIGINT assets could from the field. And anyway, there were overriding security considerations which militated against control in the field.

In practice this produced a compromise in which tactical commanders were given complete control of certain mobile assets, while the rest of the SIGINT system remained under DIRNSA control. But where was the water's edge? Were strategic airborne assets properly controlled by DIRNSA in a war zone? What about smaller assets like ARDF? What about major field sites?

In Vietnam the control of theater assets erupted into a donnybrook. Periodically a Wise Man would appear to decide the issue and, like Solomon, divide the assets. This would work until the next SIGINT asset arrived in the theater, and the battle would be joined again. NSA's relationship with the armed services emerged from Vietnam poisoned, the fabric of cooperation shredded. It took many years, and the retirement of many of those directly involved, to restore a semblance of harmony.

Centralization of SIGINT just made the conflicts worse. For almost two decades it was the overriding tendency within the cryptologic community. We believed that centralization was good because

a. it permitted us to get complex cryptanalytic and other technical problems quickly back to a place where they could be worked on;

b. it concentrated all the interrelated pieces of a problem where they could be looked at. The [redacted] problem was a classic. Not until we could look at this

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

problem globally (i.e., in NSOC) were we able to produce the most discerning and timely reports, and to provide valid indicators; and

c. it permitted centralized security control, so that raw information was not leaking out of the system worldwide.

The problem with centralization, of course, was that it pulled in the opposite direction from the theater commander. And it occurred at a time when the Defense Department was trying to enhance the authority of the Unified Commands. Thus the conflict over the attempt to achieve unity of command – either in the direction of the theater commander or the cryptologic authority – was inevitable.

Some of you may have heard of Drake's Law, jokingly postulated by a former deputy director several years ago: "Centralization is always bad, except at my level." The theater commander wanted to centralize everything in his theater, but wanted to be free from JCS-level interference. The same tendency was at work within the cryptologic community. NSA tried to pull everything back to Washington, but our own people in the field could see that it wouldn't work in wartime. And so it sometimes didn't. Our initial efforts to support theater commanders from Washington proved slow, and often failed us. We took some serious hits for trying to do too much from Fort Meade. This reinforced the problems we were having over the control of theater SIGINT assets, and made the climate for cooperation even more poisonous. Tactical commanders took every failure to provide quick information from Fort Meade as additional justification for their control of theater assets.

How good are we are applying the SIGINT lessons of the last war to the next one? Actually, since Vietnam our record has been pretty good. We probably learned more from the loss in Southeast Asia than from most of the wars that we won. However, we have never had a very good system for thrashing through the last war and publishing *doctrine* to apply to the next conflict. Like the British, we just muddle through. The Army has a highly developed system of doctrinal development which we in the SIGINT business have never adopted. As an institution, NSA has been far better at crisis response than at long-term planning.

Just how far we have come in solving doctrinal problems was illustrated during the Desert War. The cryptologic community responded far more effectively than during any previous war. Especially in the early part of the war, however, there were organizational hiccups in integrating SIGINT support with those who were to be supported, and in marshalling resources from cryptologic organizations that were structured around a peacetime environment.

We should take a close look at our warfighting doctrine and compare it with the peacetime organization. The objective is not to write the past into the future, but to identify the problems that always seem to come up. If we don't do this, they will continue to come up, and our future will always be a prisoner of our past.

(~~TSUO~~) Mr. Johnson is a senior historian and chief of research and writing with the Center for Cryptologic History. He has had over thirty years of experience in SIGINT, primarily in operational assignments. He began his service with the Air Force in 1964, and from then until his retirement in 1985 served in a variety of SIGINT assignments around the world. Since joining NSA in 1985, he has served alternately as a historian and in operational and foreign relations jobs. He earned a Ph.D. in American history from the University of Maryland in 1975. He has taught history at Pennsylvania State University, University of Maryland, and the U.S. Air Force Academy. Mr. Johnson is a prior contributor to Cryptologic Quarterly and has also published historical articles in academic journals. He is a certified Collection Officer.