WN or R No: R-2093-ACDA

Copy No: 2

Assigned to:

Project No: 6356

Contract No:

Task Order No:

Bill - note your debt to Bill Griego's memo to Amrm 7/18 WN 74 Abe

16-17

Temporary cover sheet for RAND external publications*

number R-2093-ACDA (DRAFT)

title BREAKOUT - Part I (DRAFT)

author(s) William R. Harris

date October 1976

*Please use this form as the temporary cover for WN's and R's released to the Publications Department for publication. Final cover and title page will be prepared in the Publications Department from the information appearing on this sheet.

HANDLE VIA
BYEMAN-TALENT-KEYHOLE-COMINT
CONTROL SYSTEM JOINTLY

~~TOP SECRET~~

HEXAGON GAMBIT [redacted] KENNEN GAMMA [redacted] EARPOP

Rand
SANTA MONICA, CA 90406

DRAFT

BREAKOUT -- PART I

William R. Harris

R-2093-ACDA

PROSPECTS FOR VERIFICATION AND WARNING

BREAKOUT -- PART I

PROSPECTS FOR VERIFICATION AND WARNING

PREFACE

This preliminary draft report was prepared for the Arms Control and Disarmament Agency by staff members of the Rand Corporation, under the terms of Contract AC6AC406. It is a "for comment" draft. Neither copies of this report nor comments on it should be forwarded directly to the Rand Corporation; they should instead be sent through the National Reconnaissance Office, Directorate of Special Projects (SAFSP-SP-3) to the attention of the author. The considerable assistance of SAFSP and the Office of the Secretary of the Air Force, Space Systems (SAFSS) requires acknowledgement, both in terms of research advice and assistance, and in providing facility support. Nonetheless, the views, opinions, findings, and conclusions stated or implied herein are in no sense to be attributed to the NRO or any of its elements, or to ACDA. Owing to the nature of the material used in this report, it has not been subjected to the customary editorial and peer review processes of Rand.

~~TOP SECRET~~

USSR COUNTERMEASURES TO SALT VERIFICATION AND WARNING: IMPLICATIONS FOR FUTURE US INTELLIGENCE PRACTICES.

Review of SALT Verification, SALT Warning, and BREAKOUT Warning Functions

Before addressing the scope of protection for "national technical means of verification" under international agreements, clarification of the respective functions of SALT Verification, SALT Warning, and BREAKOUT Warning, is essential.

Although the word verification connotes action to demonstrate, establish or test the truth or correctness of fact or theory,* in the established parlance of the Strategic Arms Limitation Talks (SALT):

> ...verification refers to the process of assessing compliance with the provisions contained in arms control treaties and agreements. It is the attempt to ascertain whether states are living up to their international obligations.**

This report treats SALT Verification in its technical sense, as the process of ascertaining compliance with the provisions of arms control treaties and agreements affecting strategic armaments.

In contrast, SALT Warning constitutes the evaluation of strategic stability and identification of hazards to national security under existing or proposed SALT treaties or agreements. The SALT Warning function includes assessment of security threats associated with SALT agreements under full compliance, as with misperceptions of strategic dynamics under an agreement, or unanticipated impacts of permitted technological developments, or investments--e.g., civil defense--not otherwise precluded.

The SALT Warning function also includes assessment of security threats associated with partial noncompliance with SALT agreements, as though interference with protected national means of verification, quantitative, or qualitative violations. Under these circumstances, the SALT Warning function intersects the SALT Verification function: the former evaluates

* Oxford English Dictionary, 1971 edition.

** U.S. Arms Control and Disarmament Agency, Verification: The Critical Element of Arms Control, ACDA Publ. 85, Wash. D.C., March

security hazards exacerbated by SALT viloations, which are targets of the latter.

As countermeasures to SALT Warning become more effective--as is hereafter indicated--arms control negotiators are tempted to establish treaty constraints which are verifiable, even though less important than other parameters in assuring strategic stability:

> Agreements restricting the quality or technical characteristics of weapons rather than their quantity are as a rule more difficult to verify. A numerical limit on anti-ballistic missile (ABM) complexes, for example, is easier to verify than a prohibition on improving air defense systems in order to give them an ABM capability. Similarly, a limitation on the number of strategic launchers is easier to monitor than a limitation on the type of warhead permitted for those launchers. *

Accordingly, many of the critical parameters affecting strategic stability are within the domain of SALT Warning, but not the domain of SALT Verification. As a result, the parameters which under the SALT I agreement and ABM Treaty are juridicially protected from concealment or "national technical means" (NTM's) interference constitute a declining share of the parameters which affect strategic stability.

One function of SALT Warning is the identification of strategic instabilities or national security hazards under conditions of full or substantial compliance with SALT agreements and associated treaties. Another function of SALT Warning is the identification of strategic instabilities or national security hazards under conditions of lapsing, abrogation, or massive overt or covert violation of SALT agreements and associated treaties. Identification of strategic instabilities or national security hazards under these conditions is a principal function of BREAKOUT Warning.

BREAKOUT Warning is a major but not exclusive component of SALT Warning. SALT Warning may involve security hazards which will increase under a SALT agreement, even or particularly one involving full

* Ibid, p. 23.

APPLICABILITY OF SALT VERIFICATION, SALT WARNING, AND BREAKOUT WARNING UNDER TREAT AND OTHER INTERNATIONAL AGREEMENTS

Agreements:	Functions: I. SALT Verification	II. SALT Warning	III. BREAKOUT Warning
Geneva Protocol,1925 CBW		I	I
Limited Test Ban,1963	P	I	I
Outer Space Treaty, 1967	P	I	M
Treaty of Tlatelolco, 1967, Nuc. Weapons in Latin America		I	I
Non-Proliferation,1968		I	M
Seabed, 1971	P	I	I
Accidents Agreement, 1971		I	I
Biological Weapons, 1972		I	I
SALT I, 1972	M	M	M
ABM Treaty, 1972	M	M	I
Threshhold Test Ban, 1974.		I	I
Underground PNE's,76	P	I	I
Outer Space Registration, 1974/76.		I	I
SALT II(?), 1976-77	M	M	M
Second Party Agreements		I	I
Third Party Agreements		I	I

M = Mission
P = Collateral protection under treaty or international agreement, of "national technical means of verification."
I = Collateral indicator

Table 3-1

compliance on both sides. BREAKOUT Warning constitutes the evaluation of hazards to national security associated with BREAKOUT environments, first during the period in which SALT agreements are in force (with full or partial compliance), then in the period of lapsing, abrogation, or massive overt or covert violation.

Distinguishing the functions of SALT Verification, SALT Warning, and BREAKOUT Warning is important in evaluating passive and active countermeasures of the Soviet Union. The legal regime tends to protect from concealment or interference those indicators which are more readily discernable, and often less important (verification parameters) than parameters critical to the strategic balance, for example breakthroughs in ballistic missile defense technology, ASW efficacy, accuracy or maneuverability of warheads, or range of delivery systems excluded from agreed ceilings.

Scope of "Noninterference" with NTM's and the Long-Term Strategic Competition

Three international agreements establish a juridicial regime for verification by national technical means. The language of all three is virtually identical. In all cases the protection of national technical means is conditioned upon use in a manner consistent with generally recognized principles of international law.* Customary national sovereignty over airspace, incorporated in the Chicago Convention of 1944, in combination with disagreement over the legal boundary of air and outer space and an historical Soviet distinction of espionage from either peaceful observation

* Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Antiballistic Missile Systems, May 26, 1972, Art. XII(1); Interim Agreement between the United States of America and the Union of Soviet Socialist Republics on Certain Measures with Respect to the Limitation of Strategic Offensive Arms, May 26, 1972, Art. V(i); Treaty Between the United States of America and the Union of Soviet Socialist Republics on Underground Nuclear Explosions for Peaceful Purposes, May 28, 1976, Art. IV(1)(a).

or verification limit the effective juridical protection of NTM's under these agreements.*

To the extent that particular NTM's required for SALT verification (are designed for) U. S. strategic counterforce attacks, battlefield intelligence in regional hostilities, or other war management missions, juridical protection of these systems may be eroded. In this context, the loss through active countermeasures of the [redacted] EARPOP, [redacted] KENNEN, or [redacted] systems would be technically feasible without resort to nuclear weapons,** and would be likely to degrade significantly SALT verification capabilities. Yet these systems are designed for and have constituencies expecting battlefield or counterforce strike intelligence.

To the extent that particular NTM's are required for SALT verification, and perhaps for extra-territorial verification of third states and the high seas under the May 1976 PNE Treaty, these systems may not receive juridical protection against selective interference during the performance of other missions. Yet, engagement of forces in other contexts may provide intelligence important in assessing the viability of the strategic balance within the SALT Warning mission. Prospects for selective interference with space systems have recently been examined in support of NSDM 333. The topic is further examined in Section 3.8 of this report. At this juncture it is important only to note that NTM's dependent upon space vehicles or communications are generally vulnerable to active countermeasures, and at best only partially protected under principles of international law which remain in dispute.

There is the further problem that prohibitions of interference with NTM's and of deliberate concealment measures are by the ABM Treaty and SALT I Agreements limited in their protection to the verification...

---

* See Memorandum from Maj. W. L. Griego to Amrom Katz, 18 Nov. 1974, Subject: "Observation or Espionage," (TS, BYE-13450-74).

** See special studies in the C-10316 study series for technical evaluations.

of compliance with the provisions of this (Interim Agreement) (Treaty). There is virtually no legal duty to withhold selective interference with NTM's as they collect other intelligence essential to SALT or BREAKOUT Warning, and virtually no legal duty to restrain deliberate concealment measures. Indeed, the language of limitation under the ABM Treaty and Interim Agreement may be read to sanction strategic cover and deception measures--excepting only designated verification parameters--as a legitimate aspect of the long-term strategic competition. Particularly as NTM's collect information relevant for counterforce attack or battlefield use will those cover and deception methods not prohibited be deployed against NTM systems.

In short, juridical protection from interference or deliberate concealment is: limited to verification requirements; eroded by prior cover, camouflage and deception practices that were allowed to continue; vulnerable to Soviet reinterpretation of international law; and often irrelevant to key SALT Warning and BREAKOUT Warning parameters. Table 3-1 is illustrative of these circumstances.

The SALT verification missions are incorporated within the SALT I Interim Agreement of 1972, which will either lapse or be superseded by a SALT II Agreement; and within the ABM Treaty of 1972. The Limited Test Ban of 1963, supplemented by the as yet unratified Threshhold Test Ban of 1974, prohibits atmospheric nuclear tests of the USSR (but not the French or Chinese, nonparties to these treaties), which would be expected to damage various NTM's.* The Outer Space Treaty of 1967 prohibits emplacement in orbit around the Earth of "any objects carrying nuclear weapons or any other kinds of weapons of mass destruction...," but not necessarily space-based satellite-disabling or interference systems which are other than nuclear, and other than weapons of mass destruction.**

* See special studies in study series C-10201, and in special studies series C-10316.
** Outer Space Treaty, Article IV.

The as yet unratified Treaty on Underground Nuclear Explosions for Peaceful Purposes, generally noted for its on-site inspection provisions, is of more substantial jurdical importance through its extension of treaty protection for national technical means of verification over land masses other than those of the US and USSR (safeguards for nuclear tests in other states, Art. VII(2)), in outer space and underwater (Art. III(2)(d)), or in yields above 150 kilotons anywhere (Art. III(2)). Because existing and projected NTM systems which are relevant to nuclear explosives monitoring are also utilized in SALT verification, this May 1976 Treaty provides an extra dimension of juridical protection.

Nevertheless, parameters of SALT Warning or BREAKOUT Warning are indicated as entirely lacking in juridical protection. Unless these parameters are among the parameters regulated by the SALT and ABM agreements, they are not juridically protected from interference efforts, nor from deliberate concealment measures which were in effect--as for example the Soviet's OMEGA emissions and observation security system--by May 1972, nor from incremental concealment measures which do not impede verification of the SALT or ABM Treaty provisions.

Limited Juridical Protection Against Active Interference

Almost forgotten by most defense analysts is that the Soviets already have developed a legalistic case for negating NRP satellites when the situation arises. The Soviets could say that certain U.S. satellites conduct espionage. Although the Soviets may have tacitly agreed to overflight by "observation satellites" they have steadfastly distinguished, externally to the world, that satellite information gathering which could be used for aggressive military purposes, i.e., space espionage, is intelligence gathering and is illegal according to the international law.

The distinction between "espionage" and "observation" was enunciated in 1960, before Soviet imagining satellites were operational. Reserving the right to protect against activities in space threatening the security/sovereignty of the state, East European jurists have found "no cogent reasons for States to proceed with the delimitation of the frontiers between airspace and outer space..."*

---

* Manfred Lachs, The Law of Outer Space, Sijhoff, Leiden, 1972, pp. 57-58. See also: U.S. Senate Committee on Aeronautics and Space Sciences, Space Programs, 1971-1975....Attitudes toward International Cooperation and Space Law, Staff Report, Vol. II, 94th Cong., 2d Sess., August 30, 1976, Chap. 5, Domas Krivickas and Armins Rusis, "Soviet Attitudes Toward Outer Space Law," pp. 135-197.

Those who maintain that the Soviet acceptance of overflight by photo satellies not only is tacit but further, it can even be "proved" by referring to statements by Soviet chiefs-of-state, or by noting their signatures on U. N. treaties or the SAL Treaty or Interim Agreement, have not read the words carefully.

(a) The Soviets agreed to United Nations General Assembly Resolution 1962 (XVIII) Attch 1). The resolution says that, ".... exploration and use of space shall be carried on in accordance with international law including the Charter of the United Nations..." (Underlining added). Prior to signing, the Soviets tried very hard to include statements outlawing space espionage.

(b) The Soviet writer, G. Zhukov, in the Soviet Magazine, International Affairs, No. 10, October 1960, pages 9 and 10, used Article 36 of the Chicago Convention of 1944 to state, "... there is absolutely no ground for alleging that espionage at a high altitude, with the aid of artificial earth satellites, is quite lawful under the existing rules of international law..." (attch 2) (Underlining added).

(c) Premier Khruschev is said to have admitted to C. L. Sulzberger of the New York Times, 15 July 1963, that satellites can be used for disarmament inspection. (Attch 3) (Underlining added).

(d) Even as recently as September 1974, G. A. Trofimenko, in the Soviet USA Institute Journal, stated that SALT verification by national means is intended to mean, "Primarily by satellite, but also by other technical observation systems." (Attch 4) (Underling added)

(e) The SALT Treaty and Interim Agreement (attchs 5 and 6) say, "... each Party shall use national technical means of verification at its disposal in a manner consistent with generally recognized principles of international law." (Underlining added).

Recapping the above items, after we flew our first successful reconnaissance satellite in August 1960, the Russians tried to have satellite reconnaissance outlawed at the U. N. They appeared to have caved in on this policy when they agreed to U. N. Resolution 1962 (XVIII). They didn't. The wording

in the resolution talked about exploration and use of space in accordance with international law. Therefore, based on this, statements by the writer, Zhukov, that the Chicago Convention was the law and the law says that espionage is illegal is still an "operative statement" to use today's terminology. In that same article, page 6 (Attch 2), Premier Khruschev says as much. Needless to say, we have tangible proof of Soviet policy regarding espionage overflights by their downing of Gary Powers' U-2 aircraft.

All of the preceding citations and quotes except one, are quite old. Some would argue that both countries' reconnaissance photo satellites have been operating in an unimpeded manner, and have been allowed to perform in an unimpeded manner, for about 14 years. Thus, it is argued a "custom" has been established and this custom rule, over a period of time, is international law (Attch 7). As the following words in Attachment 7 states regarding the custom, "... that the 'rule' involved...is in accordance with a constant and uniform usage practiced by the States in question..." I contend that the Soviets have never agreed to the custom/rule of espionage from space based systems upon the preceding arguments.

The Soviets have carefully articulated a case, over the years, that could have grave consequences for allowing for negation of U.S. reconnaissance satellites, if politically, the timing of such negation is appropriate to their major objectives. Such a circumstance could be motivated for a variety of international considerations or by even the inadvertent or deliberate disclosure of our capabilities.

Our best satellite photography, which has a resolution of about half a foot, is better than the intelligence estimate of the Soviet's best--three feet. Let us say that the Soviets find out that our systems have a resolution of less than half a foot. Do they now consider it to be espionage as opposed to observation? (At what resolution does observation end and espionage

egin?* Or is intent also involved?) The Soviet answer could be espionage, since the military advisors to the Soviet NCA's could argue that this exceptional unilateral capability by the U.S. is unacceptable, and action should be taken. Since the ground work has previously been established for alleging space espionage, then negation could have support from world opinion.

Or, in another example, the Soviets and other nations find out about our capability at the same time. These other nations would publicly look to the Soviets for a response. What was acceptable "privately" to the Soviets (tacit approval) may not be so when confronted by worldwide discussion, and especially that from their communist satellite allies. Having to react, the Soviet answer here could be a forced one and it would be the declaration that the U.S. was conducting space espionage and should desist. And as indicated above, they have a variety of ASAT methods available to implement their declarations if needed.

Multi-Purpose Reconnaissance And Protection of NTM's

One of the trends in the NRP now is the move toward tactical support of military commanders by providing near-real-time imagery or SIGINT. KENNEN typifies the imagery. The provision of space derived SIGINT information within two hours regarding Syrian SA-6 locations during the October 1963 Middle East war between Israel and the Arab states typifies the SIGINT example.

One view has been put forth that NRP satellites have a "cloak of sanctuary" associated with them because they are part of SALT's national technical means of verification (NTMV). Tactical use of the system is supposed to antagonize the Soviets and thus places the systems at risk since they are being used in a non-NTMV. That argument is incomplete. The systems

*An analogous issue was addressed by a USIB study. In that instance the question was: How much do the Soviets know about our overhead space reconnaissance capability?

would be at risk if the Soviets perceive that the satellite contribution to these type conflicts are serious enough to warrant considering negation of the satellites (or ground stations). The NTMV aspect will only be a major secondary consideration. In the verification context the means of negation excludes use of the nuclear ASAT but includes possible use of the co-orbital non-nuclear ASAT, high and low powered lasers, ECM jamming, attempted command takeover, or ground station or facility attack. These activities are characterized as the Active Interference or Physical Damage/Destruction levels. (See paragraph 3.)

Breakout could also occur while this type of ASAT activity is conducted during conventional conflict with the hope of achieving strategic advantage when the U.S. space NTMV have been negated due to the conventional conflict and their replacements or backup systems have not been able to fill the information gap in the interim.

c. Peacetime/Crisis. It is not necessary for the Soviets to consider breakout only as a prelude to conflict or to take advantage of one. Because of their overall worldwide objectives, they may, under the cover of a benign world environment attempt a breakout during a peacetime environment to get strategic advantage. This mode could involve a gradual buildup of negating actions that go beyond the U.S. interpretation of SALT violations. If no protests are made by the U.S. at the SCC then the boundary for violation could be transgressed even for their creeping violationism.

These methods would involve passive measures such as CCD, EMCON, and encryption. Even occassional covert active harassment or degradation or even destruction (at the upper limit of these scenarios) could occur if the Soviets felt they could do so without U.S. knowledge. These means could include low-level laser illuminations, deceptive jamming, occassional command takeover, or insertion of deceptive information into SIGINT or imagery systems.

VULNERABILITIES TO PASSIVE AND ACTIVE COUNTERMEASURES

Asymmetrical Security and Counterintelligence: Implications

Asymmetrical capabilities in foreign intelligence, counterintelligence and security constitute targets of opportunity for strategic deception planners The USSR operates with significant security and counterintelligence advantages over the United States.

Perhaps the most significant security advantage to the Soviet Union involves access, through extensive press and SIGINT coverage of the United States, to systematic feedback on which of Soviet security efforts are successful and which are not. Because only a small portion of the parameters of importance in the strategic competition are subjects of concealment constraints under SALT, there remain recurring opportunities for Soviet security services to engage in field tests of the "Hiders and Finders" game which Amrom H. Katz proposed back in 1961."**

Further, with approximately one-tenth of one percent of the U.S. labor force cleared for SI/TK access, there is the substantial probability that human agent penetrations provide Soviet security services additional feedback on the approximate parameters of U.S. knowledge and ignorance of Soviet strategic activities. Thus, even if the Soviets do not gain access to data systems on the specific means of collection, access to the trial-and-error results of the Soviet security services may be critical in the design of special security systems for those special projects or activities which are designed to be withheld from our view.

---

* There is presently no single official history of the strategic deception practices of the United States, classified or unclassified, for the period 1941-1976. Unofficial reviews include: Barton S. Whaley, Stratagem: Deception and Surprise in War, Center of International Studies, M.I.T. Cambridge, Mass., 1969; William R. Harris, Counter-Deception Planning, R-1230-ARPA, 1973, classified and withdrawn from publication; and an incomplete manuscript by H. Wentworth Eldredge, prepared under ARPA sponsorship.

** Hiders and Finders: An Approach to Evasion and Inspection Technology, P-2432, The Rand Corporation, April 26, 1961, in Bulletin of the Atomic Scientists (December 1961).

The SALT Talks themselves provide, in some respects inevitably if there are to be such discussions, opportunities to test the efficacy of special security measures.*

Of greater concern that the imbalance of security efficacy resulting from feedback is an apparent but much less certain imbalance of foreign counterintelligence resources.**

Foreign counterintelligence activities are conducted to destroy, degrade, neutralize, or misdirect the operations of hostile foreign intelligence services.*** These activities include the collection and utilization of information concerning the protection of foreign intelligence systems, sources or methods, or other national security information.**** Beyond the denial of intelligence, asymmetrical counterintelligence capabilities may permit the advantaged side to undermine SALT Warning or BREAKOUT Warning capabilities through:

---

* "...A vexed American official unburdened himself in these words: 'We have tabled three proposals in minute detail. They complain bitterly about the degree of detail, yet they've learned a great deal about our programs. They've told us nothing. All we've gotten in return is general statements. ...We make presentations. They complain... That obliges us to get into even more detail. Let's face it. They are learning a lot, but nothing else is happening.' John Newhouse, Cold Dawn, The Story of SALT, Holt, Rinehart, and Winston, New York, 1973, p. 193.

** These observations are derived from prior review of extensive depositions of recently-retired CI chiefs and senior staff officers of CIA and the FBI, and from informal interviews of present officials, conducted by W. R. Harris.

*** See U.S. Senate Select Committee to Study Governmental Operations with Resepct to Intelligence Activities, Final Report: Foreign and Military Intelligence, Book I, 94th Congress, 2d Session, 1976, p. 620.

**** Executive Order 11905, Section 5.

- timely identification of the preconceptions and expectations of adversary decision-makers and intelligence analysts, of value in designing deception operations which reinforce rather than overcome perceptions.*

- selective degradation of critical warning capabilities, without alarming adversarial decision-makers through noticeable interference with national technical means of verification.

- near-real-time monitoring of the status of adversarial warning and countermeasure indicators, so as to reduce risks of premature detection and to preserve cancellation options.

Among the assumptions which generally result in the neglect of relative counterintelligence capabilities in assessments of arms control verification, two are widespread.

First, there is the assumption that national technical means, even when identified with some specificity, are less vulnerable to spoofing than the human source of COMINT channels which are more consciously scrutinized for deception.

Second, there is the assumption that national technical means are relatively dissociated from the hazards of inference, when in fact most interpretations of data derived from national technical means proceed on the basis of previously-embedded notions, derived from human sources

* "After studying the pernicious effect of deception upon predictive performance, one may conclude that the greatest test of intelligence systems is distorted light, not darkness." W. R. Harris, Counter-Deception Planning, R-1230-ARPA, Feb. 1973 ed., p. 37. In 50 cases of 20th century wartime deception studied by Barton Whaley, deception planners chose to reinforce rather than overcome preconceptions in about 33 cases. Intensity of surprise, measured by casualty ratios, was greater for the set of cases involving reinforcement of preconceptions. See Whaley, "Bodyguard of Lies," unpublished MS, 1973.

and particularly COMINT data which generally reach analysts, and sometimes reach photo-interpreters and ELINT staffs before preliminary inferences from NTM systems.*

The principal technical foreign counterintelligence asymmetry which has been identified in the last several years involves an apparently pervasive communications security (COMSEC) vulnerability affecting microwave communications of common carriers serving the industrial base for both the BYEMAN and ZO-- contractor systems.** In short, virtually every one of the systems which comprise the national technical means of verification is managed by a prime contractor and subcontractors providing component parts and services, all with recourse to the common carrier telephone system of the United States.

An example of the degree of prior Soviet counterintelligence awareness of BYEMAN systems was obtained through a special monitoring effort of the first launch of the HEXAGON system. According to the Chief of S Group of the National Security Agency, the basic mission, and imaging swath width was entered into the OMEGA warning system without delay,

---

* See, for example, the remarks of Ted Greenwood, in "Reconnaissance and Arms Control," Scientific American, Vol. 228 (Feb. 1973), at page 24: "Although the utility of these (non-reconnaissance) information sources cannot be denied, they do have the disadvantage of relying on inference. Reconnaissance and surveillance, on the other hand, are dependent primarily on the physical properties of electromagnetic sensors and therefore provide less ambiguous information and broader coverage than other techniques."

One advantage of the KENNEN system, assuming the availability of sufficient PI personnel to avert data processing bottlenecks, may be a timeliness which may reduce "contamination" of analysts' preconceptions by data derived from human source and COMINT channels that are particularly vulnerable to spoofing.

** These remarks are derived from review of COMSEC studies undertaken in 1974-76 by S Group of the National Security Agency, by S Group contractors in the SCORER I Project, by project-by-project review of BYEMAN system COMSEC vulnerabilities in conjunction with an S Group representative, and by informal interviews in 1976. Press leaks respecting A and other ZO systems may trigger CI reviews: "...disclosure that the United States has used submarines in Soviet territorial waters to monitor Russian weapon tests have greatly diminished the flow of this vital intelligence," according to former Defense Secretary [redacted]

and NSA-monitored chatter indicated an apparent Soviet confirmation of prior knowledge.

Of critical importance in projecting U.S. SALT Warning and BREAK-OUT Warning capabilities is the substantial lead-time required to provide even minimal end-to-end protection for communications affecting BYEMAN and ZO systems.

Similarly, past decisions to design collection systems which did not encrypt telemetry, uplink channels, or command systems left these links vulnerable to more precise understanding, as a prerequisite to either passive or active countermeasures. With planning lead-times, and high costs of retrofitting or even new configurations for planned Block changes, these vulnerabilities are not quickly or cheaply overcome.

A critical and persisting uncertainty respecting the control of a major part of KGB-directed U.S. human counterintelligence assets compounds uncertainties as to the reliability of communications intelligence systems targeted against the Soviet Union.

As to those communications intelligence systems within the BYEMAN security apparatus, there is now solid evidence supporting the conclusion that the mission and configuration of the [redacted] system should be thoroughly understood by KGB and GRU counterintelligence. As to the [redacted] system, it appears that since at least 1975 a 105-foot radar dish and possibly also COSMOS 775 have been focussed on these activities. Even if data streams do not diminish, these systems are increasingly vulnerable to deception.

The other principal source of communications intelligence involves in-country collection by the Central Intelligence Agency. To the extent that collection efforts depend on agents-in-place for technical assistance, these activities are subject to counterintelligence attack by KGB and GRU organs. Because recruitment and operational leads are in part derived from Soviet intelligence defectors, and because the reliability of a subset of these

defectors has for many years been questionable,* it is possible that cascading effects of KGB counterespionage activities may render even a portion of in-country intelligence collection vulnerable to deception targeting.

If, on the other hand, the mutually-supporting data of this subset of defectors from the 1960's and 1970's is bona fide, then neither the principal agent sources within the Soviet intelligence services nor the portion of in-country COMINT facilitated by these assets would be as vulnerable to deception efforts as might otherwise be supposed. Further, if these defectors of the 1960's and 1970's are to be believed, the principal deception organization of the Soviet Union, Service A of the First Chief Directorate, KGB, is an organization of modest size and capabilities.**

The principal conclusion to be drawn is one of the wide range of uncertainty respecting the impact of Soviet counterintelligence capabilities on U.S. SALT Warning and BREAKOUT Warning capabilities.

If we can rely on a set of generally-consistent defector interrogations, we should not exaggerate the capacity of Soviet counterintelligence to deceive our sophisticated and expensive systems of collection. If, on the other hand, these defectors are themselves part of the problem, the cascading effects may be substantial, or may have effects on both the messages which our NTM's convey and the embedded preconceptions/expectations that elucidate the interpretation of NTM data.

---

* The principal critic of their reliability has been James Angelton, former Chief of the CI Staff, CIA.

** Informal interview with the Chief of Research Analysis, CI Staff, CIA, September 20, 1976.

Because human sources can provide unique data, the temptation to believe in their reliability may overwhelm rationality.* In closed societies the home security service generally has many advantages over foreign agencies. Even in a relatively open society, England in World War II, as summarized by one of the British deception controllers:

> "Not only have double agents been run on a long-time basis but they have been run so extensively that we can think not in terms of a number of isolated cases but in terms of a double-agent system... we actively ran and controlled the German espionage system in this country."**

In appraising the impact of possible counterintelligence asymmetries, Allied insecurities affecting NTM's should be considered along with the direct U.S. insecurities of NTM's and possible indirect repercussions of human agent network unreliability.

[redacted]

from that organization. Intelligence reaching other NATO allies is vulnerable not only to traditional agent-penetrations but also to the insecurity to Allied communications.*** Once again, remedial efforts take time, and leave Soviet counterintelligence planners with a period of opportunity which may extend into at least the early 1980's.

The following Sections 3.4 and 3.5 shift from this review of counterintelligence vulnerabilities to inferences regarding past and projected Soviet passive countermeasures. These inferences are based upon samples of (unclassified) Soviet literature and practice which, some argue, may constitute a sample of the unsuccessful concealments, intentional non-concealments, and inferior dissimulation and simulation efforts: namely, those which have not accomplished their objectives.

---

* "... The fact that we have so many facts and details under review makes it obvious to us (deception controllers) that a certain message if sent ought to 'blow' an agent. But in truth it probably or almost certainly will not... In short, it was extremely, almost fantastically difficult to 'blow' a well-established agent..." Sir John C. Masterman, The Double-Cross System in the War of 1939 to 1945, Yale Univ. Press, New Haven 1972, pp. 57-58.

** Ibid, p. 27.

*** See the report of Dr. Robert Hermann to the Director, NSA, 1975.

> "...It is perhaps tautological to suggest that we have never found anything that the Soviets have successfully concealed. This is a self-contained proposition. But because we have indeed found many things that the Soviets have built and deployed, it is possible that a certain kind of self-contratulatory smugness has crept into our intelligence system.*

It is neither possible to identify that which is detected but not understood, nor possible to detect that which has been successfully concealed. On these premises, the following review of Soviet passive countermeasures constitutes an imprecise sample of a lower threshold of projected Soviet capabilities.

What is known about Soviet capabilities, in contrast to Soviet practices, is limited. Even as to Soviet practices which degrade strategic warning we know little.

Part of the lack of knowledge may be ascribed to lack of priority for systematic inquiry. It is only in 1975, then again in 1976 that an inter-agency assessment of Soviet camouflage, cover and deception proactices and capabilities has been attempted. These efforts do not draw on long traditions of sensitivity to possible deception indicators ("counter deception intelligence"), nor upon staffs with substantial knowledge of deception tradecraft -- except in these inter-agency efforts.

The first sustained effort to collect data on Soviet deception practices (not addressing efforts of the 1950's)

* Amrom H. Katz, quoted in W. R. Harris, Counter-Deception Planning, R-1230-ARPA, February 1973 edition, p. 67.

arose within the A Group of the National Security Agency in 1970-71. Among stimulii were intercepts of implementation of a national emissions control (EMCON) program, now believed to be part of the OMEGA countermeasure system.

In 1973 the Director of the National Photo-Interpretation Center (NPIC) directed one staff PI to investigate Soviet observat security and deception techniques. By late 1976 these two experts have been transferred to other functions.

A dispute among senior counter-intelligence officials over appraisals of defector reliability and the likelihood of Soviet control over substantial assets of US intelligence remains unresolved after more than a decade of concern. Internal compartmentation has limited the capacity to grasp and assess the meaning of patterns of double agent network deception.

In short, where we have looked we have found greater evidence of extensive Soviet deception practices than where we have not loc And we have looked sporadically, and with a limited number of participating analysts. Analysts with greatest expertise have bee rotated to other tasks.

In addition to the lack of knowledge occasioned by lack of systematic inquiry, we suffer from the previously mentioned parad of not knowing what we have not detected, and not identifying what we do not understand. In sum, only a lower bound of Soviet

Duplicate

[redacted]

In 1973 the Director of the National Photo-Interpretation Center (NPIC) directed one staff PI to investigate Soviet observat security and deception techniques. By late 1976 these two experts have been transferred to other functions.

A dispute among senior counter-intelligence officials over appraisals of defector reliability and the likelihood of Soviet control over substantial assets of US intelligence remains unresolved after more than a decade of concern. Internal compartmentation has limited the capacity to grasp and assess the meaning of patterns of double agent network deception.

In short, where we have looked we have found greater evidence of extensive Soviet deception practices than where we have not loc And we have looked sporadically, and with a limited number of participating analysts. Analysts with greatest expertise have bee rotated to other tasks.

In addition to the lack of knowledge occasioned by lack of systematic inquiry, we suffer from the previously mentioned parad of not knowing what we have not detected, and not identifying what we do not understand. In sum, only a lower bound of Soviet passive countermeasure capabilities may be inferred from available data.*

* A forthcoming Inter-Agency intelligence report on Soviet Cover and Deception will be utilized in the final version of this section.

Highlights of the evolution of Soviet passive countermeasure capabilities are likely to include the following:

- Development of theater deception operations in 1941-1942.
- Integration of strategic deception operations in Stavka planning in 1943, and combined arms, and inter-Allied strategic deception activities in 1943-1945.
- Spoofing of U.S. strategic warning ("Indications & Warning") in 1948 (March "War Scare"), in 1950 (European scare, delaying deployments to Korea), in 1956 (invasion ofHungary)(Bomber runs over Turkey during Suez), and in 1968 (Czech invasion), among others.
- Integration of Maskirovka operations within a Department (later a Service) of the KGB in 1959.
- Active counter-measures against aerial imaging, failing in 1956-1960 (U-2 shootdown), including camouflage, and signals deception.
- Activation of a nationwide emissions control (EMCON) and observation security (OBSEC) system in 1969-1971. This OMEGA system was in place in time to qualify then-current practices as licit concealments under the SALT I Agreement of May 1972.
- Utilization of "systems concepts" in passive countermeasures for the OMEGA system by 1974. For example, transport of strategic missiles, and indicators of submarine construction are shielded at different locations, in similar time frames.

(Add further evidence from 1976 CCD report, and summary ~~of~~ ambiguous evidence on active interference. Add key findings from NSDM 333 and C-10316 study efforts).

Implications for SALT Verification, SALT Warning, and BREAKOUT Warning

The preceding review of Soviet passive countermeasure capabilities and practices suggests that SALT Warning capabilities of the United States are likely to deteriorate in the late 1970's. That is, the capacity of the United States to identify on a timely basis threats to strategic stability is likely to decline, even without assuming resort by the USSR to active countermeasures against NTM's. As hereafter indicated, modest modes of active interference, or selective interference are realistic threats in the next several years.

It is essential, then, to accelerate prudent investments in a more reliable SALT Warning system, through anticipation of Soviet passive countermeasures, and active countermeasures, in the design of national reconnaissance programs.

Among our vulnerabilities, which for the Soviets constitute resources for passive countermeasures, several are not quickly remediable. The COMSEC vulnerability is pervasive, within the United States and within Allied governments. It is important to recognize that with manufacturing delays and massive capital requirements for common carrier systems, ~~and~~ B and Z industrial base requires priority attention. So does NORAD, and other government organizations which are ill-equipped for voice or digital communications in a secure mode.

The foreign counterintelligence vulnerability is pervasive. A quality control screening is underway within CIA. Both CIA , which in the past had a CI shop aloof from the rest of that organization,* and the FBI are in process of reviewing CI methods and objectives. These efforts will take time, but may result in the contribution of U. S. foreign counterintelligence staffs to the timely identification of deception channels and deception patterns which could constitute early warnings of BREAKOUT.

* See U.S. Senate Select Committee, Final Report: Supplementary Detailed Staff Reports, Book IV, 1976, p. 47.

As this report is being written, the Director of Central Intelligence is responding to the recommendation by the President's Foreign Intelligence Advisory Board that U.S. counterintelligence resources be centrally coordinated. The traditional restriction of foreign counterintelligence jurisdiction to agent networks and defense of personnel and installations has deprived the United States of the assistance of those CI-trained planners who are accustomed to evaluate projects as inter-active with our adversaries' strategic choices. Design criteria for national reconnaissance programs must include coherent evaluation of alternative countermeasures of our adversaries.

With the escalation of NTM system costs, it is only realistic to review budgetary costs (about seven percent of the national intelligence budget) of analysis and intelligence production. A modest investment in quality control efforts, the testing and retesting of intelligence channels believed to be identified by the Soviet Union, and the analysis of patterns of possible cover and deception, is small by comparison with overall costs.

Past Soviet concealment practices under ambiguously-drafted SALT I and ABM Treaty obligations have soured many on the value of including within Treaty constraints and non-concealment structures those parameters which are difficult to verify. However, as one projects the costs of passive countermeasures in relation to the costs of collection by NTM's, the importance of agreed constraints upon concealment is apparent. Thus, at the same time that we should be humble about our capacity to verify, we should seek inclusion within Treaty constraints for those parameters about which we fear cover and deception, and about which we have a fair chance of identifying cover and deception measures should they occur.

If Soviet objectives include the utilization of information and secrecy as resources in the long-term competition with the United States--as the Soviets have done in the past--then there will in any event be many opportunities, even without specific violation of SALT "non-concealment"

provisions of a future SALT agreement, the tasks of SALT Warning will expand. These tasks will be further exacerbated by excluding from "non-concealment" obligations activities or limitations which, in any event, are difficult to detect and assess.

Even as to passive countermeasures, it would be imprudent to rely on international agreements by themselves. The integration of strategic cover and deception planning throughout the entire national and special reconnaissance programs of the United States is long overdue. In the past, some modest elements of "cover" have been designed for Program A, and to a greater extent for Programs B and C. However, there are occasions when a project in one program would serve as the best cover, or cover mission for another project in another program. Further, some space-based activities may provide "cover" for ocean-based activities, and vice versa. Coordinated U.S. counterintelligence management can contribute to an appropriate mixing of perceived NTM "roles and missions" in the eyes of Soviet planners. Three objectives are in mind:

- the misallocation of adversary passive countermeasures.
- quality control sampling for each mission, early in each mission, and in relation to prior missions.
- sampling of Soviet cover and deception activities, among the warning signs of BREAKOUT.

Lastly, in considering alternative investments to cope with active countermeasures, it is important to assure at least as competent an effort to degrade the hazards of passive countermeasures. For short of war, in which satellite attrition is an important strategic objective, there should be little incentive to incur the reciprocal costs and risks of identifiable active countermeasures, when passive countermeasures will suffice.

Further specific recommendations are included in Part V of this Report, Summary of Conclusions and Recommendations.

V. PROSPECTS FOR VERIFICATION AND WARNING: CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS & RECOMMENDATIONS

- SALT Warning capabilities of the U. S. are likely to deteriorate in the late 1970's, even if the USSR does not resort to active countermeaures against NTM's.
- It is essential to accelerate prudent investments in a more reliable SALT Warning system, both to anticipate destabilizing developments with SALT Treaty compliance and to identify BREAKOUT should it occur.
- Communications Security (COMSEC) vulnerabilities are pervasive within the United States and within Allied Governments. Priority COMSEC investment status for both the BYEMAN and ZO-- industrial base, and for affected government communications is important in reducing the efficacy of passive countermeasures.
- Coordinated management of U. S. counterintelligence resources should contribute to SALT Warning under ~~under~~ Treaties and to BREAKOUT Warning should BREAKOUT be attempted covertly.
- Quality control efforts, designed in part to identify and assess passive countermeasures, appear to offer benefits at modest cost.
- Where our capacity to verify is limited, but likely to be degraded by concealment or deception measures which may be detected, SALT Treaty coverage may contribute to mutual restraints in cover and deception.
- Strategic cover and deception planning should be integrated throughout the entire national and special reconnaissance programs of the United States. Objectives include: (i) misallocation of adversary passive countermeasures; (ii) quality control sampling for each mission; and (iii) sampling of Soviet

cover and deception activities, among the warning signs of BREAKOUT.

- o In designing measures to protect against active interference in accordance with NSDM 333, passive countermeasure protection should be commensurate, since there should be little incentive to incur costs of active countermeasures when passive measures suffice.
- o Measures to enhance the security of NTM's and other U.S. intelligence activities are essential. The Hermann Report's proposal (1975) to decompartmentalize SI, TK, and E channels might be considered in conjunction with measures to protect advanced NTM systems, and in conjunction with consideration of legislation to protect U.S. foreign intelligence sources and methods.
- o Practices which preclude intelligence analysts' access to reports of possible SALT violations, or other activities which affect strategic stability should be eliminated, so as to enhance the presently-difficult prospects for adequate SALT and BREAKOUT warning.
- o In recognition of the increased likelihood that principal NTM roles and missions have been identified by Soviet counterintelligence, prospects for in-country collection by technical means, assisted by operational personnel, should be reevaluated.
- o Prospects for Third Party Intelligence Exchange Agreements with all nations bordering on the USSR should be evaluated, and appropriate initiatives taken, particularly so as to provide 24-hour coverage of key sectors in anticipation of nighttime construction activities.

- Additional treaties and other international agreements--a sampling of which is attached as Table ' .--should be evaluated, for purposes of enhancing verification and warning, for clarification of the boundaries of the licit and illicit, and for purposes of increasing the number of states to be affected by active countermeasures in space.
- Criteria for incremental NTM systems should include among selection criteria: performance under passive and active countermeasures; difficulty of mission identification and countermeasure design; detectability of collection patterns; variability and adaptability of collection patterns; and replaceability.
- Humility is essential in evaluating vulnerability to countermeasures which we may have failed to detect or to understand.
- A basic R&D program of the federal government is necessary to reduce prospects for technological surprises.
- To enhance SALT verification and warning prospects, a supplemental ACDA-sponsored project should consider vulnerabilities of ocean surveillance systems within the ZO-- compartmentation system.

Table . . Possible Treaties and Other International Agreements to Enhance SALT Verification, SALT Warning, BREAKOUT Warning

Possible Treaties or Agreements	Functions:				
	I. SALT Verification	II. SALT Warning	III. BREAKOUT Warning		
1. Protocol to SALT II. designated test ranges non-concealment non-encryption designated verification systems	E,C	E	E		
2. Protocol to Accidents Agreement of 1971, Art. 7. non-interference with space systems, ocean surveillance systems	C	-	-		
3. Treaty on Remote Sensing of Earth codification of remote sensing in accordance with int'l law	C,I	I	I		
4. Convention on Provision of Remote Sensing Services to UN Specialized Agencies	I	I	I		
5. Additional Third Party Agreements					
PRC	E	E	E		
Other States	E	E	E		

E = Enhance performance of function, in event of treaty or other international agreement compliance

C = Clarify boundaries between licit and illicit activities

I = Increase number of affected states in event of active interference with national

HEXAGON GAMBIT [redacted] EARPOP [redacted]
GAMMA

~~TOP SECRET~~

WSO or R No: R-2094-ACDA

Copy No: 2

Assigned to:

Project No: 6356

Contract No: AC6AC406

Task Order No:

Temporary cover sheet for
RAND *external publications**

number R-2094-ACDA (DRAFT)

title BREAKOUT - Part II

author(s) Robert Perry

date October 1976

* This form is used as a temporary cover for DRAFT Reports submitted to a client for review and comment.

HANDLE VIA
BYEMAN-TALENT- KEYHOLE-COMINT
CONTROL SYSTEM JOINTLY

~~TOP SECRET~~

HEXAGON GAMBIT [redacted] KENNEN GAMMA [redacted]
EARPOP

Rand
SANTA MONICA, CA. 90406

~~TOP SECRET~~

DRAFT

BREAKOUT - PART II

Robert Perry

R-2094-ACDA

DRAFT

RAND
SANTA MONICA, CA. 90406

CONTENTS

PREFACE

This preliminary draft report was prepared for the Arms Control and Disarmament Agency by staff members of the Rand Corporation, under the terms of Contract AC6AC406. It is a "for comment" draft. Neither copies of this report nor comments on it should be forwarded directly to the Rand Corporation; they should instead be sent through the National Reconnaissance Office, Directorate of Special Projects (SAFSP-SP-3) to the attention of the author. The considerable assistance of SAFSP and the Office of the Secretary of the Air Force, Space Systems (SAFSS) requires acknowledgement, both in terms of research advice and assistance, and in providing facility support. Nonetheless, the views, opinions, findings, and conclusions stated or implied herein are in no sense to be attributed to the NRO or any of its elements, or to ACDA. Owing to the nature of the material used in this report, it has not been subjected to the customary editorial and peer review processes of Rand.

I. VERIFICATION: THE REQUIREMENT

United States verification of Soviet compliance with existing and pending arms limitations agreements is universally assumed to be essential to continuation of those agreements or their extension. The mere existence of verification devices is sufficient of itself, to ensure compliance. In U.S. terms, the validity of the agreements hinges on successful verification, which by definition implies U.S. confidence in the adequacy of the various "national technical means" that are called upon to provide evidence of compliance with the agreements. Nor is the central issue merely the credibility of negative evidence; the lack of indications of major violations is but one aspect of the compliance and verification of credible verification. Ultimately, the United States must be confident also that the various kinds of reconnaissance satellites on which the mechanics of verification depend can detect, and U.S. interpreters can diagnose, any attempt by the Soviet Union to make extensive advance preparations for a sudden breakout. That requires success in tracking and evaluating tests of advanced weaponry, in identifying and appreciating the significance of any unusual test, development, or construction activity that might signal

the pending creation of a capability either to deploy unconventional weaponry or to deploy quantities of unnoticed or undetectable more-or-less conventional strategic weapons; and in accurately assessing indicators of possible intent to make advance preparations for an eventual breakout, the initial stages of which are being clouded or concealed. Those are not all of the attributes of "successful" verification, but they are among the most critical.

The adequacy of any verification system is ultimately determined by the same criteria that apply to all other defense mechanisms involving both people and technology: How well does it serve its intended function? Unhappily for such assessments, the failure of the mechanism becomes evident only retrospectively. Failures cannot be detected in advance and only imperfectly can they be anticipated. Further, acting on an anticipation of failure is not simple; a complex of technological, budgetary, political, diplomatic, social, and institutional influences that condition responses to vaguely perceived threats of uncertain substance.

The purpose of a verification system in any arms control setting is no more than to provide acceptable indications that no violations of the underlying agreement have occurred.

Existing strategic arms limitation agreements between the United States and the Soviet Union are monitored by what have with precise vagueness been described as National Technical Means of Verification (NTMs). Several kinds of "national means" may be relevant, but the fundamental reliance of the United States is overhead photography performed from reconnaissance satellites. "National Technical Means" by definition, excludes espionage from the category of acceptable verification mechanisms. Espionage is nowhere defined in the formal agreements and annexes that compose the Soviet-U.S. arms limitations treaty and the subsequent Vladivastok protocol.

Verification by international control (inspection teams) was, until 1961, the "in principle" mechanism regarded by all major powers as the only acceptable means of enforcing arms control and disarmament agreements. The term "existing national technical means" was introduced into consideration in November 1961, by the Soviet Union, as an alternative to international inspection. It was intended originally to apply solely to a ban on tests of nuclear weapons in the atmosphere, but the Soviets subsequently insisted that a ban on underground nuclear tests could be similarly enforced.

The limited nuclear test ban treaty of 1963 acknowledged that international inspection was unnecessary for verification of compliance with agreements covering the atmosphere, the seas, and outer space. The inability of the nuclear powers to agree on a mutually acceptable inspection process prevented extension of the ban to underground testing. The Soviet position at that time was that token inspections might be conducted, but that widespread inspections of the sort proposed by the United States and the United Kingdom constituted espionage. The only substantial Soviet variance from that position was acceptance of the somewhat far-fetched proviso that installations on the moon and other celestial objects might be inspected by all comers to ensure compliance with the 1967 ban on the emplacement of nuclear weapons in outer space. (The treaty does not contemplate "inspection" of earth satellites, which by definition are not "celestial bodies.")

For practical purposes, the technology of 1950 was adequate to police a test ban covering nuclear detonations in the atmosphere, in the oceans, or in outer space, but neither in the 1960s nor later would the United States agree that "national means" were sufficient to establish, with certainty,

that a seismic event was or was not of natural origin. Actually, the general adequacy of seismic sensors probably was sufficient by 1975 to distinguish between earthquakes and "small" nuclear explosions but could not routinely be counted on to distinguish "small" from "medium" underground explosions of nuclear devices.

Unproductive discussions of inspection mechanisms for verifying troop reductions in Europe have been intermittently in progress since the early 1960s. Although the general notion of inspection posts and liaison missions has been accepted "in principle" by the Soviet Union, disagreement about the permissable number of the first and frequency and freedom of movement of the latter have again prevented any agreement. What constitutes "espionage" has been the sticking point. In 1963 the Soviets refused to join in bilateral budget discussions which, in the view of the United States, would have increased American confidence in the actuality of a Soviet announcement of reductions in military budgets. (U.S. defense budgets were similarly cut back.) In 1964 the Soviet Union rejected an American initiative on freezing existent levels of strategic delivery systems for nuclear weapons; again, the United States proposed inspection on site as a precondition of agreement.

(In that instance Soviet numerical insufficiency was so pronounced that a "freeze" had no real chance of acceptance.)

By 1961, the United States had acquired a useful if modest capability to determine the numbers, status, and position of Soviet strategic delivery systems. By 1964, that capability had so improved that the United States was fully cognizant of the significant inferiority, both in numbers and quality, of Soviet missile and bomber forces. Starting in August 1960, the United States had successfully orbited a number of increasingly proficient satellite reconnaissance systems and had recovered photographic imagery that clearly demonstrated the hollowness of Soviet claims to strategic parity, much less superiority. The quality of returns from such satellite missions improved appreciably during the first decade of operations. Early missions (1960 and 1961) were able to establish how many intercontinental ballistic missiles the Soviet inventory contained, their locations, and in a general way, their operational readiness. That much could be learned from the outputs of photographic instruments which could distinguish objects about six meters across in their narrowest dimensions; by 1970 objects measuring about 45 centimeters were routinely distinguishable

from 90-mile orbits, and, for the most part many were identifiable. In best circumstances, details as small as 20 centimeters could be resolved.

The probability that such capabilities would come in to being by the early 1970s was well appreciated in the reconnaissance community as early as 1965. In that year, the Arms Control and Disarmament Agency first argued that limitations on numbers and kinds of missile launchers could be adequately verified by inspection from satellites. (Signal intelligence and electronic intelligence--SIGINT and ELINT--were by that time contributing some useful confirmatory data.) By 1967, the President had accepted such a premise for the purposes of conducting informal discussions with his Soviet counterpart. The assumption of the time (in which the Central Intelligence Agency and the Joint Chiefs of Staff did not then concur) was that numbers of ballistic missiles, of bombers, and of submarines could be adequately verified from satellite photography although distinguishing between intercontinental and lesser-range ballistic missiles would be difficult. Sea-based and mobile missile launchers were then widely assumed to be impervious to positive identification and assured numbering.

The position of the Joint Chiefs in the Spring of 1968 was that exclusive reliance on verification of strategic arms inventories by satellite inspection would unwisely burden the threat assessment process, that such an approach would make the United States dependent on unverifiable assumptions about capability to detect violations soon enough to permit an effective response. They argued also that using the product of satellite reconnaissance as the sole source and support for a claim of violation would compromise the entire collection system; then, as later, U.S. authorities generally assumed that the Soviets did not comprehend the very remarkable capability of U.S. satellites to portray a broad range of military activities (including much research and development and testing) being conducted within the Soviet Union.

In August 1968, in preparation for the opening of discussions about a strategic arms limitations treaty, the National Security Council accepted the premise that the United States could agree to unqualified reliance on "national means of verification" and that American negotiators should attempt to induce Soviet acceptance of

selective inspection of sites or activities where activities were ambiguous and could not be adequately confirmed by looking down from orbit.*

In the course of the protracted 1970 negotiations which finally put strategic arms limitations in the context of a prospective treaty, the Soviets ultimately rejected all proposals for on-site inspection. Further, when discussions of "national technical means" progressed to matters of detail and interpretation, the Soviets explained informally that in their view "national means" precluded reliance on espionage. Soviet spokesmen illustrated the point by contrasting space observation with U-2 operations (referring explicitly to the 1960 Gary Powers episode). The principle of non-interference with national means proved mutually acceptable (it had initially been entered by the United States), but in the end the United States would not agree to the inclusion of MIRVs in the list of prohibited growth items on the grounds that "national means" could but inadequately

* The Soviet Union was willing to require close inspection of suspect locations for both the non-proliferation treaty and the seabed negotiations; in neither instance, of course, would inspection of Soviet territory be necessary.

confirm compliance. The Soviets would discuss on-site inspection only in terms of a pointless agreement that either side could request it but that the requested party need not agree. Similarly, the Soviets refused to accept the principle of selective on-site inspection as an element of the anti-ballistic-missile provisions of the agreement; prohibition on certain ABM-related radar construction activities, which were assumed by the U.S. to be readily verifiable from space, represented the principal element of the "no-upgrading of SAMS" provision on which the United States insisted. Concealment was expressly excluded (with the qualifier that "This obligation shall not require changes in current construction, assembly, conversion, or overhaul practices" on the part of either party). "National Technical Means" were defined only to the extent that they should be used "... in a manner consistent with generally recognized principles of international law." The qualifier was of Soviet origin.

Those verification provisions implicitly expressed both the American assumption of adequacy and the Soviet understanding of what constituted acceptable means of

verification.* The agreed limitations constrained numbers and sizes of ballistic missiles, expansion of ABM forces, numbers of submarine-carried strategic missiles, and numbers of heavy bombers.

American assumptions of the adequacy of verification devices were predicated on notions which derived from the perceived capabilities of systems designed in the 1960s to perform tasks deemed vital to the collection of strategic and technical intelligence of that period. By 1970, when the SALT I treaty was drafted, the United States was phasing out the last of its first-generation surveillance systems (CORONA), introducing a much more capable system (HEXAGON), and starting the development of a near-real-time system that promised to provide continuing coverage, at levels of resolution on the order of [redacted] centimeters, of the entire Soviet land mass (KENNEN, as anticipated in 1970). The chief instrument for technical intelligence of the sort required to establish details of the configuration of missiles, bombers, and submarines was a much improved

* The importance of such implications will be addressed later in this section.

version of the GAMBIT system, originally conceived in 1960 and first successfully orbited in 1964.

Were the Soviets aware of the rather remarkable capabilities of the more advanced satellite systems of 1970, or of the pending emergence of a system capable of all-daylight-hours coverage of the Soviet land mass at comparatively high (by 1965 standards) levels of resolution? Probably not. All the available evidence suggests that Soviet progress in reconnaissance by means of photographic satellites lagged behind that of the United States by five to seven years, and that in the construction of devices requiring the conceptual and electronic complexity of KENNEN the lag may have been as much as 10 years. For practical purposes, by the late 1960s the United States had become capable of performing 1960-era equivalent U-2 reconnaissance operations using spacecraft. If Russian technical intelligence experts were aware of that circumstance before 1971, they do not appear to have alerted their SALT specialists.

But by 1976, the Soviets had become fully capable of distinguishing between "broad coverage" (HEXAGON) and "high resolution" (GAMBIT) missions, by all indications had a

realistic appreciation of the capabilities of each, and were acting on that information. The change could have occurred by reason of the gradual relaxation of the original tight controls over the distribution and use of satellite reconnaissance photography in the U.S. (and by allies) during the 1970-1976 period, but it was just as likely to have derived from continuing Soviet R&D program in satellite photography. Even without a relaxation of controls, realization of the potential of satellite photography would have occurred, in time, as the Soviets succeeded in efforts to improve their own systems. Indeed, appreciation of American capabilities was more likely to precede than follow the completion of R&D. Using their own satellites to view their own activities, the Soviets would tend to credit the American satellites with superior performance; American authorities disclosed details of Soviet activities that did indeed reveal capabilities approaching the limits of existent 109 American satellite reconnaissance, and if the Soviets were capable of extrapolating from their own rates of progress to probable American rates of progress they would inevitably have credited the Americans with resolution, contrast, and coverage potential greatly superior to Soviet

systems. The expansion of concealment and deception efforts in the Soviet Union in the period 1973-1976 provides considerable support for the argument that both Soviet capabilities and Soviet appreciation of American capabilities were rapidly improving.

On such grounds it seems no more than reasonable to assume that in late 1976 the Soviet Union had acquired a rather good understanding of the abilities and limitations of the traditional photographic satellite reconnaissance systems of the United States. Soviet specialists quite probably understood fully what the United States had considered to be "adequate" capabilities for arms limitations verifications as of 1970, and very likely appreciated later American improvements, though perhaps not their magnitude.*

* Which should not suggest that the Soviets could replicate American achievements in all respects. Satellite reconnaissance requires a particular and demanding compound of optical electronic, and chemical technologies, properly ordered, and most of which have become unique to the United States. As in other instances, the Soviets have standardized their reconnaissance satellites, have limited the scope of technical changes, and have substituted bulk or quantity for technological elegance. But in satellite photography, elegance is precisely the essential element. Conventional and more mundane Air Force satellite programs, and NASA programs, lag three to five years behind reconnaissance programs in achieved levels of applied technology. And they generally have been more costly, when comparable levels of achievement are compared.

II. CAPABILITIES AND ADEQUACY

Three U.S. assumptions underlie past and proposed arms limitations agreements:

(1) U.S. National Technical Means can provide conclusive evidence of compliance or non-compliance with agreements.

(2) A rapid expansion of Soviet strategic capabilities could not be concealed well enough, or long enough, to permit the generation of a serious threat to the strategic balance.

(3) So long as the Soviet Union credits those assumptions, no serious effort to "break out" of the arms limitations agreements will be attempted.

The third of those assumptions is self evident, if the first two are valid. But it hinges on questions of the extent to which the first and second are reasonable, and prospects of their transience.

Assumptions of "conclusive evidence" hinge on several premises. The first and probably most important is that sufficient information can be obtained from current and

planned reconnaissance satellites to reconfirm, periodically, Soviet compliance with the terms of the arms limitations agreements. By implication, that premise implies that the verifiable elements of the Soviet strategic arms inventory with which the United States should be concerned are similar to those considered while the treaty was being negotiated (relatively large sites or objects readily identifiable as missile launchers, intercontinental bombers, or anti-ballistic missile hardware). A derivative implication is that U.S. capabilities will improve at a rate consistent with the need to detect and identify unconventional weapons or to establish the concealment of conventional weapons.

Present and contemplated systems in the U.S. satellite intelligence inventory, all of them potentially subject in one way or another to measures which may degrade, interrupt, or preclude their effectiveness, include:

Code Name	Orbit	Application; Arms Control Relevance
989 (P-11)	Varies	ABM/SBM, some air defense radars; limited
[redacted]		
GAMBIT	75-225 nmi	Photo; [redacted] resolution photo, 5-mi frame width
[redacted]		
HEXAGON	82-144 nmi	Photo; 2.5-foot resolution, 300-mi swath
KENNEN	[redacted]	
647	Sync	IR; detect ICBM via IR with limited low-thrust detection ability

The nature or U.S. capabilities was changing in 1968-1970 and is continuing to change in ways that may be inconsistent with impressions of potential for continuing improvement.

KENNEN, for example, is viewed as a potential replacement for either or both GAMBIT and HEXAGON, although it lacks the resolution capability of the first and the broad area coverage of the latter. That circumstance arises partly in the largely ignored circumstance that the capabilities of both GAMBIT and HEXAGON have improved since KENNEN was conceived and that the potential for further improvement exists.*

KENNEN [redacted] GAMBIT and HEXAGON have lifetimes of three to six months, returning film capsules at intervals of one to six weeks as circumstances require. One of the attractions of KENNEN was that its deployment would obviate the necessity for frequent launches; [redacted] Although one intelligence gap of more than

* A similar set of circumstances marked the development and introduction of HEXAGON in the period 1965-1970. HEXAGON was designed to provide the coverage of CORONA (the original surveillance satellite) at the resolution of GAMBIT. But in the five years between the start of intensive work on HEXAGON and its first use, the quality of GAMBIT photography improved enormously. For that matter, various proposed improvements of CORONA (which were rejected largely because HEXAGON was scheduled and because budgets would not readily accommodate both HEXAGON development and CORONA improvement) could conceivably have provided many of the realized HEXAGON capabilities at considerably less cost. In the event, GAMBIT proved to be indispensible.

four months occurred in the mid-1960s, the recurrent frequency of CORONA, GAMBIT, and HEXAGON launches from 1961 onwards (necessitated by their relatively short orbital lives, as compared to KENNEN) ensured, as a matter of course, that a failed system could be replaced rather promptly and that no gross lapses in coverage could easily occur. Further, capabilities for Soviet interference with the photographic satellites were scant and for all practical purposes interference would have been obvious. None of those attributes characterizes KENNEN or the era of its probable use. Opportunities for both overt and subtle interference with satellite reconnaissance have improved with the development of more effective anti-satellite capabilities and the consequence of successful interference with or the accidental failure of three successive KENNEN missions would be to create an intelligence gap of six months to a year and more, depending on timing and circumstances. If GAMBIT is kept in the inventory after KENNEN's introduction (which seems likely given the absence of any replacement capability for high-resolution technical intelligence photography), it conceivably would be possible to orbit one or two GAMBIT systems to acquire intelligence. But without the availability

of relatively recent broad-span reconnaissance on which GAMBIT effectiveness is heavily dependent, GAMBIT would be most unlikely to spot potentially significant activity in areas remote from those routinely covered--existing missile and test sites, naval bases, and ABM installations. GAMBIT is a pointing system, and must be aimed at the area of interest that it photographs; the Soviet Union contains millions of square miles in which such systems as mobile ICBS or ABMs conceivably could be emplaced. Without information about aim points, GAMBIT loses effectiveness.

Three main points need be made: (1) Soviet opportunities for interference with reconnaissance have improved, both because of the nature of U.S. systems and because of the quality of interference mechanisms; (2) the vulnerability of U.S. systems has increased, making them much more attractive targets for interference than was the case as recently as five years ago; and (3) the combination of improved opportunity and greater payoff appreciably enhances the attractiveness of interference. The risk of detection has decreased, the prospective returns are great, and the likelihood that the U.S. can quickly replace a damaged or demolished reconnaissance system is vanishing.

The implication of such developments is plain: the assurance that U.S. imagery satellites of the late 1970s and early 1980s can routinely acquire conclusive evidence of non-compliance with arms limitations agreements exists only so long as the systems continue to operate without being interfered with and without encountering unexpected and extended interruptions of service because of accidental failure. If conclusive evidence of Soviet violations is not at hand, is there assurance of an effective U.S. response? Should a gap in coverage occur, however caused, the Soviet Union would automatically acquire the opportunity to deploy, undetected, any of several destabilizing strategic systems. Soviet realization of those circumstances and that opportunity could provide a marvelous justification for undertaking to "break out" of the existing arms limitations limits without risking verifiable detection. It would, in effect, encourage a Soviet decision to attempt breakout.

U.S. technological capabilities for imagery returns have improved enormously in the past five years. The total vulnerability of imagery systems has increased proportionately. The considerations that presumably conditioned Soviet appraisals of opportunities and risks in the 1965-1975 period have also changed.

Verification was initially conceived of in terms of a process that would proceed under conditions of no interference. New measures of concealment and deception were prohibited by the terms of SALT I. But deception and concealment have increased and opportunities exist for further enlargement without violating the letter of the original agreement. To that extent, verification is now obliged to function under conditions of passive interference. Can it function effectively, as the United States must define that qualification, under conditions of passive plus active interference? What would be the American response to a breakdown of satellite imagery capabilities which could not conclusively be attributed to active interference?

To address such questions, one must turn first to the issue of what contributary capabilities the United States has or can assemble in support of verification efforts.

Seven general categories of overhead reconnaissance exist: imagery in the ordinary visual spectrum, signal intelligence, electronic intelligence, communications intelligence, infrared signals, [redacted] Mostly the vehicles are satellites, although aircraft still have utility in peripheral reconnaissance. Additionally, agents, defectors, and open-source information contribute

to assessments. Some are inadequate for verification assessments, for various reasons; others are inapplicable. Communications intelligence can have extreme value--but in most circumstances it is not wholly credible and, in any case, the absence of credible communications intelligence says nothing except that the source being interrogated is uncooperative. Without confirming imagery, much of the output of signal and electronics intelligence is of dubious worth because, by its nature, it becomes available through the implicit cooperation of the agency that originates the signal. In any case, Soviet expertise in suppressing emissions that contribute to communications, signal, and electronics intelligence is generally conceded to be high.

[redacted]

of the sort most appropriate to a preemptive strategic strike it could be highly destabilizing. Both the United States

and the Soviet Union have actually orbited radar reconnaissance systems (although the American system was a pure R&D system) and the Soviets have tested an ocean surveillance satellite in various applications. In the absence of optical reconnaissance capability, radar might provide some useful information about changes in previously observed force dispositions and such, but is is unlikely to return information of the sort required to confirm that the Soviets are deploying some strategic weapon in kind, quantity, or quality that constitutes a strategic threat.

Defectors and agents might be the most productive sources of information during a hiatus of overhead reconnaissance, but the credibility of their information may well be low, the Soviets have a remarkably effective security system and notoriously good counter intelligence and the United States has become increasingly dependent on technological rather than human sources for its intelligence inputs (and thus may be unable to obtain credible intelligence from agents in time or crisis and may be unwilling to base major decisions on such information). The prospects, overall, are not attractive.

In an objective sense, is there any alternative source of information with the credibility of imagery returned by reconnaissance satellites? If the information being sought, or subject to confirmation, has to do with the rapid build-up of a new Soviet strategic capability, the answer probably is "no." Good communications security, including encryption, rigid discipline in radar operation, and routine jamming are likely to prove sufficient to forestall the acquisition of wholly credible source information if the Soviets dedicate their considerable resources to concealment of a buildup. Blinded, or partly blinded, the only effective response the United States could make to unverifiable indications of a Soviet buildup of strategic weaponry would be to invest in a counterpart buildup, and if the Soviets were successful in making extensive surreptitions preliminary provisions for a quick buildup, a delayed U.S. response might well be dangerously ineffective.

What capability that currently neither exists nor is programmed could provide some insurance against such events? The first and most obvious requirement would appear to involve the preparation of a backup capability for use in both strategic reconnaissance and verification activities.

That response, which has been variously proposed at intervals during the past 15 years, is certain to be costly. Indeed, in the past that has been the chief argument against so proceeding. Nevertheless, creating a back-up capability remains attractive.

Past proposals have generally conceived of a relatively low resolution system (one to three meters) for scanning Soviet deployment arrangements. In an era in which high resolution has become an increasingly essential ingredient of assessment, in which concealment and deception have become more prevalent, in which the fine details of a suspect item or installation may be essential to understanding of capability or potential, scanning systems are unlikely to be wholly adequate. It is, for example, entirely reasonable to assume that the Soviets, if they set out covertly to deploy some new array of strategic weapons, might design whatever installations they proposed to be essentially undetectable at resolutions more gross than 90 centimeters (which is probably representative of their own imagery capabilities as of 1975-1978). Were that true, a scanning system of the type proposed in the past would provide little useful information. It would have to be accompanied by, or supported

by, a high resolution pointing system. Short-lived scanning and pointing systems sent up to provide reassurance against Soviet strategic redeployment actions following the breakdown of routine imagery would also represent a useful signal of Soviet intentions. However adroit some subtle interference with "routine" verification systems, it would presumably not be effective against short lived, special-purpose verification systems, while active Soviet interference with efforts to confirm Soviet dispositions would presumably be interpreted as confirming that suspicions of Soviet breakout intentions were warranted. Defining or specifying the technical characteristics of such a system pair is beyond the scope of this discussion, as is any detailed consideration of cost tradeoff factors. But that appropriate systems could be designed cannot be doubted; film-optics-systems, vehicle, and recovery devices appropriate to such applications have been accessible to U.S. designers for nearly a decade. As for cost, the investment requirements must be balanced against alternatives, and without high confidence means of confirming that the Soviets were not building a destabilizing strategic capability during a period of U.S. ((vision impairment)), the only alternative would be to commence whatever counter-building up operations seemed

essential. That conceivably could lead to a major arms buildup in the United States, and given the current costs of weaponry it would be unlikely to cost less than several hundred times the cost of developing and maintaining an adequate backup verification capability.

One of the near-term problems created by consideration of such options is that some of the essential ingredients of an appropriate U.S. response are not as plentiful as in the past. Starting from scratch, the capability to manufacture appropriate photographic reconnaissance systems would require from two to four years to assemble. Perhaps more pertinent, the ongoing shift away from expendable boosters to such reusable boosters as the Space Shuttle implies that special measures would have to be taken to ensure the continuing availability of boosters capable of putting such reconnaissance systems into orbit. Similarly, with the gradual rundown of GAMBIT and HEXAGON production and operations, routine capsule recovery could become troublesome. Nor is the availability of essential ground stations for command and control indefinitely assured; dedicated ground station capability has been essential to every reconnaissance system of the past and the need is not likely to diminish in the future. All in all, it is not a simple problem.

As with most complex weapon systems, reconnaissance satellites of all types are taking longer in development, are costing more, and are providing smaller and smaller increments of performance improvement with each investment in quality improvement. The original CORONA photographic system experienced its first (unsuccessful) test flight roughly two years after development began and operated successfully about one year later. Six to seven years of effort devoted to the principal variants of the original SAMOS-series reconnaissance satellites proved fruitless; all of those photographic satellite programs had been abandoned by 1965. (SAMOS infrared and ELINT satellite variants were somewhat more successful.) GAMBIT, in its original form, was rather more than four years in development and took about five years to achieve its original design goals. The improved GAMBIT satellite, which used many of the key subsystems of the original, required about three years to develop. HEXAGON spent nearly six years in development after two years in planning gestation. KENNEN, if it achieves operational status by the end of 1976, will have been in development for nearly seven years, although the first two of those years had more of a research than a development ~~cost.~~ flavor.

Costs have changed even more dramatically; CORONA cost a few tens of millions per unit; each KENNEN will cost [redacted] Early CORONA vehicles could return detail at the 6 to 8-meter resolution level for a few tens of thousands of square miles per mission; KENNEN will return detail of between [redacted] width. Although estimates are notoriously unreliable, it is not unreasonable to assume that such capabilities could be made available for a specialized film-carrying satellite in three to five years. That may actually constitute the physical limit of resolution achievable with conventional film and optics, although it is no more than prudence to recall that as recently as the mid-1960s the "physical limitations of film, optics, and atmospheric dispersion of light" were assumed to constrain resolution achievable from orbit to about [redacted] The switch from film to electro-optical systems has negated many assumptions

about area coverage limitations; major questions of spectral limits and resolution limitations remain to be answered.

Nevertheless, it is becoming increasingly apparent that the kinds of major improvements in performance that characterized earlier advances in reconnaissance technology are not readily come by today and are likely to be even more difficult of achievement and more costly in the future. If events in other fields may be used as indicators of what may occur for reconnaissance instruments, it is reasonable to conclude that as the United States approaches the limits of achievable performance and advances come more slowly, Soviet instruments and capabilities will progress along the lines earlier followed by American designers and, in five or six years, Soviet designers will not only be approaching the same physical limits but will have a good appreciation of the maximum performance achievable by American devices. (Appreciations of reconnaissance capability usually precede achievement by about five or six years--the period required to proceed through development from concept to operational article--so the Soviets may today be approaching a good appreciation of present American capabilities in film-carrying systems. Appreciations of that sort are subject to uncertainties that lessen confidence in time, of course.)

Such trends imply that Soviet understanding of American capabilities for verification probably do not lag far behind the reality of those capabilities. They also suggest that further major improvements along traditional lines of coverage and resolution are not probable. In that circumstance, should the Soviets conclude that it was possible to develop, produce, and deploy new strategic systems that could not be seen at or below the real threshold of U.S. detection capabilities, the option of attempting a clandestine breakout could become rather attractive.*

In the end, it can reasonably be argued that the technological capability of United States reconnaissance systems to verify Soviet compliance with the terms of arms limitations agreements in existence before 1976 is adequate. In the absence of interference with the functioning of those systems, either from natural causes or by Soviet design, the national capability also seems adequate. But when account is taken of the possibility either of malfunction or of effective interference, the assessment rapidly

* The political or economic rationale for such a decision is addressed in earlier sections of this report.

loses validity. And, of course, bringing additional systems into the limitations agreement is quite another matter.*

* For example, the detectability of cruise missiles, or more properly the ability of satellite reconnaissance to distinguish "short range" cruise missiles from counterpart missiles with intercontinental capabilities (when launched from forward carriers, either aircraft or submarines) is very limited. Technology current in 1973 supported the assumption that any air launched cruise missile with a volume greater than 125 cubic feet and surface or submarine launched missile with a volume greater than 150 cubic feet was a potential strategic weapon. Verifying intercontinental capability by monitoring infrared signatures of test missiles is an unlikely prospect; rockets with less than 10,000 pounds of thrust frequently are not picked up by infrared detectors; scan area and frequency limitations constrained the utility of existing satellite-borne detectors and conceivable improved versions. Cruise missiles could be tested adequately at less than their maximum operational ranges; indeed, normal Soviet practice in testing ballistic missiles has been to devote most initial testing to limited range operations and to conduct one or a very few maximum range tests. Further, the range of cruise missiles is not highly correlatable with observed size; merely inserting a larger fuel section can convert a nominal "short range" cruise missile into one with twice the presumed range.

In sum, most candidate restriction on cruise missiles (size, test range operations, thrust) did not appear to be verifiable with sufficient assurance to provide confident assessments of compliance with any controls on the deployment or the development of cruise missiles.

III. VULNERABILITIES AND COUNTERMEASURES

United States verification capabilities can be adversely affected if existing systems are degraded, if their operation is interrupted for any significant period, or if they are prevented from performing their assignments. Those outcomes can occur from either active or passive Soviet actions; the consequence is much the same whether the satellite functioning is affected (active interference) or effective concealment and deception measures degrade that function (passive interference).

GAMBIT, the most useful of space reconnaissance systems for acquiring details of Soviet weaponry, installations, and situations, will provide about 120 days of on-orbit coverage of Soviet territory annually during and after 1977. HEXAGON, which provides broad area coverage and surveys most of the Soviet Union (excluding areas of little interest) daily, will be on orbit for about 180 days a year from 1977 through 1979 and presumably will be phased down as KENNEN assumes its general responsibilities. HEXAGON and GAMBIT have distinctive orbital signatures, although their somewhat different inclinations (97° and 116° respectively) have on two occasions (as of late 1976) been exchanged; the first such instance apparently confused Soviet trackers, with the result that GAMBIT, in a nominal

HEXAGON orbit, observed events and equipment previously concealed. Since 1975, Soviet space track monitors have readily identified and distinguished between the two, with the result that some items that GAMBIT could provide detail on have been left visible to HEXAGON passes but have been removed or concealed from GAMBIT fly-bys. That practice effectively degrades the performance of the GAMBIT system; similar measures effective against both systems also degrade HEXAGON returns. The relative frequency of coverage makes concealment of major construction enterprises, installations, and test operations difficult, since for all practical purposes only 60 to 90 days a year, splintered into rather brief periods, have recently been devoid of either HEXAGON or GAMBIT operations. Nevertheless, a determined evasion effort probably could conceal conclusive indicators of such systems as mobile ICBM's from GAMBIT, and the limitation on HEXAGON resolution makes concealment from that system somewhat easier. Planning around GAMBIT missions is the easiest evasion measure, but with its "best" resolution capability of [redacted] centimeters, GAMBIT can pick up some subtle indicators of certain evasions. Further, both GAMBIT and HEXAGON are subject to irregular degradation of returns by the presence of an average 60 percent cloud cover over the Soviet Union.

GAMBIT and HEXAGON are fundamentally incapable of providing useful information about mobile ICBM systems that resemble earlier systems, about non-standard ABM installations, about warhead variations, and about items and activities similarly lacking in distinctive "signatures." Given the frequency and high predictability of cloud cover, a combination of Soviet planning around satellite phases and conducting sensitive activities in darkness or under seasonal cloud cover probably could be effective. Non-standard installations might go unnoticed, or unremarked, a prospect that makes SAM upgrading to ABM capability worrisome. Identification and verification of suspicious activity could well require better resolution and more frequent coverage than GAMBIT can provide. As recent experience with grain storage sites and underground factories has demonstrated, installations without distinctive site signatures tend to go unremarked. Providing a rather mundane, seemingly common "signature" for some sensitive construction would not be difficult if a determined effort to do so were made. The abundance of "light industry buildings" in the Soviet Union, and the rather great size of some, provide opportunities for conducting some sensitive operations under the cover of opaque roofs and walls.

Interruption of GAMBIT and HEXAGON coverage by reason of either interference or accident is not implausible. Random accidents are difficult

to anticipate, which makes their exploitation equally difficult, but "accidents' can be arranged. Soviet interference with the command links to the photo reconnaissance satellites was for many years treated as infeasible because of its technical difficulty because of the assumed high probability of U.S. discovery. By 1976, neither of those was considered to be an impossible barrier. More active, but still subtle, interference by Soviet forces, either by particle-beam or laser weaponry, has generally been discounted because the requisite installations for generating powerful particle-beam would presumably be located during construction, and because most reconnaissance satellites have carried laser detectors of one sort or another for the past 10-12 years.

The likelihood that the Soviet Union would attempt to attack various of the reconnaissance satellites, particularly the photo satellites, has not had great credibility in the United States since signature of the arms limitations treaty. Earlier, there was greater concern about the prospect. The probability that the Soviets would so interfere with U.S. satellites was generally deprecated because as the Soviets developed their own satellite capabilities and became more dependent on them, particularly the surveillance of Chinese and Middle Eastern activities, it was assumed that the costs to the Soviets would be so great that extreme motivation would have to develop before serious consideration of such an attempt

There is, however, a second set of rationales for Soviet attacks, probably by intercept, on various of the U.S. reconnaissance satellites. The photographic satellites are obvious targets; they return the vast bulk of information critical to arms limitations verification. Two aspects of the situation of 1976 deserve particular attention. First, there is the possibility that the Soviet Union's technical intelligence specialists have only recently become aware of the remarkable performance potential of American satellites. The negotiations that preceded agreement on the sanctuary aspects of "National Technical Means of Verification" were marked by discussions of the differences between verification and espionage. Notably, reference to the U-2 incident of 1960 was occasionally used to define the Soviet conception of the distinction. If the best the Soviets had been able to conceive of in the way of repeatable photo-satellite resolution in 1968-71 was the one-meter detail that represented 1965 levels of U.S. capability, that sort of distinction would be reasonable. Otherwise it would not, because in fact the United States was able to approximate U-2 product from satellites by the early 1970's. What would be the U.S. response if the Soviet Union announced that operations of HEXAGON systems were permissable under the "National Technical Means" clause, but that GAMBIT represented

espionage? That seems an unlikely event if only because modest changes in the operations of either HEXAGON or GAMBIT could make the two indistinguishable on orbit. A decrease in coverage would result, but the United States could presumably compensate by increasing the frequency of launches.

A more dangerous prospect could characterize KENNEN operations.

[redacted]

[redacted] Even if the Soviets later publicly relented and withdrew from their initial stand, the gap in coverage would provide an unobserved interlude during which they could undertake the rapid deployment of some system, the only constraint being sufficient advance preparation to insure emplacement of the system before the Americans could restore their overflight capability.

Soviet opportunities and capabilities for actively interfering with various of the ELINT, SIGINT, and COMINT satellites are more limited. Generally, orbits are higher and the difficulty of intercept is greater. The vulnerabilities of such satellites lies in their continued dependence on the cooperation of the Soviet Union. Microwave intercepts of highly valuable information can fall off to nothing if the Soviets resort to tight communications security, good encrypting, or land line transmission. Radars can be tested on frequencies unlike those they are scheduled to use in operational circumstances. The difference between a mobile IRBM and a mobile ICBM can be as little as duration of burn or the presence of a third booster stage. Infrared signatures tell little about capabilities if burn times are artificially abbreviated and stages are tested in pairs rather than in threes. Such deception and concealment measures do not constitute violations of the arms limitations treaty. By the same token, moreover, the Soviet Union could quite validly claim that active interference with such satellites was not prohibited by any treaty--and it is not. The Soviets have repeatedly and explicitly said that they would not permit espionage; that definitions of espionage have been scant and vague does nothing to lessen the threat.

The attractiveness of such measures to the Soviet Union presumably will increase as it becomes increasingly apparent that the United States in committing its resources to the development, fabrication, and operation of smaller numbers of ever more expensive, ever more fragile--and ever more capable--reconnaissance satellites of all classes. The chief vulnerability of the U.S. validation system, or that part of it dependent on the continued effective functioning of reconnaissance satellites, lies in that circumstance. Not only are the individual satellites more complex, and thus more likely to be disabled by damage to one or more subsystems [redacted] considerable), but they are longer lived, which means that replacements are more widely spaced and will be appreciably delayed. Soviet deployment of an effective means of degrading, interrupting, or preventing the operation of one or more of the reconnaissance satellites on which verification is critically dependent is becoming more probable as the susceptibility of individual satellites to such measures becomes more pronounced and as the total U.S. verification mechanism becomes increasingly dependent on the continued functioning of several interrelated satellite systems. Therein lies the chief vulnerability of the U.S. verification process. Development of

a gap in coverage sufficient to permit prepositioned, prepared Soviet strategic weapons to be emplaced without being noticed represents the greatest danger to the "conclusive evidence" requirement for verification; concealment of the dispersal of new weapons becomes more than a possibility once that opportunity develops. If the opportunity arises because disabilities of ambiguous origin concurrently or consecutively affect several critical reconnaissance systems, the U.S. has at best a quandry and at worst a crisis to contend with. If the Soivet Union does not credit the assumption that U.S. technical means can indeed verify a breakout attempt, the breakout attempt becomes that much more likely.

In the past, U.S. concern for the possibility of some clandestine development program that would provide a technological breakthrough for the Soviet Union and destabilize the strategic arms balance has been lessened by the assumption that the United States would be able to detect evidence of such a development program well before it could have important consequences. Test range information, construction activity, and sightings of prototypes or test articles have provided evidence of Soviet development enterprise. But are the Soviets proceeding, in the late 1970's, along the same paths that produced signals so indicative of intent and progress in the 1960's? If Soviet institutions and processes are changing, will U.S. intelligence gathering mechanisms be able to track progress as in the past?

Departures from the perceived Soviet norm have troubled U.S. intelligence analysts in recent years. The underground grain storage sites provide an interesting case in point. Defector-provided information was the key to locating and identifying those sites; the construction activities that accompanied their establishment and the site signatures that identified them had been visible for several years, but such signatures were not on the lists of items that should be remarked and observed.

U.S. observers are increasingly unable to explain Soviet intent and Soviet goals in technology, to understand why the Soviets have invested in some kinds of testing or built installations that have no U.S. counterparts. Bafflement has become more pronounced recently, perhaps because the continuing improvement in the quality and frequency of reconnaissance returns has made "enigmatic" activity more apparent. But it is also conveivable that we are indeed losing our ability to anticipate the directions and goals of Soviet R&D. How then can we realistically expect to be able to identify and estimate the importance of novel events even if they are wholly observable?

Given such uncertainties, what should verification capabilities focus on if the assumed threat is breakout? Concealment and deception are well established Soviet practices; maskirovka is the common term for a doctrinal

policy of concealment and deception in strategic or tactical matters. The objective, in all instances, is to confuse an antagonist's appreciation of the location, size, and capability of Soviet forces. Thus, the Soviets routinely make every effort to prevent unfriendly access to technical detains which might disclose performance characteristics of their military systems. Cloaking readiness status is another routine precaution. Past Soviet actions have included constructing dummy installations, covering production and weapons sites, and camouflage. That those efforts have been regularly detected says something for the quality of U.S. surveillance, but it is conceivable that other and more successful measures of concealment and deception have escaped notice.

There has been, from time to time, some consideration of the possibility that the Soviets are selectively clumsy and ineffective, or that an obvious, discernable camouflage scheme is intended to divert attention from some other, far better effort. The substance of that argument is difficult to establish; penetrating some hitherto unsuspected camouflage arrangement would at least demonstrate that the Soviets are more capable than we might have assumed, but it would not either prove or disprove the thesis. A more obvious interpretation might be that Soviet reconnaissance satellites are less capable than their American counterparts, and

that the Soviets have no real appreciation of American capabilities. The ability of a GAMBIT camera system to resolve camouflaged details that frustrate HEXAGON would suggest a certain insensitivity on the part of Soviet camouflage experts, but again it neither proves nor disproves the case.

An interesting U.S. experiment that might usefully be conducted in order to lessen uncertainty about the concealability of Soviet activities potentially relevant to breakout would be a variant of the "hiders and finders" exercise proposed by Amrom Katz several years ago. An example case could involve an effort on the part of an Army or Air Force unit to construct dummy ABM sites at various places in the United States, with a concurrent effort on the part of U.S. satellite operators to discover and identify the activity. One of the objections to conducting such an experiment in earlier years was its cost, not solely in dollars, but in terms of the film that would have to be expended on U.S. targets that might more usefully be devoted to Soviet targets. The availability of KENNEN could make that objection irrelevant; the residual problem would concern only the costs of whatever national resources were devoted to the "hiding" phase by photo interpreters who (again) presumably could be more usefully occupied in searching for real Soviet concealment activities. Nonetheless, if the costs were marginal

the investment conceivably could be highly worthwhile. Means of minimizing the investment presumably could be contrived if interest in the outcomes were sufficient.

A special kind of deception may be implied by the so-called III-X silos, which are cylindrical, include explosively removable silo doors, and in which are installed launcher-type suspension equipment. About 150 such installations are under construction or have been completed; the Soviets say they are new, hardened ICBM launch control centers. But the earlier control centers have not been dismantled. Once the silo doors are in place, U.S. satellites can not determine to what use the installations have been put. It is inherently unlikely that the Soviets could covertly install ICBM's in the holes as long as periodic photo coverage of the installations was assured; nor is it probable that the Soviets would attempt the covert installation of missiles while there remained a remote possibility of detection by means of satellite overflight. Nevertheless, in the absence of assured coverage by U.S. photo satellites, the Soviets probably could rush missiles into launch positions, replace the doors, conceal or obscure the residual signs of the installation, and thereby come into possession of 150 to 200 more ICBM's than were charged against their SALT-regulated totals.

Alternatively, were some separate provisions made for the emplacement of radar equipment, it is conceivable that the Soviets could put boosters complete with multiple ABM warheads in the III-X silos. Earlier studies have indicated that some Minuteman could be so modified, were the United States inclined to make Minuteman fields self-defensive. The notion is not so novel as to be beyond the conception of Soviet planners. What would be required to make it feasible is no more than assurance that no American photo satellites would pass overhead while the operation was in progress. Perhaps it is more reasonable to conclude that the silo-command center installations are indeed silos and that they were built to provide for a near-instantaneous upgrading of Soviet ICBM strength in the event of SALT-I abrogation--by either party. Whatever the rationale, it is not likely to become apparent to a reconnaissance satellite collecting photographs, and there seems little probability that Soviet communications security would be sufficiently loose to permit word to leak out by way of in-the-clear messages.

What is important in this instance is not necessarily that a potential for breakout may have been created. Adding 150 to 200 additional ICBM's to the Soviet inventory would be destabilizing, but it is not likely to give the Soviets anything resembling a dominance in strategic weapons. An

effective ABM system could be quite another matter, which suggests that the better part of wisdom would be to keep an eye cocked toward tests of anything that might be turned to ABM purposes and to pay particular heed to any construction that might represent site preparation for the rapid installation of ABM radars. What may be more critical is that we have not contested the assertion that installations that look like silos are actually control centers, or that they could not be rapidly converted to silo uses if the Soviets so desired. The highest risk may lie in the possibility that "control centers" could be clandestinely converted into launch installations for ICBM's or even ABM's during an interval of inaction by U.S. satellites.

Soviet capability to destroy American satellites is unquestioned, but as yet we have no real fear that destruction could be accomplished without alerting us to its source. There is no obvious advantage, other than that of getting a head start in a new arms buildup because convertible installations are available, to killing American satellites openly and then proceeding to convert "command centers" into real missile sites. But there could be a considerable advantage to interrupting American surveillance by means that could not confidently be ascribed to Soviet actions, then converting the installations and concealing the evidence, and thereafter accepting the resumption of surveillance.

The evidence of the III-X silos alone suggests very strongly that continuity of U.S. coverage can not be allowed to lapse for an extended period. We do not appear to have evidence that "command centers" are indeed dual purpose, or that any preparations have been made to stockpile missiles or develop ABM's for future placement in them. Intent is not credibly determinable. But if the Soviets have indeed chosen to proceed along lines of preparing for a rapid buildup of some uncertain capability and have been obliged by the obviousness of construction signatures to disclose the existence of dual-capable installations while denying the capability, it is also conceivable that other and more concealable installations are under construction elsewhere. Were that the case, an interruption of surveillance that was anticipated by the Soviets could provide the opportunity of any number of adjustments of the Soviet strategic force structure. The best that the United States could hope for would be to discover the buildup upon the resumption of surveillance. A worst case could include a non-attributable interruption followed by a refusal to permit surveillance to resume once the United States regained the capability for it. The worst case presumably would involve an ineffective resumption of surveillance after the evidence had been appropriately disposed of and the completed installations concealed or camouflaged.

For all such scenarios, the only certain protection for the United States would be clear assurance that no lapse of coverage could extend sufficiently to allow the completion of a clandestine deployment. That means having a sufficient stock of backup systems to fill the gaps created by two or three successive failures or, alternatively, a dedicated crisis response system sufficiently capable (in terms of coverage and resolution to return information at the required level of detail. Either announcing or demonstrating the existence of such a capability presumably would discourage the Soviets from attempting to exploit a contrived gap in routine surveillance. (A demonstration accompanied by a controlled leak of information probably would be the best mechanism, but that is a matter for consideration in the event, not in the anticipation of it.)

Problems of resolution and coverage requirement have troubled most proposals for the development of a crisis capable system. And most have been dismissed, in the end, on grounds of unwarranted cost. For a system adequate to the needs of verification during a breakdown of the ordinary surveillance process, it is likely that both high resolution and broad area coverage would be needed, the first to inspect the details of suspect installations, the second to identify suspicious sites. In fact, such a system does exist in concept and probably could provided appropriate advance measures were taken. GAMBIT can actually be flown at relatively

low altitudes; in the 1960's, quite by accident, GAMBIT was successfully operated at altitudes of less than 60 miles, and the returns were quite good. That expedient presumably could be employed deliberately as a device for enhancing the already respectable resolution of GAMBIT, were ground details at the extreme capable of operating, at least marginally, in an area-coverage mode. In 1970, when there appeared to be some possibility that the inventory of CORONA satellites would be exhausted before HEXAGON became reliably operational, the National Reconnaissance Office sponsored the development and fabrication of "HIGH-BOY" and "HIGHERBOY" kits which, when installed in a GAMBIT reprogrammed for operations at altitudes above 300 miles, would provide adequate area coverage.

Were minimum cost to become an objective of a crisis capability reconnaissance system, GAMBIT might be ruled out. In that case, a cheaper (but nonetheless costly) course could be to build a small set of CORONA-style satellites adaptable to launch from any of several expendable boosters which could be kept in ready storage for several years. The frequently proposed but never approved CORONA J-4 system probably would represent a reasonable starting point; in combination with Thor boosters it might serve the intended purpose quite capably. But again,

those are details for resolution in the event of a policy decision that investing in a backup or crisis surveillance system is intended worthwhile.

Quite apart from the problems posed by the possibility of Soviet interference with American verification instruments, overt or covert, lies the issue of third-party interference. Two classes of events require consideration: successful attempts by some third power to prevent surveillance of its territory, and the side effects of upper-atmospheric tests of nuclear weapons by a non-signator to the test ban. Either could put both Soviet and U.S. satellite systems out of commission for considerable periods.

Like the Soviets, the Chinese vigorously oppose activities they classify as espionage. They appear to be aware, at least in a general way, of the capability of satellite reconnaissance. Placement of their initial missile sites, their manner of conducting nuclear tests, and efforts to conceal troop and equipment deployment details testify to that. Although it seems reasonable to believe that the Chinese would refrain from interfering with American reconnaissance satellites on grounds of self interest (in the present political alignment, the United States would probably warn

the Chinese of any major buildup of Soviet forces along the Sino-Soviet borders), that situation could change radically with a realignment of internal Chinese policies.

It is, for all practical purposes, quite impossible to overfly the Soviet Union by satellite without also overflying China. In the instance of a Sino-Soviet reproachment, would the Chinese consider interfering with American satellites, perhaps using techniques or weapons provided from Soviet inventories, while permitting Soviet satellites to operate unchallenged? The ideological argument that American satellites are conducting espionage while satellites of the Socialist Coalition are merely protecting world interests is not impossible of composition.

A second prospect is that the Chinese might conduct an upper atmospheric test of nuclear weapons as part of a long-range program to develop an ABM capability. Most American (and presumably most Soviet) satellites are subject to degradation from the effects of passage through the debris of a nuclear explosion.* In particular, film-carrying satellites

[redacted]

would be affected adversely. The Chinese might simply ignore such possibilities on the grounds that their interests required such tests and that consequences for satellites were not their concern. Or they could consciously decide to undertake such tests, fully knowing the consequences on the basis of reasoning that degrading Soviet reconnaissance returns was more important to the Chinese than any consequent rundown of American capabilities. The calculation of intent and motive is complex and, moreover, is subject to fluctuation as Chinese policy perceptions change in the post-Mao era.

IV. INSTITUTIONS AND TECHNOLOGY

None of the reconnaissance devices now in the U.S. inventory was originally conceived of as a verification instrument.

No extended review of the requirements process that nominally preceded a decision to proceed with the development and deployment of current satellite systems (the core of the "National Technical Means") is possible here, nor is one needed. But a brief summary of the decision processes that typically attended the introduction of such systems as

satellites), GAMBIT, HEXAGON, and KENNEN may be useful.*

Basically, institutional and technological preferences of several kinds have tended to dominate the "requirements" for various reconnaissance satellites. National Security Agency predilictions for [redacted] while the development of a technical capability to collect the fine details of telemetry (and some communications intelligence) was responsible for the decision [redacted] HEXAGON selection was the end product of a competition between a proposed system then called FULCRUM and a somewhat less ambitious system known as S-2. HEXAGON was the first system developed wholly by the CIA; had its competitor been selected, CIA satellite development capability probably would have disappeared. KENNEN was eventually approved for development, after having temporarily cancelled in favor of a film-readout modification of GAMBIT, mostly because the CIA sponsors of KENNEN were considerably better at controlling the decision process of the time. [redacted] POPPY systems (EARPOP) in the inventory because the Navy desperately wanted a capability

* Details may be found in a multi-volume History of Satellite Reconnaissance prepared for the National Reconnaissance Office between 1964 and 1975.

for conducting sea surveillance and counting ships, [redacted]

[redacted]

[redacted] or because the United States had a pressing need for better radar-order-of-battle information. No U.S. reconnaissance, surveillance, or montioring satellites were developed solely in response to a formal requirement originated by the United States Intelligence Board or the President's Foreign Intelligence Advisory Board or any predecessor or successor organization. "Requirements," when they appeared, tended to be expressions of desired system performance phrased in terms of some newly conceived or recently tested technological capability.

Thus, verification, when first considered wholly in light of what "National Technical Means" might support, was viewed as an alternative application of an existing capability. Perhaps the nature of the verification process, as then perceived, made that inevitable. But the trend of satellite reconnaissance system evolution has made that an increasingly complex calculation. In 1967-1968, when for all practical purposes the United States concluded that the Soviet Union would never agree to effective on-site inspection to police arms limitations agreements, CORONA and GAMBIT were photographic reconnaissance satellites of the time, communications

intercept was minimal (from satellites), and the balance of ELINT collection dealt with radar order of battle and technical data collection. CORONA and GAMBIT launches were relatively frequent (they were gradually tending down from a rate of one a month), most systems were comparatively inexpensive (CORONA cost about $10 million, on orbit, per launch), and reprocurement needs were sufficiently large to warrant to the creation and maintenance of a sizeable reconnaissance satellite production capacity. HEXAGON was an order of magnitude more capable than CORONA, but it cost more in about the same proportion, and rather than being replenished at two to four-week intervals, it was destined to remain in orbit for three months. The progression to an improved GAMBIT was along the same lines: the system became more costly, more capable, in terms of resolution, and lived longer (90 rather than 30 days). KENNEN is intended to be still better than HEXAGON [redacted]

[redacted]

[redacted]

If one were writing requirements for an imaging satellite system capable of verifying the terms of the existing strategic arms limitation agreements, would he settle on systems resembling HEXAGON, GAMBIT,

and KENNEN? The answer might be yes. Indeed, a KENNEN system that performed in accordance with expectations probably would be sufficient to verify the status of missile silos, submarine construction activities, and ABM installations of the conventional sort. But that answer would have to be qualified to some extent by anticipations of Soviet actions. If but one or two HEXAGON and GAMBIT systems are to be procured and launched each year (and perhaps only one or two GAMBITS, in all), and KENNEN

[redacted]

[redacted] there is in effect no reserve for contingencies. The accidental demise of one satellite will create a gap in coverage; two successive KENNEN failures could be calamitous if no HEXAGON were available to be sent into orbit; a combination of KENNEN and GAMBIT failures could well create a massive gap in coverage. (The four-month gap during the mid-1960's was treated as a crisis.) Thus a realistic requirement for verification via reconnaissance satellite would almost surely take account of the need for providing against gaps in coverage, however caused, for both high resolution and area coverage. Finally, the requirement would have to take adequate account of replenishment questions; something would have to be made available to go on with if the principal resource for verification were temporarily withdrawn.

Alternatively, a requirement would have to consider vulnerability and its influence on both the nature of systems and the prospect of providing substitute capability were the primary systems to be incapacitated.

What institution will support requirements of that sort? In theory, the United States Intelligence Board (or its replacement) should do so. But USIB-style organizations have for 15 years been the captives of attractive technology. One particular problem arises in the relationship between the USIB and the Central Intelligence Agency, which is not merely the intelligence using agency but also assesses reconnaissance system requirements and is the advocate-developer of reconnaissance satellites. Except casually, the Arms Control and Disarmament Agency has had no effective voice either in the "requirements generation" process or in the selection of systems. Verification may not be the paramount justification for maintaining an effective satellite reconnaissance capability, but it certainly has a better claim to that status than do some of the more time-honored "requirements."

The rationale for dedicating a satellite system to verification purposes was first worked out more than 15 years ago. It prompted the assembly of numerous studies and analyses some 10 years ago, but became increasingly less influential thereafter.* The justification seemed inadequate. But if breakout is now viewed as a potentially serious threat to the continuing security of the United States, then it follows that many--even most--of the classical tasks of satellite reconnaissance may have more current relevance to verification than in the past.

There would appear to be some value to a dispassionate evaluation of the national requirements for dedicated verification devices with emphasis on satellite reconnaissance systems, taking account of contingent requirement

* See, for instance, ACDA memo to DepSecDef/ISA, 18 Feb 1963; a five-volume study titled, "Project Fair, Observation Satellites for Arms Control," was available in 1965; NRO studies of an "Arms Control Satellite" were underway in the Spring of 1969; extensive studies of the capabilities and limitations of existing reconnaissance satellites in arms control and verification applications were undertaken by the Electromagnetic Systems Laboratories (for the CIA) in 1969 and continued into 1975.

for capabilities, for assessing the vulnerabilities of current and proposed systems, and for insuring the continuation of both broad area and high resolution coverage in the event of a temporary breakdown of the principal reconnaissance systems.

Even more fundamental is the need for a reassessment of the rankings of various requirements, including the requirement for data relevant to the verification task. Can validation needs be adequately satisfied by drawing on the fund of intelligence collected in pursuit of technical intelligence and strategic disposition information? Again, the obvious answer would appear to be "yes, if..." The "if" covers that intangible quality of assured coverage, security from serious degradation of returns, and insurance against interruption (or the effect of interrupting routine coverage).

V. FINDINGS AND IMPLICATIONS

This section of the report has addressed questions having to do with requirements for verification, with U.S. capabilities for providing credible indications of Soviet actions (and to some extent, intentions), with the perceptions and the probabilities of adequacy of verification, with vulnerabilities, with a range of potential responses to perceived inadequacies, and with some of the practical (institutional and technological) problems of response. It has been addressed, in all instances, to those aspects of the verification process that bear on the possibility of a Soviet breakout.

Fundamental to U.S. acceptance of the strategic arms limitations agreements of the past five years has been the premise that U.S. National Technical Means of verification will adequately satisfy the national interest. That premise arises in several widely accepted, interrelated assumptions. The first is that U.S. "National Technical Means"--by which is principally meant reconnaissance satellites--are technically capable of detecting and confirming any Soviet attempt to evade the agreed arms limitations. The second,

which arises in the first, is that the non-interference clause is largely self ensuring: undetected active interference with American satellites will be so technically difficult as to pose great risks of disclosure while the political consequences of detected active interference would be unacceptable to the Soviets. It is further assumed that a growing Soviet dependence on satellite reconnaissance (and other space systems) will discourage any Soviet efforts to interfere with American satellites.* A final assumption, woven through the others, is that sending American reconnaissance satellite capabilities will provide adequate insurance the success of any Soviet effort to exploit developing concealment and deception capabilities.

Nonetheless, a variety of political and technological opportunities for compromising the adequacy of American verification capabilities that do exist have been suggested here. Some arise in the terms of the arms limitations

* One aspect of the calculation that has not been addressed here is the credibility of a U.S. response to Soviet attacks on American satellites. In fact, no effective U.S. anti-satellite system currently exists, although proposals for its creation were being evaluated in 1976. But the prospects of war in space lie beyond the scope of this study and have therefore been ignored.

ref 333?

agreements, or interpretation of those terms. The Soviet Union has repeatedly demonstrated that it does not consider itself bound to honor the terms of any unilateral U.S. interpretation of those agreements. The case of the III-X silos--or "control centers"--is informative. The Soviets carefully observed the mutually agreed restrictions on building new silos, but the "spirit" of the prohibition was ignored. Similarly, the Soviets agreed to limit increases in the sizes of dimensions of existing silos to 15 percent, and did so in the case of the replacement of SS-11 by the SS-19--but the unilateral U.S. statement that an increase in the volume of the missile by 30 percent or more would be viewed as a breach of the "spirit" of the agreement was dishonored. As Secretary Schlesinger put it, "... there is a violation of our interpretation of our unilateral statement, but I am not sure what binding force that has on the Soviets."* The Soviet Union has evidently observed the letter but is unconcerned about variant interpretations.

* Hearing before the Subcommittee on Arms Control of the Committee on Armed Services, United States Senate, 6 March 1975.

Among the politically uncertain elements of the arms agreements is that arising in the lack of a definition of "National Technical Means." The Soviet position on the distinction between espionage and verification may well be critical. Concealment clauses are also vaguely specified--by design.

In a technological sense, the increasing complexity, fragility, long on-orbit lifetimes (coupled with consequent long lead times for replacements), and costs of U.S. reconnaissance satellite systems, when viewed in the light of improving Soviet capabilities for interference with those satellites, could have ominous implications for the future.

Such circumstances provide both openings for Soviet exploitation of opportunities that may arise and invitations to explore the openings. They also serve to identify vulnerabilities in U.S. positions, policies, and technologies. So long as the Soviet Union credits the assumption that U.S. National Technical Means of verification are adequate, no major effort to subvert them is likely. But it is also reasonable to assume that past Soviet performance is a good guide to the future, and than an obvious and easy opportunity

to subvert American capabilities will be explored. The United States has no present means of assuring that subtle Soviet interference with the functioning of reconnaissance satellites will be promptly detected, and (more important) no real capacity for promptly replacing satellites that for uncertain reasons have become disfunctional. A lengthy gap in coverage of Soviet strategic weapons dispositions would be alarming enough in its own; a gap anticipated--or precipitated--by the Soviets would provide what might be an irrestible opportunity to emplace new strategic weapons without detection. Were that emplacement subsequently concealed, the Soviets could acquire a lasting and appreciable strategic advantage: mobile ICBMs, a significant enhancement of ABM capability, or the deployment of massively improved ICBMs would represent such an advantage. Were such an emplacement impossible to conceal after it had been completed, the Soviets would at least acquire a momentary advantage and a major lead in a new arms race.

No existing U.S. instrument of verification was designed for that purpose, though they adequately serve present and past needs. Future needs may be quite different. The requirement for verification adequacy may not be satisfiable,

in the long term, by continued reliance on systems designed to serve diverse national needs that were defined without much concern for verifying Soviet compliance with arms limitations agreements. At the least, the requirements process should be reviewed to ensure that the principal needs of verification have been given adequate weight. In particular, there appears to be a valid need for readdressing the requirement for a backup system (or systems) that could be called into service if one or more surveillance satellites are incapacitated. Adequate technological resources still appear to be available, although the course of satellite development makes their continued survival uncertain: by 1980, if present trends do not change, the capability of creating and producing a backup satellite system may have been compromised.

The existent arms agreements do not, of course, inhibit the development or deployment of strategic weapons not covered specifically by the terms of those agreements. The ability of U.S. analysts to interpret the intent of and to discern the proposed applications of novel Soviet technological developments does not seem to be improving with the passage of time. That, too, may become troublesome in five or ten

years. It could become particularly troublesome if, at some near future time, the United States were to be wholly reliant for verification purposes on one or two verification systems that were vulnerable to unattributable degradation or interruption of service, of that could be precluded from adequately performing their assignments.

In the end, it would seem that many of the principal assumptions about the long-term adequacy and credibility of U.S. verification processes are flawed. Technological opportunities for Soviet interference are improving, the probability of being found out is diminishing, the penalties may seem smaller as the advantages of a successful breakout become more attractive, and the range of potential U.S. responses to interference with National Technical Means is narrowing through the winnowing away of system options.

Whether the Soviet Union might choose to act on opportunities and vulnerabilities of that sort depends on more than perceptions of technology, of course. The excuse or justification presumably would arise elsewhere, in the complex political, economic, and diplomatic developments of a troubled international age. But if for some reason the Soviet Union should elect to explore the opportunities for

upsetting the strategic balance without necessarily alerting the United States either to the decision or to subsequent enabling activities, a Soviet perception of vulnerable U.S. verification processes and technologies could only serve to encourage a breakout decision. Offsetting any Soviet perception of such U.S. vulnerability may be as important as the reality of assured U.S. means of detecting a Soviet breakout attempt in its embryonic stages.