Coordination and Cooperation in Counterintelligence

Basic principles and some new challenges to CI.

Austin B. Matschulat

It is axiomatic that the structure and functions of a counterintelligence service, or of the counterintelligence part of an intelligence service, are determined by the activities of its chief adversaries more than by any other single factor.[1] Any realistic discussion of US counterintelligence thus must begin with the two Soviet services, the KGB and the GRU, respectively, the state security service and the military security service.

The scale of the effort that has been made and continues to be made by Soviet intelligence is difficult to exaggerate. Some 21,173 Soviet nationals reside in the 77 non-Communist countries of the world, of whom 5,943 are officials. At least 60 percent of these, or 3,560, are in fact intelligence personnel. Moreover, the Soviet services work very closely with the 19 intelligence services of the seven Communist governments of Eastern Europe. During the 1950's the Soviets dominated these services through a system of senior advisors whose word was law. Although this control has been somewhat relaxed during the 60's, close coordination continues. The testimony of defector Major Laslo Szabo before the Armed Services committee of the House of Representatives in March, 1966, amply bore this out. Szabo served in the AVH, the Hungarian foreign intelligence service, for 20 years before he

defected. (He is now 43 years old.) He was given a full year of training by the Soviets in Moscow, starting in September, 1957. He testified that the AVH printed and distributed forgeries defaming the US, at Soviet direction. One instance was the dissemination of a forgery of *Newsweek* magazine in late 1963, principally in Asia and Africa. He said that another AVH officer, Bela Lapusnyik, who defected in Austria in 1962, was murdered by poison in a Viennese jail on AVH orders carried out by the Czechoslovak foreign intelligence service. His testimony shows the unified nature of the clandestine Communist attack and illustrates the fact that it is still directed centrally from Moscow. It also helps to explain why the attack at the subterranean level is not affected by what is happening at the diplomatic or open level. The attack does not slow down, for example, because of thaws in diplomatic relations between the US and the USSR.

Our defenses against this attack are of two types, passive and active. These two kinds of defense are commonly called security and counterespionage, and they constitute the twin halves of counterintelligence. All US departments and agencies with intelligence functions are responsible for their own security abroad.[2] Within CIA, responsibility for security is divided in two different ways. Basically, CIA and all other agencies are trying to defend three things: its personnel, its installations, and its operations. The first two, security of personnel and security of installations, are in the Agency jibe responsibility of the Office of Security. Responsibility for the third element, the security of operations, is in turn divided between the operating divisions, which have a line function, and the counterintelligence staff, which has the staff responsibility. This kind of division clearly requires close coordination, and this in fact occurs on a daily basis.

US practices in physical security abroad are not uniform but are also not widely divergent. Our safes are much alike. So are our guard systems, floodlights, pass control systems, and the rest. The same is true for security of US installations, where one of the chief dangers is hostile audio penetration. In this area uniform measures of defense are ensured through the work of the Audio Countermeasures Committee of the US Intelligence Board.

One significant difference in personnel security measures is inherent in the basic nature and functions of the military as contrasted with CIA. A military officer typically serves a tour of duty in the intelligence specialty and then moves on. Intelligence is only one of the many functions of the

armed forces, which need well-rounded officers. CIA personnel, in contrast, usually spend their entire professional lives in the same business. The result is a steady growth in sophistication, including counterintelligence sophistication, and the added advantage of a far smaller turnover rate in personnel. It also means that Agency people with access to classified information usually have a functional need for it. They are themselves a part of the process of getting and reporting that information.

The point is, however, that even though the security of each element overseas is its own responsibility, the hard fact is that US intelligence security is essentially indivisible. The exchange of intelligence within the US community is vast and growing. The future will see an even greater exchange, chiefly as the result of the adoption of automatic data processing systems and community projects like COINS, designed to let us query each other directly by machines. The possibility has therefore increased, and will continue to increase, that successful operations by the opposition could obtain information originated by any element, if not all elements of the intelligence community.

The security of our foreign operations is also indivisible, and is also a community responsibility. It differs from other kinds of security work in that it does not employ set defenses, although it also must be based on basic CI principles. The security aspects of each operation must be hand-tailored, and no operations should be planned, let alone launched, without security being a primary consideration from the beginning. Counterintelligence specialists are not firemen, to be called in only after disaster has struck. They must be brought into the picture from the outset and remain throughout the life of any operation, if that operation is to be secure. Through their knowledge of the adversary services and their CI expertise, they are particularly adept at foreseeing complications.

The interdependence of the US counterintelligence community is also manifest in our relationships with liaison services. We cannot cut off these relationships because of concern about security, but experience has certainly shown that we must calculate the risks involved as realistically as possible in the knowledge that the US is now Soviet target number one. Between 1917 and the mid-30's the Soviets focussed their attention chiefly on France, in large part because of the presence of the large white Russian colony in and around Paris. They were eminently successful, a fact from which we continue to suffer today.[3]

From the mid-30's to World War II the Soviets' emphasis shifted to England. Again they scored notable successes. Consider, for example, the case of George Blake.

George Blake, born George Behar, was tried at the Old Bailey in London on 3 May 1961. He was found guilty of offenses chargeable under the Official Secrets Act—that is, of spying for the Soviets—and was sentenced to 42 years of imprisonment. He was born in 1922 in Holland of a Dutch mother and an Egyptian Jewish father who had become a British subject. Blake served in the Dutch underground and became involved in the ill-fated British operation codenamed North Pole. In July 1942 he left Holland, on British orders, and travelled through Brussels and Paris to unoccupied France and across the mountains to Spain. He was taken by ship from Gibraltar to England. After nine months in the Royal Naval Volunteer Reserve he was assigned in July 1944 to MI-6, the British Secret Intelligence Service. He served in The Hague, London, and Hamburg, went to Cambridge for a Russian language course, took some technical and tradecraft training, and was posted to Seoul, South Korea, in November 1948 as the first British intelligence representative there. His official or cover position was that of vice-consul. In July 1950 he and his colleagues were taken prisoner by the North Koreans and were held until April 1953.

Blake later insisted that he became converted to Communism during this period. This is doubtful Rebecca West, in her brilliant book *The Meaning o f Treason*, speculates that he may have become a Communist agent during his service in the Dutch underground. In any event, the damage he inflicted was enormous.

According to his story, he decided in October 1951 to offer his services to Soviet intelligence. He wrote a letter which was handed by the North Korean intelligence service to the ubiquitous Soviet apparatus. He suggested that all British prisoners be interviewed, to protect him against suspicion. This was done, and from October 1951 to January 1952 he was able to meet securely with a Soviet case officer. This part of Blake's story, incidentally, was confirmed by the Polish Deputy Minister of the Interior and chief of the secret police, Col. Alster, a Jew, who defected to the West after learning in late 1960 that the Soviets were planning secret anti-Semitic measures. Among the Soviet spies Alster identified was George Blake.

Between April 1953, the date of his release from imprisonment, and April

1961, when he was arrested, Blake served the British and Soviet intelligence services in London, Berlin, and Lebanon. According to US calculation he furnished the Soviets with 4,720 pages of documentary material during those eight years. As a result Soviet intelligence scored some smashing successes. A highly placed penetration agent, a Russian, was identified by Blake and then killed by the Soviets after being identified by Blake. General Robert Bialek, the Inspector General of the People's Police in East Germany, defected to the West at the time of the June 1953 uprising. His apartment in West Berlin was only a block from Blake's. In February 1956, acting on information from Blake, the East Germans under Soviet control kidnapped General Bialek and brought him back to East Germany. He died in a Soviet prison.

Blake attended joint meetings at which CIA legal-travel operations into the USSR were disclosed. He also attended meetings concerned with audio operations against the Poles in Berlin and against a Yugoslav military mission there. He was present at joint planning sessions concerning the activity of the anti-Soviet Russian emigre organization known as NTS. Four NTS leaders, who had previously entered and left the USSR, were caught on their next trip as a result of Blake's information, and were never heard from again.

Blake served only five years and four months of his 42-year sentence. On 23 October 1966 he escaped from Wormwood Scrubs Prison. The facts of the escape demonstrated beyond doubt that it was engineered by the Soviets. The buoying effect upon the morale of Soviet spies everywhere can be easily imagined.

Counterespionage

The other side of the CI coin—counterespionage—has one purpose which transcends all others in importance: penetration. The emphasis which the KGB places on penetration is evident in the cases already discussed from the defensive, or security viewpoint. The best security system in the world cannot provide an adequate defense against it because the technique involves people. The only way to be sure that an enemy has been contained is to know his plans in advance and in detail. Moreover, only a high-level penetration of the opposition can tell you

whether your own service is penetrated. A high-level defector can also do this, but the adversary knows that he defected and within limits can take remedial action. Conducting CE without the aid of penetrations is like fighting in the dark. Conducting CE with penetrations can be like shooting fish in a barrel. The famous case of Col. Oleg Penkovskiy is an instructive example.

Penkovskiy was born in 1919 of aristocratic Caucasian parentage. His father, an officer in the White Army, disappeared in the post-revolutionary fighting in 1919. The son joined the Soviet Army in 1937 and was commissioned in 1939. During World War 11 he became a regimental artillery commander. In 1945 he married the daughter of Lt. Gen. Gapanovich. From 1945 to 1948 he studied at the Frunze Academy and from 1949 to 1953 at the Military Diplomatic Academy. He was then posted to the GRU. In January 1955 he arrived in Turkey as the assistant military attaehe and as acting head of the GRU residency there. He quarreled with a superior, Major General Rubenko, and was sent home in November 1956. He was embittered by the quarrel and its outcome. He began to think about getting in touch with the Americans. During 1958-1959 he was given technical instruction in missiles, and he began to accumulate information against the day when he could deliver it to the West. Having no safe means of hiding the copies that he had made of key documents, he carried them around for two years sewn into his clothing. In 1960, as a member of a scientific-technical committee, Penkovskiy had legitimate reasons for meeting foreigners, among whom was an Englishman, Greville Wynne, who delivered certain materials provided by Penkovskiy to the British Embassy in Moscow. Wynne also delivered a letter from Penkovskiy to American authorities. In April 1961 Penkovskiy was a member of a scientific-technical delegation visiting in the West. Intelligence contacts were made. However Penkovskiy's three applications for visas for further travel to the West, all made in April-July 1962, were refused by the KGB. He was last seen at liberty on 6 September 1962.

The Penkovskiy case illustrates the great value of penetrations. There can never be enough of them. It illustrates the need for effective and secure liaison relationships. And it illustrates the necessity for coordination in all counterespionage activities. In the US intelligence community, the responsibility for the management of counterespionage is lodged with CIA. Specifically, the responsibility of being the community's coordinator for espionage and counterespionage is assigned to CIA by National Security Council Intelligence Directive No. 5.

Such was not always the case. In the late 50's, when the basic principles of NSCID 5 were hammered out, a good deal of parochialism had to be overcome. During the drafting process, certain proposals were made which would have had the effect of destroying centralization and returning the US intelligence community to the competitive and fractionalized conditions of the past. General Truscott, then the Deputy Director of Central Intelligence, read these proposals and said: "Knowing General Eisenhower as I do, I should not wish to be the person who would bring these recommendations to him."

In these later days, however, there is general realization that the Soviet services and their extensions in the Communist countries of Eastern Europe are a highly integrated system, and that we cannot cope effectively with a coordinated attack if we ourselves are uncoordinated. The security problem we can handle in a decentralized fashion because security rules are pretty much the same for all. But counterespionage must be centralized. As we have noted, the heart of counterespionage is the penetration operation—and we could not possibly achieve reliable penetrations on a fragmented or departmental basis.

The same is true of the other principal kinds of CE operations. To be effective, all require a central command post. In addition to the penetration, this is true of all efforts to induce defection. And it is true with respect to the deception operation.

This type of CE operation is based upon an established channel of communication with the enemy, and the purpose is to insert into this channel misleading information which will cause the enemy to take action which is contrary to his own interests. The need for centralized direction is clear. It is not possible to mislead the opposition by a series of uncoordinated bright ideas. It can only be done according to a central plan.

The need for central coordination is just as great in the employment of the double agent. He is a center of controversy today in intelligence circles because such operations are hungry consumers of time and manpower. From beginning to end, a DA operation must be most carefully planned, executed, and above all, reported. The amount of detail and administrative backstopping seems unbearable at times in such matters. But since penetrations are always in short supply, and defectors can tell less and less of what we need to know as time goes on, because of their cut-off dates, double agents will continue to be part

of the scene.[4]

Audio surveillance, another important CE tactic, also must be centrally coordinated. It is a form of physical surveillance, which means sustained drudgery. It may many times depend for success on effective liaison relationships. Although Americans are technically gifted, no amount of such expertise will suffice if the operation is badly managed.

In the past three years the Soviets have been publishing more and more about their own intelligence exploits and key personalities. This also underlines the need for centralized effort on our part. All of this material is being examined and when it concerns intelligence matters, it is being translated into machine language and stored on tape. By now a substantial percentage of the counterintelligence held in machine language by CIA was derived from overt materials.

New Directions

Ever since World War II the Soviets have devoted more and more time and energy to a third kind of subterranean attack in addition to espionage and counterespionage. This involves propaganda and disinformation, including forgeries, designed to convince people all over the world that Soviet accusations against the US, its military forces, and its investigative services, are true. This kind of operation is called covert, rather than clandestine, because of a basic distinction. A clandestine operation, if properly conducted, remains totally concealed. The authorities in the target area never know that anything happened. A covert operation, on the contrary, must have a product, such as a radio newscast, a newspaper article, a forged document or some other tangible. For this reason the service carrying out a covert operation knows from the start that it cannot keep the activity itself a secret; it aims instead for plausible denial. The object is to be able to say, "We didn't do it—someone else did." The fact that a product is surfaced gives the CI man something to work on. He has one end of the trail of evidence in his hand. What he wants to do, of course, is follow it all the way back to the source. In other words, counterintelligence work carried out against covert activity uses the same methods as does CI waged against espionage and counterespionage. What we need to do is to spot

the Soviet hand behind the visible product.

We therefore study, for instance, the African, West German, or American writer whose work consistently echoes the main Communist lines. Such themes have become familiar: the US government is fascistic; in America all minorities, including the poor, are ruthlessly oppressed; American foreign policy is bankrupt, a mere display of brute force; CIA and the FBI are Gestapo-like organs; CIA, in particular, has usurped the function of the State Department and is secretly making policy; America is dominated by commercial interests—Wall Street, the United Fruit Company, the big oil companies; the American negro can win equal rights only through violence; and there are plenty of others. When we see these themes played and replayed—often appearing first in a supposedly nonCommunist publication, then picked up and replayed by Tass and Radio Moscow, then repeated in Africa—we seek to learn all we can about the original author and the magazine or paper in which the piece first appeared. However far to the left the tone of such an article may be, the question is whether it is legitimate, in the sense of being an indigenous attack. If so, we can do no more than grin and bear it. Intelligence services can't be cry-babies, and they can't get into a public arena and slug it out with attackers who, no matter how hostile, misled, or mendacious, are nevertheless expressing their convictions in their own terms.

But the picture is very different if the supposedly non-Communist writer is in reality a Soviet agent, receiving the standard Soviet package of material from which to work, holding secret meetings with a Soviet case officer or a go-between, and accepting Soviet money. This sort of thing is as deadly as spying.

In sum, the US needs to pay more attention to counterintelligence operations against Soviet covert action. We need to identify the agents, double some of them, place surveillance on them and their case officers, and finally mount operations to recruit Soviet CA specialists.

The Team Approach—Vietnam

Just as the Soviet disinformation campaign underlines the need for centralized effort, the Vietnam problem has placed a premium on

coordinated effort. When hostile clandestine pressure grows strong, the US counterintelligence community shows a correspondingly greater capacity for working together. This has happened with respect to Vietnam. The first and gravest CI problem there, which persists, is that there are simply not enough specialists engaged in fulltime counterintelligence work. The need for tactical military intelligence has been so great that our CI potential has been largely drained off to meet the need for more order-of-battle and POW information, more analysis of captured enemy documentation, and the like. The CI teams of both the Army and the Marine Corps spend most of their time collecting tactical military intelligence. Compared to these activities, the OSI detachments and the detachments of the relatively new Naval Investigative Service are much less burdened with positive requirements, but these are primarily security, not counterespionage, units.

The second grave problem is to determine the extent to which the North Vietnamese have succeeded in penetrating the government and the intelligence services of the South. The Republic of Vietnam has an extensive CI network. It consists of the Central Intelligence Organization, the Military Security Service, and the Vietnamese National Police. But they too are constantly diverted from long-range projects by the pressing need for tactical collections. The security program in the South simply does not work because the government has expressed and implemented its willingness to accept as citizens of South Vietnam all Viet Cong who profess to have had a change of heart.

The first step toward coordinated action that had to be taken was to identify the enemy. As long as we persisted in using "Viet Cong" as an omnibus term for everything Communist, we were unable to understand events. In February 1967 CIA called together the elements of the CI community and outlined the problems as it saw them. The meeting was attended by representatives of the Defense Intelligence Agency, the Assistant Chief of Staff for Intelligence, the Naval Intelligence Command, the Air Force's OSI, and the CI element of the G-2, Marine Corps. Task forces were created. CIA provided space and equipment, as well as personnel, and furnished the researchers the counterintelligence collected up to that time.

Before February 1967 the US had only some scattered and largely unverified pieces of information about the military intelligence structure of the North Vietnamese and about the Central Research Directorate of the North Vietnamese Ministry of National Defense. What was known of

the intelligence structure did not match the typical Communist pattern, and strength estimates were obviously far too low, when judged against the wide range of North Vietnamese intelligence activity. The first research targets to be selected were the Security Sections, called the An Ninh, of the Communist Party of North Vietnam, which are physically situated in South Vietnam. These security sections are built around cadres of intelligence personnel trained by the North Vietnamese Ministry of Public Security and infiltrated south. The Ministry of Public Security, like the rest of the government in the north does not recognize the government in the south and considers South Vietnam as its own territory, temporarily and illegally occupied in part by the American gangsters. Hence the An Ninh elements are regarded by their Headquarters as security forces. The Ministry receives a constant flow of information from these security sections and issues a steady stream of orders to them. The sections also contain South Vietnamese Viet Cong personnel who have been recruited and trained in South Vietnam. Our present An Ninh strength estimate is approximately 20,000.

Because of the view held by the North Vietnamese, these forces carry out not only espionage and CI functions but also public safety and security functions, judicial, police, and even penal functions. At district and higher levels, they also have an "Armed Security Unit" of the Security Section. It is the assigned mission of this unit to seek out, harass, and if possible destroy the intelligence and security organizations and personnel of the opposition—chiefly the Americans.

Other elements of North Vietnamese intelligence and CI are now under study; and it is expected that additional papers, designed primarily for use in the field, will be forthcoming on such subjects as technical intelligence, and the Central Research Directorate. In June 1968, CIA published "The DRVN Strategic Intelligence Service: Cuc Nghien Cuu." Computer programs are now being used to cope with the increasing flow of CI.

In short, the team approach is paying off. Cooperation is excellent, and the results are proving useful to all.

It is no accident that our research into the An Ninh, its functions and structure, has revealed close parallels to the KGB. In Vietnam, too, the Soviet advisory system is at work. The only effective answer to the centralized clandestine war which Moscow wages relentlessly against us is the internal cohesiveness and cooperation of the US

counterintelligence community.

BIBLIOGRAPHY

1 See A. C. Wasemiller's "The Anatomy of Counterintelligence" in *Studies* XII 4, p. 9 ff.

2 The Soviets have adopted the opposite system: the civilian service, the KGB, is responsible for the security of the GRU.

3 See the novel *Topaz* by Leon Uris (reviewed in *Studies* X11 1, p. 88).

4 It is important to be clear about this matter of defectors. What a pre-World War II defector has to say is still important. We shall not win this war against Soviet intelligence without true depths of expertise. When a Soviet defects, when he walks into an American embassy, the worst thing that can happen to him is a confrontation with incompetence. Strong-arm methods will not work with him. It's no good grilling him, or making him the objective of a squeeze session. Soviet intelligence officers are told over and over that if they come over to the American side, they will be ignored as individuals, and squeezed like lemons. What the defector most needs is the attentions of someone who knows his world.

Posted: May 08, 2007 08:23 AM