TITLE: Security As An Intelligence Community Concern

AUTHOR: Patrick L. Carpentier

VOLUME: 10 ISSUE: Fall YEAR: 1966

STUDIES IN INTELLIGENCE

A collection of articles on the historical, operational, doctrinal, and theoretical aspects of intelligence.

Past progress and future desiderata in interdepartmental safeguards for the secrecy of intelligence.

SECURITY AS AN INTELLIGENCE COMMUNITY CONCERN

Patrick L. Carpentier

In the past half-dozen years we have seen an interesting and valuable evolution from an agency to a community concept of security for intelligence, in spite of difficulties that have stood in the way of the interdepartmental approach to protective measures. In the following pages we trace this recent evolution and look at the prospects ahead. Our purpose is generally to promote wider open discussion of those security questions which all our intelligence agencies have in common and particularly, with respect to some major problems which have been recognized within the community for years but whose resolution requires executive or legislative action, to contribute to a broadening appreciation of their critical importance that can ultimately lead to such action.

E Pluribus

Security has traditionally been a departmental matter, something for each agency head to administer as final authority in his domain. This disjunction of authority derives from the fact that the agencies of the government were each established for a distinct national purpose and given corresponding prerogatives and responsibilities. Security concepts and standards, like other departmental programs, were shaped by internal considerations. The disjunction is strikingly illustrated in the fact that an employee terminated for security reasons by one agency can, if found eligible by the Civil Service Commission, be taken on by another. These departmental prerogatives remain in force in the intelligence community; a concerted community program has to be built on a basis of mutual understanding and common purpose. Only the President or the Congress could dictate general

security measures beyond the minimum requirements now established by basic executive order and legislation.

In these days of joint intelligence activities and widespread dissemination of materials extending beyond the intelligence community proper, the traditional security concept does not give intelligence agencies, particularly those producing sensitive materials, the protection they require. For sensitive intelligence the basic executive orders and legislation have had to be supplemented by agreement on special measures. The inadequacy of the minimum standards is especially evident when budgetary considerations are permitted to dictate the degree of security that is provided—a situation most likely to prevail outside the intelligence community, where the threat of hostile penetration is not fully recognized and community agreements cannot be enforced.

The statutory responsibility of the Director of Central Intelligence to protect sources and methods, as set forth in the National Security Act of 1947, is not accompanied by any implementing authority. Allen Dulles, in *The Craft of Intelligence*, expresses the opinion that the legislative history shows an intent to limit this responsibility to CIA intelligence assets. In practice, at any rate, the DCI has never exercised command authority over other agencies in regard to the protection of intelligence. If it were practicable to confer such authority on him it would obviate the difficulties of the voluntary approach to concerted measures, in which strong departmental prerogatives are partially compromised in order to achieve workable solutions that are still not completely satisfactory.

Even CIA assets, moreover, cannot be limited to the confines and protection of the Agency, and the same thing is true for all other intelligence agencies. The intelligence effort has become continually more interwoven. Thousands of reports are exchanged daily; innumerable joint meetings are held. Indeed, it is doubtful that any one agency can now carry out any major intelligence activity in isolation. The resultant danger of widespread damage from a single penetration was illustrated in the recent cases of Sgt. Jack Dunlap and Sgt. Robert L. Johnson, in which practically every agency in the community suffered seriously.

Thus the most effective security program imaginable in any individual agency goes for naught; the level of security is that created by the lowest standards maintained anywhere in the intelligence flow. And the flow, as highlighted in the case of Sgt. Johnson, a

career soldier assigned to the Armed Forces Courier Service, extends beyond the circle of the intelligence community. The adversary, seeking a point of penetration, will concentrate on the weakest links. The security problems of one agency therefore become the problems of all others affected and their resolution a common concern. One such problem has been the lower personnel security standards set up for military personnel. Substantial remedial action is now being taken, but major problem areas remain.

The USIB Committee

In this atmosphere dominated by departmental prerogatives but tempered by recognition of the need for coordinated action, the United States Intelligence Board in early 1959 instituted a community program for the protection of intelligence assets by establishing its Security Committee. During the first years the Committee members each remained jealous for the prerogatives of their own agencies. It took three years of negotiation to chalk up the first major accomplishment, the issuance of DCID 1/7, approved 21 February 1962, establishing uniform control markings and procedures for the dissemination and use of intelligence. But now the mutuality of all agencies' interests has been fully recognized. Interagency discussion is uninhibited and information is freely exchanged within the limits of effective security. Seldom if ever is any agency with serious interests in a security problem not informed fully and made a participant in the remedial action. Limitations on concerted Committee action have been reduced for the most part to matters that lie beyond the authority of the intelligence agencies.

Another major accomplishment of the Committee has been the establishment of a coordinated community mechanism to investigate security breaches more effectively and without duplication. In July 1962 a USIB policy statement established responsibilities for the exchange of counterintelligence and security information. Damage assessments and remedial recommendations covering audio penetrations of U.S. embassies led to the establishment in December 1964 of a USIB Committee on Technical Surveillance Countermeasures which more effectively promotes and coordinates technical inspections and R&D programs. The Security Committee has also prepared damage assessments and recommended remedial action in espionage cases. Personnel security programs have been substantially enhanced through Committee efforts. The Committee initiated the President's

Directive of 23 May 1960 forbidding unauthorized disclosures of intelligence and an Agreed Guidance of 29 June 1960 implementing the Directive.

Excellent examples of coordinated community measures are the systems of compartmentation maintained for the protection of various categories of sensitive information. The special protection given compartmented information, however, has unfortunately tended at times to depreciate the importance of protecting uncompartmented information. A document classified Secret or below within a system of compartmentation is subject to higher standards of both personnel and physical security than one marked Top Secret without a code word. Those responsible for the handling of Oleg Penkovskiy, for example, would presumably have found code-word standards of protection advantageous in their operation.

There is to be submitted to the USIB shortly a proposed DCID establishing uniform personnel security standards for access to compartmented intelligence information. It will greatly enhance personnel security and simplify its administration not to have independent standards for each community system. A major accomplishment will be the extension of the same standards to both civilian and military personnel. Uniformity should also greatly facilitate security processing in joint projects. Hopefully, this approach will be carried to its logical conclusion and eventually cover all intelligence, not just compartmented systems. In essence, this would mean a distinct and unified personnel security program for all intelligence personnel and outsiders who have continued access to intelligence. The operation of the proposed DCID may give impetus to this eventuality.

Similarly in the matter of physical security. Executive Order 10501 of 5 November 1953, "Safeguarding Official Information in the Interests of the Defense of the United States," sets the basic minimal standards, which, particularly for the storage of Secret material, do not give adequate protection in vulnerable areas abroad. The Security Committee took up this problem in 1961 during a government-wide review of the Order and considered certain measures specifically designed for locations overseas. Budgetary considerations, however, prevented departmental representatives from taking a firm position on these measures in spite of their recognizing the hazards of inaction. Hopefully, the stringent physical security given compartmented information will eventually be applied to all intelligence or at a minimum to sensitive uncompartmented materials.

Legislative Needs

It has been recognized that the secure administration of a sensitive agency requires that its head have absolute authority, when he deems it in the national interest, to remove any employee summarily, without recourse to administrative review. Only thus can the highest standards of personal integrity, loyalty, and security be kept inviolate. The first summary removal authority seems to have been granted in 1940 to the Secretaries of War and Navy (50 App. USC 1156)—a wartime measure directed against possible subversives. Then the Director of Central Intelligence was granted similar authority in 1947 under Section 102 (c) of the National Security Act. This authority has been affirmed by the courts, and one case appealed to the Supreme Court was refused a review. The Director of NSA has by recent legislation (PL 88-290, March 26, 1964) also been given such authority under delegation from the Secretary of Defense.

An Act of August 26, 1950 (PL 733) granted discretionary removal authority to eleven specified agency heads, and Executive Order 10450 of April 27, 1953, "Security Requirements for Government Employment," extended this authority to all agencies of the government. This Order serves as the basis for the personnel security programs of all community agencies, either as enabling authority or, in agencies like CIA that operate under a separate authority, as a model in establishing criteria for employment. Removal procedures required by it, however, are formal and detailed, quite inadequate for serious cases. Statutory authority for summary removal should still be given the administrative heads of all intelligence organizations.

Today Restricted Data, classified information on nuclear energy matters, is probably afforded without comparison the most distinct safeguards given any category of classified material. Its protection is specifically required by statute (Atomic Energy Act of 1954 as amended). Special personnel security criteria for access to atomic energy information have been established. Only for Restricted Data may a judicial injunction be petitioned against threatened disclosure. CIA has without success proposed similar statutory protection for "Intelligence Data" whose peculiarity in sources and methods requires it. The present espionage laws are not adequate: conviction under them depends upon proof of intent to harm the United States, and classified information must be produced in open court to demonstrate the damage. No injunction is possible.

An ad hoc committee of the USIB prompted by the defection of NSA employees Martin and Mitchell considered several proposals for remedial legislation. The committee was unable to come to an agreement, however, and further efforts were abandoned.

Although there has been official recognition at the highest levels of deficiencies in the espionage laws, other remedial proposals that have been made on numerous occasions have all been similarly unsuccessful. A major reason is undoubtedly the consideration that too stringent espionage laws could be given broad applications that would encroach upon civil liberties and basic freedoms guaranteed by the Constitution. The hard fact remains, however, that as things stand, purposeful acts of espionage have occurred and undoubtedly will continue to occur without adequate legal redress. It should be possible to secure adequate legislation against these within the framework of constitutional limitations. Efforts in this direction must not be abandoned but renewed at the earliest propitious time.

Press Leaks

These considerations lead us to the continually plaguing problem of unauthorized disclosures of intelligence materials, specifically through public information media. A great deal of time and effort have been expended in the investigation of such occurrences without appreciable effect. This problem impinges directly upon the freedom of the press, perhaps the most jealously guarded of the constitutional guarantees. Here again the espionage laws are completely inadequate; the criminal element inherent in espionage, intent to harm the United States, is not even present. Usually some high-level official makes the disclosure deliberately in order to elicit public support for a program which he considers to be in the national interest. Motivation is suggested by the fact that most disclosures occur during periods of budgetary debate. Personal gain for an enterprising reporter can also be a factor.

The resulting damage to sensitive sources and methods, delicate international relations, and the national welfare has unfortunately led to no positive action to abate the problem. Newsmen, admonished on occasion by security authorities for acting against national interest, have shown no concern; they have been assured by the releasing official that the information leaked is not damaging. Such an official is usually well removed from intelligence collection activities, has no understanding of source protection, and feels no guilt at circumventing

the established channels for public dissemination which would have provided for a security review.

The question of remedial action in this area inevitably brings up the British Official Secrets Acts, which afford practically absolute protection against unauthorized disclosure of any information originating within the British government. They have been interpreted to cover even the premature release of certain wills which happened to be of popular interest. They make the mere fact of unauthorized disclosure sufficient to prosecute; the defendant must prove that his act was not unlawful. Moreover, the court proceedings are held in secret to protect the information involved.

In the United States such legislation, by almost overwhelming legal consensus, would be unconstitutional. But the fear of unconstitutionality has also inhibited any effort to pursue lesser legislative measures which could be effective within the constitutional framework. A Commission on Government Security instituted by Congress in 1955 to study ways to "establish fair, uniform, effective, and realistic measures to safeguard both the national security and the right of individuals" was aghast at the problem. It recommended making it unlawful for any person to disseminate information classified Secret and above to any unauthorized person and unlawful for anyone to receive such information knowing or having reason to believe it to be classified, with punishments of a $10,000 fine or 5 years in jail or both. As usual, the proposal received little attention.

The general belief that any corrective measures would meet with strong opposition from the press may not be completely accurate. Responsible American newsmen have spoken in favor of an official secrets act, not of course one with the extreme stringency of the British Acts, but some kind of controls for public information. Some disapprove, for example, of the publication of personal memoirs of government officials in the know so soon after their resignation as to affect sensitive activities and the work of their former fellows still in the government. They know how easy it is to develop sensitive information from government contacts, and they deplore the fact that if a responsible newspaper withholds from publication some matter of sensitivity it is only likely to be scooped by a less conscientious rival.

In a recent book on the British Official Secrets Acts, *Not in the Public Interest*,[1] Mr. David Williams decries the travesties resulting

[1] Reviewed in *Studies* X 2, p. 97.

from excessively broad applications of them, but he does not question the frequent need for executive secrecy. He describes an informal, nonofficial "Services, Press and Broadcasting Committee," originally formed in 1912, consisting of representatives of the government, the press, and now broadcasting and television. The Committee issues to news media "D" (Defense) notices specifying matters which are sensitive and asking the forbearance of editors. Mr. Williams does point out that "D" notices have sometimes been used to cover up departmental errors. Nevertheless, this kind of active participation of the press in its own disciplining in the national interest seems to be a promising approach to the problem.

Perhaps an ad hoc committee of representatives from responsible news media and from the government should be constituted, preferably by executive action, to study the problem and submit recommendations. They could consider among other things the feasibility of such a permanent committee to review proposed releases and furnish guidance in sensitive matters. If the whole field of national security information seems too broad a jurisdiction for it, it could be limited to sensitive intelligence information.

There is one other aspect of public release that calls for brief mention. The release of national intelligence requires USIB approval, but there is no provision for joint review of releases by individual departments concerning matters falling within their jurisdiction. Such releases, however, may be based upon and revealing of intelligence collection efforts, and the effect on these efforts should be evaluated in advance by those responsible for their protection. It has been the exception rather than the rule that a proposed release has not been submitted for this kind of evaluation, but the impact in these cases has been so substantial as to make it worth reaffirming that coordination with all affected parties should be accomplished prior to release. In almost every instance the release can, if necessary, be rewritten so as to protect the sources without interfering with its substance.

Conclusion

Security problems are not the unique property of intelligence, but the integrated character of community activities requires that all agencies and all their personnel join here in a common front. Nor can it be a static front, or a matter of adherence to minimum standards. Opposition penetration techniques are constantly shifting as areas of

vulnerability are exposed; security efforts must be dynamic and flexible to counter them.

Departments that have administrative control over intelligence components and activities should recognize the distinct need for protection of methods and sources that sets intelligence apart from nonintelligence activities. The intelligence chiefs should have latitude and discretionary authority wherever possible, in order to participate in a community approach to security. The difficulties are complex, particularly with the advent of machine systems which give voluminous access to information automatically.

Intelligence acts as chief promoter of security measures for the nation because it is most aware of the hostile threat, dealing with it daily. Some measures to achieve greater security are difficult to harmonize with a free society, and that is why they have not been taken in the past. But the nation needs to keep a constant watch on the balance between security and personal freedoms. If the imbalance is too great in either direction, then corrective action is warranted in the national interest. Perhaps this paper will help focus thoughtful attention on the question.