

Toward A Basis For Exploiting
Intelligence In The National Interest

"National Security" and "National Interest" are terms which, if each is defined very broadly, can mean essentially the same thing, and if defined very narrowly can mean "guns" and "butter." A mix of these two extremes, put in perspective, can be helpful. In an unthreatening world, no effort (cost) would be expended in defending one's self; in a very threatening world, all one's effort would be expended on self-defense and if defenses were inadequate, extinction would result. In fact, reality is a mix of proximate and remote risks and benefits of such a variety that trade-offs are made in the expenditure of effort as between "interest" and "security." Interest and security are coupled in this view: immediate threats to security are met, at a cost to interest, with "off-the-top" resources; remote threats are created or discounted in the pursuit of interest.

As a way of quantifying this, I postulate that, on a scale of value appropriate to both "interest" and "security," an action which causes a gain in the interest metric by one unit can in turn decrease, with some probability and at some future time, the security metric by more or less than one unit -- all conditioned by intervening events. If one must buy back on the security value scale the cost incurred then, if the present value of the interest gain is greater than this buy-back cost, the earlier decision was a good one; otherwise it was not. Thus if there is a potential cost due to national security risk resulting from a prospective national interest benefit, proper questions are

- What is the cost associated with the risk?
- When is it likely the cost will be incurred?
- What are the conditional (scenario) probabilities associated with these two questions?

An example might make this concrete: the contribution to national income derived from the sale of high technology (computers, large scale integrated circuits, etc.) processes and factories to the Soviet Union is clearly in the national interest. Such a sale makes American jobs, moves American influence overseas to a "denied" area and improves American world prestige for the implied Soviet deficiency in the technology area. However, such a sale is conceivably even possibly contrary to national security. Computers and integrated circuits are the sine qua non of efficient and effective modern weapon systems which can threaten American national security.

It is the speculative nature of the foregoing paragraph which is important: what is the national interest and what -- with some precision -- is the threat? There has been since at least late 1971 an apparently sincere effort by both policy-makers and the intelligence community to work together effectively on energy, economics, narcotics, terrorism, and the like. At the same time, however, there is a prevalent unease or dissatisfaction that an adequate job was being done.

I assert that progress has been slow for two reasons: we have not made systematic the comparison of national interest values and national security values, and as a consequence, we have not had the confidence required to move large amounts of resources to national interest related intelligence; on the other hand, the national interest community -- that identified by the codeword "butter" -- has not structured itself to use abundant and complex intelligence relating to interest.

These two value systems are now separate and the way to change the situation is to tie them together by a mutually regenerative feedback between them. It appears that the intelligence community is willing and capable of responding to the needs of the "interest" community. If circumstances are left as is, an evolution in each community will take place with the result that better intelligence will be provided and it will be used more

effectively. We could, however, short-circuit this evolution by adapting a national security process known to be effective -- some see it as too effective -- to national interest problems.

What follows is a synthesis of the elements of the national security (military-industrial complex, MIC) process. It is the working of this process which as a byproduct develops DoD inputs to NSSM studies; the result of which is an assessment of policy options. To the degree that the non-DoD inputs result from similarly disciplined processes, NSSM study results are balanced. In an area where options are conditioned by both national security and national interest (e. g., where both an NSSM and a CIEPSM are required for implementation), it appears that all inputs are not so rigorously arrived at. The suggestion is therefore that the national security process should be adapted to clarifying "national interest" policy options.

1. Threat perception is the starting point initiated or suggested to the policymaker. It leads to customer intelligence requirements of a general nature as in the DCI's Key Intelligence Questions and generates the necessary, permanent process of their development. These general requirements lead to:
2. Intelligence acquisition through the intelligence process (requirements and priorities for collection, processing, production and analysis and dissemination). The intelligence acquisition permits a threat description not complete in all dimensions but providing a basis for:
3. Threat definition in the context of the customers' perception of the threat. The definition may be elaborated in an informed community in and out of government (e. g., MIC), which then puts forward:
4. Systems* concept formulation to gain capability for countering the defined threat. The conceptual

* System is meant to connote either hardware or software (i. e., organizational or logical) constructs which produce deterministic results.

countering systems might by class be offensive, defensive or non-competitive and must be proved by state-of-the-art assessments and by systems analysis. When realizable or very probably realizable systems are identified then:

5. Cost/benefit calculations based on net assessment (i. e., system analysis of A's "threat" vs B's "counter" in which responsive strategies are permitted to develop) should be carried out. This mandates establishing a value system or "metric" for assessing and/or rationalizing various kinds of costs, risks, and benefits. When the costs and benefits of candidate approaches (systems) are identified they could become inputs to the NSSM/CIEPSM study and provide the basis for identifying policy options. In any event, when the cost-beneficial system (or class thereof) is found, then:
6. System definition (specification) in terms of performance, cost, schedules, reliability, risks, initial operating capability, etc., is made, and agreement is reached (a contract made) with the organization responsible for actions leading to the capability.
7. System RDT&E* is an iterative process of items 1-6 above leading to a prototype system on the one hand and incidentally a better understanding in the intelligence process (#2) of the threat indications. Conditioned by the system's being hardware or software, the prototype might be an "all-up" copy, a "breadboard" or "brass board," an operating mock-up, a new computer simulation or a "game." When the system meets defined specifications adequately, then given a decision to go ahead:
8. System procurement is implemented: for hardware systems, replication might be large; for software systems, final procurement could have been accomplished in the RDT&E phase, i. e., in obtaining the prototype. Finally:

* Research, development, test and evaluation

9. System operation and maintenance (O&M) is carried on.
Some monitoring of O&M is required to assure that the desired objective (countering the threat) occurs and that costs and benefits are as assessed or that discrepancies are understood and corrected if possible.


Clearly, the foregoing process is too elaborate if the national interest is getting a negotiator ready for a GATT meeting. However, the organized approach it conveys is appropriate to enduring, complex or chronic problems relating to national interest. How to propagate such an approach is not evident. The NIO's and the ICS as DCI bearers of different aspects of intelligence community interests could -- given highest level support -- be the catalysts for change toward the relevant aspects of the structure shown above. The present time of flux in the intelligence community and in the government is a good time to start trying.

Office of the Director
of Central Intelligence

May 7, 1974

Messrs. Slighton and [redacted]

[redacted] Attached is a note to me from [redacted]
[redacted] To be blunt, it reinforces my prejudice
that systems analysts should be seen and not
heard. [redacted] got Leo Cherne quite stirred
up with his suggestion that we (i.e., the DCI)
ought to organize an "intelligence-industrial
complex" to serve functions (beneficial in
[redacted] eyes) similar to those now performed
by the "military-industrial complex." It took
me several minutes over the long distance
telephone to get Cherne off the chandelier and
reassure him that this brain storm [redacted]
was neither stimulated nor endorsed by
Mr. Colby or anyone else I had encountered
in the DCI's office. After you have had a
chance to look over this paper I would like to
discuss it briefly.


George A. Carver, Jr.
Deputy for National Intelligence Officers

→ SAC Chrono
1- RA

STAT

STAT

STAT

STAT

STAT

STAT

STAT

MEMORANDUM FOR: Mr Carver
George - attached is a paper I wrote a few weeks ago after some conversations with Leo Cherne of PFIAB. Maybe it would be of interest.

[Redacted] 4/18
(DATE)

ME - please send this in with your packet

FORM NO. 101 REPLACES FORM 10-101
AUG 54 WHICH MAY BE USED.

Thank, J. (47)

STAT