

~~SECRET~~

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

Warning and Crisis Management

[REDACTED]

~~THIS ARTICLE IS CLASSIFIED SECRET. HANDLE WITH CARE. CONTAIN ONLY IN ITS ENTIRETY.~~

Editor's Note: Mr. [REDACTED] presented this paper in the Friedman Auditorium on 26 October 1983 as one of the featured speakers during "A Special Fall Conference on Crisis Management" (24-28 October 1983), sponsored by the Communications Analysis Association. We feel that Mr. [REDACTED]'s comments on this topic—of extreme importance within the intelligence community—will be of interest to many of our readers.

1. INTRODUCTION

You see standing here before you a survivor of an unusually large number of crises which have faced this country since 1960—almost a quarter of a century. As an Arabic voice transcriber here at NSA, I was directly involved in [REDACTED]

[REDACTED] I was involved in the Cuban Missile Crisis and the U-2 shootdown as a senior reporter and briefer; and in the problems of Algerian independence as a section chief; and then at the White House coping with the '67 Arab-Israeli War, the Czech invasion, the EC-121 shootdown, the Sino-Soviet fracas at the Amur River which was followed by the Cultural Revolution, the Indo-Pakistani War, the capture of the *Pueblo*, the Vietnam War; and then returning to the National Sigint Operations Center (NSOC), the fall of Saigon, the tree cutting incident in the DMZ and the first KAL shootdown. I managed to miss direct involvement in the Iranian hostage crisis, Poland, and the Falklands, but I was discovered having fun in T and was brought back to the Warning business in time for the continuing crises in Lebanon and Central America, the death of Brezhnev, and the most recent KAL shootdown. There are undoubtedly many others that I've overlooked, but the point of the litany is that I have seen many of these crises firsthand and from differing perspectives: as an analyst, reporter, briefer, manager, user, and now something undecipherable called a National Intelligence Officer for Warning.

If there is anything that characterizes these crises, it is the fact that they were all different. Most were described as having at least elements of intelligence failure; and with each crisis the focus of U.S. activity was different, moving from the White House, to the Department of State, to the JCS, to nowhere in particular.

In my presentation to you today, I want to discuss the close correlation between "warning" and crisis management, to try to put the "failures" of the past in some perspective. I want to demonstrate that this is not 1941 and that we have reasonable confidence that a "Pearl Harbor" will not recur. As a matter of fact, I would like to dispel the myth of Pearl Harbor, which continues to color our approach to crises. Finally, I want to talk very specifically about crisis management, what it means and what still must be done.

2. WARNING DEFINED

When we speak of Warning, we are referring to a communication of a threat implicit in a wide spectrum of activities by nations, ranging from prudent defense preparedness through substantial force structure and readiness buildup to acts of political, economic, terrorist, or military aggressiveness.

~~HANDLE WITH CARE. CONTAIN ONLY IN ITS ENTIRETY.~~~~SECRET~~

As forces improve, modernize, and change structure, opposing forces respond, and the balance, as well as the resultant force potential, is measured against the most recent assessment. In the broadest sense, the existence of standing military forces, some of which are at a high state of readiness, demands continual reassessment because this tends to reduce the amount of major additional mobilization required. This iterative process changes the threshold against which threats, and thus warning, are measured. To avoid a blurring of the impact of the total change, warning goals must be defined across a spectrum of time and events. As such, the warning process and definitions provide a baseline to view holistically the changing environment. The resulting complex warning situation will still be characterized by ambiguity, incremental development and reassessment, and incremental warnings to decision makers; but it will have data points over time that facilitate our examination and judgment.

The critical part in the warning communication that brings the threat, the assessments, and the significance of the changed environment together is action by the decision maker. The leader must weigh the evidence provided him against the risks of being wrong and make his personal decision. In this sense, the completion of the warning process cannot occur until the principal policy official decides that it should. In essence, the capstone of warning is a policy decision; not an intelligence one.

One of our major dilemmas in Warning is that the constant search for early warning results in a warning process that trades certainty for time. Warning that is given early is almost certainly ambiguous, but it provides time for developing and executing courses of action that are low in cost and high in probability of crisis deterrence.

As warning assessments become more certain, policy makers focus on crisis avoidance or crisis containment, but the costs and opportunities lost increase rapidly. In the most unambiguous warning—an attack is being executed—decisions are limited by the crisis to a reactive set. Options, choice of forces and resources, planning time, and political maneuver are minimized, and the cost of mistakes may be extreme.

Strategic Warning

Within the spectrum of warning there are two categories that have historically been the focus of attention—strategic warning and tactical warning. These are DoD/JCS definitions. Strategic warning is a notification that enemy-initiated hostilities may be imminent. This notification may be received from minutes to hours, to days, or longer, prior to the initiation of hostilities. This accepted definition is useful only in the generic sense. It is deficient because, first, a notification can be a one-way conversation or an intelligence product without a guarantee or recognition, understanding, or feedback. That is, we in the intelligence community shout out the door “here they come” and then retreat back to our barbed wire and cipher-locked sanctum sanctorum. It is also directed primarily at hostilities without consideration of the war preparations necessary before hostilities can start.

Tactical Warning

The accepted definition of tactical warning is a notification that the enemy has initiated hostilities. Such warning may be received any time from launching of the attack until the battle is joined or the weapons arrive on target.

The definition of tactical warning is so absolute—the bullet has been fired, the attack has been launched—that it is virtually no warning at all. Therefore, it is necessary to expand the definitions to encompass the preparations for conflict which may begin years prior in

weapons research. To expand the warning concept, it is necessary to talk about *warning of a developing crisis*, *warning of war*, and *warning of attack*.

Warning of a Developing Crisis

The first of these, *warning of a developing political or economic crisis*, is a communication about a political or economic event which may or may not be induced by external forces, but which heightens instability sufficiently to destabilize a country or region, or may result in consequences inimical to U.S. interests or security. The national actions that occur in a developing crisis are often related to military capabilities.

In a growing crisis, for instance, we would foresee Soviet preparations to defend their interests, to take a stiffer political or economic stand with demonstrations of force readiness, to achieve a better bargaining position in the crisis, or to divide NATO's political integrity by taking actions in another theater—particularly one where U.S. and NATO security interests seem to diverge.

Warning of War

Warning of war is the communication of a judgment that a state or alliance intends, or is on a course that risks, war and is taking measures to enable it to go to war. This communication concentrates on the national decision to prepare a nation or an alliance for war, as well as on other actions deriving from this decision which are not of a pure military nature such as propaganda, civil defense, unconventional warfare, economic sanctions, weapons developments, and mobilization.

The decisions to prepare for war are deliberate and most likely to follow a long period of extensive planning. In Europe, where forces are in relatively high readiness and economic and military contingency planning is the norm, the first political decisions to prepare for war have already been made. The extent of contingency preparation over an extended period of time could facilitate a decision toward war because the capability to employ military force is planned and an executable course of action is defined.

We believe that warning of war will be a series of incremental warnings; the judgments will be tentative, and uncertainties will be relatively high as to the purpose of the preparations. There is not likely to be early community agreement as to their meaning. Only when the predominantly military phases begin will the climate for a coordinated warning be established. Even so, the warning of war should provide evidence on the nature of the decisions made, the extent of measures underway to convert to a wartime footing, an estimate of when measures will be largely completed, and a judgment about when the Warsaw Pact will be ready for hostilities.

Warning of Attack

As noted, *warning of attack* is a communication about the activities of the armed forces of an adversary state or alliance. It communicates intent declaring that the adversary intends, and is preparing its armed forces for, an imminent attack. The information in this warning must be more precise than that in warning of war if it is to support action to cope with a more specific harm.

This warning is affected by the threshold established in the iterative process of assessment and reassessment. If the force available for war is more ready or more capable, then the margin of warning is changed and warning must be given earlier to be effective as a tool of policy makers.

~~SECRET~~

For example, there is general community agreement that plans for attack on NATO exist. If the ability to carry out these plans is enhanced by improvements in force capability, then the stability of the situation is changed if the perception of a military advantage is established. Therefore, warnings cannot be based on instantaneous assessments. They must be grounded in trends, capability growth over time, and developments that forecast intent to act. Warning of war should assess the ability of the adversary to implement plans and how a scheme of attack may be fortified by a change in the use and capabilities of forces.

We are confident that certain key military activities, such as the pattern of movement of ground force units to initial combat positions, would allow us to predict the likely scope, location, and timing of such an attack; but this warning of attack would come relatively late in a crisis since it would be based primarily on observable military force activities.

This type of attack assessment would be the major concern of intelligence and other policy makers following the initial warning that the Warsaw Pact was taking steps to go to war in the near future.

Acceptance of Warning

The *acceptance of the warning* that is given is a final step in the process which draws upon the information-gathering machinery of government to develop coherent evidence of the likelihood of an event of great concern to national policy makers. The process culminates in the mind of the decision maker when he is persuaded that the likelihood of the event is so high that he should set aside considerations to the contrary and take action to counter or to mitigate its consequences.

In the case of warning of war, pressures to disregard inchoate evidence of the likelihood of conflict are great. First, there is the risk of setting in motion precautionary measures which might be misinterpreted by the opponent as hostile acts, and themselves precipitate the conflict. Second and third are the economic and political costs of mobilization of forces to the nation for an event which may not transpire or which may be delayed. The risk of crying wolf to a political leader in a democracy are much greater than those incurred by a leader in a totalitarian society. Public confidence in the sagacity of a democratic leader is easily eroded by evident errors of judgment, particularly in matters of great moment, such as peace and war. In the final analysis, no warning occurs without a policy decision.

3. WARNING METHODOLOGY

There have been many cycles of warning interest including new approaches, postmortems, and the seemingly inevitable new organizations and reorganizations. But many of the old lessons are being neglected today, and genuine warning theory is in danger of being lost. Thus, some words on warning methodology are in order to help us understand the warning process.

In the past several decades, the major focus of attention was on avoiding surprise—a legacy of Pearl Harbor. This tended to shroud the real issues which are deterrence, avoidance, or containment of harm. Put simply, harm is the subject of warning, not surprise. Action by decision makers is our objective, as opposed to keeping people informed.

In the past, the subject matter of warning was almost exclusively military threats from Communist states. While the danger of surprise remains an important subject, the real warning issues are broader. They include military, economic, political, terrorist, and

~~SECRET~~

technological issues. They don't come in neat conceptual packages, but they all represent potential harm to the U.S.

The Cognitive Warning Cycle

International warning issues are best classified as gradual events, as compared to a domestic warning such as a flash flood or a tornado which is sudden. Common sense suggests that almost all warning issues are gradual. After every surprise or warning failure, events over time are explained and clearly seen by hindsight. If we are to predict potential harm, we must understand the *cognitive warning cycle*.

That cycle may be viewed as a six-step process. For intelligence analysts, it includes *recognition, validation, definition, and communication*. For decision makers, there is *evaluation and action*.

Before a warning can be given, a harm must be recognized. Most often harm is recognized, but judgment errors in dismissing the danger are commonplace.

Early *recognition* is often the weakest link in a warning system because of the limited information available in the earliest stages of a danger, the ambiguity of that information, and the intentions of the actors, as well as deficiencies in dealing with uncertainty and ambiguous evidence. Chronologies, case studies, pattern analyses, and indicator lists are all valuable aids to recognition. But the ability to recognize harm at an early stage hinges largely on a disposition to perceive change and discontinuity rather than on continuous and "normal" evolutionary sequences.

Validation is essential to insure that the recognized danger is genuine. It includes tasking additional collection and adding analytical attention to the issue. Once again, acceptance of a danger as valid includes complex processes, such as agreement about what constitutes a danger and applying evidence to an hypothesis, or forming a new hypothesis to accommodate new information.

Definition is the process of filling in the blanks about a danger, as to its nature, gravity, timing, duration, and probability of occurrence. At a minimum, these elements must be communicated in a warning, though they need not be quantified precisely. Most often they will be only partially known. Failure to touch on all elements risks generating confusion and lack of confidence in the decision maker who will instinctively seek sources that will satisfy his basic information requirement.

Research into the Pearl Harbor surprise generated much attention to *communication* and the related step of *evaluation* by the decision maker. It is important for intelligence organizations to recognize that these functions are vital to formulating the warning as well as to stimulating the decision maker. Communication within an intelligence agency and evaluation by its top management are almost simultaneous with the same functions in the decision-making chain. Moreover, the two interact throughout the duration of the event.

Communication between the warner and recipient is one of the factors that distinguishes warning from other intelligence analysis or production activities. A person's receptiveness to warning is influenced by an already formed outlook towards a problem. Put another way, *effective warning is a function of the amount of information which must be contradicted*. Since the object of warning is to stimulate action, a dialogue must develop between the warner and the audience so that they can gauge over time each other's vigilance tendencies, preconceived notions, and general expectations.

Evaluation is often done by planning or working groups who study the problem or by executive action to probe or test the situation. The effectiveness of this evaluation step is enhanced when the warners receive the information results flowing from tests the executive

~~SECRET~~

employs. These include diplomats, armed forces, business channels, and other resources outside the intelligence community.

In a sense *evaluation* begins the *action* step and shifts the focus to the executive or decision-making chain. The evaluation does not relieve the warner from issuing follow-up warnings; the decision maker probably does not believe the warning yet.

Though presented sequentially, the functional steps are best understood as nearly simultaneous, continuous, interactive, and iterative. Completion of the functional steps is likewise no recipe for warning success. Even in warning successes, invariably some of the information is misleading or wrong. Other successes result from being right, but for the wrong reasons. Nevertheless, one condition for success in a warning system is that its participants understand each other and their progress in coping with an issue.

Warning Outcomes

Let's change pace slightly and talk about warning outcomes. It takes no flash or brilliance to discern the three warning outcomes: *success*, *failure*, and *false alarm*. It is easy to reconstruct the cognitive process after the fact, once the outcome is apparent. The larger challenge is to employ insights to increase warning success. To do this, we need precise definitions and understanding of organizational handling processes.

Success. Warnings are intended to self-destruct. A warning is successful when the harm it predicts is deterred, avoided, or contained. When the prediction of harm is accurate and comes true, the warning has in fact failed. Warning success is not an information handling exercise; it requires action to cope with a danger. Long before the harm strikes, low-level actions can begin. When planners wait for clarity, they risk being overtaken by events.

Although too late for deliberate planning moves, a warning is still successful when it permits crisis managers to activate contingency plans and other prepared responses. By this time, the danger is likely to be both valid and reasonably well defined. Low-cost opportunities have been sacrificed for this clarity. Countermeasures against a more certain danger may be more truly aimed, but they will certainly be more costly.

The least effective and least successful warning is the notice just before harm strikes. Some equate it to "no warning" since the decision maker is still surprised. Those in the decision-making chain are placed in the role of damage controllers with barely enough time to react. Additionally, warning at this late time contains little margin for error.

Successful warning is more complicated than is generally considered. It takes into account the various roles played by the decision makers and their requirements for increasingly more precise information. The best chance for avoiding harm is when evidence provides a *reasonable basis* for action, not when the danger is likely to occur beyond a reasonable doubt.

Logically, gradually developing dangers should never give rise to surprise, but, ironically, the very action of providing repeated warnings reduces the likelihood that they will be heeded. Therefore we must discuss warning failures.

Failure. The ultimate warning failure would be a massive first-strike attack for which no warning was issued or for which the warning was ignored. This kind of total surprise, the ultimate systemic breakdown, is hard to imagine, despite the Pearl Harbor experience, because there would be a transition to crisis through a series of crisis issues.

False Alarm. Attempts to identify the developing harm lead to false alarms. False alarms are probably the most exaggerated of warning issues, primarily because the term is misapplied. A false alarm is a danger which has been identified but later proved not to exist.

~~SECRET~~

False alarms tend to increase skepticism about subsequent warnings and vigilance is not increased. Nevertheless, follow-up explanations help preserve the credibility of intelligence.

On the other hand, warning of a danger that proves to be a near-miss is a warning success, not a false alarm. The harm has been recognized and communicated, but some part of the warning was proven in error. Research suggests that near-misses increase sensitivity to warning by generating a sense of relief that leads to future vigilance. Actions taken to prepare for the danger are judged well taken in retrospect, provided the recipient knows the miss was a close call. Failure to distinguish a false alarm from a near-miss reduces credibility and raises the "cry wolf" stigma. Intelligence managers should be aware of the need to explain false alarms.

The most important thought about misses or false alarms is that we can be exactly correct if we wait for the missiles to be launched, but our job is to provide warning as early as possible and that introduces ambiguity and some misses.

The Problem of Repeated Warnings

The most difficult warning process is the repeated warning about a gradually developing danger. It causes a conditioning which reassures the recipient that the danger can be handled. When the harm becomes familiar, the decision maker is reinforced in his belief that actions already taken or under way will suffice. Repetition negates vigilance, the exact opposite of what warning seeks to achieve.

To sustain sensitivity, subsequent alerts must do more than repeat the original alarm. They must update the conditions: the danger has become more severe, the attack is expected sooner than before, the foe's readiness is greater, etc. Such language perpetuates vigilance and confidence in the warning medium.

In contrast, reports that give details about capabilities or threats which have already been reported may be good current intelligence but are poor warnings. The community's process of defining and refining the danger actually tends to undermine the effects of its warnings by conveying the explicit or implied message that the danger has not changed. The effect is to cancel the sense of alarm or heighten frustration.

Failure to exercise care so that the overall coverage has consistency and continuity postpones action until a gradual harm has gathered momentum. Warning success can be transformed into a warning disaster.

Institutional Handling Processes

The institutional processes that lead to success or failure are not well understood and are not predictable. One of the reasons for this is that the national warning system is a mix of formal and informal collectives, networks, and agencies, operating as a loosely grouped confederation. Nevertheless, most people in government think mainly of formal warning mechanisms when they are asked about the national warning system. What are they? In the formal mechanisms, two handling cycles are discernible: the mainstream and the sidetrack.

The Mainstream. In practice, completion of the analytical steps influences the attitudes of analysts and managers toward the warning issue—it builds consensus. Consensus governs the way a warning issue is handled by intelligence and presented to the decision-making chain. It also tends to insure that validation and definition are continuing processes.

When consensus is achieved early in favor of the existence of a threat, the warning issue will be treated in mainstream fashion. This means that it will be the center of increasingly frequent current intelligence coverage; frequent and exhaustive assessments, research reports, and estimates; and endless meetings, briefings, and less formal actions.

~~SECRET~~

However, a community consensus can simply be wrong, in which event the result is a complete surprise to the intelligence analyst and the decision maker alike. Mainstreaming may not guarantee a warning success, but it can contribute greatly to warning failures.

The Sidetrack. Sidetracked warning issues travel a low visibility road. Available information never gathers enough mass to displace the hypotheses and judgments which must be contradicted for the issue to enter the mainstream. Although some analysts remain concerned, the issue receives virtually no current analytic coverage and no extra collection.

The sidetrack process need not lead to warning failure any more than mainstreaming leads to warning success. However, when an issue moves along the warning sidetrack, the chances of institutional warning success are reduced unless some stark evidence is produced.

Informal networks, old boy nets, may be able to convey an effective warning by contradicting the consensus. Ironically, the informal warning system seems incapable of working well without the formal structures; the two seem to depend on each other for either to work. The various transitions by the institutional warning systems from routine business to increased vigilance seem to stem most often from informal actions or agreements through phone conversations, luncheons, and other informal "vehicles." The nature of the interaction is not clear and usually ignored in treatments of the national warning system. These points of tangency, however, may be the most important nodes in the system for achieving warning successes.

4. EXAMPLE OF A CRISIS: THE OCTOBER '73 MIDDLE EAST WAR

In our view, the lack of warning of the Egyptian attack that started the October '73 Middle East War was an intelligence failure which must be shared equally by the intelligence community and the decision makers. President Nassar declared his intention, in March 1969, to create a situation that would enable the Egyptians to cross the Suez Canal. He also explained his plan. First, destroy the frontal Israeli-Bar-Lev Line using artillery. Second, commandos were to cross the Canal and raid Israeli strongholds. Third, attacks on the Bar-Lev Line would be intensified and a penetration made to attack installations deep in the Sinai. In the last stage his forces were to cross the Canal in a large-scale operation and occupy the East Bank of the Canal in order to break the status quo. Thus, the plan was declared openly along with the goal of the war.

In July 1969, Israel attacked Egypt in a preemptive air operation. Nassar agreed to a 90-day ceasefire. On the first day of the ceasefire, Nassar moved large numbers of surface-to-air missiles (SAMs) to the Canal.

Over time, the Israelis and the U.S. came to believe that Sadat had abandoned Nassar's plan. We knew all there was to know about Egyptian and Syrian military capabilities but failed to predict the war in 1973.

What were some factors? Israeli force superiority was proven again and again. In the Sinai War (1956), the Six-Day War (1969), the War of Attrition, in border incidents, in air-to-air encounters. Israel also had U.S. equipment, training, and tactical advantages. The Israelis did not believe that the Egyptians would initiate hostilities without the air superiority that they clearly did not have. Add the concept: Egyptian need for air superiority as viewed by Israelis.

Would any country undertake a war it could not win militarily to make a political adjustment? The few viable assessments of a potential war were effectively sidetracked, as the consensus view—shared by the U.S. and Israel—prevailed.

~~SECRET~~

5. SOME COMMENTS ON THE WARNING PROCESS TODAY

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

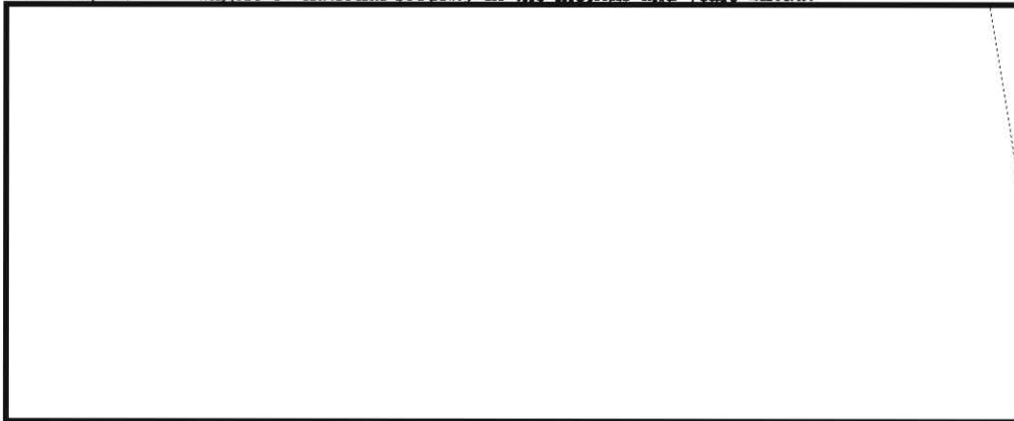
The National Warning System has learned from the errors of the past, and both the developments in technology and, more importantly, the maturation of our analytic understanding of warning significantly strengthen our hand today.

Our technical collection and processing capabilities have evolved to a highly capable and responsive state, and these systems continue to improve rapidly with technology.

Today, we are able to quickly modify the focus of our collection efforts and rapidly process and disseminate the product which gives our analysts a near-real-time view of developments throughout the world. Our collection is also more comprehensive with a growing capability in the Third World and on economic targets.

Our analysts are better trained. The average analyst today not only comes to the intelligence business with impressive credentials but is trained in intelligence schools, senior service schools and revisits to the academic community. Our analysts are provided with the automated tools of the computer revolution. Data is more accessible, and the manipulation of that data is becoming easier.

But, the picture is not all positive. The technical revolution has resulted in changes which have complicated our ability to warn. First, the near-real-time nature of many of our systems causes many analysts to become current intelligence analysts. They are being driven by current events and are unable to look beyond the events of yesterday or tomorrow to anticipate the dangers to national security in the months and years ahead.



Modern communications have clearly assisted us in strengthening our ability to move warning information around. Indeed, you hear that NSA had been leaders in this field, proving time and time again that you have mastered the art of providing direct, tailored support to tactical forces around the world. But more importantly the dramatic improvements in communications technology have changed the way in which crises develop and wars are waged. The tight coupling of our C³ systems, with the improvements in our weapons delivery systems, allow little margin for error and demand the earliest possible warnings.

Communications and information technology coupled with the worldwide interests of the major powers no longer allow us the luxury of focusing on single problem areas. In fact, most major strategic confrontations may well be preceded by terrorism, sabotage, or other destabilizing acts in areas of the world far removed from the principal threat, precisely so that we may be diverted from the real threat.

In today's world the threats are high and the margin for error very slim. We are in a continuing chess game in which the rules often change, in which players drop in and out,

~~SECRET~~

CRYPTOLOGIC QUARTERLY

and in which the perceptions of the adversaries are often more driving than the realities. This is the warning business and the stakes are national survival. Modern warfare, even when fought with conventional weapons is not the same as in the past. The threat of rapid escalation and sudden unbalancing of critical equations looms large. Ambiguity in the warning process is a way of life, and consequently the policy and decision-making community must learn to accommodate that ambiguity. The role of warning is to help that community to avoid harm, so that our options ameliorate the perceived threat.

Warning is the critical element for our national preparedness. We must refine our analysis, live with ambiguity, and take the risk to make early judgments. Early warnings expand our options, decrease our costs, and increase our opportunities to avoid harm.

As difficult as it is to predict the future, it may be more difficult to convey that judgment to our policy and decision makers. Whether their perceptions are most influenced by previous policy, a different view of the world, a generation gap, or other factors, the individual sensitivities of the recipient are important.

Our approach to warning is basic: we want to communicate clearly and follow up. We want to be practical—warning analysis responsibility rests at every level of intelligence. As Bill Casey says, "Warning is everyone's business." We want to be realistic by strengthening the bonds and understanding among decision makers, operators, and intelligence personnel before the crisis occurs.

We must define the elements of the warning problem because these are not clearly and universally understood.

Even assuming that the warning was acted upon by the decision maker in a manner designed to avert the threatened harm, that harm may nevertheless arrive, and we have a crisis on our hands.

6. CHARACTERISTICS OF A CRISIS AND RELATED PROBLEMS

A crisis may be described as having three characteristics: (1) it threatens our national interests; (2) there is significant compression of time for decision, action, and reaction; and (3) the situation often surprises the decision maker or at least frustrates him as a result of his inability to avoid the crisis.

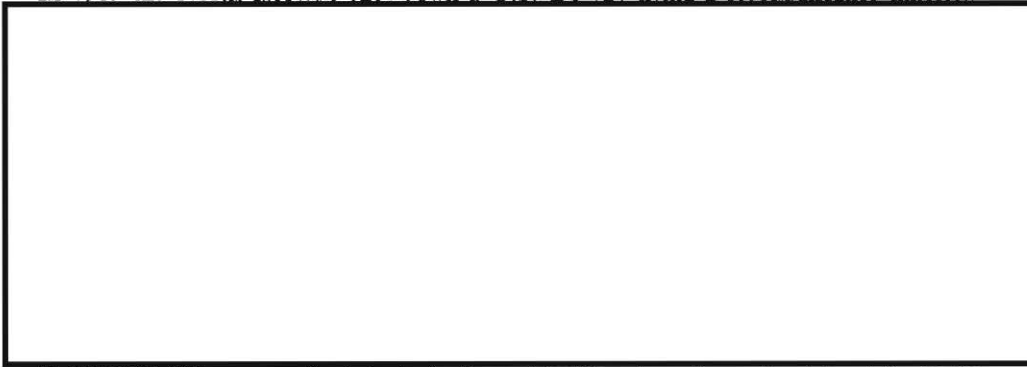
The threat to national interests is a dimension of the crisis of which we often lose sight. That is, the decision maker, or the intelligence and operational communities may see or conjure a threat where none exists. Thus we often have self-generated crises. One of the key responsibilities of the intelligence community is to provide information concerning the threat itself in order to determine the reality of that threat to national interests. In seeking to learn about the threat, often there is an increase in collection and processing activity which is occasionally judged by others to be the first signs of a crisis. Indeed, this is one of the problems with NSA's Sigint Alert today. Too often it is looked upon as a warning of a developing crisis, when in actuality it is a management tool to enable a more detailed and accurate assessment of a potentially threatening situation. If NSA has done its job, then most crises will have been preceded by a Sigint Alert. However, it does not and should not follow that every Sigint Alert will be followed by a crisis.

The nature of the crisis, particularly when some measure of surprise is involved, greatly compresses the time allowed for assessment and action. This is a many-dimensioned problem. First, there is the problem of collecting and assessing all relevant information and providing it to the decision maker quickly and accurately. New collection systems and modern communications help with that problem, but there are still delays. When the White House or the Pentagon or even NSA is being asked by the *New York Times* what is happening and what are we doing about it minutes after the event, the pressures are felt all

~~SECRET~~~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

down the line. How is the composite story pulled together? How do we track and report an evolving situation? Tough problems.

In 1969 the North Koreans shot down a U.S. EC-121 flying a reconnaissance mission.



Fortunately the community has evolved considerably since then—the late sixties/early seventies. In fact that was one of the major stimuli for the creation of the NSOC. (I'm sure most of you have seen the NSOC videotape which began with General Johnny Morrison, "I remember that night in February 1969 when the Sigint Command Center called me. . . .")

But not all has improved. Our ability to move that graphic presentation from NSOC to the White House and the rest of the community is as primitive now as it was then.



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

7. CRISIS MANAGEMENT: COMMENTS AND SUGGESTIONS

The goal of the community must be to provide the best and most accurate and timely assessment and then move on to other dimensions of the crisis.

Having initially reacted, then it becomes incumbent on both the community and the decision maker to again look at the longer term goals and begin actions which will help bring the crisis to a favorable solution. This is the key to effective crisis management, moving from the reactive mode to the active—recognizing that the assessment period must end and beginning to look at the problem in terms of our abilities to bring it to a satisfactory resolution. The policy decision maker clearly carries a major role, but there is a responsibility incumbent on the warning community not to lose sight of the real issues and to concentrate on assessing the enemy's weaknesses and vulnerabilities to assist and even guide the decision makers in their actions. The community must also focus on enemy reactions to U.S. actions. How are our actions being perceived, and is that perception one which will somehow lead them to take other actions for which we may be unprepared? It is most important to realize that the warning process continues through the duration of the crisis, just as it does through the duration of any war.

During the KAL shutdown there were two critical issues which I don't think that we as a community adequately focused on. The first was that in attempting to assess Soviet awareness of what had happened, we should have looked more thoroughly at their public utterances, searching for clues as to whom they were addressing their propaganda—their

~~SECRET~~

own people or the West. And also how were they going to play the incident with a view towards how we could counter their propaganda campaign?

Who in the community should be taking the lead once the damage-limiting actions have been taken? Unfortunately, the community tends to be broken into current intelligence analysts and long-term analysts, and the middle ground often gets short shrift.

As noted earlier, the warning process, i.e., recognition, validation, definition, communication, evaluation, and action is a continuous, iterative process. After the steps have been taken to contain or ameliorate the crisis, then steps must be taken to control the nature, direction, and outcome of the crisis in a manner most beneficial to national interests. The dialogue between the warner and the decision maker becomes even more critical. Not only is the warner trying to show the direction of the crisis, but it is incumbent that the warning community look carefully for the reflections of actions being taken by the U.S. An understanding of how U.S. actions are perceived and reacted to is critical in trying to develop further actions in the crisis management chess game.

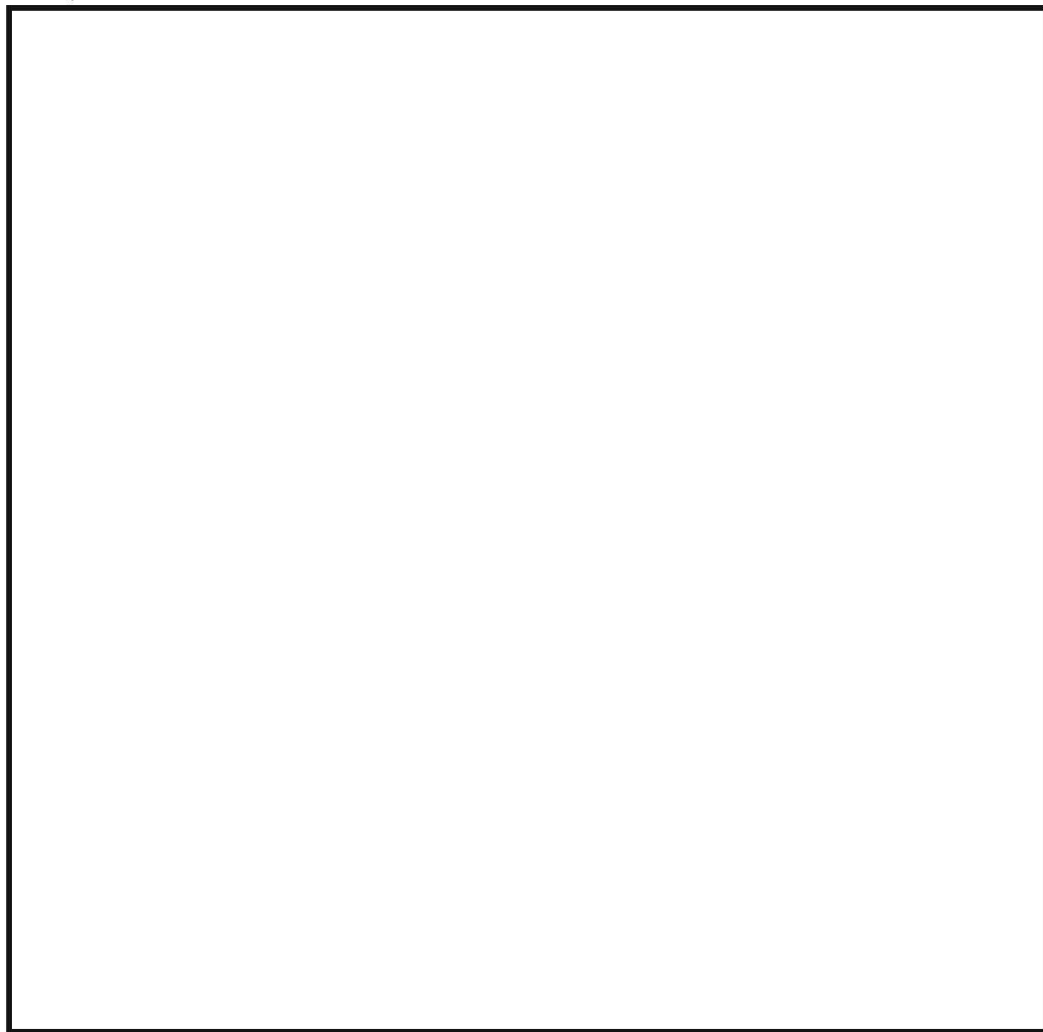
Whatever the characteristics of the national level decision-making process, the network of command and operations centers becomes critical to ensuring the best possible flow of information. In the late sixties/early seventies we looked at the big six: the National Military Command Center, the National Military Indications Center, NSOC, State OpCen, CIA OpCen, and the WHSR. In the mid-seventies we saw the addition of the Service Watch Centers, and today we are seeing the further addition of similar activities at Energy, Commerce, Treasury, the Federal Emergency Management Agency, and finally the Decision Support Facility at the National Security Council. This growth is a manifestation of part of my message. We are no longer able to work our warning problems in neat little compartments. The relationships between foreign and domestic policy, between military action and economic sanctions, between terrorism and commerce, are becoming too close. We must therefore develop new concepts which will enable us to cope with the new environment.

With the exception of a few modest technical upgrades, the major centers are functioning in a fashion very similar to that of the early seventies. In fact, with only minor exceptions, there have not been any substantial improvements in the operating capabilities. In some areas there may have even been some backsliding. In the "good old days" my colleagues and I were extremely close, and crises stimulated even closer interaction. Several major technology initiatives evolved from this group. The secure facsimile—WASHFAX—and the secure conference call—NOIWON—evolved as community initiatives from this group. But there has been a dearth of such initiatives ever since. This is not the result of deteriorating community relationships. On the contrary, relationships amongst the agencies and departments of the National Security Community are better than ever. Rather, I believe it results from the pressure put on the key players because of the improvements in real-time information gathering and processing, and the impact it has on the principals to demand even more current intelligence reporting.

When I moved to my current position a year ago, the desire of the chiefs of the operation and command centers to work together to improve the interfaces between the operating centers was unanimous. Therefore, as one of my first initiatives, I reestablished

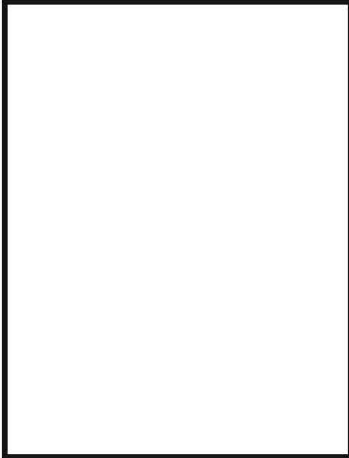
~~SECRET~~

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



(b)(1)
(b)(3)
OGA

Many of you sitting in the audience today will be the future leaders of the Agency and, indeed, the Community. You are the ones who can help us to solve these major problems, and it will be through making a slave of the technology and not the other way around. The technology is providing us with some incredible opportunities for growth, it will be up to you to make sure that the technology pays off, through good, enlightened management.



(S-CCO) Mr. [redacted] has served in his present position as National Intelligence Officer for Warning and Director of the National Warning Staff since October 1982. He joined the Agency in 1962 as an Arabic Voice Transcriber. In 1966 he became NSA Liaison Officer to the White House and in 1969, Director of the White House Situation Room and member of the Senior Staff of the National Security Council. Returning to NSA in 1974, Mr. [redacted] became Deputy Chief of Operations and Current Reporting and in 1976, Chief of that organization, where he was responsible for the operations of the National Sigint Operations Center (NSOC). He next served as Chief, Office of Support to Military Operations and in 1979 was transferred to the Telecommunications and Computer Services Directorate, first as Executive and later as Chief of the Policy and Management Staff. In February 1982 he was assigned Chief of Information Resources Management (T5). Mr. [redacted] was awarded the Meritorious Civilian Service Award in 1974.

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