NSA TECHNICAL JOURNAL (U)

VOL. XXV FALL 1980 NO. 4

NSA TECHNICAL JOURNAL (U)

Editorial Policy

Articles for the *NSA Technical Journal* may be written on any theoretical, doctrinal, operational or historical aspect of cryptology. The criterion for publication is whether or not the article has sufficient technical merit and makes a genuine contribution to cryptologic literature.

Contributions and Distribution

The *NSA Technical Journal* is published four times a year under the direction of the Publisher. Telephone: OUTSIDE: 8277; SECURE: 2355. This publication is designated as a working aid and is not subject to receipt, control or accountability; distribution is made by copy number to the subscribers. Any cleared and indoctrinated person may be permitted access to the *Journal* by a regular receiver of the *Journal* or by the Library. The *NSA Technical Journal* may not be reproduced, in whole or in part, or dispatched outside the Agency without the express approval of the Agency; this approval may be obtained from the Publisher or the Editor. Extra copies, those for which there is no further need, or those belonging to subscribers who are leaving the Agency permanently should be returned to the Editor for disposition.

Articles for the *Journal* should be sent to:

Editor, *NSA Technical Journal*
M62, SAB-2

Manuscripts should be accompanied by an abstract and should be double spaced with generous margins. Two copies, an original and a carbon, are required, and a third copy should be retained by the author. Artwork should be complete when submitted and should be adequately identified. All material used in the publication of an article is destroyed when no longer needed unless the author requests that it be returned to him.

NSAL—S-221,685

THE NSA
TECHNICAL JOURNAL

VOL. XXV FALL 1980 NO. 4

NOTES AND ANNOUNCEMENTS

1981 CMI ESSAY CONTEST

Papers are now being accepted for the 22nd annual CMI Essay Contest. All entries should be submitted t(b)(3)-P.L. 86-36 5, B3534, x(b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36, C2W86, x2560; o(b)(3)-P.L. 86-36 42, 1A098, x4902, by March 31, 1981. Typewritten manuscripts are preferred, and three copies are required. Necessary diagrams and drawings should be included.

The purpose of the contest is to recognize professional accomplishment and to foster documentation of new and/or important ideas in cryptomathematics. At the annual CMI banquet, prizes of $100, $50, and $25 will be awarded in accordance with the recommendations of the panel judges. All entries submitted will be considered for publication in the *NSA Technical Journal.*

All NSA employees, including nonmembers of the CMI, are eligible to enter the contest. In addition, any member of the CMI who is not an NSA employee may also enter. Papers may be submitted on behalf of their authors, provided the author is eligible and consents.

Any writing on cryptology or a significantly related topic may be entered. Security classifications are permissible. Compartmented papers will not be accepted, but any techniques or ideas originating in compartmented problems may be reduced to a noncompartmented level. All *NSA Technical Journal* articles of the current contest year will be automatically considered as entries.

Papers published outside NSA are also acceptable as entries. Authors may wish to perform some revision or addition to make the relevance of the subject to cryptology or related topic more explicit. If such relevance to cryptology is not or cannot be supplied, judges may use its absence as a primary reason for eliminating the paper from further consideration.

The CMI will select the panel of judges, whose names will be announced when all papers have been submitted. Judges of the contest are not eligible to enter. Criteria for judging are: (a) Relevance to mathematics and

The entire text of pages iii and iv is UNCLASSIFIED.

cryptology, (b) Significance of the contest to Agency operations, (c) Interest of the paper to Agency professionals, (d) Quality of the writing.

1981 CLA ESSAY CONTEST

The fourteenth annual essay contest of the NSA Crypto-Linguistic Association is now open, and papers will be accepted until May 1, 1981. The purpose of the contest is to encourage writing on topics concerning the application of linguistic knowledge to the solution of Agency-related problems so that organized information can be disseminated among professionals in this field. At the spring meeting of the CLA, prizes of $100, $50 and $25 will be awarded in accordance with the recommendations of the panel of judges. All entries submitted will be considered for publication in the *NSA Technical Journal.*

Any NSA employee, regardless of his membership in the CLA, is eligible to enter the contest. In addition, any member of the CLA who is not an NSA employee may enter. Papers may be submitted by others on behalf of their authors, provided the author is eligible and consents. Judges, however, are not eligible.

Any writing on language or linguistics may be entered. Security classifications up to and including TSC are permissible, but techniques and ideas originating in compartmented problems must be reduced to a noncompartmented level. Note that *NSA Technical Journal* articles of the current contest year will *not* be automatically considered as entries. The authors or someone acting for them must enter their articles in the contest.

Typewritten manuscripts are preferred, and three copies should be submitted. Necessary diagrams or drawings in finished form should be included. For more information on judging criteria and contest procedures, contact Jim Child, E7 (FANX), 7129s.

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

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

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

A Computer Simulation of the Vulnerability of Frequency Hopping Communications Systems to a Follower Jammer (U)

(U) Frequency hopping techniques are being used to protect radio communications from the effects of brute force jamming techniques, such as noise or partial band jamming. Frequency hopping communications systems may, however, be highly resistant to brute force jamming and still be vulnerable to follower jamming. It is desirable to know the extent of this vulnerability. One way to estimate this vulnerability is to model the frequency hopping radio and follower jammer using a computer simulation program. JAMHOP, written in FORTRAN, is such a simulation program. Examples are given showing how JAMHOP can be used to estimate the relationship between FH system hop rate and vulnerability of the FH system to a follower jammer. Both single and multiple emitter scenarios are considered.

I. INTRODUCTION (U)

(U) This paper describes a computer simulation program which can be used to determine the anti-jam protection provided by frequenc(b)(1) ing (FH) for a specified communications system against a specifie(b)(3)-50 USC 403 (b)(3)-18 USC 798 jammer. Parameters in the program can be varied to represent a(b)(3)-P.L. 86-36 frequency hopping radio and follower jammer, and the scenario in which the radios and jammer are deployed can be varied. The results are given as FH system bit error rates.

(U) The objective of this paper is to show the relationship, in a representative tactical scenario, between the hop rate of a frequency hopping system and its vulnerability to a follower jammer.

(U) The simulation program, named JAMHOP, is written in FORTRAN. A copy of JAMHOP and the equations used to calculate bit error rates are included as an appendix. The program is demonstrated by simulating a follower jammer attempting to jam four different hypothetical frequency hopping communications systems.

NSA—S-221,649

II. CHARACTERISTICS OF A FREQUENCY HOPPING TRANSMITTER (U)

(U) Frequency Hopping (FH) is a spread spectrum technique that can be used to provide a communications system with resistance to jamming. Because the operation of frequency hopping systems has been described elsewhere in detail (see references [1, 4, 5, and 6], only that information necessary to describe the simulation program will be given here.

(U) A frequency hopping transmitter hops from one frequency to another over a wide bandwidth as it sends out its data. The frequency slot that the signal occupies at any one time is determined by a generated sequence. The same sequence is being generated (after synchronization) by the FH receiver, enabling it to choose the correct frequency on which to receive the transmitted signal.

(U) Frequency hopping provides jam resistance because it is difficult for a jammer to either jam enough of the total frequency hopping bandwidth with enough power to disrupt communications or follow the frequency changes fast enough to disrupt communications.

(U) Information on actual frequency hopping communications systems now in development is not freely available at this time, so four hypothetical frequency hopping systems will be used to illustrate the operation of the simulation program. A summary of their parameters is given in Table 1.

Table 1: FH System Parameters (U)

(U) As shown in Table 2, the four hypothetical transmitters have hop rates ranging from 100 to 2000 hops per second and transmit between 200 and 10 bits per hop in order to maintain an overall 20 kbps data rate.

Table 2: FH SYSTEM HOP RATES (U)

(Table 2 is UNCLASSIFIED)

	Transmitter 1	2	3	4
HOPS PER SECOND	100	500	1000	2000
BITS PER HOP	200	40	20	10
DUTY CYCLE	.8	.7	.5	.4

20 Kbps DATA RATE

III. CHARACTERISTICS OF A FOLLOWER JAMMER (U)

(U) One method of disrupting FH communications is by detecting the transmitted frequency for each hop and then sending a jamming signal on that frequency to arrive at the FH receiver before the hop is completed. A jammer which uses this tactic is called a follower jammer. (See reference [4] for a more detailed discussion of follower jammer operation.)

(U) Because no hostile follower jammer has yet been identified, it is necessary to make the following assumptions about what such a jammer would be like:

1. (U) The jammer sweeps its assigned band using a compressive receiver [2], checks each signal detected during the sweep to determine if it is hostile, and stores the frequency of each hostile signal in a first-in-first-out stack. If the number of detected FH signals is greater than the stack depth, the excess FH signals are thrown away.

2. (U) When the jammer has finished its sweep, if the stack contains a hostile signal it is jammed using the full jammer power. If the stack (b)(1) is more than one signal, time sharing is used to attempt to jam all (b)(3)-50 USC 403 (b)(3)-18 USC 798 (Time sharing means using the full jammer power but only a fracti (b)(3)-P.L. 86-36 available jamming time to jam each hostile signal. For example, if two signals were being jammed, each would receive full power for half of the available jamming time.) Power sharing could conceivably be used instead, but is not considered at this time.

3. (U) The jammer knows the signal structure of the frequency hopping system, particularly the hop duration (thus allowing it to use an optimal jamming pulse duration), and the jammer catalogs the frequencies used by the frequency hopping system so that it does not waste resources jamming any non-frequency hopping signals.

4. (U) If the stack contains no hostile signals, the jammer's receiver begins to sweep its assigned band again. Whether the stack contains hostile signals or not, the jammer's receiver maintains its sweeping rhythm.

IV. THE JAMMING ENVIRONMENT (U)

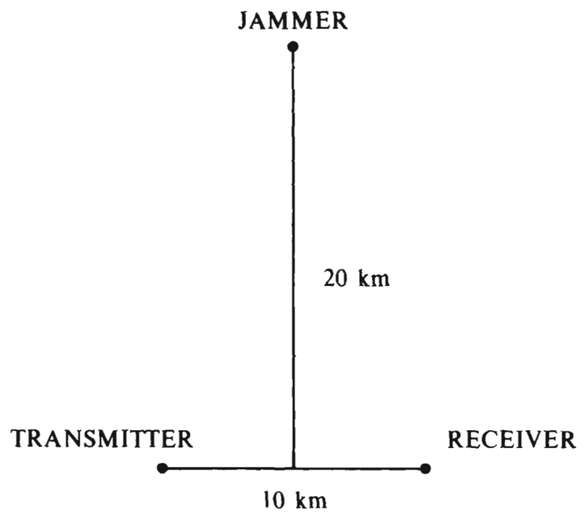
(U) At times there may be only one frequency hopping radio being jammed by one follower jammer. There may be, however, several frequency hopping radios in the same area. The maximum frequency load specified in the program is the number of frequency hopping radios in the area, in addition to the one targeted by the jammer. Whenever additional frequency hopping radios are present, they are assumed to have the same characteristics as the target radio. In particular, they would each have the same duty cycle, so they would seldom all be transmitting at the same time. All of these FH radios must be jammed simultaneously, unless one (or a select few) of them can be picked out by the jammer's receiver. (It is very difficult to pick out only one transmitter in a multiple user environment. One possible method would be to sort incoming FH signals by power, and jam only those with power above a preset threshold. Another method would be to use direction finding to jam only those FH signals in the same sector. A combination of these two methods could also be used.) An example of one follower jammer against one FH radio (one-on-one) and one follower jammer against many FH radios (one-on-many) will be shown later.

(U) It is assumed that there are no friendly radios operating in this band. If there were, the jammer would store their frequencies in a table and look them up as necessary to ensure that it did not accidentally jam them. Table top terrain is assumed in this simulation model, with no attenuation due to trees, mountains, etc. An attenuation of $1/R^2$ was used in the simulation; a more sophisticated propagation model will be added to JAMHOP later.

(U) Finally, the background noise due to the environment is assumed to be −105 dBm. Bit error rate thresholds are assumed to be 10^{-1} for voice and 10^{-3} for data transmissions. The threshold for voice transmissions was chosen based on the vulnerability of 16 kbps continuous variable slope delta (CVSD) encoded voice communications at 10^{-1}, and the threshold for data transmissions was chosen based on low speed teletype data.

(U) The relative positions of the transmitter, receiver, and jammer can be varied (and different altitudes are also possible). For the results that follow, the receiver is placed ten kilometers away from the transmitter and the jammer is placed twenty kilometers away from the midpoint of the transmitter-receiver line and perpendicular to it (Figure 1). All are at zero altitude.

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



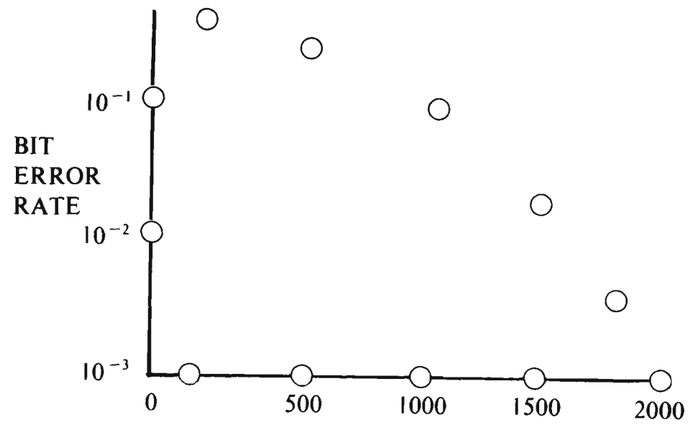
UNCLASSIFIED

(U) Figure 1

V. EXAMPLES OF JAMHOP SIMULATION RUNS (U)

(U) A simulation was run to obtain an estimate of the bit error rate that would be produced by the specified follower jammer against each of the four hypothetical frequency hopping communications systems which were described earlier. Ten transmissions for each radio were simulated, representing radio messages of 30 seconds duration each. The results for one jammer against one FH radio are shown in Figure 2. A voice transmission is successfully jammed in this scenario if the hop rate is less than 1000 hops per second. A data transmission is successfully jammed in this scenario if the hop rate is less than 2000 hops per second.

RESULTS (ONE—ON—ONE)

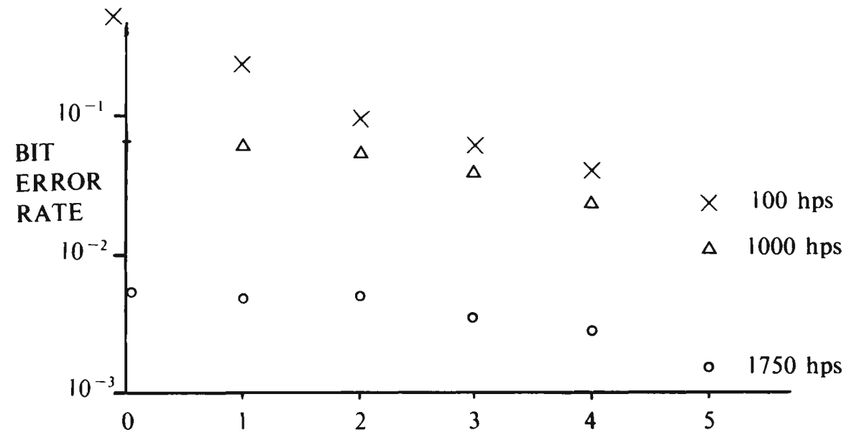


UNCLASSIFIED

Figure 2

(U) The same simulation was run with one jammer against from two to six FH radios, and the results are shown in Figure 3. Mutual interference is not considered here (see [7] for detailed analysis of the mutual interference problem). In this one-on-many scenario, a voice transmission would be difficult to jam successfully. A data transmission is successfully jammed if the hop rate is less than 2000 hops per second.

RESULTS (ONE—ON—MANY)



UNCLASSIFIED

Figure 3

VI. FAST FREQUENCY HOPPING (U)

(U) The results obtained in the simulation runs described above can be used to determine a definition for fast frequency hopping. Many definitions have been put forth, such as "faster than 1000 hops per second" or "when the hop rate is faster than the information rate." However, it is proposed that the definition of a fast frequency hopping system vary depending on the parameters of the FH system, the parameters of the follower jammer, and the scenario; and that a fast frequency hopping system be defined as "an FH system that is not vulnerable to a follower jammer." In the specific scenarios given here, a fast frequency hopping system would be one with a hop rate of

2000 hops per second or faster. If brute force jamming is not effective and follower jamming is not possible, then prediction of the hopping pattern is necessary to jam the system. Use of a secure code to determine the hopping pattern removes this vulnerability.

VII. AREAS FOR FURTHER STUDY (U)

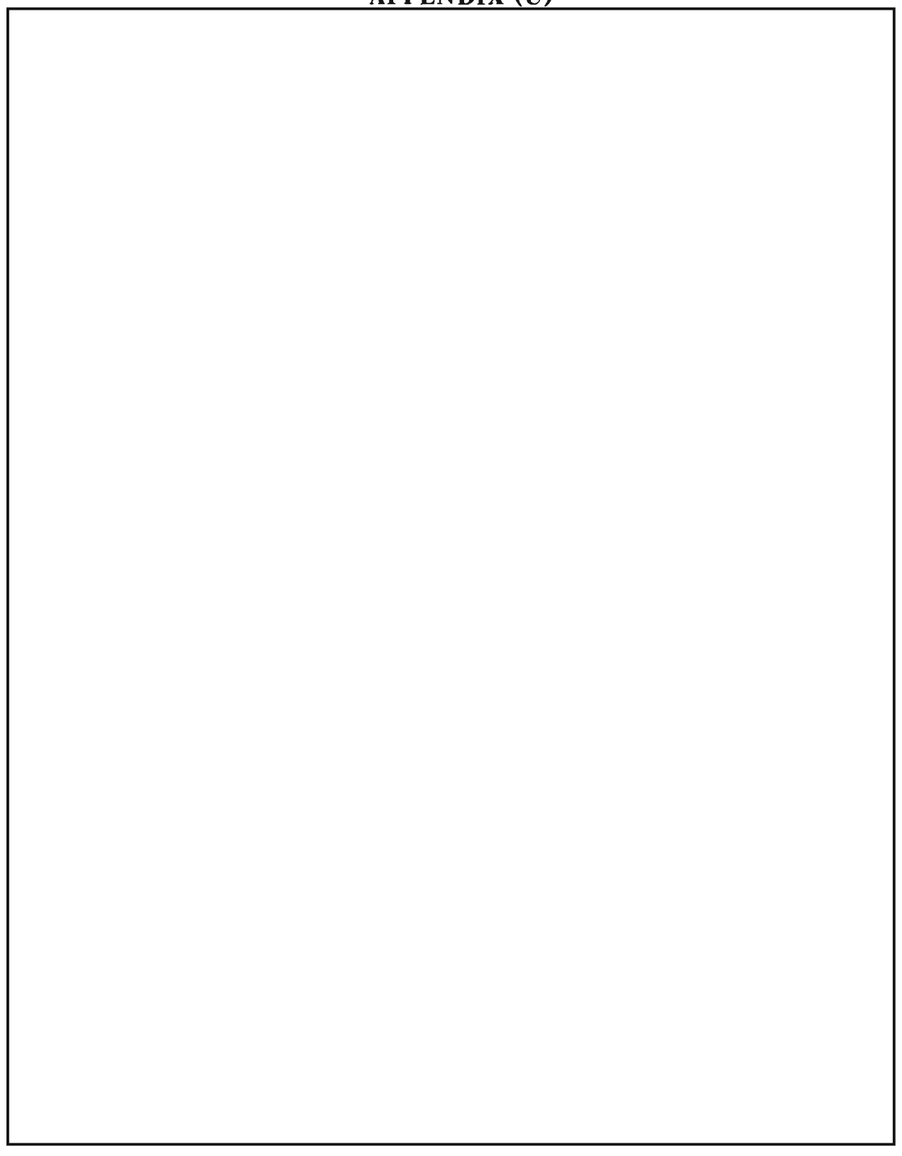
(U) Further study is needed in a number of areas:

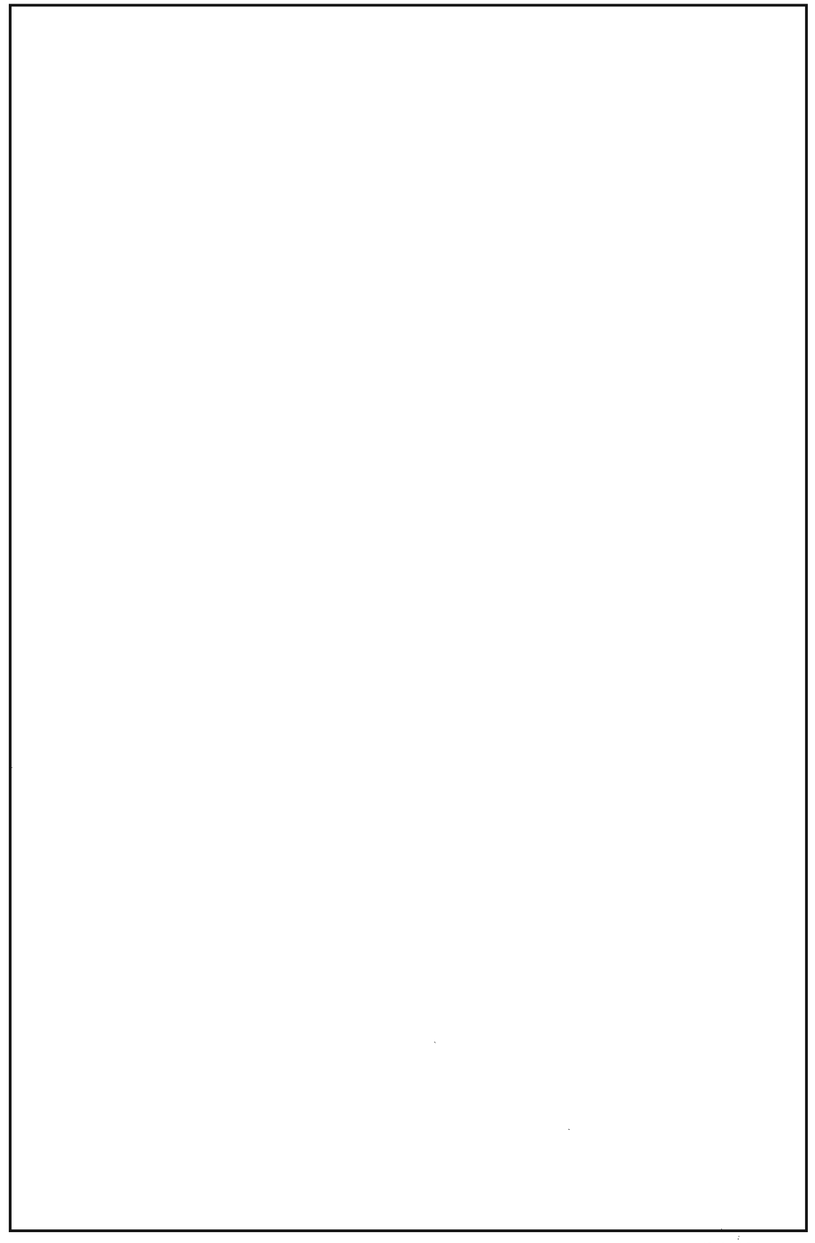
1. (U) A comparison of time sharing versus power sharing for the jammer needs to be made. It is conceivable that a power sharing jammer would be more effective against FH systems than the time sharing jammer. This approach could then be incorporated into JAMHOP.
2. (U) The different environments in which a frequency hopping system is likely to operate need to be examined. As shown by the results of the one-on-many example, the distance to the jammer and the number of FH transmitters operating simultaneously can greatly affect the vulnerability of a frequency hopping system to a follower jammer. Accurate data in this respect is needed to evaluate the anti-jam protection that any particular frequency hopping system could offer.
3. (U) A certain amount of anti-jam protection for the information carried by a frequency hopping radio can be obtained by using more than one hop to transmit each bit, by using interleaving, by using sophisticated modulation and detection techniques, or by using error correction coding. The degree of protection possible and the best way to obtain it need to be examined. Combining these methods with frequency hopping may be a more effective anti-jam technique than frequency hopping alone.
4. (U) Fast frequency hopping transmitters are protected against follower jammers, but both slow and fast frequency hopping transmitters may be extremely vulnerable to broadband or partial band jamming (or other forms of jamming). This vulnerability needs to be investigated.
5. (U) The vulnerability of a frequency hopping communications system to jamming during the synchronization period needs to be studied. If a frequency hopping system can be prevented from synchronizing, then there is little point in investigating its vulnerability during communication.
6. (U) Most important of all, for validation, the results obtained by this simulation of frequency hopping vulnerability (and the results obtained by other studies) need to be compared with the results of field or lab tests of actual frequency hopping radios, once the equipments become available.

REFERENCES (U)

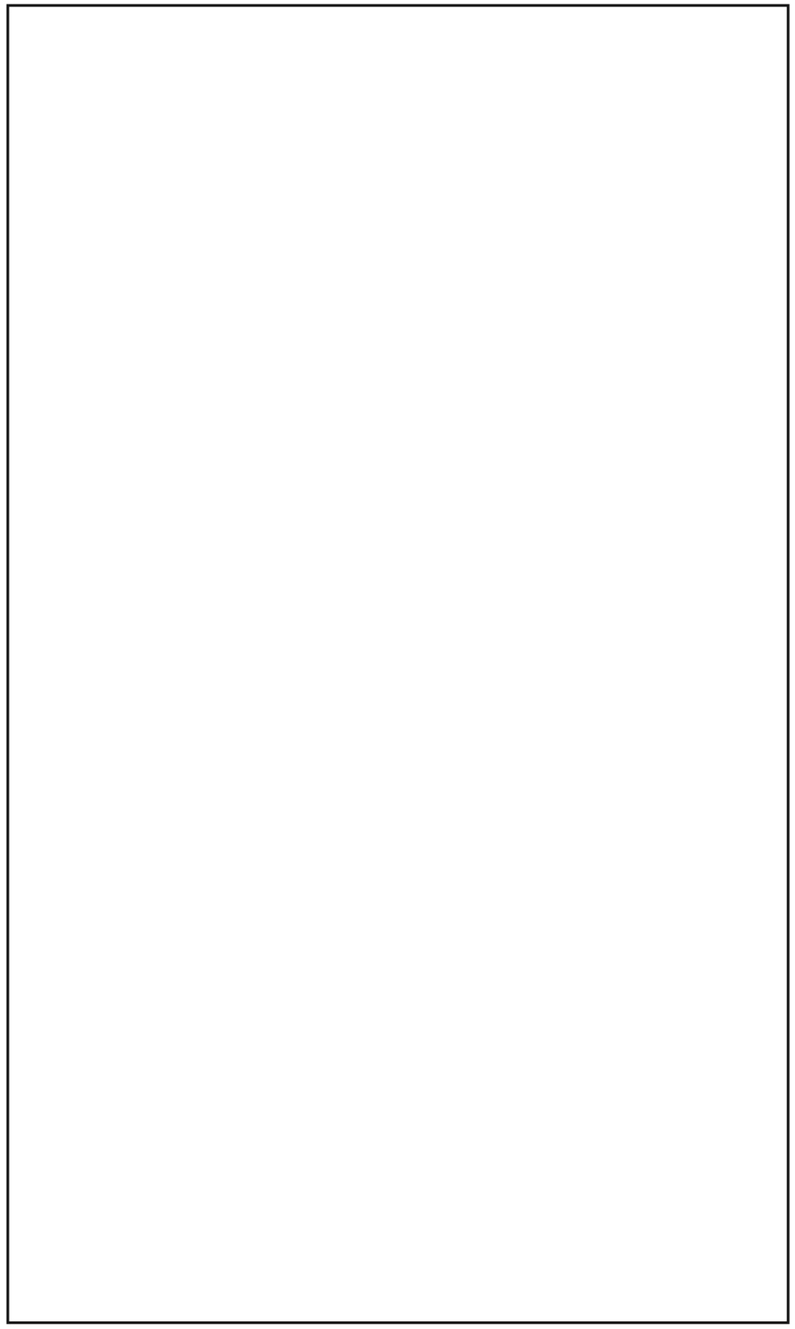
[1] (U) Dixon, Robert C. *Spread Spectrum Systems.* John Wiley and Sons, New York, 1976.
[2] (U) Hewitt, Harry. "Microscan Revisited—Candidate for the Agile Environment." *Electronic Warfare*, Vol. 8, No. 5, September/October 1976, p.49.
[3] (U) INSCOM. *Threat to SINCGARS.* U.S. Army Intelligence and Security Command, Intelligence and Threat Analysis Center, Arlington Hall Station, Virginia, 30 April 1979.
[4] (U) McCarriar, Thomas L. Jr. "Frequency Hopping System Response to Follower Jammers." *Proceedings of the Twenty-Third Annual Joint Electronic Warfare Conference* (1978), US Army Test and Evaluation Command, Aberdeen Proving Ground, Md., 31 May, 1979.
[5] (b)(3)-P.L. 86-36 read Spectrum System Jamming Response." *NSA Technical Journal*, Vol. XXII, No. 3, Summer 1977, p. 93.
[6] (U) Sanders Associates, Inc. "Micro-Vulnerability assessment of Sigint and Jamming Techniques Against Tactical Radios." Federal Systems Group, 23 August 1978.
[7] (U) Torrieri, Don J. "Simultaneous Mutual Interference and Jamming in a Frequency Hopping Network" (Draft). DARCOM, CM/CCM 79-6, June 1979.

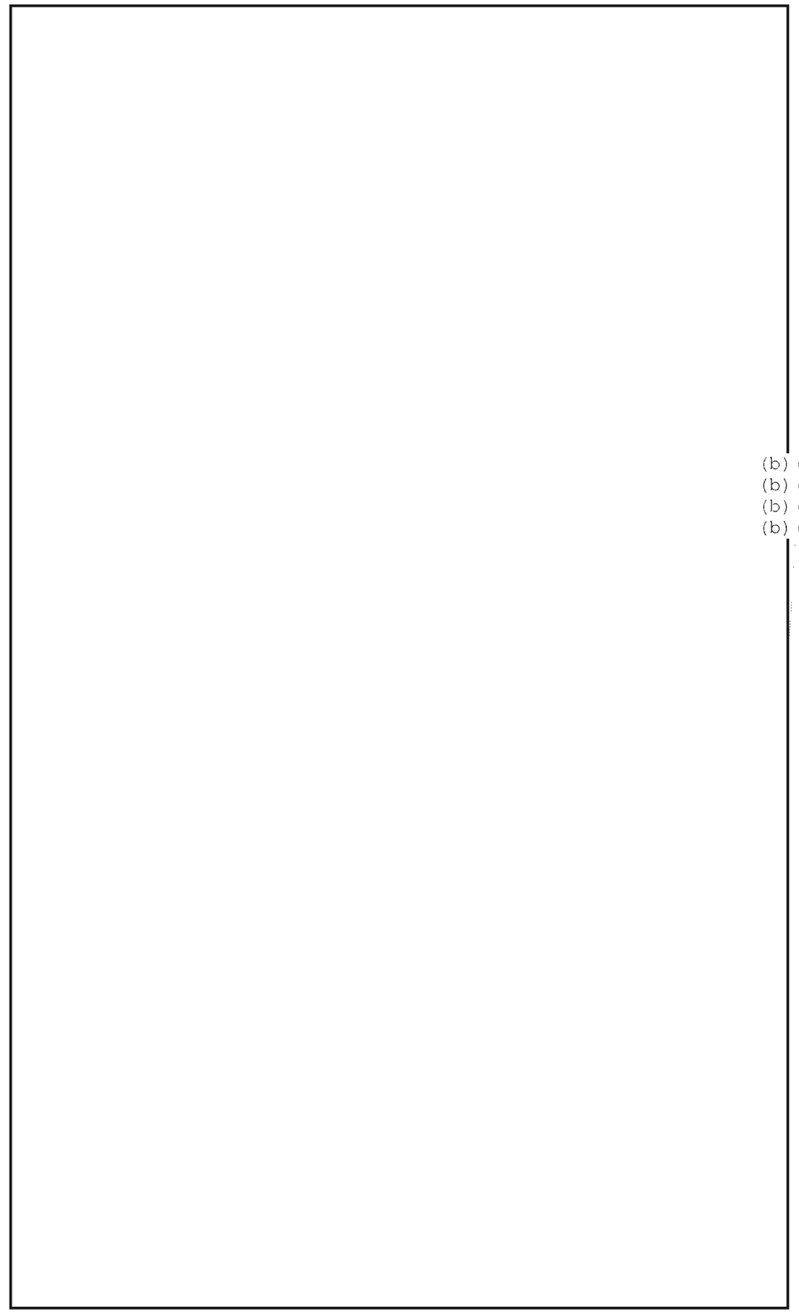
APPENDIX (U)



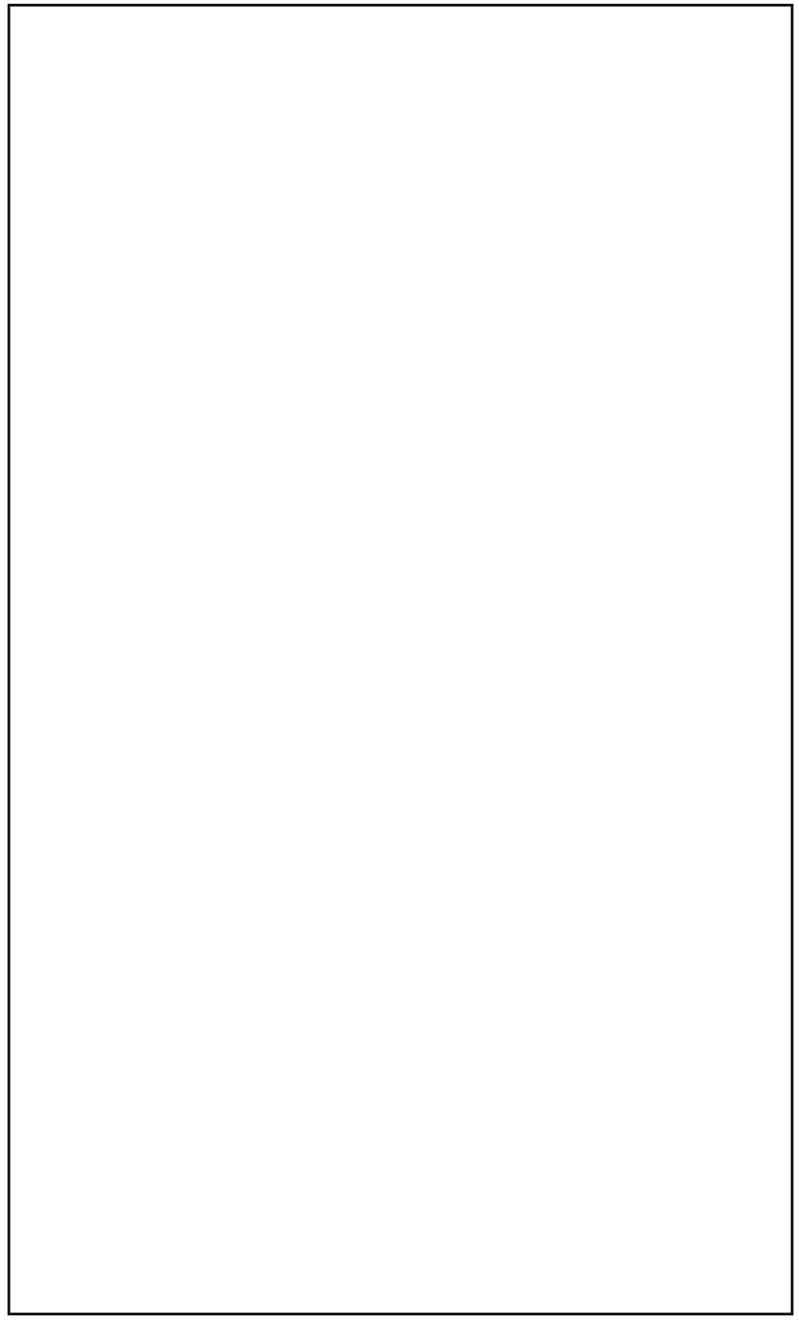


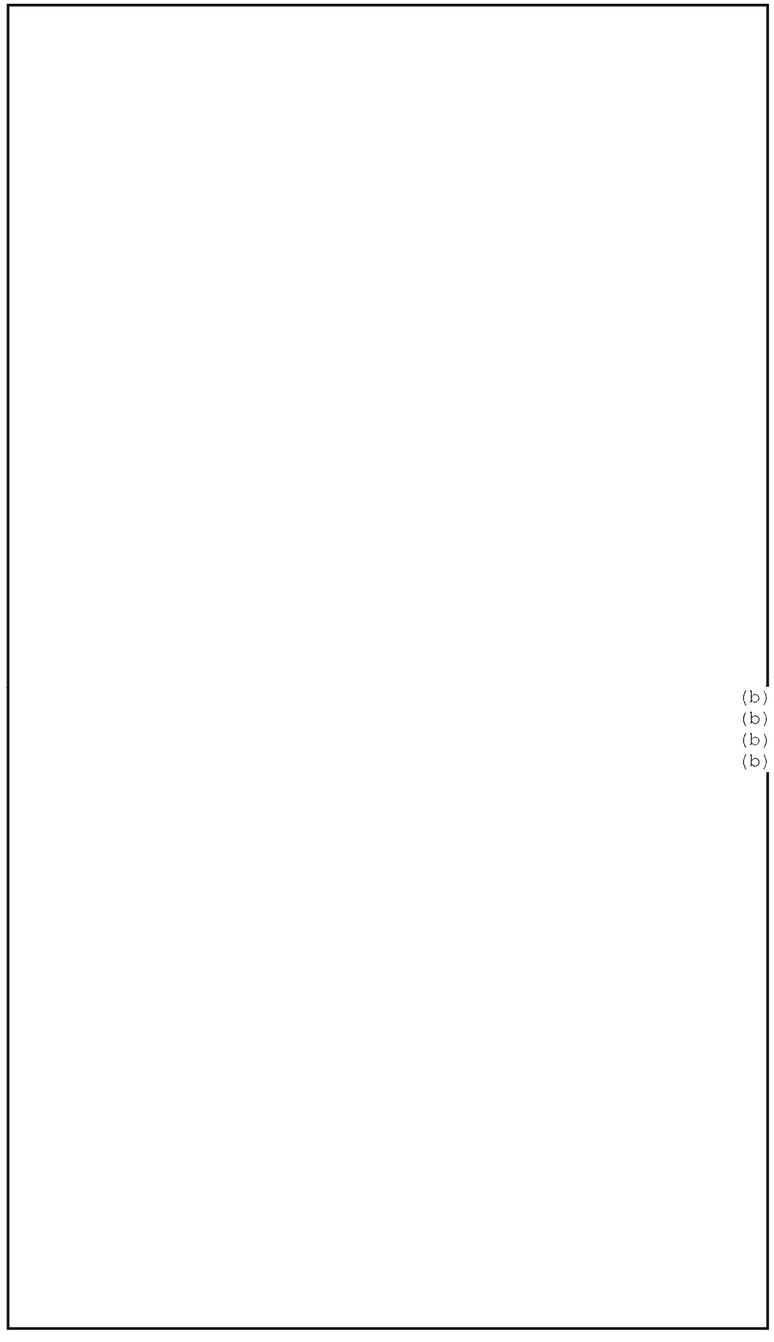
COMPUTER SIMULATION



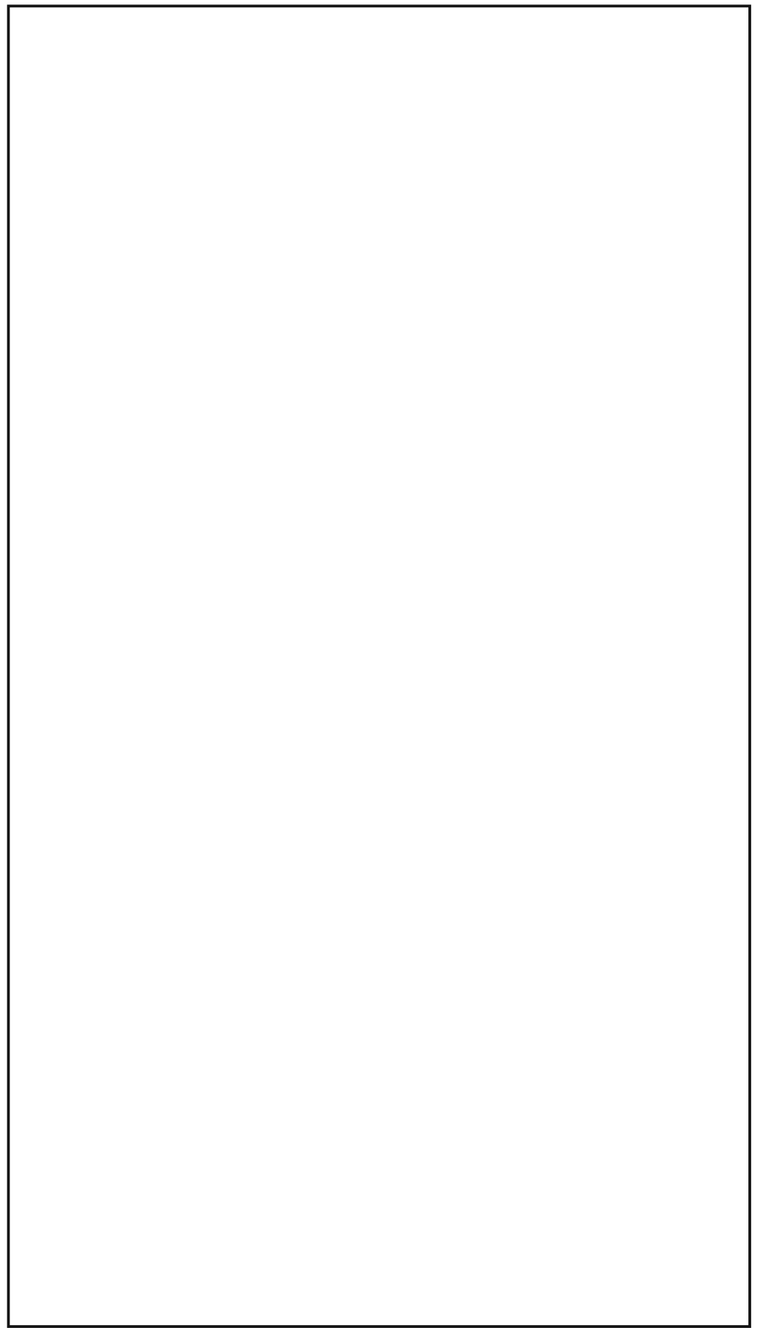


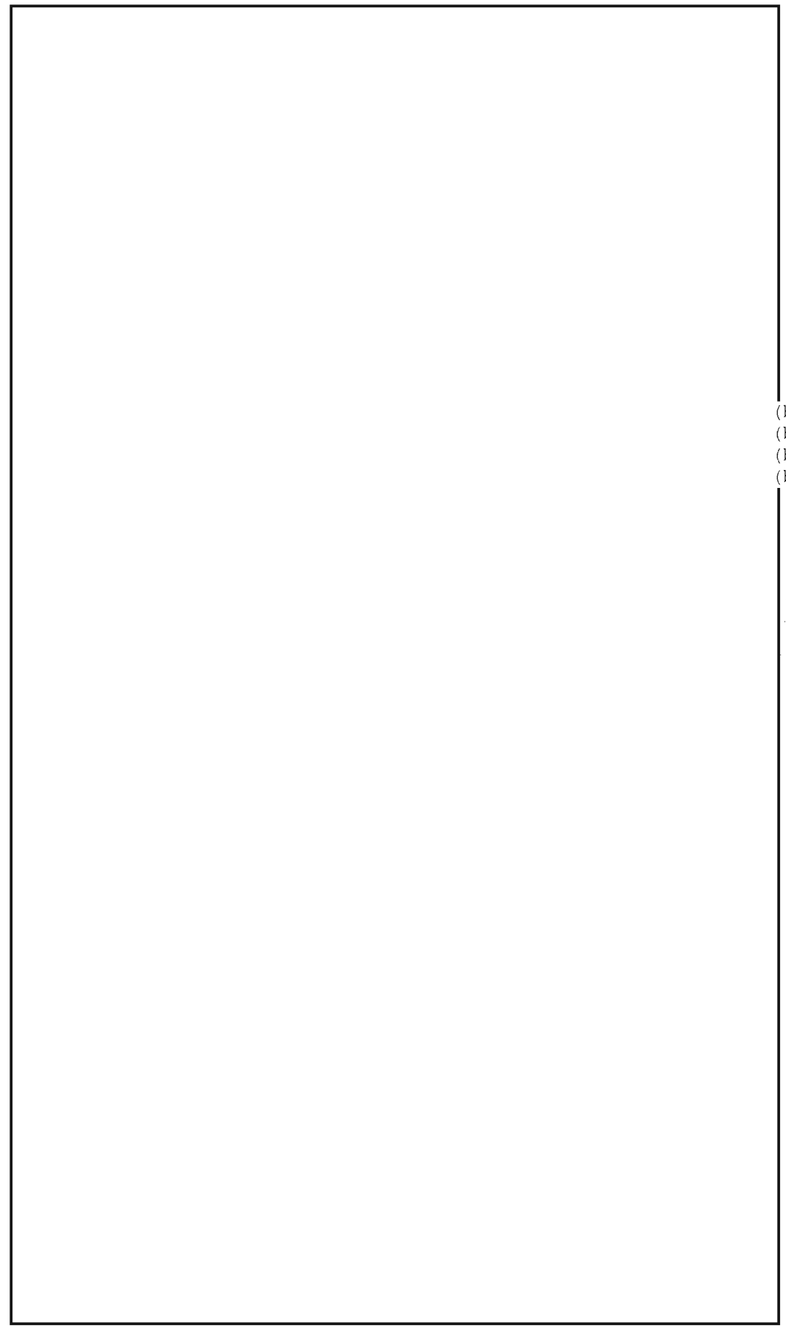
COMPUTER SIMULATION



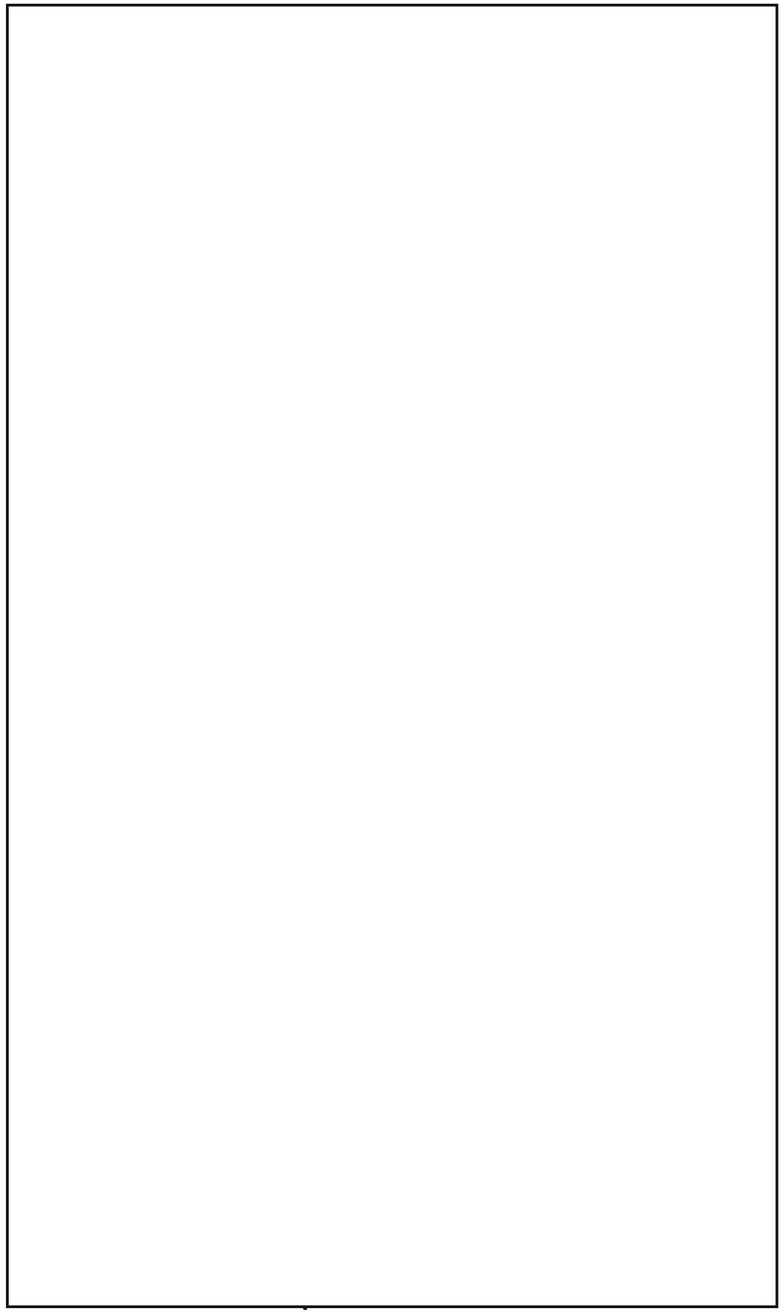


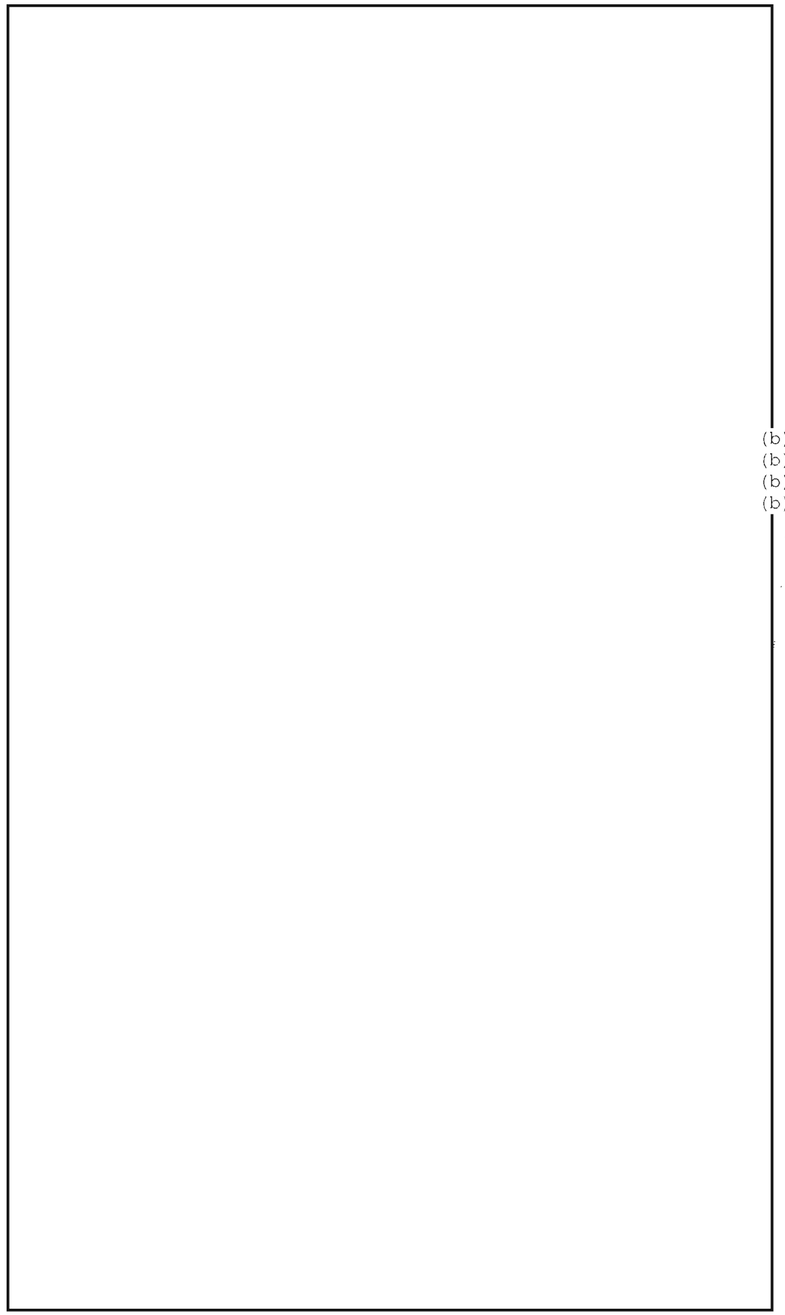
COMPUTER SIMULATION



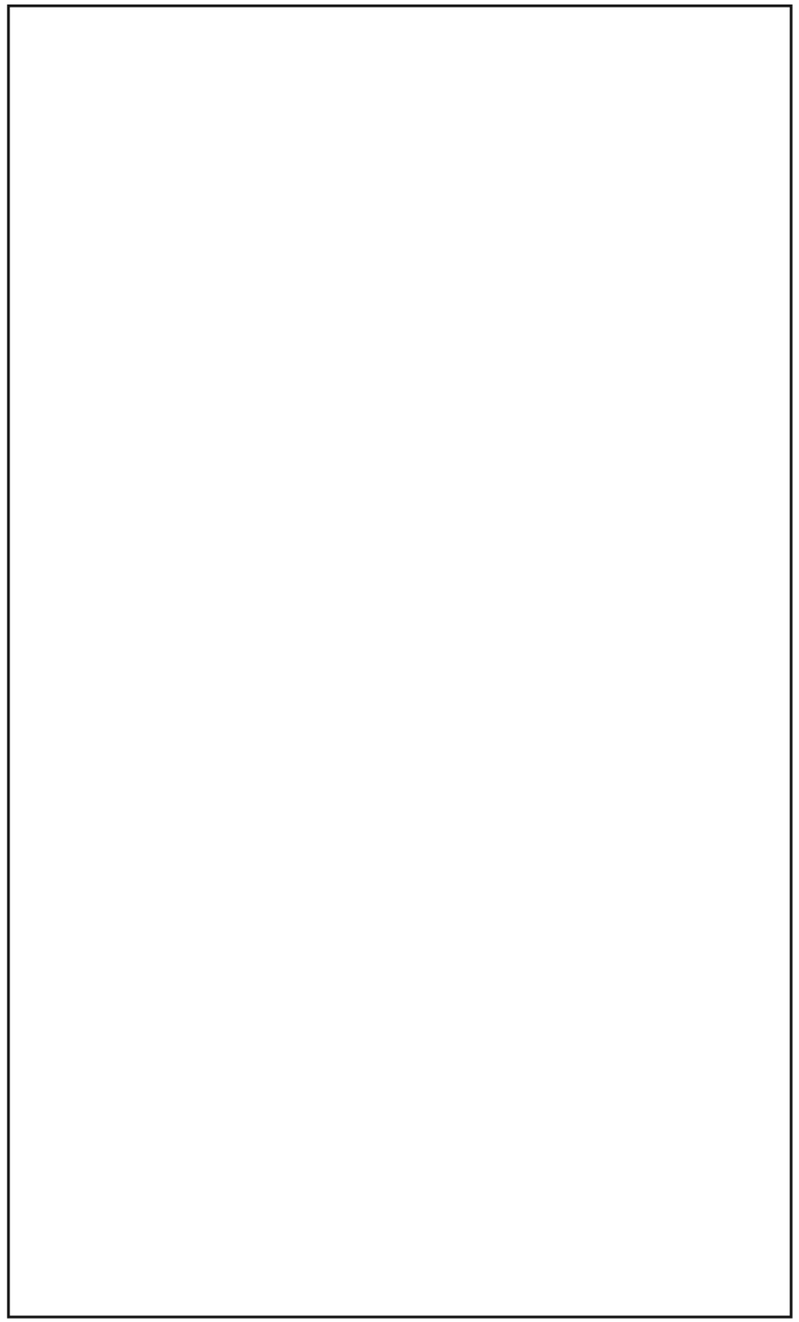


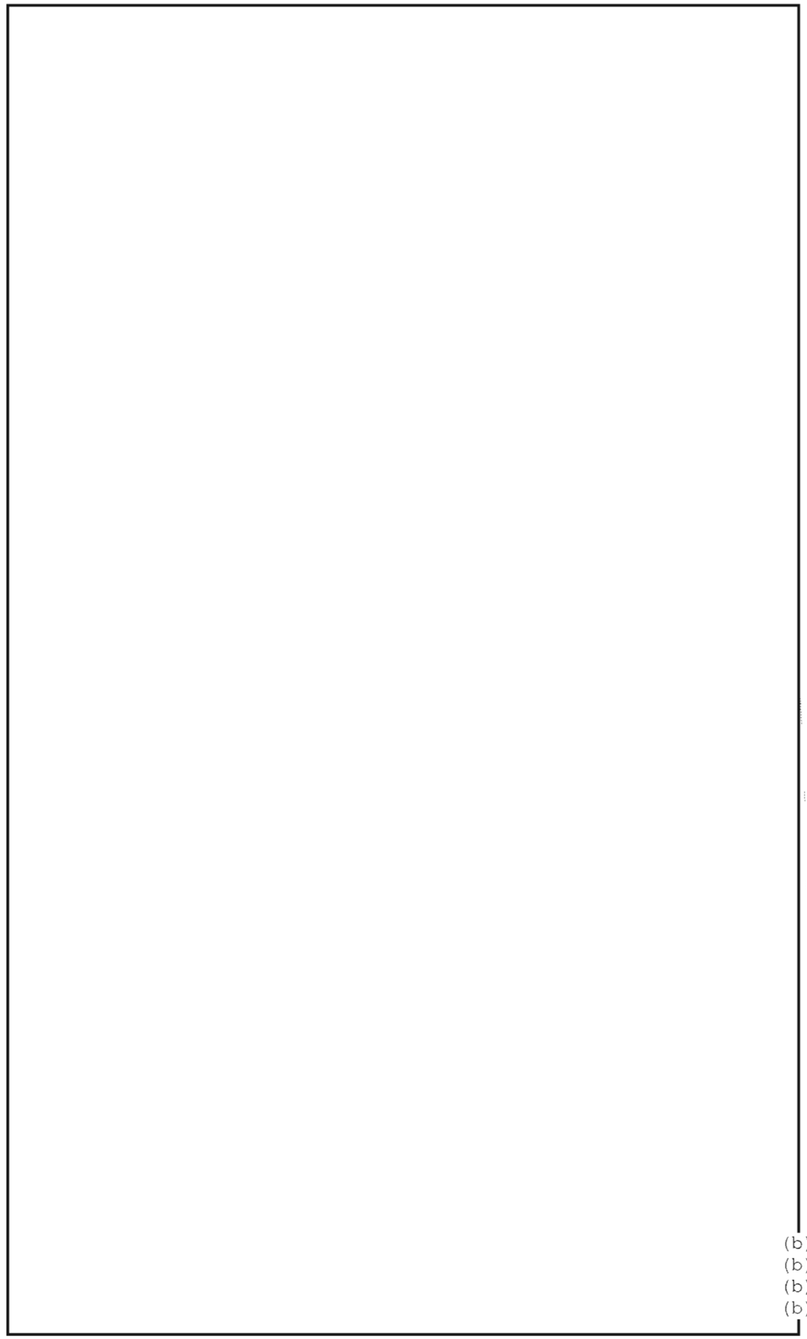
COMPUTER SIMULATION



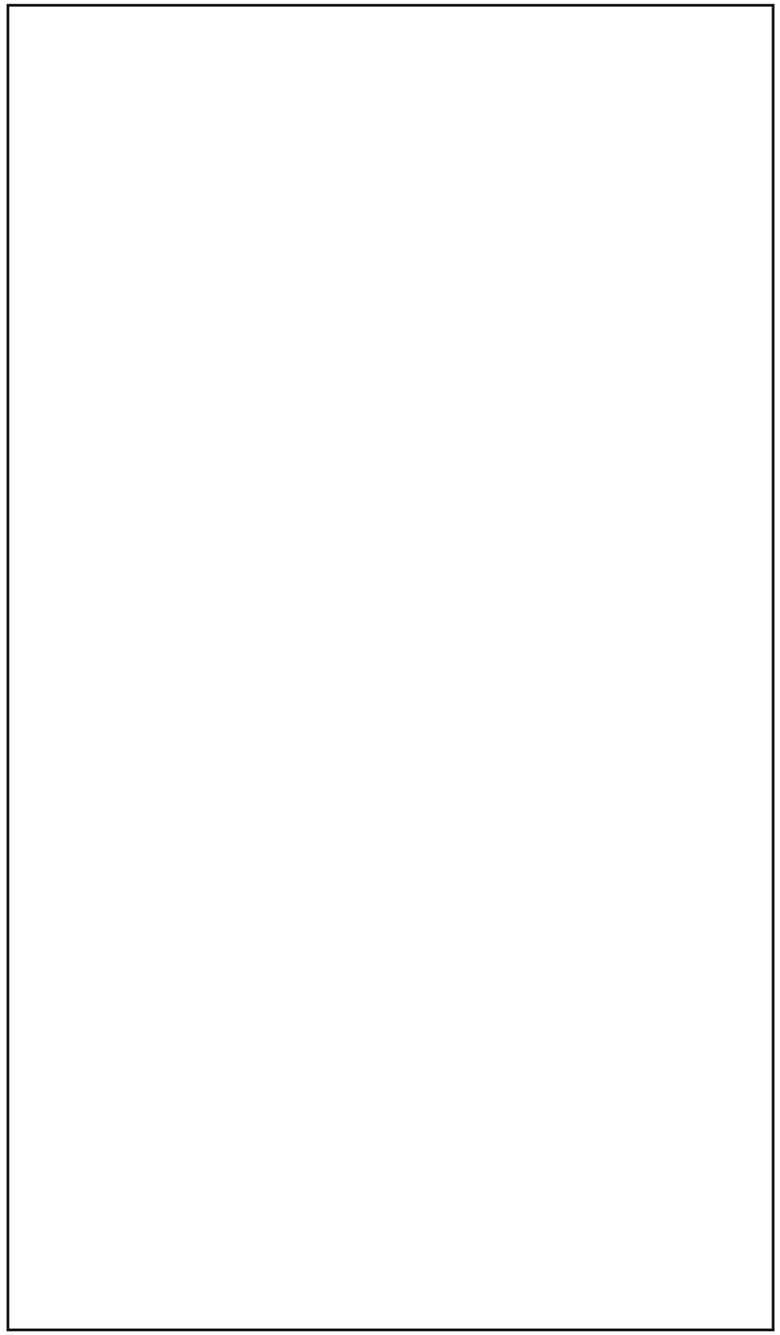


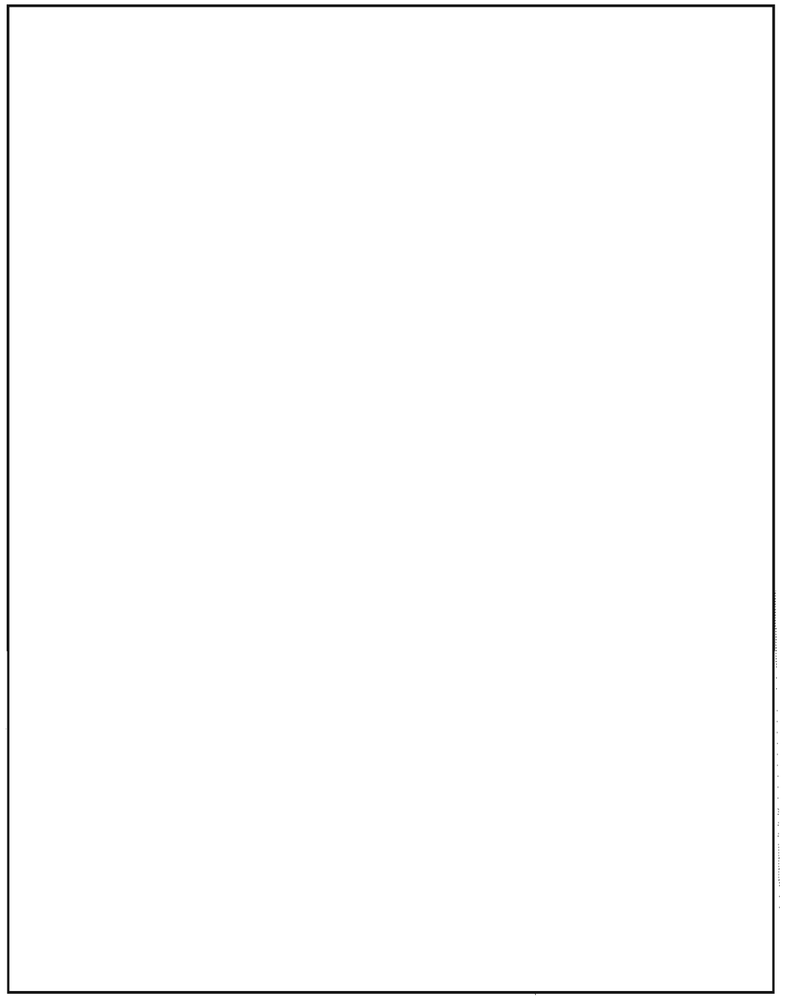
COMPUTER SIMULATION





COMPUTER SIMULATION





German Radio Intelligence*

ALBERT PRAUN

A senior German officer's view of communications intelligence operations in the North African and European theaters of the Second World War.

THE SIGNIFICANCE OF ELECTRONIC WARFARE

Toward the end of World War II about 12,000 signal troops of the German Army were engaged in intercepting the radio traffic of an increasingly powerful enemy. With the decline of the information gained by intelligence through aerial observation, prisoner of war interrogations, and reports from enemy agents, communication intelligence became increasingly important. In spite of the constant attempts of all the enemies to improve radio communication and increase its security, German signal troops were able again and again to gain access to the information transmitted by this medium.

Thanks to communication intelligence, German commanders were better informed about the enemy and his intentions than in any previous war. This was one of the factors which gave the German command in the various campaigns of World War II a hitherto unattained degree of security. The fact that, during the final years of the war when the German Army Command was leading exhausted and decimated troops without reserves, it was able to offer less and less resistance to clearly recognized measures and intentions of the Allies, and that Hitler was unwilling to acknowledge the true situation on all fronts and the growing enemy superiority as reported in accurate detail by communication intelligence, is one of the deep tragedies of the German soldier.

---

*Lieutenant General Albert Praun served as Germany's Chief of Army and Armed Forces Signal Communications from 1944 to the end of the Second World War. This article is taken from a history of the same title prepared for the Historical Division, Headquarters, European Command, U.S. Army, and later released by the Office of the Chief of Military History. Readers will note references added by the translator of the original [*tr.*] and by the editor of the *Technical Journal* [*ed.*]. No effort has been made to amend General Praun's text to reflect recent work on communications intelligence and its role in the Second World War. Some minor changes in spelling, punctuation, and wording have been made, and the text has been abridged to focus on operations involving American and British forces.

This article is classified SECRET in its entirety by authority of the Department of the Army, 22 January 1953. Review on 22 January 1983.

INTERCEPT OPERATIONS AGAINST GREAT BRITAIN (1940–41)*

After the conclusion of the Campaign in the West OKH (Oberkommando des Heeres, "Army Command") ordered Army Group A to initiate radio intelligence operations against the British Isles. This intelligence mission, which was given in the form of a preliminary order on 2 July 1940, was supplemented by mid-July with requests for the following specific information: present location of former British Expeditionary Force units; organization, strength and disposition of Regular Army and Territorial Army forces in the British Isles, as well as of forces shipped to England from the Dominions, with special emphasis on Canadian troops; transfer of units from the mother country for service in the Near East (Balkans) and Middle East (Egypt and North Africa); defensive measures initiated by permanent coastal defense forces and mobile defense forces; and coverage of the channel coast, this being the immediate objective for a German invasion in accordance with plans for Operation Seeloewe.† (The operations of the assigned intercept units, including intercept, areas are shown in Chart 1.)

In spite of intensive searching during the first four weeks (July 1940), it was impossible to intercept any messages of the kind which had been sent by mobile elements of the British Expeditionary Force on the Continent. To be sure, a few messages were picked up, but they could neither be followed for any length of time nor assigned to any regular net traffic, and frequently they were so brief as to preclude even the taking of accurate bearings. The few messages intercepted, though encrypted in a rather simple field cipher, were not enough for cryptanalysis purposes. In the final evaluation these observations were interpreted to mean that the seriously decimated divisions of the British Expeditionary Force first had to be reorganized, re-equipped and rehabilitated, and that in any event they were not yet ready for large-scale training exercises.

On the other hand, there was always regular traffic from fixed stations believed to be operating as "coast defense sector stations" with a net control station near London. This traffic was easily intercepted because of the failure to change call signs and frequencies. Messages handled by this net provided material for the first attempts at cryptanalysis. However, there was hardly any chance to draw conclusions of a tactical nature from the traffic analysis of this coast defense net, since it was apparently operated by well-trained personnel who observed strict radio discipline.

After this initial period, which extended through August and September 1940, radio traffic emanating from mobile units increased in volume. By means of radio bearings four "training areas" (see Chart 1) could be

*This section was written by Colonel Randewig, the commander of intercept units attached to Army Group A during 1940–41. [*ed.*]

†Seeloewe ("Sealion"), The German plan for the invasion of Britain. [*ed.*].

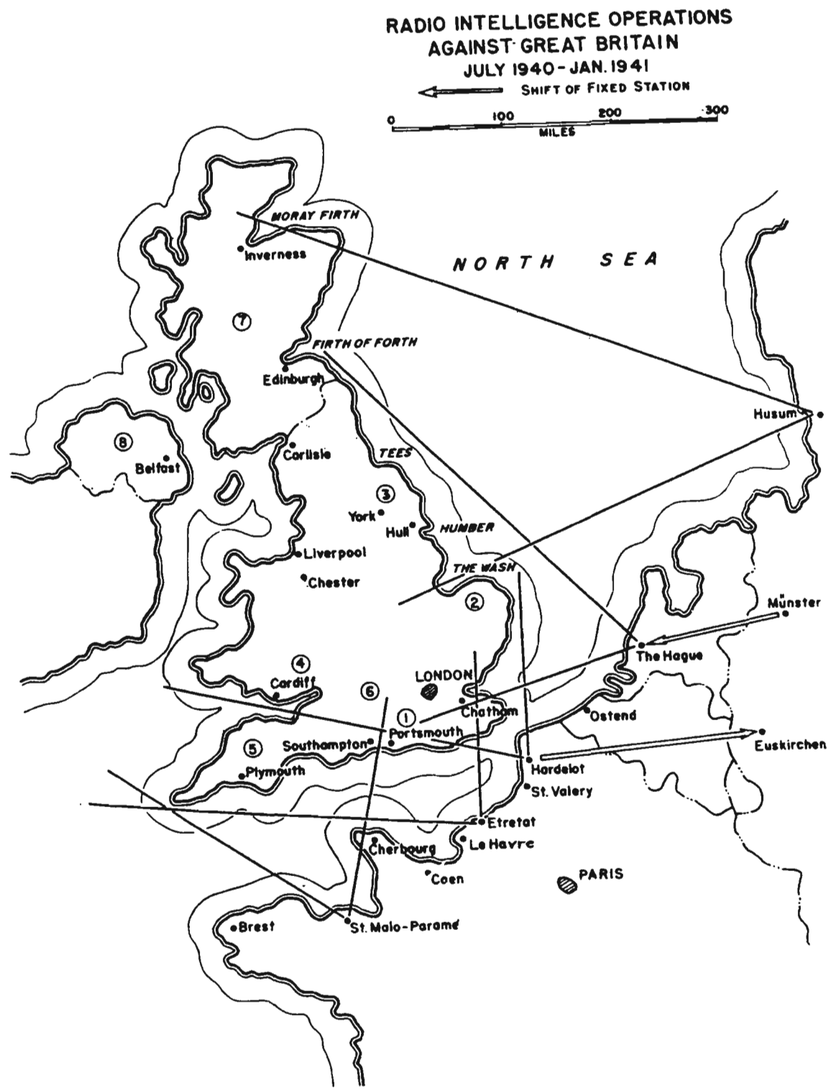


CHART 1

plotted: The Downs, including Sussex, Kent and Surrey; Norfolk, with Wells-on-Sea, the first locality identified; York, between the Humber and Tees; and Monmouth, along the northern shore of the Bristol Channel.

In the beginning the training exercises in these areas were still characterized by the same excellent radio discipline which was observed by the fixed nets, such as rapid tuning of transmitters preparatory to operation, brevity and speed of transmission, and avoidance of requests for repeat. In spite of the use of a single frequency for each net and the systematic use of call signs, inter-net relationships could only be guessed at; it was impossible to draw any conclusions from them regarding organizational structure. No cryptographic errors were committed which could have led to the solution of their ciphers.

Transmission efficiency gradually diminished, probably because the training given radio operators had been too short and inadequate. Names of localities appeared in the clear, and in the course of time abbreviations of unit designations were intercepted which were increasingly easy to identify. Thus, it was possible to locate the Norfolk training area by the term "Wells-on-Sea brigade," and the unit to which this brigade was attached was clearly revealed by a repeat request in clear text. Subsequently, the new numerical designations of the two London divisions were identified in the same way. Unit designations were mentioned so frequently that it was finally possible to prepare a complete list of units of the British field armies, including Canadian forces, and the composition of divisions down to infantry and artillery battalions. At the same time the territorial headquarters, as well as the corps headquarters in command of the "Mobile Defense Forces," and thus the top-level organization, also became known. This information became available even before a single radio message could be solved. At first, the carelessness with which unit designations were revealed raised the suspicion that this was all part of a deliberate deception. The enemy would not have committed such serious violations of security rules unless his own monitoring system was a complete failure. The accuracy of German intelligence estimates was subsequently confirmed by the contents of other messages.

As a result of the information gathered about the composition of enemy forces, the Germans increased their regular intercept coverage of the training areas, especially those in southern England, with an eye to their intended landing operations. The constantly increasing radio traffic now also permitted analysis of the nets' structure and plotting of headquarters areas by the direction-finding units. In this manner it was possible to trace the concentration areas of the divisions assigned to coastal defense and to follow the course of several anti-invasion exercises. During these exercises it was always possible to determine command nets and sometimes the link with the RAF, while unit nets could rarely (and armored traffic never) be picked up at all. In several instances it was possible to distinguish between tactical (lower echelon) and command traffic. By combining the two, the purpose of training

exercises could be inferred. It was learned that in case of a German landing the coastal defense forces were to withdraw at first and then destroy the invader by means of mobile tactics after reassembling and forming centers of gravity.

During intercept operations a few of the identified divisions disappeared from the radio picture for varying periods of time, some altogether. Their whereabouts in the interim could not be ascertained in most cases. In no instance was it possible to obtain reliable information about their movement overseas, which, however, was subsequently presumed to have taken place. A coincidence led to the discovery of a troop movement from Carlisle in northern England to Belfast in Northern Ireland, which the Luftwaffe was ordered to reconnoiter and attack. The Germans made the mistake of neglecting to observe overseas radio communication with adequate means at the same time they were intercepting traffic between points within the United Kingdom. Nevertheless, the over-all picture of the disposition of the enemy forces continued to be known, especially since many of the cryptographic systems in use were broken after about September 1940.

Summing up, British army radio traffic in 1940–41 can be appraised as follows: Messages could be easily intercepted for three reasons: each net operated on a single frequency, frequencies were changed only at regular intervals, and the British used a call sign system which facilitated the identification of the NCS and secondary stations. Nor were these defects offset by the excellent radio discipline which the British observed in the beginning. When the latter deteriorated, even the most skillful encipherment could no longer guarantee security. Secrecy was lost by the mention of towns, areas, and troop designations in the clear. The careless way in which radio operations were carried out suggests that the British underestimated German communication intelligence.

INTERCEPT OPERATIONS AGAINST GREAT BRITAIN AND THE UNITED STATES (1942)

No substantial changes were made in the British radio system until the summer of 1942. The Bergen Fixed Intercept Station in Norway was established and it covered Great Britain, Canada, the United States, and the American bases in Iceland, Greenland, and Central America. Altogether, these areas were covered by about 150 receivers. British nets could be easily detected because they continued to use call signs taken from the "call sign families," for example, FBA, FBAE, FBB, etc. Moreover, clear-text messages transmitted both by phone and CW provided many valuable hints about the morale of the troops. Grid coordinates were easily solved, even if the fliers did not make the mistake, as was frequently the case, of radioing place names and grid coordinates in the clear, after which the ground station would immediately relay the very same designations in code.

The Canadians had to a large extent adopted the British procedures (call signs, frequencies, and cryptosystems) but they were distinguished by characteristic details, so that they could be identified even before cryptanalysis was instituted. The presense of the Empire troops in the British Isles was detected by recognition of their individual characteristics. Still more revealing were the messages sent by foreign units stationed in England: Poles, Belgians, French, Norwegians, and others.

Until its integration into the Regular Army, the traffic of the British Home Guard showed special characteristics which made it easy to observe its activities, organization, strength, and deployment. Valuable intelligence was obtained, either through the mention of individual troop units or of tactical doctrine, by observing RAF units which were attached to the Army. Such intelligence covered a variety of subjects, including individual aircraft, liaison staffs, and airfields. It enabled the Germans, for example, to follow every detail of an engagement during maneuvers, including the identification of tactical objectives as provided by British reconnaissance planes, the operations of major formations, and reports sent upon completion of a bombing mission—all from the interception of clear-text messages.

Maneuvers in general were a fertile source of information, because the procedure signs (in the clear) which headed each message could be recognized immediately. Command post exercises provided an abundance of information about unit designations, physical location, organization, equipment, state of training, officers' names, in short, all the small pieces needed by intelligence for building up a complete jig-saw picture of the situation. Warnings exchanged between operators about impending inspections by their superiors showed that there was a lack of radio supervision.

In the spring of 1942 a large-scale maneuver was carried out south of London, called "Operation Tiger," which lasted several days. Two motorized divisions and several RAF units participated, and their composition and strength were clearly recognized in a short time. The course of the exercises were followed so exactly that by sending over the Luftwaffe the Germans could have converted the maneuver into a real combat action. These German intercept successes were shortly afterward confirmed by British press and radio reports.

Until the summer of 1942 no difficulties were encountered in intercepting American radio communication, with the result that inter-net relationships could be clearly ascertained. From the more distant areas of the United States only the sky waves were heard, while troop exercises could not be picked up at all. Even after the subsequent coordination of British and American operation procedures there were still many characteristics which made it easy to distinguish the units of each Army. They used different operating signals and different abbreviations for identical service branches

and units. In phone communications differences in enunciation provided the most striking contrast. Translators did not find it difficult to master both "English" and "American" literary, colloquial, and military styles, as well as slang expressions. Special dictionaries and glossaries of idiomatic phrases were supplemented from current intercepts.

In the United States proper the activation of divisions and other units could be followed almost perfectly. Their stage of training could be ascertained from transfers to various camps. Their degree of combat readiness and their impending shipment overseas became evident from the assignment of APO numbers. These APO numbers were then carefully followed. If they appeared in connection with an eastern port, for example, New York, it was clear that the unit concerned was to be shipped to Europe, whereas western port designations, for example, San Francisco, meant shipment to the Pacific.

American units were recognized soon after their arrival in the British Isles by the previously known APO numbers, and their subsequent whereabouts could be traced from clues similar to those provided by the British units. Thus, all major American units were currently identified.

A special source exploited by German communication intelligence was the transmission of officers' promotion notices. The typical message (in clear text) began as follows: "The President intends to promote you to . . .Do you accept?" These "promotion messages" supplemented our locator files and enabled us to draw various inferences. If the unit of the officer in question had been previously known but its present station had not been traced, a promotion message transmitted, for instance, to Iceland would thus provide the Germans with its location.

In the spring of 1942 a new transmitting technique was introduced in American long-distance communication (both domestic and foreign) that dried up this excellent source of German intelligence. The Euskirchen station, which was charged with cryptanalysis of this traffic, solved the riddle within one week, however, by means of tape recordings and systematic analysis. It was finally discovered that the process used was a rapid system of wireless telegraphy which differed from the usual method by the number of current impulses. This was the "Radiotype"* method. A tremendous number of military and business messages were soon intercepted. After a short while the receiving operators were able to "read" the message tapes as fast as Morse code. Fortunately, after a pause of one week, military messages in clear text became more frequent for a time. This mistake was not discovered by the Americans until later, at which time they began to encipher these

*Referred to as "War-type" in the original. "Radiotype" is a six-impulse teletype system developed by International Business Machines and used temporarily by the U.S. Armed Forces. [*tr.*]

mechanically transmitted messages. Since it was no longer possible to solve them, work on these messages was discontinued.

In the summer of 1942 the British introduced new radio techniques, which were also widely adopted by the Americans. At El Alamein the British captured the entire equipment of the intercept company attached to the German Africa Corps. As will be explained at length in the section on Africa, they recognized their former misktakes and quickly corrected them on all fronts. However, these new methods were not introduced everywhere simultaneously, but at first only in Africa. German intercept troops in western Europe were thus able to adjust themselves in time. German communication intelligence now encountered considerably more difficulties in evaluating the traffic. Call signs and frequencies were changed at irregular intervals, which made it impossible to recognize inter-net relationships. It required some time and considerable experimentation before other distinguishing characteristics enabled German traffic analysis and direction finding units to overcome these difficulties. The numerous, informative messages in clear text disappeared. One of the best sources of intelligence were the careless transmissions of the RAF, over whose radio discipline the British Army apparently did not exercise any control or supervision.

The landing operation at Dieppe in August 1942 provided not only the Allies but also German communication intelligence with some interesting lessons, successes, and failures. The preparations for this operation were completely concealed from German radio intelligence. The participating Allied units observed exemplary radio silence up to the actual landing. This procedure was the correct one and later resulted in the same degree of surprise during the landings in North Africa and during the invasion of Normandy.

Even after the landing at Dieppe, with its ensuing radio traffic, German radio intelligence did not immediately recognize what was going on. The first intercepts were received with good signal strength by The Hague Fixed Intercept Station. Somewhat later the station in Etretat heard some extremely weak signals which failed to reveal the general situation. The Hague station had no data regarding their precise direction, but because of the strength of the signals, believed that fighting was going on in the Netherlands. With this in mind, it inquired at the local Army headquarters, where nothing was known. OB West had not been notified. The report was transmitted very inefficiently from the attacked units through the long chain of command to OB West. By the time the nature and location of the event had been clarified in this irregular manner, German communication intelligence was once again working systematically. The interception of all messages from Dieppe was centrally controlled from St. Germain. Enemy messages became more numerous and informative until around noon, then remained at the same level for a while, only to become fewer with the disengagement which took place in the late afternoon, and then disappeared entirely during the cross-

Channel evacuation. OB West could be informed more rapidly about every phase of the fighting through radio intelligence than through the communication channels of the field units. Encrypted messages were solved even during the course of the attack. However, the numerous code names for targets, terrain features, and the like, could not be interpreted during the brief course of the operation. Conspicuous in these codes was the frequent mention of colors. Captured documents subsequently revealed that these indicated beachhead sectors. Since this procesure was repeated during later landings, any mention of colors came to mean to German communication intelligence: "Imminent danger of invasion."

AFRICA AND THE NEAR EAST (1941–43)

In March 1941 the German Africa Corps was given one intercept platoon, which was soon enlarged into an intercept company to which were assigned English-language cryptanalysts from the intercept command station. The company was equipped with receivers and direction-finding instruments suitable for use in a tropical climate. The personnel had had experience in intercepting British traffic ever since the Campaign in the West and therefore knew the weaknesses of the British radio system. During operations against the United Kingdom the Germans arrived at the conclusion that the British were underestimating the successes of German communication intelligence, and this became even more obvious in Africa. Here, in mobile desert warfare, radio was the only possible form of communication—a medium as dangerous as it was valuable—and the British used it more carelessly than ever. A clear and accurate picture of the opposing British Eighth Army with regard to all the details of its composition, the origin of its divisions (South Africa, India, and so forth), and its morale and plans, was rapidly gained as the result of the mistakes described in the preceding section. These mistakes included clear-text radiotelephone and telegraph messages mentioning geographical data, the names of individuals, and unit designations; the failure to mask such terms properly; and the use of extremely simple ciphers and routine call signs. German intelligence in Africa also had some exceptionally lucky breaks, as, for example, when it was able to report on impending British operations after solving messages sent by the American liaison officer.

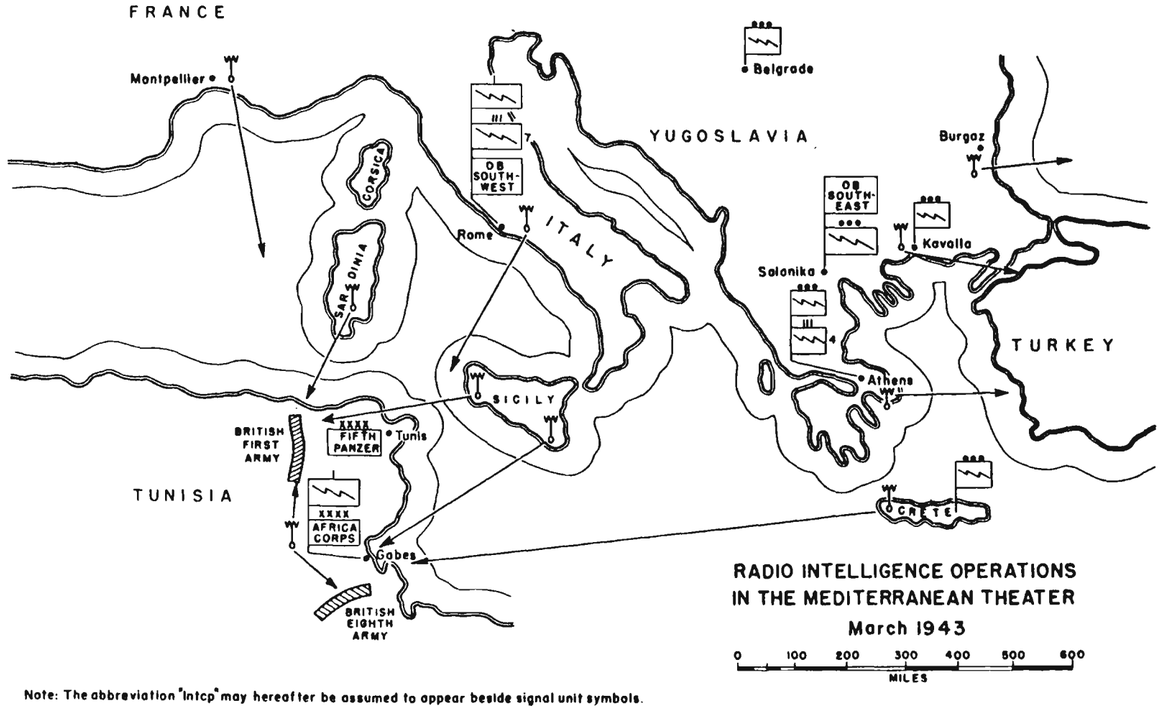
In the summer of 1942 a German submarine operating in the eastern Mediterranean captured a ship on which was found a complete set of radio codes used jointly by services of the British armed forces in the Mediterranean theater from Gibralter to Egypt. The security of radio communication in this area was a matter of vital concern in safeguarding the British supply line. The submarine, which had been assigned to other tasks, was immediately recalled after reporting this valuable prize. Because it was then possible to decrypt rapidly all British radio communications using these codes, German countermeasures at sea and in the air were especially

successful for the next two weeks. Then this traffic ceased entirely. The British had become suspicious and did not resume radio operations until six weeks later, after couriers had been able to deliver new codes throughout this far-flung theater of operations.

The excellent results obtained by communication intelligence provided Field Marshal Rommel with accurate and welcome information, on which he could base his bold and varied tactics. His peculiar talent for gaining unexpected success in armored warfare, where radio communication played a vital role, had already brought him a number of startling victories as commander of a panzer division in the Campaign in the West. In the desert Rommel encouraged this new method of tactical reconnaissance, especially since the results of German air reconnaissance were limited by British air superiority. To facilitate the detailed evaluation of information by the intercept company, Rommel's chief of staff always had two field trunk circuits at his disposal to handle incoming telephone and teletype traffic. During all his inspection trips to the front Rommel was personally informed by radio about all important results obtained by radio intelligence. It may be assumed that the British did not employ any radio intelligence of their own against the German Africa Corps; at least they did not succeed in solving Rommel's codes. Thus, German radio intelligence was able to work unsuspected by the British.

Rommel also made use of radio deception by having several radio stations simulate large forces far to the south in the desert and suggest an encirclement. On repeated occasions radio intelligence was able to observe that the British were taken in by this strategem, and that apparently without any confirmation by their reconnaissance planes they sent tanks and motorized artillery, once even an armored division, to oppose the fictitious enemy. On one other occasion, however, German radio intelligence was unable to detect a British armored division which had advanced far to the south, since it had observed absolute radio silence for several weeks, as was subsequently confirmed by a captured regimental commander.

In front of El Alamein the intercept company was able to report the reinforcement of the British forces and their preparations for an attack with which the German–Italian forces could not possibly cope. The intercept company and its evaluation center were imprudently stationed far in advance of Rommel's headquarters and only a few kilometers behind an Italian sector of the front which was subsequently penetrated by British tanks in late October 1942. While defending itself the company lost more than a hundred dead; the company commander was seriously wounded and died in a Cairo military hospital. Because of the surprise achieved by the tank attack, there was no opportunity to destroy the valuable intercept files. Thus, the enemy captured the German records of intercepted British messages and codes and the analyses prepared by the German intercepted service, as well as German and Italian radio schedules and ciphers.



Note: The abbreviation "Intcp" may hereafter be assumed to appear beside signal unit symbols.

Chart 2

German units in the Balkans operated under the Commander of Communication Intelligence (Four) subordinate to OB Southwest. Units assigned to the African theater reported, after February 1943, to the Commander of Communications Intelligence (Seven), subordinate to OB Southwest.

Except for the results obtained from observing the British Eighth Army, German radio intelligence had little success, inasmuch as nothing important could be intercepted except British command messages, which could not be solved. German radio intelligence worked together with its Italian counterpart against the British. This cooperation was extremely cordial, but furnished few results of any importance.

The proposal to supplement radio intelligence operations, then directed exclusively against the east, by a chain of intercept stations directed toward the south and extending approximately from the Balearic Islands to Sardinia, Sicily, and Crete was rejected, since Anglo-American landings in Africa were believed out of the question because of the vulnerability of Allied supply routes to submarine attack. In addition, there were supposedly not enough intercept units available for such a precautionary measure.

The Allied landings in French West and North Africa on 7 November 1942 came as a surprise because of the secrecy afforded by radio silence. The unpredictable sky wave radiation on the short wavelengths, preferred by the British and Americans for military traffic, was responsible for accidental success on the part of German radio intelligence. The intercept stations in Norway, the Netherlands, and France which covered the west, chiefly England, picked up almost all Allied messages following the landing and were able to work without the assistance of direction-finding stations to the south, since a sufficient number of localities were mentioned in Allied messages. On the first day of the landing the Bergen (Norway) Fixed Intercept Station received the messages with good signal strength. Bergen immediately recognized their importance and reported them to St. Germain. Since the traffic resembled that used at Dieppe, especially with regard to the use of colors to designate beachhead sectors, there was no longer any doubt that a landing had occurred.

In spite of or because of the long distances, the signals in question were also well received in the St. Germain area, even including traffic between regiment and battalion, since the short wavelengths were used almost exclusively. A large volume of messages was received, which was not surprising in view of the strong Allied forces committed. There is nothing new to be said about enemy radio procedure at that time. In spite of all attempts at uniformity American traffic could still be distinguished from the British. The former was generally characterized by greater carelessness. Field codes and ciphers were solved and a large number of careless messages in clear text appeared once again.

German radio intelligence gathered information about the following points: all beachheads, the neutralization or desertion of French troops, the progress of the advance into the interior, some of the advance routes and objectives, supply problems, cooperation between air and ground units, the order of battle of the landing forces and their tactical organization during the advance. After the arrival of the first elements of General von Arnim's Fifth Panzer

Army, reports were heard from armored reconnaissance elements about German positions, movements, and engagements. Added to these were the usual details, such as names of officers and reports on casualties, armament, and equipment; in short, the entire course of events were followed in detail by a branch of German communication intelligence that actually was assigned an entirely different mission on another front. It is hardly an exaggeration to say that during at least the first phase of this campaign almost one hundred percent of the Germans' information about the enemy in this new theater was provided by communication intelligence.

The next step was to forward this information to the German forces in Africa without undue loss of time. At that time OKH approved the essential features of the once-rejected plans for establishing a theater of operations, Oberbefehlshaber Suedwest (Commander in Chief, Southwest, or OB Southwest), and the requisite measures were swiftly taken. First, an army intercept company, supported by a Luftwaffe communication intelligence unit, was sent to Taormina in Sicily, and later, for technical reasons, to Marsala at the western tip of the island. There the company operated quite successfully, since it was close to the front and the Americans still failed to observe radio discipline. This unit rendered valuable service to the German command. In February 1943, the position of Commander of Communication Intelligence (Seven) was created with an evaluation center in Rocca di Papa, south of Rome, under OB Southwest (Field Marshal Kesselring), whose headquarters was in nearby Frascati.

Because of the favorable results obtained by communication intelligence, its relations with all Army and Luftwaffe headquarters were excellent. For example, at a conference in the headquarters of OB Southwest, the Commander of Communication Intelligence reported a British message just received which revealed that there was a considerable traffic jam in a certain wadi (dried up river bed), the location of which could not be determined by cryptanalysis but could be surmised, since several columns were blocking the wadi. Kesselring radioed orders for planes to reconnoiter this wadi. Air reconnaissance confirmed the intercept while the conference was still in progress, and a short time later a report was received that the troop concentration had been successfully bombed.

Errors in interpretation also occurred. However, such instances were rare, since all unconfirmed reports were given with reservations. For example, prior to the invasion of Sicily a British message spoke of a successful landing. Since only one direction-finding team was available, only one bearing could be taken. The reading suggested a point on the southern coast of Sicily. As was subsequently revealed, no landing on Sicily had taken place, but a landing exercise had been carried out on islands off the African coast which lay in the path of the bearing taken. This experience made the intelligence analysts more cautious in their judgments. As a result, one of them did not immediately report a landing on the Italian mainland from

Sicily, because he believed that this, too, was a training exercise. In this case, however, it was the real invasion.

The Communication Intelligence Commander's request to save the intelligence company in Africa from impending capture and thus preserve it for future action by transferring it to Italy was turned down because of Hitler's order that no men or equipment were to be evacuated from Africa. Thus, only a small part of the valuable personnel and radio equipment could be saved. The conduct of the personnel of the company, with whom radio contact was maintained until the arrival of the enemy tanks, was excellent. They reported that they had destroyed all valuable matériel, and that every man was aware of his duty after being captured.

SICILY AND ITALY (1943–45)

Since enemy air superiority seriously hampered German air reconnaissance during the fighting in Sicily and southern Italy, communication intelligence played a more and more important role. One corps commander summed up this trend by saying he no longer needed an intelligence officer (G-2) for compiling reports on the enemy situation, since the only available sources of information were the intercepts furnished by communication intelligence.

In the course of the numerous landings during the following months the enemy was again able to achieve surprise by maintaining radio silence. In between landings, however, German communication intelligence was able to gain information that was instrumental in countering these landings.

During the fighting in Sicily an intercepted message, revealing a planned minor landing on the northern shore of the island, was transmitted not only to OB Southwest and to *Korps* Hube, which was then fighting in Sicily, but also to the intelligence officer of Luftwaffe commander, Field Marshal von Richthofen. The intelligence officer did not report this message immediately but waited until the regular staff meeting, which was held later. Consequently, the Luftwaffe was unable to carry out counterattacks in time. Richthofen was furious and immediately ordered that in the future all such reports should not go through channels but should be sent directly to him or his chief of staff and simultaneously also to the Luftwaffe field agencies concerned. During a similar but bigger landing, which was supported by naval artillery, another message intercepted by radio intelligence resulted in the timely and effective bombing of the enemy's ships offshore, which compelled him to call off the operation.

The problem of quickly informing front line units of all intelligence reports concerning them was solved in other theaters by drastic decentralization whereby small teams were located in the vicinity of division staffs. The time-consuming route through the chain of command was thus avoided. In Italy, however, centralized intercept methods could work with greater technical efficiency, and a large evaluation center could provide better results, in view

of the many languages spoken by the enemy. Thus, all tactical intelligence information of importance to the lower echelons were encrypted in a special cipher and broadcast by a powerful station, with the exception of secret operation reports, which were forwarded through the customary channels. These radio warnings saved many lives, especially among artillerymen, and were gratefully received by all.

In evaluating the results obtained by German communication intelligence in this theater during the last year of the war it should be noted that the enemy signal personnel had learned in the course of the war to respect German communication intelligence. The Germans now had to strain every effort to detect and exploit the inevitable weaknesses in Allied radio communication. Messages which offered little prospect of success were now given secondary consideration. These were chiefly command message from division to higher headquarters. Main emphasis was placed on front-line traffic forward of division. The difference between long-range and short-range intelligence had gradually disappeared, since the former relied more and more on the information obtained by intercepting enemy radio traffic in the forward lines.

In Italy the British and Americans had coordinated their radio techniques to such an extent that there were hardly any differences to be noticed. Apart from pronunciation and subject matter their respective transmissions could be distinguished only by a few operating characteristics and some differences in troop designations. It was simpler to recognize units which did not speak English. The French used their old peculiar methods and were fairly easy to identify, while the Brazilians offered no difficulties at all.

In all cases it was possible to obtain information from mistakes made by the enemy. The sending of messages in clear text furnished unit designations, terrain data, and officers' names. Attempts to disguise operating signals and grid coordinates were still unsuccessful. The cryptographic systems used by the higher echelons continued to resist analysis, but many field ciphers could be broken. In this connection it should be acknowledged to the credit of the Allies that only a few of these messages in field ciphers revealed events of tactical or strategic importance, at least not directly. On the other hand, it was frequently possible to draw conclusions.

On the whole, however, enemy radio communication was so good that German radio intelligence was confronted by a crisis in March 1944, since it had become almost impossible to ascertain Allied intentions in time. It had also become difficult to recognize the order of battle during the withdrawal and transfer of units, and changes in command. But then, as subsequently happened in France, the Allied air forces came to the rescue.

Intensive study of intercepts covering a fairly long period disclosed a definite relationship between preparations for offensive operations and the assignment of air liaison officers to front line divisions. Assault divisions which did not have an air liaison officer were assigned one, while other

divisions were assigned a second one. The air liaison nets were easy to intercept, since the system used was of a lower quality than that employed by the British and American ground forces. This knowledge in turn enabled the Germans to predict accurately when enemy attacks would begin. German Army interception of the Allied strategic air force revealed the points of main effort of reconnaissance flights, and target areas, which helped to clarify the enemy's overall plans.

Some trivial details furnished information to communication intelligence, as is shown by the following examples. An impending attack against German defenses in the Naples area was detected in time because a small supply unit mentioned that rum was to be issued on a certain day. Since it was known that the British issued rum to their troops before an attack, it was possible to warn the German defenders.

The following was heard from a British station at Lake Commachio: "The German troops are retreating in a hurry and even the Italians are advancing." The presence of the British unit was already known, but this message confirmed the first employment of Italians in combat on the Allied side. The radio operator of a French unit described his anticipated amorous adventures in Naples. No French units had previously been detected at the point from which he sent his message.

It is difficult to understand why the Allies, at least during position warfare in this theater, failed to mask their offensive ground operations by maintaining radio silence just as they did during surprise landings. Unlike the situation in the desert, their telephone lines in Italy were certainly adequate for this purpose. As was the case in Russia, this carelessness was probably due to a feeling of absolute superiority. Nevertheless, the manner in which enemy radio operations were conducted offered the weaker defenders much information which cost the attackers losses which could have been avoided.

DEFENSE OF WESTERN EUROPE (1944–45)

Following the spring of 1944 German communication intelligence in Italy and France noticed a shift in heavy enemy concentrations from the Mediterranean area to England. American and British elite divisions, which had previously been observed in southern Italy or elsewhere in the Mediterranean theater, appeared in the British Isles. The following is an example of German intercept work during that period: An American airborne division (the 82nd?) had been reported for quite some time in southern Italy when it suddenly disappeared. About three weeks later over a hitherto unidentified net in England there was transmitted a reference to the search for a soldier against whom a girl in the United States had instituted paternity proceedings. The shipment number of this soldier tallied with the code designation used by the missing airborne division. When communication

intelligence reported this finding and suggested that the airborne division might have been transferred to England, the Armed Forces Operations Staff replied facetiously that the division had most likely been transported by submarine, but that no transports of this kind had been observed near Gibraltar. Nevertheless, the new radio net was put under special observation for any characteristics of this airborne division, and indisputable evidence of its presence in England was soon secured. It subsequently turned out to be one of the first invasion units to be reported.

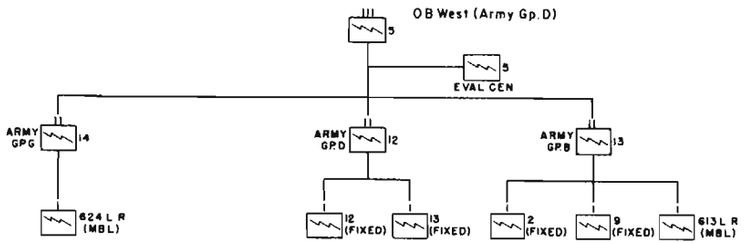
The methods employed in intercept operations against Great Britain did not change substantially during the last eighteen months of the war. Chart 3 enumerates the German radio intelligence units which were available in 1944. A subsequent comprehensive evaluation prepared some time after the start of the Allied invasion showed that approximately ninety-five percent of the units which landed in Normandy had been previously identified in the British Isles by means of intensive radio intelligence. Thus, one may conclude that the information provided by communication intelligence was quite adequate and that the German Supreme Command was in a position to calculate the strength of the enemy forces. Locator cards, regularly issued by the communication intelligence control center, contained precise information about newly organized divisions, and the appearance or disappearance of radio traffic from and to specific troop units. The intercepted radio activity during the numerous landing exercises furnished a picture of the projected invasion procedure. It was impossible, however, to obtain any clue as to the time and place of the landing. The radio picture did not change noticeably until the last day before the invasion. All previously known and observed types of traffic continued as usual. No radio deceptions were recognized. No kind of radio alert was observed before the landing. According to later reports the first wave sailed on short notice.

The Allies scored a great surprise on 6 June 1944 by the imposition of radio silence. Any different action would have been a grave blunder not to be expected of an enemy who had had five years of varied wartime experience, both good and bad, with German communication intelligence, and which after a long period of preparation was now launching the decisive battle of the war.

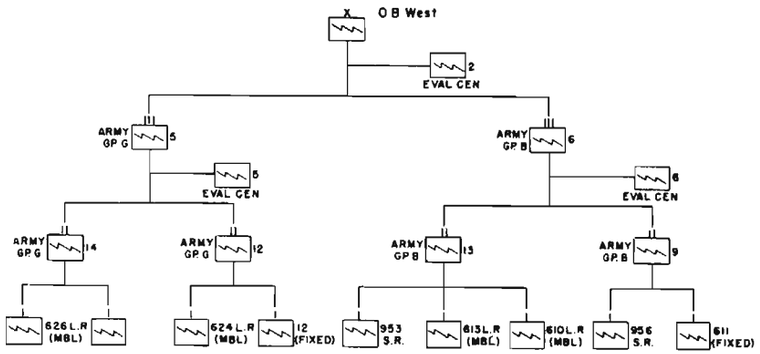
The German radio intelligence organization in the West had been prepared for the invasion during the preceding months. Its actual beginning, therefore, brought no special changes. The entire organization was so well integrated that it could handle the additional workload. Gradually all monitoring of unimportant areas, such as Ireland, Spain, Portugal, and Brazil, was discontinued in order to save personnel and equipment and to release all available men for intercepting the traffic of the Allied forces that had landed. Since the evaluation data had been distributed to all units, it was possible to transfer the intercepting of new radio traffic from one unit to another at short notice. This was only possible, however, because all the units had

ORGANIZATION OF RADIO INTELLIGENCE UNITS UNDER O B WEST

(A) At The Start Of The Allied Invasion Of France, June 1944



(B) After 1 January 1945



Note: Headquaters Designations Beside Signal Unit Symbols Indicate Physical Location Of The Signal Unit: Long Range Is Indicated By The Initials L. R. And Short Range By The Initials S.R.

Chart 3

thoroughly trained and experienced personnel. Breakdowns in the command net caused by enemy air attacks reduced the speed with which intelligence results were transmitted, but this difficulty was overcome by a prearranged plan which was put into effect all along the line from the unit furthest forward back to the communication intelligence control center.

After the initial landings, long-range intelligence at first produced only minor results. This was explained by the fact that the Allies did not wish to offer any clues to enemy radio intelligence and therefore restricted their radio communication. Moreover, the short distances withing the beachhead areas probably permitted the issuance of verbal orders and reports. In addition, the enemy was able to use telephone connections, which were not disrupted by any Luftwaffe interference. The expansion of the beachheads resulted in the transmission of so many radio messages that a fairly clear picture of the enemy situation was speedily obtained. An even greater wealth of information was provided by short-range radio intelligence and divisional combat intelligence. The signal officer for OB West moved his short-range intelligence company to Seventh Army headquarters near Caen to improve short-range intelligence operations. The reports on the situation emanating from communication intelligence about forty-eight hours after the beginning of the invasion listed most of the enemy divisions and included data on the enemy army group then in command.

The postwar press gave much attention to the opinion expressed by General Jodl, the Chief of the Armed Forces Operations Staff, who said that a second landing was expected north of the Seine and that therefore the German reserves and the Fifteenth Army stationed in that area were not immediately committed in a counterattack. The information obtained by communication intelligence did not support this assumption. The chief of the control center of Communication Intelligence West was asked to express his personal opinion on this matter during a conference of the Western Intelligence Branch. He said that a comparison of the number of units already recognized with those previously identified in Great Britain permitted the conclusion that most of the Allied forces had already been landed and that the remaining ones were insufficient for a second landing. Any still uncommitted units would be needed to feed the current battle. This opinion was shared by the Western Intelligence Branch, but was in contradiction to that of the Armed Forces Operations Staff. The estimate of the situation was given some validity by the fact that a short time after the beginning of the invasion a British landing craft had been captured near Boulogne. However, it seemed obvious that this enemy craft had lost its way.

It should be noted that unfortunately not only in this instance but throughout the war General Jodl, as well as Hitler himself, frequently showed a lack of confidence in communication intelligence, especially if the reports were unfavorable. However, orders were issued as early as the time of the Salerno landing that all favorable reports should be given top priority

and dispatched immediately, regardless of the time of day. Moreover, Communication Intelligence West was required to furnish a compilation of all reports unfavorable to the enemy derived from calls for help, casualty lists, and the like. When, during the first days of the invasion, American units in particular sent out messges containing high casualty figures, the OKW was duly impressed. In contrast, the estimate of the situation prepared by the Western Intelligence Branch was absolutely realistic and in no way colored by optimistic hopes.

As already mentioned, short-range radio intelligence and combat intelligence provided such an abundance of information that even in Normandy any attack of division strength and greater could be predicted one to five days in advance. The American field cipher device was compromised. To be sure, messages enciphered by this system could at first be solved only after a delay of from two to four days. Later on, when more data had been gathered, only a few hours were needed. The British cryptographic service was unchanged: while the Army was as efficient as ever, the RAF continued to be careless. As in Italy, communication intelligence maintained routine interception of the messages sent by air liaison officers attached to British Army headquarters, who thereby revealed the intentions of the enemy command. There was no cryptographic cooperation between the Army and the RAF, nor was there any unified control in this field.

In spite of low personnel strength and disrupted signal communication, German communication intelligence proved capable of covering the Allied forces' advance to the Rhine by reporting the approximate composition and strength of the enemy units as well as the boundaries between forces of different nationality. Battle-tested divisions were more careful in their radio operations than new ones. The Americans generally observed less radio discipline than the British, and thus provided a better source of information. During the first excitement of the invasion, both the Americans and the British often transmitted in the clear. The Canadians, who formed the numerically weakest landing contingent, supplied quantitatively the least information. Among the American forces, Patton's army was the easiest to observe.

The U.S. Seventh Army, advancing from southern France, offered the greatest difficulties, since it maintained exceptional radio discipline and cryptographic security. It could be plotted only by intensive D/F operations. This fact may perhaps be attributed to the Seventh Army's previous combat experience in Africa, Sicily, and southern France, where its forces had learned to deal with German communication intelligence. In any event, the Seventh Army furnished an interesting example of a major command's having trained its subordinate unit commanders and signal officers to observe such a high degree of radio discipline that the sources of enemy intelligence were restricted to a minimum.

Another American army, possibly the Third, could be easily observed, because its messages were transmitted in a careless manner and because it used very primitive ciphers below division level. In addition to revealing valuable tactical information, this army gave way its passwords to the Germans twenty-four hours in advance.

Even during the fighting along the West Wall, in fact until the end of the war, the results gathered by short-range communication intelligence teams attached to newly activated or reorganized divisions were always in proportion to the interest shown by the respective division commanders, the intelligence officers, or the signal battalion commanders. All the divisions which took an active interest in efficient short-range intelligence operations were remarkably successful against an enemy who was becoming more and more careless.

Especially interesting was the information obtained by communication intelligence during the Ardennes offensive. Before the German surprise attack it was evident that the enemy was not cognizant of the German preparations, since the assembled armies—the Fifth and Sixth Panzer Armies—observed radio silence. Communication intelligence clearly recognized the composition and low strength of the American units in the sectors which were to be attacked. The enemy had not fortified his lines or placed any reserves in readiness. On the morning of D Day, 16 December 1944, a message in clear text from the U.S. First Army stated that the Germans had overrun the American positions and caught the troops by surprise "while asleep." Then followed reports of U.S. withdrawals and information about the furthest points of advance reached by the German armored spearheads, as well as reports of heavy losses.

Soon afterward, German radio intelligence scored another great success which, though it could no longer be exploited operationally, might have led to heavy American losses. This was the result of a serious blunder on the part of the Americans. A few days after the offensive began, a new net of the American military police was picked up. It was established beyond a doubt that MP units with radio transmitters had been stationed at all important road crossings, in fact, along all main rear area traffic arteries. They reported all major troop movements so that German communication intelligence was able to ascertain very quickly that troop units were being transferred to the Ardennes breakthrough area from all zones of action, except the French. The MPs used an easily broken cipher intermingled with a good deal of clear text—probably for the sake of speed—and thus provided the Germans not only with information about the composition of U.S. troops, but also an accurate picture—by mentioning advance guards, march velocities, and column lengths—of the time when the German thrust could be expected to meet with increasing resistance. It was also perfectly clear to the Germans that these reinforcements were not made up of makeshift emergency units, but that the Americans were throwing in complete formations, including even some elite armored divisions. By so doing they

indicated how confident they were that the Germans would no longer be in a position to attack those parts of the front from which these troops had been withdrawn.

This phone and CW traffic provided additional valuable information later on, for example, when radio intelligence was able to predict the transfer of a U.S. armored division to the Liége–Aachen area twenty-four hours in advance.

German communication intelligence continued to function smoothly in the West during the subsequent course of events up to the end of the war. The Germans always knew well in advance about enemy concentrations, such as the one at the Remagen bridgehead, and about the direction of intended armor thrusts. They had no difficulty in discerning, for example, where and with which divisions General Patton intended to strike. The enemy gradually abandoned caution with the result that many messages of a highly classified nature were sent in clear text. The intelligence officer of Army Group West, as well as Field Marshall Kesselring, estimated that the information obtained by their communication intelligence amounted at that time to ninety-five percent of the German enemy intelligence, inasmuch as air reconnaissance was then a thing of the past, very few prisoners were captured, and agents could no longer get behind the enemy front.

Because of the growing German impotence on all fronts, the command was unable to exploit the results of communication intelligence in proportion to its great value. Because of the overwhelming Allied superiority in manpower and matériel during the last years of the war, the value of German communication intelligence was largely theoretical.

APPRAISAL OF RADIO COMMUNICATIONS IN BRITISH AND AMERICAN ARMIES IN THE EUROPEAN THEATER

The British Army

British radio communication was the most effective and secure of all those with which German communication intelligence had to contend. Effectiveness was based on World War I experience in radio procedure and cryptology, in which the British Army learned many a lesson from the Navy. The higher-echelon cryptosystems of the British were never compromised in World War II. The radio operators were well trained and performed their work in an efficient and reliable manner. Nevertheless, there were also some defects. Feeling safe because of the security of their cryptosystems, the British neglected to take into account the openings which their radio communication left to German traffic analysis. Plain-text addresses and signatures contained in otherwise securely encrypted messages revealed the make-up of the British nets and thereby also the tactical interrelationship of units in which the Germans were interested. The stereotyped sequence in which stations

reported into their nets indicated the structure of the chain of command, while British field ciphers were too simple and did not provide adequate security over extended periods of time. Either the British overestimated the security of their own systems, or underestimated the capability of German communication intelligence. The same was true of the radio traffic of British armored units, which used such simple codes and so much clear text that the Germans arrived at the conclusion that the British were unaware of their field radio communications being observed.

In spite of impenetrable higher-echelon cryptosystems, excellent operating procedures, and efficient personnel, the security of the British radio communication in the United Kingdom during 1940–42, and especially in Africa in 1941–42, was so poor that, for instance, until the battle of El Alamein Field Marshal Rommel was always aware of British intentions. It was Rommel who repeatedly emphasized the predominant significance of radio intelligence reports in making an estimate of the enemy situation.

In this connection it may be pointed out that by no means all German field commanders recognized the utility of radio communication and intelligence. Many of them were quite prejudiced against these technological innovations. This may help to explain why the performance of some field commanders and their subordinate units so conspicuously surpassed or fell short of the general average. They were the ones who either deliberately or unconsciously simplified or complicated their mission by making full use of or neglecting the facilities which were at their disposal.

What surprised the Germans was that the many tactical successes scored by Rommel as the result of his unusally profound knowledge of the enemy situation did not arouse the suspicion of the British and lead them to the realization that their own carelessness in radio communication was at fault.

According to British statements the most important booty captured during the breakthrough at El Alamein were the German intercept records. A quick analysis of this material opened their eyes and led them to introduce immediate reforms. The correction of the mistakes they had made over a period of several years and the thorough reorganization of their radio communication did much to improve their security.

Whereas the RAF failed to adopt the superior radio operation procedures of the British Army and Navy, other Allies who subsequently entered the war, especially the United States, introduced the proved British methods, much to their advantage. Only France failed to do so, much to its disadvantage.

During the last year of the Italian compaign the exemplary conduct of the British, with their wealth of experience, confronted German communication intelligence with a variety of problems. In this slower and more orthodox type of warfare strict control by the British achieved a high degree of radio discipline and was able to eliminate most of the national idiosyncrasies that

characterized their radio communication. The standard of security in the Italian theater was extremely high.

The U.S. Army

American radio communication developed very much along British lines. Up to 1942 domestic military traffic in the United States and that carried on by the first units to be transferred to the British Isles revealed certain distinctive features, such as APO numbers, officer promotion lists, and unit designations and abbreviations which were at variance with their British equivalents. German communication intelligence had no difficulty in driving wedges at points where these features occurred and in compromising the security of American radio communication. The manner in which the U.S. Army handled the traffic showed that its radio operators were fast and experienced. The comments made in the preceding section pertaining to the British cryptosystems are also valid for those of the Americans. The use of field cipher devices complicated German radio intelligence operations, even though their cryptosecurity was far from perfect.

The Americans deserve credit for the speed with which they adopted British operating procedures in 1942. They must have recognized the progress made by their Allies, particularly after El Alamein. The Germans observed a continuous process of coordination aimed at eliminating the easily discernible differences between British and American procedures, except for linguistic differences which could not be erased. However, the radio discipline observed by British and American units alike while they were stationed in the United Kingdom deteriorated rapidly and reached the very limit of minimum security requirements as soon as U.S. troops entered combat. The abundance of radio sets with which American units were equipped tempted the inexperienced U.S. divisions to transmit far too many CW and voice messages in the clear. They thereby provided the German command with many clues regarding the tactical situation and U.S. intentions and enabled German cryptoanalysts to solve many an American cryptosystem. This criticism pertains particularly to the initial engagements in North Africa, and to the subsequent actions in Normandy and France in general, and to a lesser extent to those in Italy. In spite of the training during combined exercises in the British Isles, the security of American radio communication was extremely poor. During the latter stages of the war the quality and security of radio communication were far from uniform in all the American armies. There were some armies whose radio traffic could hardly be observed, with the result that their intentions remained a secret. Other armies, either deliberately or unwittingly, denied themselves the benefits of radio security. Needless to say, in spite of their obvious superiority, this deficiency proved detrimental to them and resulted in needless losses.

The comments made with regard to radio silence and deception in the section dealing with British radio communication apply equally to that of the Americans.

Apparently there existed no centralized U.S. radio command agency responsible for raising the average performance to the quality and security standards set by the most disciplined units, or for keeping in check the arbitrary and unsatisfactory operating procedures of certain armies. Incidentally, the conclusions at which the Germans arrived on this subject were confirmed by MP radio operations during the Ardennes offensive. In this instance all established rules were violated and, given a somewhat less unfavorable distribution of forces, the final outcome might have been very different, since the German top-level command had complete information on U.S. plans and operations. These happenings were in paradoxical contrast to the otherwise exemplary security measures taken by the Americans.

In conclusion, it may be said that the Americans' high-echelon nets were just as secure as their British counterparts. Tactical net operation should indeed have measured up to the required security standards. Actually, however, overall security was compromised by the many openings given to German communication intelligence by insufficiently disciplined lower-echelon units. That a maximum of security *could* have been achieved was demonstrated by the efficient radio operations of the U.S. Seventh Army during the last year of the war, when the results obtained by German communication intelligence operations in the path of this army dropped to an extremely low level. Unified control and strict supervision would surely have led to greater security among the U.S. forces in general.

Work Breakdown Structure: A Better Implementation to Manage Software Overruns

Few software systems are delivered on time and within estimated costs. This paper looks at some of the reasons for such overruns and suggests a method to limit their size through the use of work breakdown structures.

INTRODUCTION

Historically, any acquisition involving software has resulted in cost or schedule overruns. There have been few exceptions. A 100 percent cost overrun is not uncommon, regardless of the size or complexity of the expected system; schedule slips of months or years are commonplace; contractor claims against the Government amount to 100 percent of the final cost of the product. All three of these events continue to occur on many contracts. Unfortunately, there are few indications that these problems are being solved. Future acquisition will experience overruns of even greater magnitude.

Many techniques have been developed to try to curb these overruns. Techniques such as structured programming, HIPO, and programming teams have been advertised as helping to curb overruns. These techniques have been implemented for a number of years on a number of contracts, but they have been ineffective. Large overruns are still common.

The overrun problem is obviously complex, and this paper offers no solution to the problem. It makes no promises to stop or limit overruns. Instead, it takes a different tack, describing a method that can be used to manage an overrun effectively. This method plans on the occurrence of an overrun; it assumes one will occur and more accurately predicts the magnitude of the overrun at an earlier point in time.

BACKGROUND

An overrun in its simplest view occurs whenever the actual cost in time or money exceeds the estimate. What causes an overrun? There is no single cause. It could be caused by lack of detailed planning, by underestimating the expected cost, or by having to wait for people or parts not under the contractor's direct control. There are many problems which cause an overrun. There is no one solution.

Classification note: All portions of this article are UNCLASSIFIED.

For this pa(b)(3)-P.L. 86-36rded Second Prize at the 1980 Spring Conference of the Computer and Information Science Institute.

Overruns receive the most attention when they are very large, when they cannot be corrected easily, and when they have a great impact on something else (i.e., another system, solution to some political problem, etc.). Unfortunately, overruns are not even recognized until they are very large, they cannot be corrected easily, and they always impact other plans. They are recognized only at the most difficult times, only when other planning or other projects cannot be changed to accommodate this overrun problem.

The most important job, therefore, is to recover from the overrun. Once an overrun is known, its cause is unimportant. The immediate task is to measure its size and then limit its growth in the most efficient and effective manner. Too often, however, the management method initiated for the contract is not flexible enough to manage an overrun. It cannot accurately measure the size; it only makes a wild guess. Its growth potential is always unknown; it is not localized. Therefore, the impact of this overrun at any point in time is still another wild guess.

A TYPICAL ACQUISITION

At the start of the acquisition process, there is a general feeling of optimism. The contractor has a reasonable understanding of the requirements to be met. He has a reasonable estimate of the cost and schedule. And he assures us that his management philosophy and policies can pull off the job. Both sides admit there may be problems, but they will be solved early with no major side effect. The honeymoon has begun.

The contract has started and progress is being measured. According to the schedule (Figure 1), everthing is going according to plan. The contract has made its way through the first few major milestones, and the contractor appears to be working at his average rate toward the next major milestone. Time and money are being spent; everything is running smoothly.

Two weeks before the next major milestone, the contractor calls and says he has a problem. He cannot meet the schedule for the next milestone. He cites various reasons and problems that he had been hoping would be solved in time but were not. Regardless, the schedule has slipped. The first overrun has occurred.

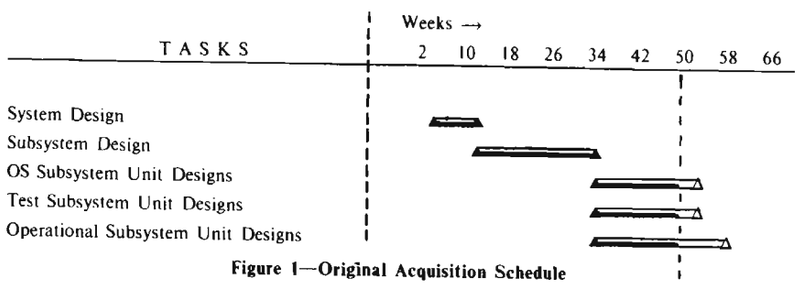


Figure 1—Original Acquisition Schedule

Eventually, the next major milestone is met. The contract advances into another phase, working toward another major milestone about three months downstream. The original schedule has been updated to show the slip (Figure 2). Progress continues to be measured. Again, time and money are being spent; everything is going according to plan.

Two weeks before the next major milestone, the contractor calls again and says he has a problem. He cannot meet the schedule for this next milestone. Agains he cites various reasons and problems that he had been hoping would be solved in time but were not. The schedule has slipped again and the second overrun has occurred. The contract is out of control. No one really cares what the causes are; the real difficulty is in recovering from the slip. More money is spent (the total amount being unknown at this point in time) to allow the contractor to finish the job.

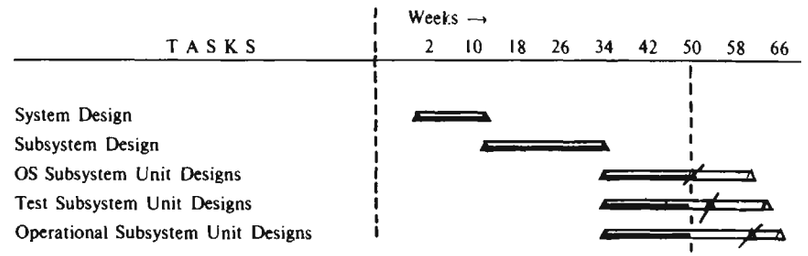


Figure 2—Schedule Adjusted for Overruns

Eventually the contract terminates. An evaluation of what went wrong and when it went wrong takes place. The evaluation points to a number of problems. Bad estimation practices were used in the initial proposal; various technical problems occurred; or any number of other problems contributed to the overrun. Solving these problems will not solve future overruns (or at least they have not thus far). They will not prevent overruns from occurring, and they will not enhance the predictability of the magnitude of the overruns.

THE REAL PROBLEM

Until recently, the easiest solution to the overrun problem has been to shovel more money to the contractor. In today's economy this solution is no longer feasible. Funds are scarce, Congress is taking a closer view of things, the taxpayers are much more interested, and we are under much closer scrutiny. Some stronger method of managing overruns must be attempted.

In reviewing the typical acquisition, we see some questions that should be asked. Why didn't we know sooner than two weeks before the first missed milestone that the milestone would not be met? Any why wasn't the impact of the first overrun known in order to prevent the second overrun? The answer to both questions is simple. We do not know how to measure

progress on a system development. We do not know where we are, and therefore we do not know when we are behind.

LEVEL 1 2 3 4 5	TASK
A D	System Software
A D 1	Operational Software Unit Designs
A D 1 A	PGM1 - Input Data Massager
A D 1 B	PGM2 - Queue Manager
A D 1 C	PGM3 - Display Manager
A D 1 D	PGM4 - Output Formatter
A D 1 E	PGM5 - Off-line Storage
A D 1 F	PGM6 - On-line Storage
A D 1 G	PGM7 - Input Link Manager
A D 1 H	PGM8 - Output Link Manager
A D 2	Operating System Enhancements Unit Designs
A D 2 A	Power Failure Recovery/Initialization
A D 2 B	Input/Output Drivers
A D 2 C	Executive Routines
A D 2 D	OS Utility Routines
A D 3	Test Software Unit Designs
A D 3 A	In-line Tests
A D 3 B	On-line Tests
A D 3 C	Off-line Tests
A D 3 D	Software Development Test Software
A D 3 E	Acceptance Test Support Software
A D 4	Utility Software
A D 4 A	Software Exerciser
A D 4 B	Configuration Control Software
A D 4 C	Data Base Processor
A D 4 D	Procedure Library Generation
A D 5	Software Support
A D 5 A	System Analyst Support
A D 5 B	Program Librarian

Figure 3—Four-Level Work Breakdown Structure (WBS)

Measurement of progress has been discussed in other literature; applying it to software has been difficult. Recently, Work Breakdown Structures (WBS) have been specified in contracts in an attempt to better measure actual work being accomplished. The concept of a WBS is simple. A large task (e.g. build a system) is subdivided into smaller, more discrete, more manageable tasks. This subdivision is hierarchical and can be done to many levels—the lowest level being the most manageable. System progress then is determined by measuring progress on each task and then combining the individual tasks' progress to show a system progress. Thus far, the correct

Figure 4

UNCLASSIFIED

combination is unknown and measurement of task and system progress is little better than it has been.

WBS TODAY

The usual way to specify a WBS is to specify the number of levels of subdivision. For instance, in a recent major contract, the requirement was to specify the WBS to at least the fourth level. The breakdown the contractor implemented for the software area is shown in Figure 3. He reported status and progress via the schedule shown in Figure 1. In the beginning, this level of reporting seemed adequate and indeed met the requirements of the contract.

As the contract progressed, the contractor reported status in Figure 4. Looking quickly at this figure, it appears that everything is on schedule. There are no problems; the next milestone will be met. Looking more objectively at this figure shows something less. For example, the first line item shows a task which is approximately 10 percent complete. But what type of measurement is this? How is it determined how much of this task is shaded and how much is not? This chart provides no key. All this chart shows is a subjective measurement of progress on a task. If this kind of measurement continues, we could find ourselves in the "90% complete for 10% of the time" syndrome. Obviously, we need a more objective measurement. The most objective measurement we can make on this task is that the task has begun, and it has not been completed. For a period of six months, this is the only objective statement we can make.

There are only two completely objective and reliable measurements of progress on any software task. These are, quite simply, (1) whether the task has begun and (2) whether the task has been completed. Only subjective measurement can be used between these two endpoints. The longer the time between two endpoints, the less reliable and more ambiguous the estimates of a system's progress will be.

Obviously, the time period specified for the task above was much too long to allow any objective measurement of progress. The lowest level task should have shorter duration. One way to ensure this is simply to require more levels of the WBS. More levels should force the lowest level tasks to be of shorter duration. Conceptually, this seems correct. However, as often happens in a contract environment, the implementation always turns out to be something different.

Suppose the WBS is as shown in Figure 3, but the contract requires two more levels. The WBS as shown in Figure 5 meets this requirement. It also defines the lowest level tasks to be of much shorter duration than the fourth level. In fact, this WBS may have been similar to the one the person writing the requirement had in mind. However, this is not the WBS the contractor had in mind. He views the tasks differently. He may come up with a slightly

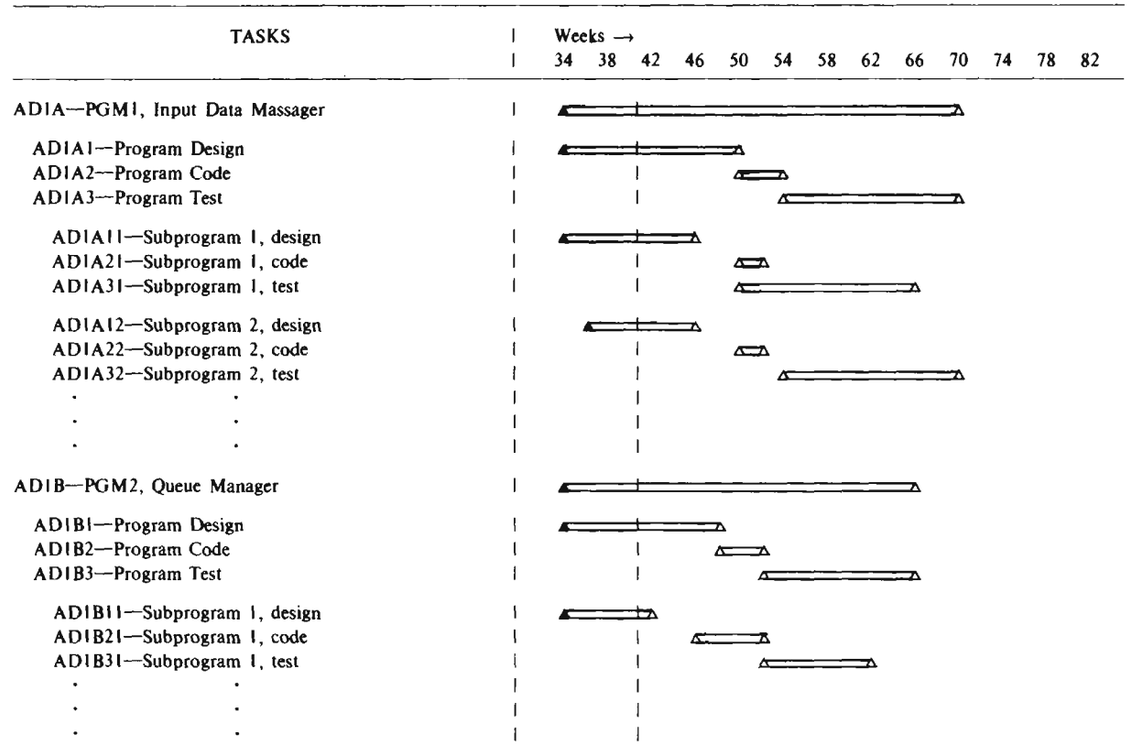


Figure 5

UNCLASSIFIED

different WBS as shown in Figure 6. The lowest level tasks are of shorter duration than those shown in Figure 4, but this still does not allow as much objective measurement as in Figure 5. The lowest level tasks still take too long.

A BETTER WBS

The main reasons for creating a WBS are to monitor the project effectively. Tasks described at high levels are very difficult to track. Structuring the overall software effort into many short-duration tasks provides many intermediate objective measurements of progress. Each WBS described earlier did not guarantee short-duration tasks. The WBS did not perform its main function.

This function must be made a requirement of the contract. One simple way is to require the Work Breakdown Structure to be specified so that each lowest level task consumes at most two weeks of time. Each high level task is subdivided into successively lower level tasks until each task is of only two weeks duration. Instead of a WBS specified to 'k' levels as pictured in Figure 7, the WBS is specified to the lowest task possible, as pictured in Figure 8. This structure is not balanced, but it more closely fits the real world environment.

A Work Breakdown Structure defined with the objective of tracking tasks over a period of two weeks should be able to provide a more objective status of the system. For example, suppose the WBS shown in Figure 5 is expanded to meet this new requirement. The breakdown of the first line item in Figure 5 may be similar to that pictured in Figure 9. We now have a more precise definition of the shaded area of AD1A; we know exactly how the percentage was obtained. There are 80 tasks, 8 of which are completed. Therefore, AD1A is 10 percent completed as the shaded area indicates.

For this particular high-level task, we know where we are and what has to be done to complete this task. If this same technique were used for each task over the entire system, we would know where we are and the amount of work that has to be done. Knowing the status of all these tasks should give us the system status at any time. Right? Not completely. Knowing where we are in the system development is very important, but it does not really show whether we can meet the schedule. Looking at the status in Figure 9, how can we tell if we are on schedule? Does the fact that the TASK M has not ended as planned mean the program is behind schedule? Does the fact that AD1A41 has begun ahead of schedule mean the program is ahead of schedule? Or by averaging these two tasks do we determine that the program is on schedule? Any of these three possibilities could exist. We cannot really determine which one does simply by looking at this chart. We know how much work has been done; we do not know where we are into the schedule.

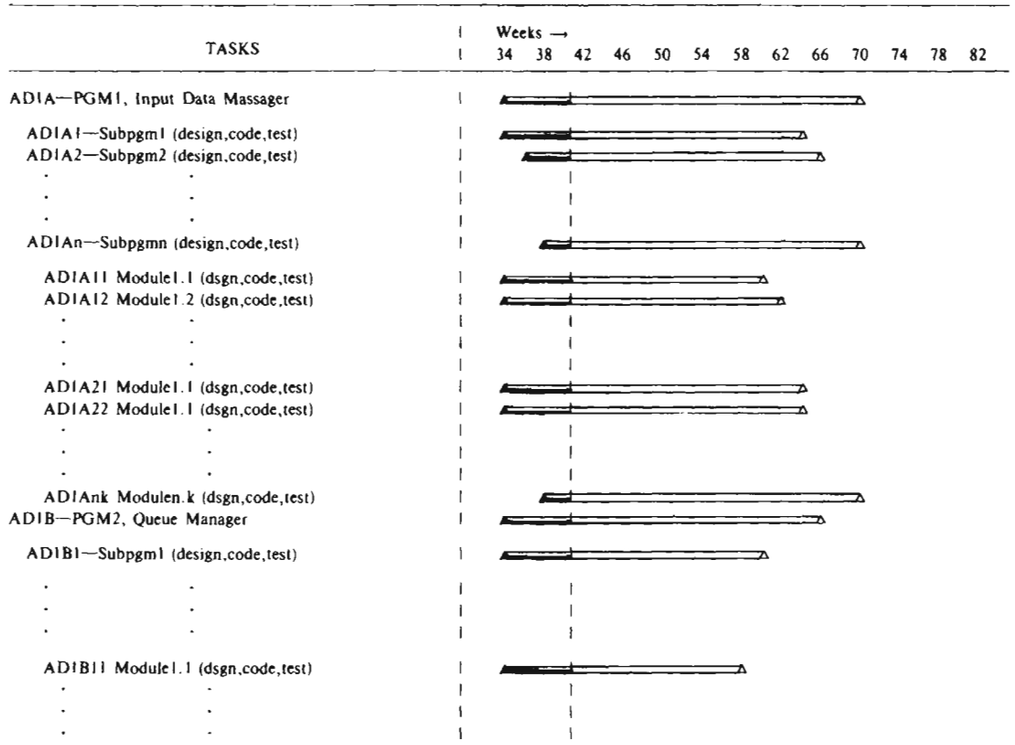

TASKS
Weeks →
34 38 42 46 50 54 58 62 66 70 74 78 82
AD1A—PGM1, Input Data Massager
AD1A1—Subpgm1 (design,code,test)
AD1A2—Subpgm2 (design,code,test)
AD1An—Subpgmn (design,code,test)
AD1A11 Module1.1 (dsgn,code,test)
AD1A12 Module1.2 (dsgn,code,test)
AD1A21 Module1.1 (dsgn,code,test)
AD1A22 Module1.1 (dsgn,code,test)
AD1Ank Modulen.k (dsgn,code,test)
AD1B—PGM2, Queue Manager
AD1B1—Subpgm1 (design,code,test)
AD1B11 Module1.1 (dsgn,code,test)

Figure 6

Figure 7—WBS Specified to "k" Level

WORK BREAKDOWN STRUCTURE (WBS)

LEVEL 1 2 3 4 5 6 7 8 9	TASK
A D	System Software
A D 1	Operational software
A D 1 A	PGM1, Input Data Massager
A D 1 A 1	Program design
A D 1 A 1 1	Define program functions
A D 1 A 1 2	Define program data flow
A D 1 A 1 3	Define program interfaces
A D 1 A 1 3 1	Define intra-program communication
A D 1 A 1 3 2	Define hardware interfaces
A D 1 A 1 3 3	Define operating system interfaces
A D 1 A 1 4	Define program structure
A D 1 A 1 4 1	Partition pgm functions to level 1
A D 1 A 1 4 2	Define level 1 interfaces
A D 1 A 1 4 3	Pseudo-code level 1 module 1
A D 1 A 1 4 4	Pseudo-code level 1 module 2
A D 1 A 1 4 5	Pseudo-code level 1 module 3
A D 1 A 1 4 6	Pseudo-code level 1 module 4
A D 1 A 1 4 7	Pseudo-code level 1 module 5
A D 1 A 1 4 8	Define level 2 structure
A D 1 A 1 4 8 1	Partition level 1 functions to level 2
A D 1 A 1 4 8 2	Define level 2 interfaces
A D 1 A 1 4 8 3	Pseudo-code level 2 module 1
.	.
.	.
.	.
A D 1 A 1 4 8 8	Pseudo-code level 2 module 6
A D 1 A 1 4 8 9	Define level 3 structure
A D 1 A 1 4 8 9 1	Partition level 2 functions to level 3
A D 1 A 1 4 8 9 2	Define level 3 interfaces
A D 1 A 1 4 8 9 3	Pseudo-code level 3 module 1
.	.
.	.
.	.
A D 1 A 1 4 8 9 8	Pseudo-code level 3 module 6
A D 1 A 2	Code
A D 1 A 2 1	Code level 1 module 1
A D 1 A 2 2	Code level 2 module 2
.	.
.	.
.	.
A D 1 A 2 H	Code level 3 module 3
A D 1 A 3	Program test
A D 1 A 3 1	Test level 1 modules
A D 1 A 3 1 1	Test using good data
A D 1 A 3 1 2	Test using bad data
.	.
.	.
.	.
A D 1 A 3 4	Test program threads
A D 1 A 3 4 1	Test thread 1
.	.
.	.
.	.
A D 1 A 3 4 V	Test thread 31
.	
.	
.	

Figure 8

AN EVEN BETTER IMPLEMENTATION OF WBS

Figure 9 lays out the tasks of the WBS on a schedule. According to this chart, however, all of the tasks could be performed independently. Every task could be performed and have no effect on any other task. Obviously, this is not possible. Many tasks depend on the completion of other tasks. Some tasks cannot be completed until others have begun. There are many dependencies between tasks which are not shown in this figure. These dependencies are used to measure progress of the system against the schedule.

These dependencies can be shown by determining the critical path through all of the system tasks. The tasks which lie on the critical path (longest schedule path) determine the status of the system. System progress depends upon progress of those tasks on the critical path.

If we define the critical path for the Work Breakdown Structure in Figure 9, we may show it as Figure 10. Now we have an accurate measure of system progress. We know where we are and we know where we have to go. If TASK M does not finish on schedule, we know we have one week before it has an impact on system progress. Likewise if TASK M does not begin on schedule, we know we have one week before it has an impact on system progress. This particular task could be ahead or behind schedule and not yet affect system progress. The system's progress being ahead or behind schedule depends only on the progress of those tasks which lie on the critical path.

The use of a Work Breakdown Structure to measure system progress, therefore, depends on two things. First, tasks must be broken down until the lowest levels are of two weeks duration. This breakdown gives an accurate estimate of work done versus work yet to do on a system. Second, the critical path for the system must be defined. System progress against schedule can then be accurately measured. One by itself can be largely ineffective. Used in conjunction, these concepts provide a very accurate estimate of progress of a system.

HOW DOES THIS HELP AGAINST OVERRUNS

Overruns have two significant traits. First, they tend to be complex and their source cannot be easily pinpointed. Second, overruns are perceived at very late—too late to change other plans to accommodate the overrun. A third trait may be that overruns tend to be very large—50 to 100 percent of the estimated cost or schedule—but this trait is simply an end result of the first two.

The methodology described in this paper deals precisely with these two traits. First, whatever causes the overrun directly affects one or more tasks on the critical path. Since each task is only two weeks long, the cause of the overrun can be pinpointed to a small number of small tasks. Instead of

battling many problems which may have caused the overrun, the software manager needs to concentrate on those specific tasks affected.

Second, by using this methodology, one can detect a possible overrun at a very early point in time. If the reporting period is two weeks, then detection is within two weeks of its start. Since each task is at most two weeks long, an overrun will be detected when any task lying on the critical path either fails to start on schedule or fails to complete on schedule. The problem is detected before it has a chance to affect other tasks—before it has a chance to grow.

As stated earlier, this methodology does not prevent overruns. It provides a framework in which the overrun can be tightly controlled. Measurement of system progress, according to task and to time, is more accurate. Breaking the work down into very small units creates a better measure of what is done versus what is left to do. Also, because of the implementation of the critical path, problems can be detected early. Both points (small tasks and critical path) help to pinpoint a possible overrun early and allow the software manager to concentrate on solving that specific problem.

DISADVANTAGES

The methodology described appears to be a simple concept, but its implementation is not simple. The major problem with this whole scheme is the difficulty of subdividing a large job into small, discrete tasks. The problem is complicated more so by defining all of the dependencies that exist between the tasks. Solving this problem is extremely difficult and requires more high-caliber management personnel at the start of the contract. These people can be expensive.

Secondly, this methodology requires constant review and revision. Much time must be spent just to review system progress. The critical path must continue to be analyzed. New task dependencies will be discovered. Work-arounds will be found which dissolve other task dependencies. This constant review and revision also requires the high-caliber contractor personnel to continue on the job. The expense continues. In this case, government personnel also monitor the system progress. They must also either spend more time reviewing the system or add more personnel to the team to perform this task.

The major disadvantages, therefore, are the cost of contractor personnel to define and implement the Work Breakdown Structure and the government manpower required to constantly review the system progress.

The cost of a contract due to the extra management personnel will be higher than the cost of a contract defined as in Figure 1. However, this higher initial cost should result in a much smaller overrun than the 100 percent overrun experienced in Figure 1. In addition, because the overrun would have been detected earlier, other options may have been available

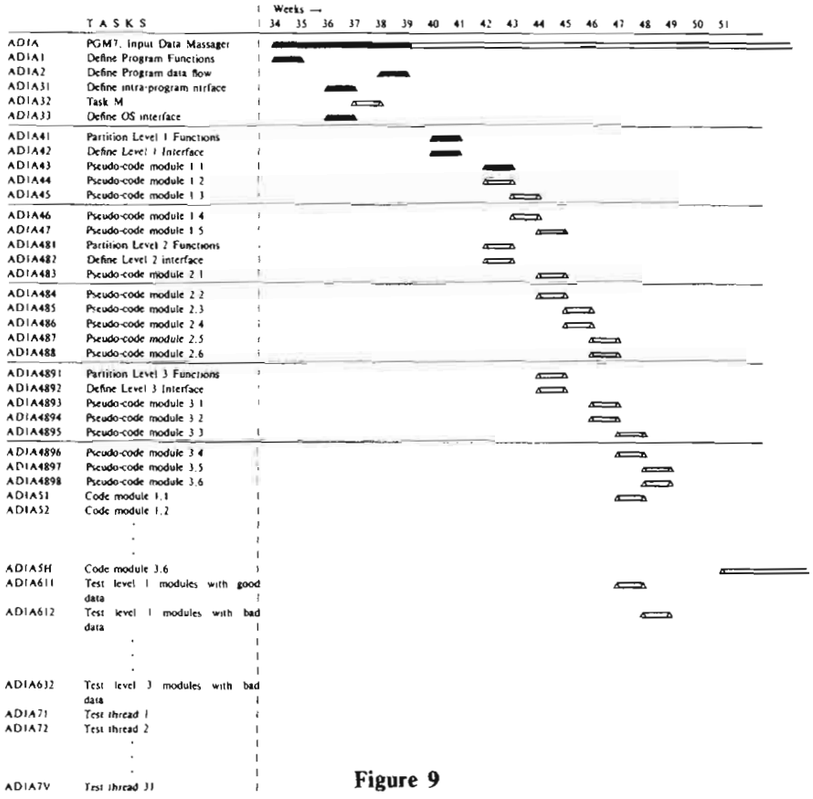
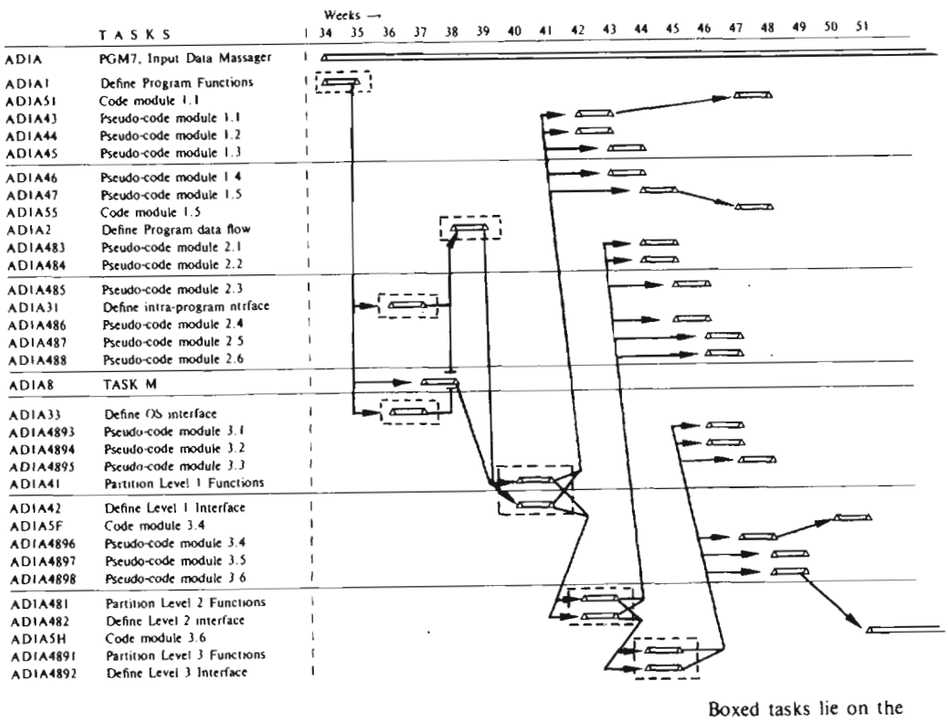


Figure 9



Boxed tasks lie on the Critical Path.

Figure 10

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

which could have further reduced the size of the overrun. The final cost of the contract should be less than if this methodology was not implemented.

Extra government personnel may not be needed to monitor system progress constantly. Some types of automation are available to help. Management tools such as PAC II can quickly determine a critical path and measure the impact of delays in those tasks which lie on the critical path. Also, the definition of a critical path narrows the areas of problems which may occur. Instead of worrying about each task in the system, the government personnel can focus on those tasks which lie on the critical path. Therefore, extra government personnel may not be required, especially if some automated tools are available.

CONCLUSION

Throughout this paper I have made a basic assumption: there is no one solution to the overrun problem. There is no tool or no methodology that will prevent overruns. Overruns will always occur. To date, they have not been managed effectively.

Usually, in acquiring a system, we have been trying to manage a process (a system development) we could not define. We have tried to control something which we could not completely comprehend. It is little wonder overruns have been so large. They are out of control before we perceive them. By that time, we are extremely limited in the actions we can take to solve the problem.

In this paper, I have presented a methodology which will help manage overruns better. Very small tasks along a critical path focus our attention to only those tasks of major importance. Because the tasks are only two weeks long, we can perceive a problem more quickly and therefore can react more quickly to solve the problem. Control of the system is tighter because the visibility into individual tasks is much greater. The methodology presented provides a framework over which this control can be exercised to successfully acquire a software system.

Contributors

~~(C~~ (b)(3)-P.L. 86-36 ("Work Breakdown Structure") — B.S.in Mathematics from Pennsylvania State University (1974); M.S. in Computer Science from Johns Hopkins University (1979(b)(3)-P.L. 86-36 NSA in 1974, as a participant in the Agency's intern program. His most recent assignment was to T3, where he worked in the Processing Software element. The article published in this issue won second prize at the 1980 conference of the Computer and Information Science Institute (CISI).

(U) (b)(3)-P.L. 86-36 ("A Computer Simulation of the Vulnerability of Frequency Hopping Communications Systems to a Follower Jammer") — B.S. in Mathematics from Brigham Young University (1978).(b)(3)-P.L. 86-36 also worked as a research and teaching assistant at BYU from 1975 to 1978. A COMSEC intern who has worked in several S Organization elements(b)(3)-P.L. 86-36w assigned to the Department of the Treasury. His article was previously presented as a paper at the 25th Electronic Warfare Conference, Monterey, California, in May 1980.

(U) ALBERT PRAUN ("German Radio Intelligence") born in 1894 in Bad Gastein, Austria, began his career in military communications in 1913, and served in the German Army through World War I, the interwar period, and World War II. In addition to the studies prepared for the U.S. Army, General Praun wrote on signals intelligence and cryptology for German publications. See NSATJ, XV, 4 (Fall 1970), for a translation of his article "On Plain Text and Cryptography."

~~(TSC)~~ (b)(3)-P.L. 86-36 [redacted] Mr. (b)(3)-P.L. 86-36eputy Chief of the [redacted] Branch, A211. Since beginning his Sigint career in 1958 as a USAF intercept operator and transcriber,(b)(3)-P.L. 86-36worked on a number of topics related to the Soviet problem, serving as a linguist, analyst, and reporter. Certified (1979) as a Collection Officer, (b)(3)-P.L. 86-36 attended Syracuse University, the University of Maryland, and George Washington University.

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

M6-Feb 81-S3-1642

~~TOP SECRET~~

WARNING

~~This Document Contains CODEWORD Material~~

~~TOP SECRET~~