

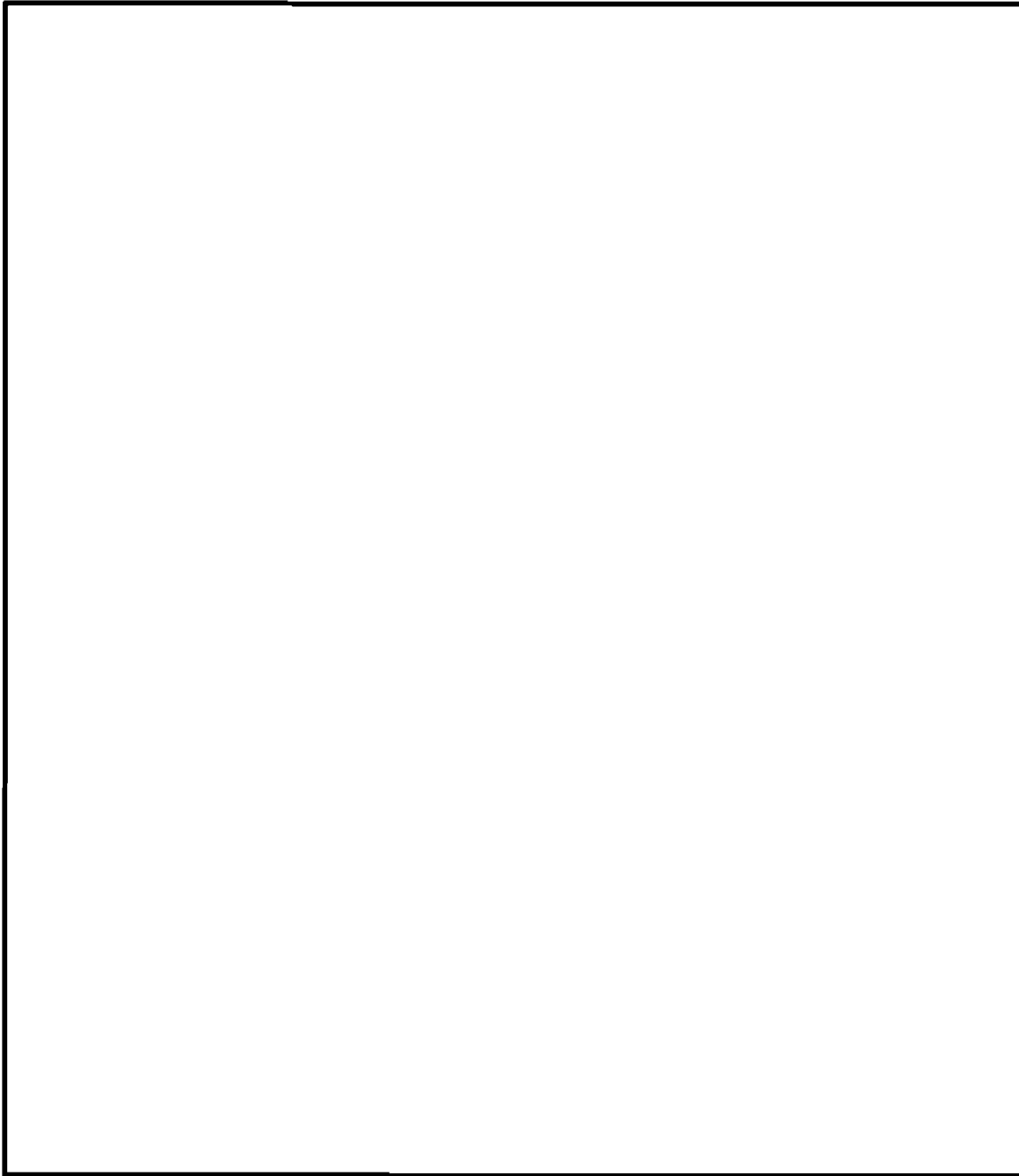
Third Party Nations: Partners and Targets (~~S-CGO~~)

(b) (3) - F.L. 86-36



(b) (1)
(b) (3) - 50 USC 403
(b) (3) - F.L. 86-36
(b) (3) - 18 USC 793

~~This article is classified TOP SECRET - Handle Via Comint Channels Only in its entirety.~~



~~TOP SECRET~~

CRYPTOLOGIC QUARTERLY

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

BACKGROUND

There are potentially both operational advantages and cost savings to be gained by a Third Party exchange agreement. As might be expected, assessments of these advantages/cost savings, in any given instance, can vary greatly depending upon one's perspective.

[redacted] But the costs of obtaining this material are often substantial, if the time spent by policy makers, negotiators, staff coordinators, material handlers, and office help are all added in. Since, in addition, a reverse flow of material [redacted] to the Third Party is usually part of the bargain, the total dollar costs and U.S. man hours involved may exceed those which would have been required for an equivalent U.S. effort.

But considerations of cost and cost effectiveness are usually secondary in assessing the desirability of a Third Party exchange. Focus is generally on the [redacted]

Also, not infrequently, after funding limits for [redacted] have been reached, a decision is made [redacted] with a Third Party, whether or not this would be cost effective. [redacted]

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

[redacted] not cost saving, is the primary objective of Third Party exchanges.

In parallel with claims of Sigint operational advantages or of cost savings to be derived from the use of Third Party resources, several arguments are available to justify the risks entailed in exchanges which foster the development of Third Party cryptologic

[redacted]

Finally, in a broader context, there are occasions where current national aims make it desirable to broaden intelligence, including Sigint, relationships with a Third Party, though benefits to [redacted] Sigint may be minor or nonexistent.

To each of these arguments there are counter arguments, which are, in turn, subject to rebuttal; and the rebuttals themselves are rebuttable, etc. Because, in these arguments and counter arguments, subjective judgment and objective fact are hopelessly intermixed, the pros and cons regarding the points made in the preceding paragraph are presented below in the form of a dialogue. The aim is to give a clear and forceful exposition of the two opposing views. The arguments against loosening constraints are designated "Conservative" and those in favor are labeled "Liberal." The phrasing of the points will attempt to reflect the conviction, even emotion, with which the issues are often viewed by each side.

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

~~TOP SECRET~~

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

General Spread of Cryptologic Knowledge/Awareness

Conservative:

There is no question that general cryptologic awareness is likely to increase either with or without [redacted] assistance to Third Parties. But Sigint success is a function of the ability to stay ahead of target Comsec development; and an ability to stay ahead is, in turn, directly dependent on the rate of that Comsec development. Cryptologic assistance to Third Parties will, without question, increase that rate.

Liberal:

The underlying rate of cryptologic development throughout the world is faster than ever before and getting even faster. Cryptologic literature in the public domain concerning advanced analytic techniques is proliferating. Inexpensive high grade cryptographic equipment is readily accessible on the open market. It is hard to imagine that the rate of Third Party cryptologic development can be much affected by a gradual broadening of selected Third Party exchanges.

Conservative:

The gap between the state of cryptologic technology in the public domain and the actual use of cryptologic technology is ordinarily very wide. When [redacted] furnishes cryptologic assistance, even if the material provided is theoretically within a Third Party's cryptologic competence, that action, at minimum, narrows that gap, bringing the actual state of a Third Party's cryptologic progress closer to, if not beyond, that which the Third Party could, in theory, achieve on its own.

Liberal:

Excessive, sometimes paranoid, concern over the alleged risk to cryptologic information already in the public domain can only hobble, needlessly, U.S. efforts to deal with present realities. Third Party Sigint capabilities and aspirations have advanced greatly since the early post-WWII period. What were regarded as necessary and sound security constraints then do not have the same applicability today.

Conservative:

Neither sound Sigint security principles nor sound banking principles have been generated by paranoia, though both are periodically out of popular favor. In both cases the price of putting long-term system stability at risk in the pursuit of short-term advantage is very high; vide, the current Texas banks/savings and loan crisis.

Enhancement of Third Party Security Measures

Conservative:

Some degree of control over the further dissemination of cryptologic information can probably be achieved by establishing an exchange arrangement with a Third Party, [redacted] [redacted] It is also questionable whether limiting the distribution of material which would have been passed on by the Third Party in the absence of [redacted] constraints would justify putting at risk the additional material supplied to or generated by the Third Party as a result of [redacted] assistance.

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

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

~~TOP SECRET~~

CRYPTOLOGIC QUARTERLY

Liberal:

We have seen again and again that when we have set tighter security rules as a condition of a given Third Party exchange, the Third Party has instituted, and so far as can be determined, abided by such rules.

Conservative:

Nations are said to have neither friends nor enemies, merely interests. It would be naive to believe that any Third Party nation will observe its solemn covenants if it suits their interests not to. In this connection, [redacted]

[redacted] Ironically, it is [redacted] which we are moving gradually toward de facto Second Party status, thereby maximizing the risks of cryptologic compromise and technology transfer after, and perhaps even before, such [redacted]

Advanced Cryptologic Capabilities of Certain Third Parties

Conservative:

Some Third Parties do indeed exchange among themselves material which [redacted]

[redacted] But a Third Party Sigint success against one target is by no means indicative of a general capability against similar targets or of a knowledge of the most effective techniques for achieving that and similar successes. In many circumstances [redacted] Sigint success has been less the result of advanced cryptologic skill than of the breadth of the [redacted] Sigint effort, a breadth of effort not, for both geographical and financial reasons, achievable by any Third Party nation.

Liberal:

The [redacted] advantage in geographical breadth of effort is steadily decreasing as cooperation, especially interregional cooperation, between Third Party nations increases. And certainly there would be only minor financial constraints on [redacted] should they decide to embark on a much expanded Sigint effort.

Conservative:

This becomes again a question of the degree and of the rate of development. Internation cooperative arrangements, in the absence of example and assistance from [redacted] will be less effective than [redacted] centrally directed effort. As to the breadth of [redacted] effort, though some increase is inevitable, it is likely to be much slower without than with the transfer of cryptologic technology from [redacted]

Liberal:

Where a Third Party, such as [redacted] are friends and allies, we should look with favor on an increase in their cryptologic capabilities. As the relative power of the United States in the world decreases, our interest in developing the competence of our allies must increase.

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

~~TOP SECRET~~

Conservative:

A friend and ally today may or may not always be a friend and ally. Cryptology is an area of technology development in which the United States still holds a substantial lead [redacted] In the light of other noncryptologic areas in which we have provided the means of achieving a technological preeminence - areas in which we are now struggling to catch up - it seems ill-advised to trade away our technological lead for marginally important [redacted] assistance.

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

Liberal:

As previously mentioned, it is often desirable to enter into a Third Party agreement in [redacted]
This has particular relevance to nations [redacted] which have or can be expected to develop a substantial cryptologic competence.

Using Sigint Assistance as "Quid" in Broader Negotiations with a Third Party

Conservative:

[redacted] Third Parties with a modest amount of cryptologic assistance may, indeed, on occasion, smooth general diplomatic or intelligence relationships with them and may on occasion be justifiable on that basis, but it is doubtful that the general use of Sigint assistance in this fashion is a wise policy, since it usually results in a series of escalating demands for more of the same.

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

Liberal:

For better or for worse, Third Party nations are aware of the availability of [redacted] cryptologic assistance of the type being provided to themselves or to other nations. Not to consider this as a legitimate [redacted] help overall U.S. political and intelligence relations can only be termed cryptologic parochialism.

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

Conservative:

Sigint exchanges for non-Sigint ends have repeatedly opened the door to a kind of [redacted] with constantly escalating demands for more cryptologic assistance. Not infrequently the negotiating philosophy of the U.S. exchange infrastructure staff itself has been that it is necessary for the health of an exchange to [redacted] i.e., by fostering a continual year-by-year development of the Third Party's cryptologic capability. As a result, an initial agreement [redacted] becomes over a period of, say, five years, a significant transfer of cryptologic technology. As for "cryptologic parochialism," criticism of this nature ("arrogance" has been a term sometimes used) has, over the years, been periodically surfaced by certain members of the Intelligence Community in reaction to NSA's refusal to permit undue risks to Sigint material: restrictions on the inclusion of Sigint technical data in end product; restrictions on the routine use of sensitive Sigint in tactical situations; restrictions on the use of Sigint as trading "wampum" in diplomatic exchanges. It can be argued that if parochialism is involved in this controversy, it might better characterize the position of organizations which, in pursuit of the short-term goals in which those organizations are currently interested, would risk the effectiveness of a weapon (Sigint) of critical long-term importance to the nation's strategic posture.

~~TOP SECRET~~

CRYPTOLOGIC QUARTERLY

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

Liberal:

It is unrealistic to plan on retreating into some cryptologic Fortress America or [redacted] The era of U.S. military/economic world dominance is over. We must learn to deal with friendly nations on a more equal basis in cryptologic as well as other areas.

Conservative:

As U.S. relative power declines, intelligence becomes more and more important as a means of directing our remaining influence and of employing our resources on those matters and on those future occasions which can be expected to have the greatest significance for major U.S. interests. We must not blunt the future effectiveness of the Sigint weapon by encouraging the development of defenses against it.

Overall Policy

Liberal:

The conservative arguments against making any basic revisions in the constraints which have, too often, burdened Third Party exchanges are characterized by a general unwillingness to recognize that, in any domain, change is inevitable and that it is neither practical nor politically feasible to forego the advantages of closer, less constrained, relationships with Third Parties. The range and difficulty of Sigint targets continues to grow, with no realistic possibility of a comparable growth in [redacted] resources. To prevent unacceptable gaps in Sigint support to U.S. military and political officials, we must make the most effective possible use of all available resources, including Third Parties. For better or for worse, either because of the greater attention now accorded to cryptologic matters throughout the world or because of a natural desire on the part of Third Parties [redacted] we are obliged to come out of the closet and deal much more openly with them about cryptologic matters.

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

Conservative:

U.S. economic and technical preeminence since WWII has made it possible, by the sheer size of increased Sigint funding, to stay ahead of many cryptographic advances by target nations. With the fading of that preeminence, other avenues to Sigint success are needed. One approach, certainly valid, even vital in some instances, is to place greater reliance on Third Parties [redacted] This approach, however, is by no means always cost effective, and more important, if employed extensively, may result in [redacted] Another approach, less likely to be counterproductive, is to focus available Sigint resources, with maximum effectiveness and efficiency, on targets of major importance, while relying to a greater degree on non-Sigint sources of intelligence regarding selected targets of less than major importance.

Whether or not the U.S. has entered a phase of absolute decline there is little question that the U.S. will cease to act as military policemen for the entire world. Certainly U.S. dominance in the Far East is no longer a rational possibility. For the purposes of Sigint planning, it needs to be recognized that Japan, China, and even India are as likely to be competitors as allies in the twenty-first century, perhaps earlier; that powerful forces within the Soviet Union are attempting to move the USSR away from military confrontation with the U.S.; that the economic/political division of Europe engendered by

~~TOP SECRET~~

post-WWII East-West rivalries is coming to an end; that global problems of overpopulation, with consequent atmospheric and terrestrial pollution and international competition for increasingly scarce resources, are likely to be the dominant international concerns after the year 2000.

Liberal:

It is not the place of NSA or of the cryptologic community to direct national policy or to make national intelligence estimates. NSA's job is to respond to intelligence information requirements according to established priorities, using whatever resources are available. It is neither politically practical nor operationally prudent for NSA to organize its efforts to address tasks and circumstances other than those specified by U.S. Sigint users.

Conservative:

NSA is responsible for pursuing policies and measures to maximize the long-term value of Sigint as an asset critical to the support of U.S. military and political action. Sigint may soon loom even larger as a support to actions in the economic sphere. Beyond that, as a member of the U.S. Intelligence Community NSA has a responsibility to make its voice heard in matters

The above arguments have no real end and the controversy no clear-cut resolution. Each participant/reader is likely to find the foregoing merely a confirmation of his or her already firmly held views.

COMMENTS

It will be apparent that the differences are as much philosophical as judgmental: whether or not today's explicit intelligence requirements must override consideration of hypothetical long-term intelligence needs; whether or not the spread of cryptologic technology and awareness is today so rapid and so pervasive as to make obsolete the customary standards for evaluating risks of cryptologic technology transfer; whether the gap between cryptologic technology development and the actual use of cryptologic technology is so great as to require that technology awareness, rather than technology development, be the benchmark against which to measure the risk of technology transfer; whether actual day-to-day management costs of a Third Party exchange, including planning, negotiation, management, and analyst overhead, often equals or exceeds the cost of doing the same task with [redacted] resources and, if not, whether the resources required over the long term [redacted]

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

[redacted] whether a less intensive Sigint effort on various targets of lower intrinsic priority would serve significant U.S. needs as well as the present effort, i.e., "How heavily should secondary intelligence requirements weigh in overall Sigint management policy decisions?" and "Are non-Sigint sources adequate to deal with such secondary requirements?"

These questions reflect problems with which the entire intelligence community is concerned, but they should certainly be addressed initially by NSA, on whose special skills and experience in Sigint matters the Intelligence Community must rely. The ultimate decision on questions relating to intelligence priorities and the tasking of intelligence sources lie clearly in the realm of DCI/DIA/JCS/NFIB, but NSA's vote even on these questions should count heavily.

~~TOP SECRET~~

CRYPTOLOGIC QUARTERLY

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

Some actions which might help to further sort out the issues raised:

- a more thorough examination of the question of the cost effectiveness of each individual Third Party exchange. A rigorous cost accounting review by "outsiders" might suggest some useful modifications in one or more of the existing exchanges.
- a (re)consideration of the cost-benefit of Third Party exchanges involving targets of lower priority.
- a review of U.S. Sigint posture vis-à-vis Third Parties for the future, assuming major realignments of international power relationships over the next 20 years.

holds a BA in International Relations from Yale University, an MBA from Harvard Business School, and a Doctorate in Jurisprudence from American University. He is certified as a Special Research Analyst and Traffic Analyst.

~~TOP SECRET~~