

Multi-disciplinary threat and response

COUNTERINTELLIGENCE FOR THE 1990s*

George Kalaris and Leonard McCoy

Background

As we contemplate the counterintelligence (CI) challenge of the 1990s and seek a CI structure and posture appropriate to that challenge, our outlook is inevitably conditioned by the discovery in the past several years of a devastating series of CI setbacks. Our most sensitive intelligence agencies have been penetrated. We have suffered damage in the strategic national defense area. Costs of these compromises are estimated in the billions of dollars. Certainly there is a basis in these recent cases for forming a perception that our national CI program has failed to carry out its mission in the 1980s.

Even with improved performance by the US Government components charged with CI responsibilities over the past decade, hostile intelligence services have inflicted severe damage on our national interests. The CI system has proved to be inferior to the excellence of its component parts. We can expect hostile intelligence services to intensify their activities against us in the 1990s. We can also expect that the present structure of the CI community, having been inadequate to meet the threat in the 1970s and 1980s, will be overwhelmed in the 1990s unless we improve it.

Thinking in the late 1970s and early 1980s about the needs, direction, and requirements appropriate to the US CI effort in the 1980s was for all practical purposes a straightline projection of what was then in hand. All that was advocated was more of the same. Even before the mid-1980s, that thinking had proved to be totally inadequate to the challenge faced. Therefore, this paper proposes a radical revision in the structure of the US CI community. The purpose: to effect changes in our CI posture which will dramatically improve our CI capacity for the 1990s.

The Challenge

US counterintelligence concentrates primarily, and appropriately, on the Soviet services as the major adversaries. As we have seen in the 1980s, we also have had to place increased emphasis on countering the East European intelligence services acting on behalf of the Soviets or in the interests of their own countries. Several of these services have scored major successes against us. In the 1990s we can expect to see even more such operations against us and our closest allies, spurred on by our opponents' success to date and by Soviet pressure for increased effort, especially in technical areas. Beyond the numerous intelligence services of the USSR and Warsaw Pact countries, we also

* This article is based on a paper the authors prepared for the Consortium for the Study of Intelligence in December 1987.

Counterintelligence

project increased intelligence collection efforts against us on the part of Asian communist countries and Cuba. In both of these areas, the US has suffered grave injury at the hands of hostile services in the 1980s.

In addition to the increasing threat from communist countries, the US must expect to have to counter intelligence operations by a growing number of underdeveloped countries, as well as operations conducted by friendly countries which are not satisfied with particular aspects of US policy or believe that the most direct way to information satisfying their own intelligence requirements is to penetrate US intelligence agencies. Operations in these areas have been discovered in the 1980s and should be looked upon as examples of what to expect in the 1990s. Most such activities will be in the classical human source recruitment category, but some of the countries most likely to be involved also have substantial technical intelligence collection capabilities. In several cases, we will find ourselves cooperating in intelligence and counterintelligence matters with these countries at the same time they are operating against us (and we against them).

A greatly increased unilateral counterintelligence capability overseas will be among our most crucial needs of the 1990s, along with the need to increase our ability to detect and counter technical intelligence collection advances by opposition services. We anticipate that increased FBI capabilities and enhanced public awareness of espionage will cause the Soviets to concentrate their recruitment activities against the American target outside the US. An increasing burden, therefore, will descend on those American intelligence organizations charged with espionage and counterespionage responsibilities abroad.

Definition

The definition of counterintelligence crafted in the mid-1950s had outlived its relevance to the realities confronting the intelligence community by the early 1970s. By the late 1970s it had literally fenced in the efforts that had to be made to counter the multi-faceted threat directed against our national security interests. It had reduced counterintelligence to a passive discipline concerned primarily with "locking up the barn door after the horses had been stolen". In the late 1970s we finally took official cognizance that the threat to our security was not limited exclusively to the human element. It became clear that collection against us by Soviet agencies using technical means was substantially greater and more significant than we had generally believed. Therefore, in the 1980s some American intelligence organizations revised their CI components to analyze and contend with this multi-faceted threat.

Fundamentally, CI for the 1990s should be defined as that discipline of the intelligence sphere that is concerned with the actions of foreign intelligence services and organizations, friendly or not, against us, employing human and technical means, which impact adversely on our national interests and goals. It naturally includes those actions which we, the CI agencies of the US, take to negate such inimical activities. Thus, CI includes, as component disciplines, counterespionage, counter-sigint, and counter-imagery. The instrumentality used by the foreign entity against us is what determines our actions to counter the effort.

Counterintelligence

The substance of CI does not change with time, but its emphasis must inevitably shift to meet the nature of the attack on our national security. Before we reach the 1990s, it is imperative that the American CI community accept the concept of a multi-disciplinary threat and the need for a multi-disciplinary response. If counterintelligence remains limited in the 1990s to what is in effect only counterespionage, we will be dealing with only one aspect. In the 1990s we must redefine the threat as the composite human and technical threat it is, and we must develop appropriate cross-disciplinary countermeasures to overcome the threat.

Not that technology transfer or state-sponsored terrorism are likely to abate, but to the extent that these threats are susceptible to countermeasures, the foreign policy, security, and police mechanisms of the government will contribute the lion's share of countermeasures and defensive operations. Actions taken to identify, monitor, control, and neutralize foreign intelligence operatives will continue to constitute the major counterintelligence contribution to frustrating these threats to our national security by hostile services. As in counterespionage, one of the most significant sources of information on such hostile activities will continue to be the penetration of the hostile service.

Under our definition, personnel security of those elements of the US Government and its contractual components whose activities have an impact on our national security interests also falls within the purview of counterespionage as a discipline. The vetting of new employees, as well as those in more advanced stages of their careers in national security related work, including contractor personnel, is a counterespionage responsibility. Our definition would also include the manufacturer abroad, under licensing, of classified American defense equipment

The Status Quo

The present counterintelligence response to the generally recognized multi-faceted threat is fragmented, with each counterintelligence component (other than the FBI) focusing primarily on the threat to its own parent organization component or program. We are not suggesting that this is in itself improper, only that fragmentation and departmentally oriented efforts do not constitute in their sum an effective national counterintelligence program. Rather, this approach impedes considerably the formulation and execution of a national program, the development of universal guidelines, and the establishment of homogeneous national CI objectives. A more integrated approach is imperative for the 1990s.

The FBI CI program continues to expand and improve, and needs only to reevaluate its capabilities under the increased multi-disciplinary concept in its CI program for the 1990s. Its involvement in Defense Department CI/industrial security operations and programs is the most important step necessary to the over-all enhancement of the domestic CI program.

With primary responsibility for CI overseas, CIA has a tremendous challenge for the 1990s. Pressure for enhanced CIA capabilities overseas has now reached irresistible proportions in the wake of revelations of repeated agent meetings overseas in all of the extremely damaging cases of "the year

Counterintelligence

(plus) of the spy". This effort will be crippled without full integration of FBI, DoD, and CIA efforts. It will not suffice for CIA to monitor the Soviets overseas, or for the FBI to do so in the US, without extensive knowledge of the Soviet primary target—the US defense complex—and without CIA and FBI participation in DoD CI and security programs set up to identify, neutralize, and exploit opposition penetration efforts directed against that target.

The greatest damage to national security has been in areas for which the DoD is responsible—national defense—as that is the target area of our major opposition. All CI resources must be brought to bear in this area. The departmental and geographical CI boundaries which we have established are not honored by the primary opposition services, which use them to defeat us. They recruit in one area and run the case in another, moving agent and operations officers about the map at will, and engendering among US CI agencies a cumbersome, lumbering coordination process which seldom catches up with opposition actions. This bureaucratic weakness was cited in a recent legislative review as having caused a crippling delay in introduction of the FBI into a major espionage case. We must eliminate the opposition advantage in this area by bringing our three primary CI bodies together at the sources of our vulnerability.

New Look Overseas

In overseas installations, we must develop new personnel configurations which take into account the shift in emphasis which the Soviets will place on their activities against us. Not only should the recruitment of Soviet intelligence officers remain high on our priority list at each foreign-based American intelligence installation; we also must substantially increase our ability to monitor the activities of Soviet intelligence officers, whether they represent a recruitment target or not.

Tokyo, Vienna, Paris, and Mexico City are today, and are likely to remain in the 1990s, the favorite agent-meeting and walk-in locales of the Soviet intelligence services. Accordingly, we must expand our coverage of Soviet activities in those cities, and others which may well be added as the opposition detects our efforts.

Technical Licensing

Extensive licensing by DoD of foreign companies to manufacture US weapons systems and technology has added another dimension to the CI problem overseas. Not only must our unilateral CI capability overseas be prepared to counter hostile collection action against these exposed targets, but we must also develop effective local liaison relationships which will assist in protecting these weapons systems and technology from hostile intelligence collection.

Personnel Staffing

A separate career track for counterintelligence analysts must be established for the 1990s as the core of the new CI component. Entry into the track must be competitive, requiring at a minimum four years actual and successful

Counterintelligence

operational experience in the recruitment and handling of agents. To ask a counterintelligence analyst with no direct operational experience to analyze and judge developments in any agent case is tantamount to asking a pre-med student to diagnose gastrointestinal anomalies. Unless the analyst has experience in handling agents, he/she really has no sound basis for evaluating behavior and spotting discrepancies. Sophisticated countermeasures will have to be developed, springing in large part from our own development of technical collection systems. This threat will dictate recruitment into counterintelligence of technically qualified officers who can keep CI abreast of technical developments and conceive defensive and counter operations against such capabilities.

The counterintelligence component of any intelligence organization cannot be the depository for has-beens. The component must command respect not only because of where it is placed on the organizational chart, but because of the quality of its officers and their individual records of achievement in the more traditional facets of the intelligence business.

Training Approach

Regardless of whatever other training is given prospective operations officers, in preparation for the 1990s the curriculum must include heavy exposure to counterintelligence information. We recommend a minimum of 50 hours of appropriate training. No intelligence officer should be allowed to venture into operations at home or abroad without a solid understanding and appreciation of the capabilities of our principal adversaries. To do otherwise is the equivalent of casting a lamb into a wolf-infested forest.

The ultimate objective in exposing all prospective operations officers to intensive counterintelligence training is not to produce 50-hour counterintelligence wonders, but rather to ensure that all operations officers of the 1990s will be acutely aware of the lessons learned in the past 65 years of our encounters with hostile intelligence agencies. Unless the first echelon of defense—the operations officer—is aware of the possibility for fabrication, deception, and misinformation, the early warning signs of a bad case may be completely overlooked, not understood, and not reported.

The Ultimate Need

Responsibility for the establishment of a national counterintelligence policy, the allocation of tasks to the various counterintelligence organizations, monitoring of progress, and resolution of inter-agency conflicts must be lodged in some entity or person. Continuation of the piecemeal and parochial approach to counterintelligence can only perpetuate damage to the national security.

Existing interagency coordination procedures, NSC interagency committees, and excellent personal relationships between the heads of counterintelligence components have not and cannot produce and implement a national policy with teeth in it, nor insure that maximum effort will be applied to a particular national counterintelligence objective.

The present structure of US counterintelligence is inadequate to fulfill the tasks posed by the CI challenge of the 1990s. A centralized authority is required

Counterintelligence

which will be capable of, and responsible for, mobilizing all US CI agencies and capabilities against the common foreign intelligence and security threats: Wherever this authority is placed, a very great role in its day-to-day functioning must be played by a newly constituted DoD CI office which is directly and vigorously involved in national counterintelligence management of service CI/Security agencies.

Within the CIA, CI must be raised out of the Operations Directorate to a level of authority within the Agency which gives it command and operational responsibility across the entire intelligence community as well as throughout the Agency itself. The level of Deputy Director may well be too low for it to have such authority. While such a step might be taken to temporize, until staffing and organizational complications are resolved, it will eventually be necessary for the CI responsibility to be placed in a DDCI for Counterintelligence. Only then will the full integration of all interagency CI capabilities become feasible.*

A number of the functions of other CIA components will have to be assigned to the "DDCI/CI", namely those elements of security concerned with personnel security, communications security personnel, DI elements working on strategic deception, and elements responsible for defensive measures against hostile technological attack. The "DDCI/CI" would have to be placed in the chain of command for oversight of all operational matters concerned with CI, and have responsibility for a portion of the performance evaluation and reassignment of all senior CIA officers.

One of the first tasks of any such new counterintelligence leadership of the 1990s should be to define its area of responsibility—specifically the elements of counterintelligence which are to be the focus of the counterintelligence community. This task is not the domain of lawyers, academicians, or dilettantes. It is the prime responsibility of those who have practiced the craft.

* On 29 March 1988 the Chairman and Vice Chairman of the Senate Select Committee on Intelligence informed the press that the Director of Central Intelligence told the committee, in closed session, that he has "reorganized the counterintelligence function within the CIA and appointed a senior official to head it."