probably furnish the necessary offensive and defensive equipment in those cases in which they believe it is needed. Albanian, Bulgarian and Rumanian offensive CBR capabilities are less than those of the other Satellites because of lack of industrial capacity. Their defensive capabilities are approximately equal to the other Satellites.

b. Discussion

(1) East Germany

(a) Research and Development

East Germany is credited with a moderately active CW and BW research and development program which is primarily defensive in nature. Projects which have been reported include reading research on available information in all phases of CBR warfare, design of protective equipment, preparation of small amounts of chemical warfare agents and production of small quantities of colored and screening smoke grenades. East Germany has the capability of mounting a BW research and development program, and there is considerable evidence of a BW defensive program under the Ministry of Health. There are no definite indications of any offensive CBR programs.

(b) Offensive Material

It is not believed that East Germany is producing or stockpiling CBR agents or munitions, but its chemical industry is well developed and quite capable of supporting a CW production program. It has qualified scientists and suitable facilities for producing biological agents, if necessary. East Germany does not have the means of producing radiological agents and does not produce munitions to deliver CBR agents.

(c) Defensive Material

Soviet gas masks and some Soviet-type protective clothing are issued to 50 to 75 percent of the East German Armed Forces. The division CBR companies are probably completely equipped with masks, gas capes and protective clothing and boots. It is believed that for the past two years VEB Medicintechnik (Medical Technology) Leipzig has been producing

gas masks modeled after the Soviet Shlem-1 mask. Protective clothing is also believed to be on order, but no evidence of any end items is available. East German pharmaceutical factories have the capability of producing enough antibiotics and medicinals to meet the requirements for mass treatment in case of BW attacks. Copies of three Soviet radiac instruments, a survey meter, a contamination meter and an individual dosage meter, are believed produced in East Germany under different designations.

(d) Organization and Training

The CBR organization, tactics and training of the East German Army are patterned after those of the Soviets. The CBR troop unit organization is not as extensive as that of the Soviets. However, a CBR company is organic to all divisions, and each regiment has a chemical platoon. The military CBR manuals in use are exact translations of Soviet manuals, and the training programs for CBR defense include the same instructional material, demonstrations and practical exercises as those of the Soviets.

(2) Czechoslovakia

(a) Research and Development

Czechoslovakia has a research and development program in the CW field which, among the Communist countries, is second only to that of the USSR. It is believed that research is conducted on nerve and mustard gases, psychochemicals, nerve gas antidotes, detection and identification of CW agents and protective materials. Considerable biological research is being conducted although it is characterized as part of the public health program. A significant RW research program is not likely in the next few years unless special assistance is provided by the USSR.

(b) Offensive Materiel

It is believed that Czechoslovakia is not producing or stockpiling CBR agents and that the Czech chemical and biological industries do not have the capability of producing any large amounts of CW and BW agents. In the weapons field Czechoslovakia is capable of producing artillery and mortar shells

as containers for toxic agents and of producing portable and mechanized flame throwers. However, there is no evidence that such items are now in production.

(c) Defensive Materiel

Protective masks, antigas capes or groundsheets, antigas boots and gloves, and personal decontamination kits are available in substantial numbers to the Czech Army. The Czech-produced Soviet Shlem-1 type gas mask is an item of general issue to troops along with Soviet, Czech and German items of protective clothing. Individual decontamination kits are available but do not include any items which are effective against nerve agents. Chemical agent detector kits are World War II German models but are believed to have been modified to include a "G" series nerve gas detection capability. Czechoslovakia is producing three types of radiac instruments, but quantities are sufficient only for training purposes.

(d) Organization and Training

Details are lacking, but is known that Czechoslovakia follows the Soviet practice in matters of organization and training. Each division includes a CBR defense company. Training procedures are the same as those of the Soviets and East Germans. CBR officers are trained at the Army Chemical Forces Training Center, "Chemicke Uciliste," at Cervena Voda.

(3) Poland

(a) Research and Development

Poland has conducted moderate research and development on CW agents including nerve agents and their antidotes since 1954. A BW research and development program has been reported, but the size of the effort is unknown. A minor RW research effort with no development capability appears to be going on.

(b) Offensive Materiel

The Polish armed forces have no offensive CBR capability. Poland has no significant stockpile of CW agents

although production of small quantities of chloroacetophenone, chloropicrin and nerve gases has been reported. Nerve gas production appears to be on a laboratory scale only. Poland has neither a BW offensive capability nor a BW agent production program.

(c) Defensive Materiel

Polish armed forces are equipped with the Soviet-type Shlem-1 gas mask. Poland also has sufficient quantities of protective materiel, either of Soviet origin or Polish manufacture, available for its military forces. Individual decontamination kits are available which are effective against the blister gases but not against nerve gases. Atropine has not been reported as available to Polish armed forces. Soviet type detector kits which reportedly include a "G" agent detection capability are available. Soviet-type radiac instruments are available in training quantities only.

(d) Organization and Training

Available information indicates that Polish CBR organization and training is patterned after the Soviet's. Moreover, the Poles appear to stress CW training more than do the other Satellites. According to some reports, wearing of the gas mask for extended periods of time while performing normal duties is mandatory, and in some units troops are required to wear masks for as long as eight hours at a time. Polish Army enlisted men receive about 35 hours of formal CBR training annually in addition to extensive training which integrates CBR and other types of training.

(4) Hungary

(a) Research and Development

Before the uprising in October 1956 a small but active program of CW research was conducted by military and civilian scientists at the Institute of War Techniques, Budapest. Work was done on synthesizing nerve gases, testing of materials for nerve gas penetration, designing gas mask canisters, developing detection instruments and protective clothing, and testing procedures for contamination of air, soil, food and water. The CW

257

activities of the Chemical Division at the Institute were suspended in November 1956. At the Military Medical Research Institute experiments were conducted on the medical effects of nerve gases and methods of treating casualties. Research on radiation sickness was also carried out. There is no evidence of any BW activities in Hungary.

(b) Offensive Materiel

Hungary is not known to be producing significant amounts of CBR agents or munitions. However, there have been reports that large quantities of nerve gases, mustard and other CW agents of Soviet origin, in bulk and in munitions, are stored in underground bunkers on the island of Haros in the Danube River within the limits of Budapest.

(c) Defensive Materiel

The Hungarian Armed Forces are supplied with Soviet gas masks, and with Soviet-type masks which are manufactured in Hungary, probably by the Muszaki Technical Works. These technical works also allegedly produce light and heavy protective clothing. There is reportedly a CW defense equipment depot in or near Budapest which contains a considerable quantity of gas masks, protective clothing, detector kits and other CW equipment.

(d) Organization and Training

Planning for CBR organization and training follows the Soviet lead. Each division has a CBR company. There is an independent chemical defense battalion at Nagytarcsa consisting of four companies, a reserve company and a noncommissioned officers' school. Another chemical defense battalion has been reported, but its existence has not been confirmed. Unit training in CBR defense is based on Soviet manuals, instructional material and procedures.

(5) Conclusions

It is estimated that the Satellites have no capability for conducting offensive chemical, biological and radiological

operations, but have a fairly good capability of defending against CBR attacks. This capability is gradually improving as supplies of new locally manufactured gas masks and protective equipment become available. In the event of hostilities the USSR can probably fill existing shortages in defensive and offensive equipment.

THE COUNTERINTELLIGENCE ESTIMATE

1. (S) The Situation

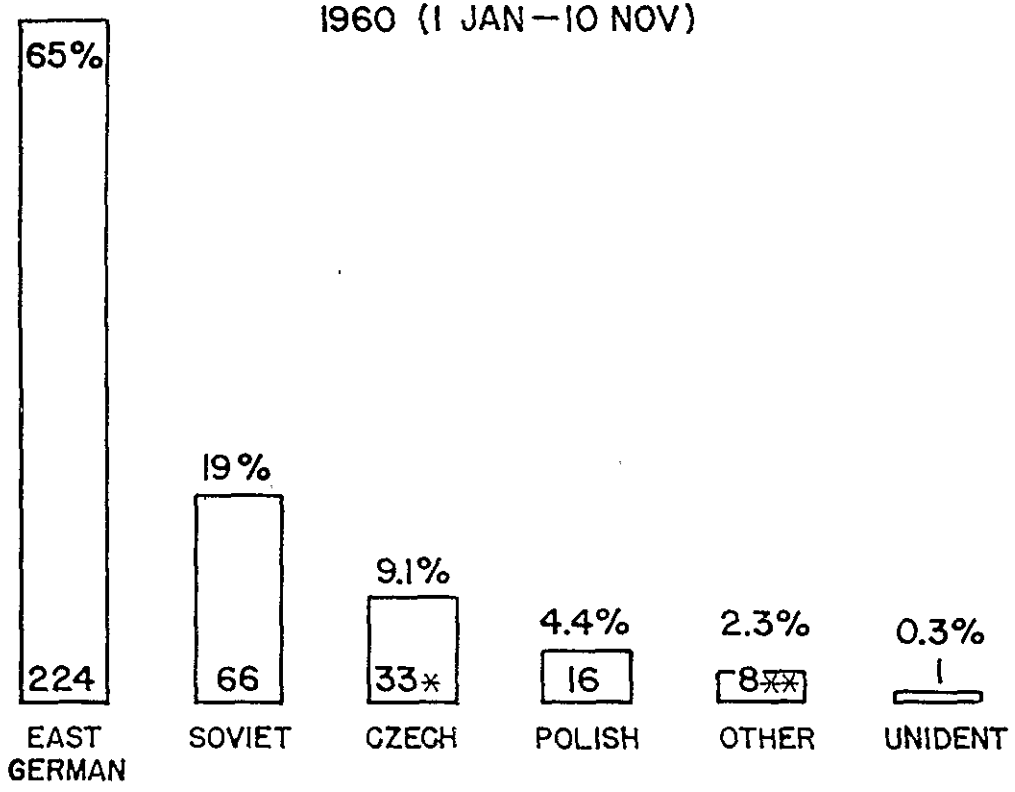
a. USAREUR Vulnerabilities

The mission, strength and deployment of USAREUR forces establish the command as a major target for hostile intelligence services. Subversive elements also conduct activities designed to force a withdrawal of USAREUR units and weaken the NATO alliance. Both the hostile intelligence services and the subversive elements have certain operational advantages and are able to exploit inherent vulnerabilities in the Allied counterintelligence systems.

(1) USAREUR units are particularly exposed to hostile intelligence operations which are conducted on an unprecedented scale from or through East Berlin, East Germany and Czechoslovakia. During 1959, 2,802 hostile agents were neutralized in West Germany; approximately 30 percent of these had missions against military targets. Incomplete 1960 statistics show 2,136 agents neutralized through October. Approximately the same percentage had military targets. During the first 10 months of 1960, 348 neutralized hostile agents (see Figure No. 36) were found to have specific missions against USAREUR units, personnel and activities. The thoroughness of hostile intelligence coverage of USAREUR is indicated by the type and location of assigned targets (see Figures No. 37 and 38). These statistics are based on neutralized agents who probably represent only a minor portion of the total number and include few of the higher level agents controlled by hostile services. The most obvious of operational advantages to hostile intelligence services is the ineffectiveness of controls imposed upon travelers entering West Germany from the Soviet Bloc areas. West Germany authorities recognize their inability to control the massive influx of refugees, legal travelers and illegal border crossers. The refugee stream alone, which during 1960 included approximately 200,000 individuals, a 25 percent increase over 1959, provided a well-exploited opportunity to introduce new agents into the West. Legal travelers who, for example, included

CONTROLLING SOVIET BLOC SERVICES OF NEUTRALIZED AGENTS WITH MISSIONS AGAINST USAREUR

1960 (1 JAN—10 NOV)



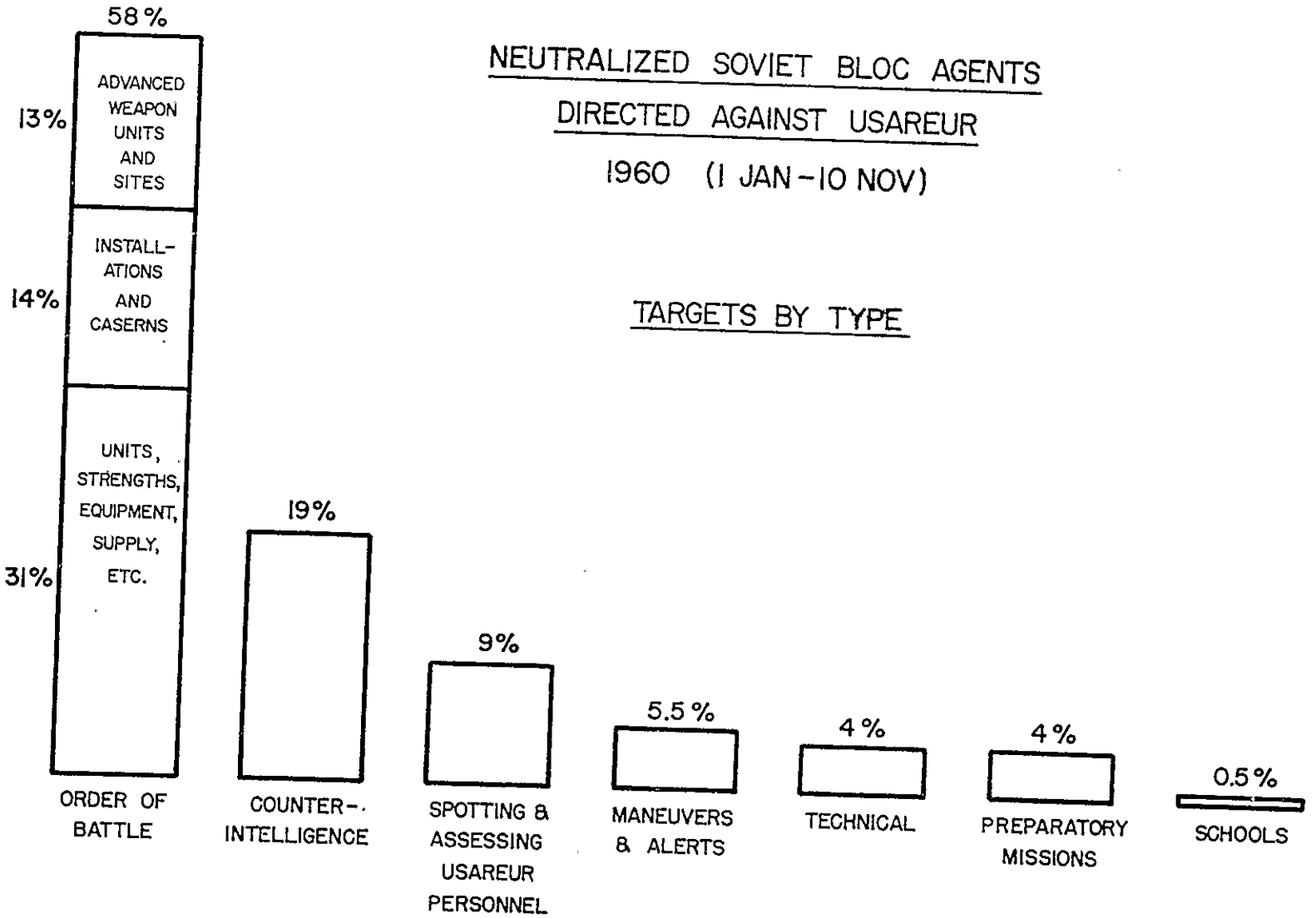
* INCLUDES 2 AGENTS WHO WERE ALSO ACTIVE FOR EGIS

** INCLUDES AGENTS CONTROLLED BY BULGARIA(1), RUMANIA(1), HUNGARY(1), AND YUGOSLAVIA(4)

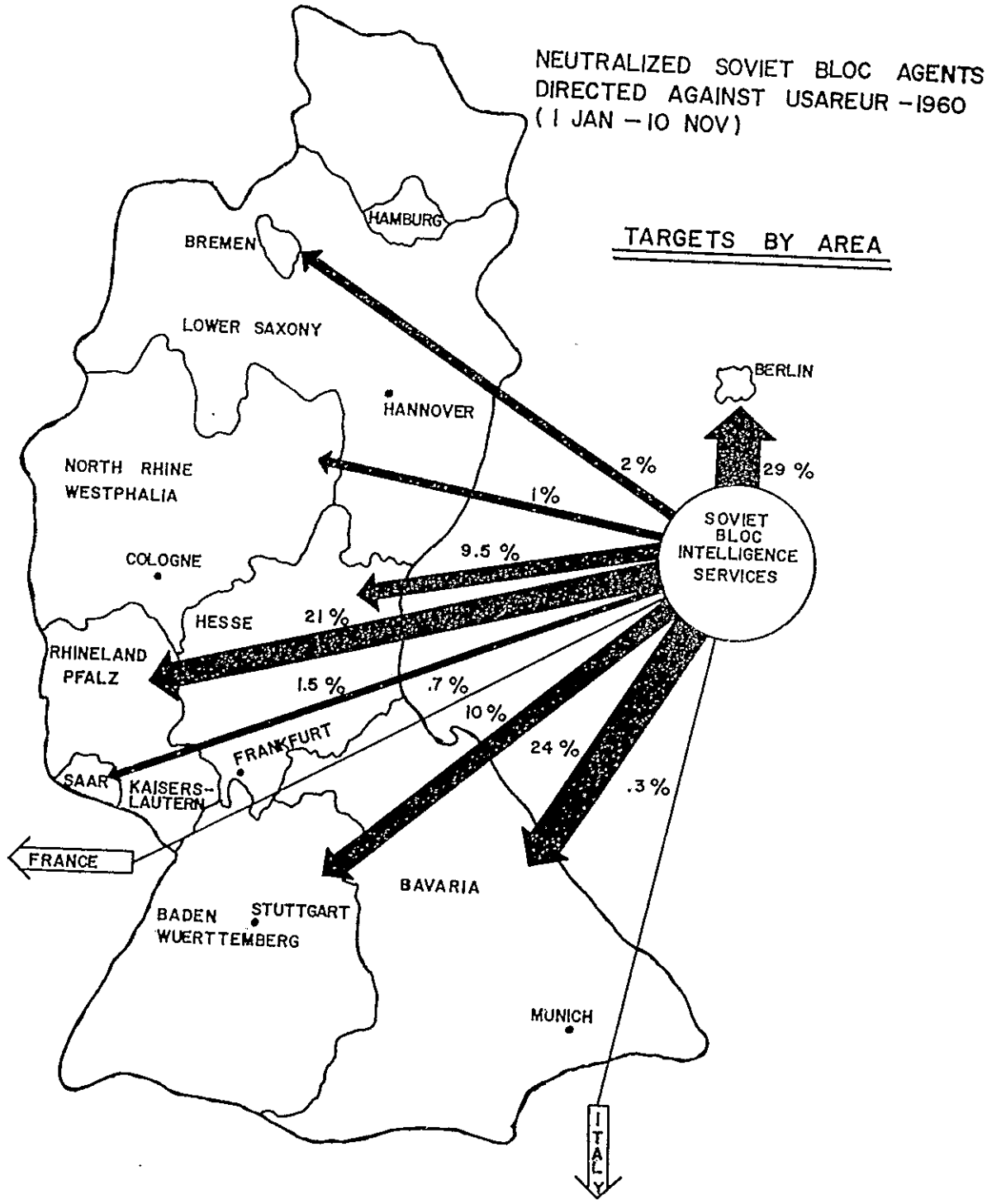
(C) Figure No. 36

NEUTRALIZED SOVIET BLOC AGENTS DIRECTED AGAINST USAREUR 1960 (1 JAN - 10 NOV)

TARGETS BY TYPE



(C) Figure No. 37



(C) Figure No. 38

Soviets, Poles and Czechs, were also used by hostile intelligence services. The Soviet Bloc services also benefit from the heavy traffic of Westerners, including USAREUR personnel and employees, who travel behind the Iron Curtain. The number of such persons who are recruited as espionage agents and returned to West Germany is too great to be controlled effectively by West German and other Allied security agencies. An increasing number of operations against USAREUR forces are being conducted from third countries, notably Switzerland and Austria, which limits the effectiveness of countering operations. West German security authorities have been more successful in their countersubversive activities directed against the illegal West German Communist Party, but are unable to block any appreciable percentage of Communist organizers and propaganda dispatched from East Germany. However, little of the Communist effort is specifically directed against USAREUR.

(2) The criticality, location and lack of defenses of many USAREUR installations and units are major factors relating to USAREUR vulnerabilities.

(a) Many USAREUR installations and activities are located in areas or on terrain which favor observation or provide secure avenues of clandestine approach. This represents a significant vulnerability since more than 15 percent of all hostile essential elements of information (EEI) associated with order of battle (OB) collection are specific missions for observation of USAREUR installations. In some cases the difficulties of obtaining sufficient land adjacent to USAREUR sites prevent establishment of a controlled perimeter beyond installation limits. In other instances operational considerations which outweigh security factors restrict defensive measures. Particularly in installations located within metropolitan areas, usually no adequate defense can be made against overt collection and observation of military activities. This has been evident in hostile missions to determine the alert status of USAREUR forces which require only casual observation of military installations. Other USAREUR installations, particularly major supply depots, are so large that application of adequate defenses is beyond current limitations on personnel and funds. Such installations, a number of which have several miles of perimeter fencing, can be kept under only sporadic surveillance by security personnel of varying reliability and efficiency. A major factor in installation vulnerability is the

widespread use of old buildings or sites which would require a prohibitive amount of reconstruction to achieve a high security standard. Certain new sites have also failed to incorporate efficient security defenses because of financial or operational considerations. The lack of physical measures combined with an inadequate level of guard personnel have made certain installations vulnerable to hostile sabotage activity. While sabotage is not considered a current hostile objective, there have been continuing hostile attempts to probe installation vulnerabilities to obtain information for wartime planning.

(b) The increasing number of NATO advanced weapon units has created a number of vulnerability problems. The nature of advanced weapon equipment, particularly that of complex missiles and associated equipment, makes it relatively vulnerable to enemy attacks. Sensitive information on equipment and atomic employment is also necessarily disseminated to large numbers of personnel.

(3) USAREUR vulnerabilities are compounded by the widespread use of local-hire personnel, many of whom have ties to Soviet Bloc countries, as direct employees of or in facilities which support USAREUR operations. A number of other USAREUR military and civilian personnel also have family or ethnic ties to Soviet Bloc countries which can be exploited by hostile intelligence services. Even personnel without such ties, but vulnerable to hostile intelligence approach for some other reason, are becoming more common targets for recruitment.

(a) The most important element of the USAREUR labor force and one which is particularly vulnerable is the local-hire group. There are thousands of local-hire employees. They work in most USAREUR installations and facilities. Several thousand of these hold limited access clearances to classified information, and others are able to maintain continuing observation of unclassified activities and personnel of interest to hostile intelligence. The value of documents and information on USAREUR which are available to local-hire employees is well documented by enemy espionage missions. In general, such employees cannot be sufficiently screened in pre-employment checks to prevent hiring of personnel who are susceptible to approach by hostile intelligence services or who have unfavorable backgrounds. The appreciable number who have relatives and travel

behind the Iron Curtain provides a valuable pool of potential agents. This group is considered by hostile intelligence to be a valuable source for exploitation; during 1960, 58 hostile assessing and recruiting missions were reported to have been directed against specific employees. Since this figure was obtained from neutralized agents, the actual number of local-hire employees who have been spotted, assessed and recruited must be much higher. Cases involving neutralized agents in local-hire positions show hostile emphasis on missions for procurement of publications, particularly field and technical manuals, information on the alert status of USAREUR forces, and spotting/assessing of additional candidates for recruitment, as well as on routine OB EEI concerning units, installations and organizations.

(b) Other personal vulnerabilities recognized by hostile intelligence services are indebtedness, heavy drinking and immoral or illegal conduct. An unusually high percentage of hostile missions reported during 1960 concerned spotting/assessing of such personnel and identification of bars frequented by USAREUR officers and enlisted men. Twenty-eight missions concerned identification of personnel who associate with prostitutes, need financial aid as indicated by local bank loan records or may be susceptible to defection resulting from marital problems or misconduct. Approximately 10 percent of the agents who were targeted against USAREUR and were neutralized in 1960 were women; six were specifically identified as prostitutes who were to contact US personnel. An additional 18 missions which were assigned to neutralized agents consisted of instructions to report on bars and hotels used by USAREUR personnel and in which an agent could be established. USAREUR personnel were also exposed to hostile intelligence because of inadvertent entry into East Berlin and East Germany. In the first 10 months of 1960, 1 officer and 12 enlisted men were detained and interrogated by East German or Soviet personnel. In six cases enlisted personnel were referred to the Soviets after initial apprehension by East Germans. Four of the detainees admitted receiving recruitment approaches or invitations to return to the East which undoubtedly would have led to an approach. Since the problem of detainees primarily results from complexities in the East-West transportation system, compounded in some instances by drinking and carelessness, hostile services will continue to have an opportunity to exploit a number of USAREUR personnel.

(4) During 1960 there were no reports of established loss of USAREUR classified documents to hostile intelligence due to failure of the administrative procedures which encompass personnel, document and installation security measures. The limited number of reports on possible compromise based on violations of security regulations did not indicate any actual losses to Soviet Bloc services. However, in one instance a hostile intelligence agency refused an opportunity to obtain one CONFIDENTIAL and two SECRET documents. This possibly indicates earlier compromise of these particular documents. Two major vulnerabilities, penetrations of the West German government and hostile exploitation of the lack of controls on unclassified documents, have presented hostile intelligence with opportunities to obtain documents and information of intelligence value. In cases involving Soviet, East German and Czech penetrations of the West German Ministries of Defense, Interior and Transportation, as well as the parliamentary defense committee, classified information has been lost. Although it has been difficult in most instances to isolate the specific information compromised, sufficient examples are available to establish loss of data on missiles, strength and troop deployment plans. High-level penetrations provide hostile intelligence with classified information which cannot be obtained from routine operations; however, the loss of a mass of unclassified documents was undoubtedly of value particularly in technical fields. Using publication listings known to have been obtained in clandestine operations and probably also available through open collection, hostile services have become extremely selective in targeting of specific documents. It is significant that 250 hostile EEI on documents were reported by neutralized agents during 1960. Although priority attention has been given to classified documents concerning divisions or higher-level units, requirements continue to be levied for unclassified publications on missiles, signal equipment, chemical warfare, radar, tanks, vehicles and other ordnance items. The loss to hostile intelligence of more than 200 unclassified and FOR OFFICIAL USE ONLY publications was reported during 1960. The majority of these were field and technical manuals providing detailed information which cannot be obtained from routine observation missions. In the more general field of information as opposed to specific documents, hostile intelligence is able to obtain appreciable amounts of classified and unclassified information of intelligence value. Established loss of classified information has, however, been limited to information on

intelligence operations. A particularly important vulnerability is evident in the lack of controls on unclassified information of intelligence value. While this apparent disregard for security is explained by the need for certain public information programs and is inherent to democratic systems, the lack of control is thoroughly exploited by hostile intelligence. Military newspapers, information bulletins, telephone directories and other unclassified media are regularly collected and used by hostile intelligence as a basic source of information of value. Unit designations, strengths and locations, new equipment, training, and personality information are typical of the OB information of value available through exploitation of easily obtained publications. Such information also serves as a means of selectively targeting clandestine operations. Hostile intelligence defectors have noted the value of such information, contrasting the tight controls in the Soviet Bloc on information of value, even though unclassified, with the apparent disregard for security in the West.

(5) The major vulnerability in the USAREUR communications system results from radio transmission of a volume of unclassified and unencrypted information which can be intercepted by hostile monitoring operations. A large portion of USAREUR telephone and teletype communications, as well as usual radio traffic, are transmitted on the microwave relay system which is susceptible to intercept. Since only a small percentage of unclassified radio traffic employs Encrypted for Transmission Only (EFTO) procedures, it must be assumed that hostile intelligence is able to monitor a major part of USAREUR electrical communications. Tactical radio communications, including those employed during field exercises, are also vulnerable to intercept. Only a relatively few reports were received during 1960 of classified information being transmitted over unprotected communication. However, the mass of unclassified information of intelligence value, such as OB and technical data, which can be intercepted and subjected to analysis will provide enemy forces with a comprehensive picture of USAREUR units, deployment and operations. This vulnerability will not be appreciably lessened until more extensive use is made of EFTO procedures. Until all communications can be encrypted, hostile monitoring operations will continue to be a major source of information on USAREUR. By contrast there has been an apparent lack of hostile attention to other communications systems. While it is possible that hostile monitoring of radio communications provides required information, the known hostile effort in land communications

is so small as to indicate a lack of interest. This is inconsistent with the value of information carried by such systems.

b. Hostile Threats to USAREUR

Espionage activity of Soviet, European Satellite and Yugoslav services is the most important current threat to USAREUR. Such operations, which are conducted on a hitherto unprecedented scale, take full advantage of USAREUR vulnerabilities and employ the resources of a massive espionage system. The subversive elements of interest, primarily the national Communist parties with supporting networks of front groups and infiltrated organizations, also pose a potential threat. However, Communist groups present less of a current threat than espionage operations since subversive activity is not primarily directed against USAREUR. Only in relation to anti-atomics and anti-NATO propaganda campaigns, which support Soviet foreign policy objectives, have USAREUR forces been specifically attacked by Communist groups as such. However, certain subversive elements of these groups do have sufficient strength to pose a potential threat for interfering with USAREUR operations. The sabotage capability of the hostile intelligence services and the subversive elements, especially if supported by enemy forces, represents a definite threat immediately before or during hostilities. Although sabotage is not considered a current threat, recognition must be given to the potential of hostile forces to harass or disrupt certain USAREUR operations.

(1) Hostile Intelligence Services

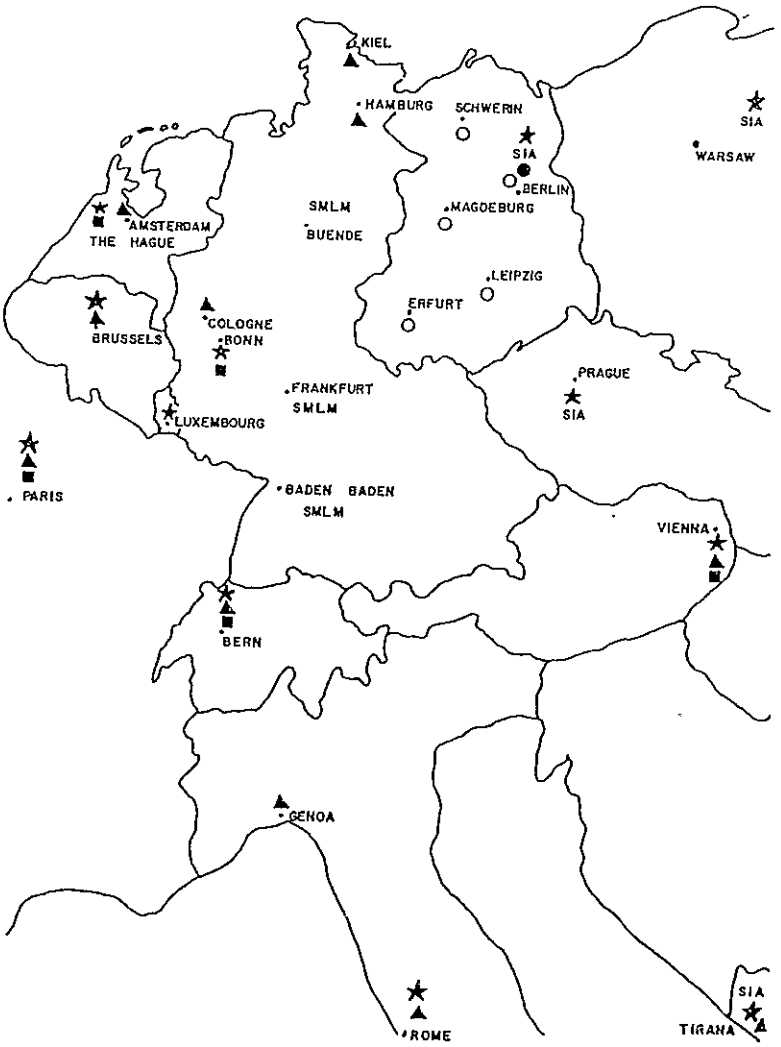
During 1960 intelligence services of the Soviet Union, six European Satellites and Yugoslavia were reported as conducting espionage operations against USAREUR. Of the European Satellite countries, only Albania was not specifically identified as being active against USAREUR. The scope and level of current activity in the USAREUR area range from the extremely active East German services in which 1,847 agents were neutralized in West Germany, 224 of whom had had USAREUR targets, to the relatively inactive services of Bulgaria, Rumania and Hungary.

(a) The Soviet Intelligence Services (SIS) are considered a major threat to USAREUR. Although the level of activity, as indicated by agent neutralizations, was less than that of the East German services, the SIS have a number of operational advantages which substantially increase their potential. Most important from the USAREUR standpoint is their access to the USAREUR area from East German bases and a network of legal residencies in Western Europe (see Figure No. 39). These provide sufficient bases of operation for recruiting new agents and maintaining contact with those targeted against USAREUR. The Soviet advisory system (see paragraph 2(a)(5) below) provides a unique advantage in exploiting the collection efforts of Satellite services. Through assignment of SIS staff members to headquarters of the Satellite services, the Soviets have access to operational leads and direct collection activity, and obtain copies of all information collected. This permits the SIS to maintain control over and monitor an extremely broad range of operations without jeopardizing their own assets. In spite of the Soviet influence, there has been no indication of any delimitations on targets or areas of operation among the Soviet and Satellite services, except as might be dictated by proximity to certain areas. While such limitations would offer some advantages in more efficient employment of collection assets, the SIS apparently prefer to permit operations to be conducted on a mass, uncoordinated basis. This system does provide depth of coverage and needed confirmation on certain targets. The Soviet services themselves conduct operations paralleling or duplicating those of the Satellites. Another phase of the advisory system, the referral of agents from Satellite to Soviet control, has been particularly exploited by SIS operations against USAREUR. During 1960 it was common for personnel approached by the East Germans as potential sources on USAREUR activities to be referred to the SIS. While this procedure was not followed in all cases, the SIS did gain access to certain USAREUR personnel through East German operations. The threat of the SIS is especially apparent in their ability to conduct high-level operations. Such operations, which normally involve recruitment of a person who has access to critical information, pose a particular threat because of SIS ability to spot, assess and approach USAREUR personnel. Soviet penetration attempts have not, however, been restricted to individuals with access to sensitive information. The SIS have shown interest in a number of low-level sources who have only limited access to USAREUR information. In addition to recruitment attempts, the SIS also conduct a number of

SOVIET RESIDENCIES, AND OPERATIONAL BASES IN THE USAREUR, AND ADJACENT AREAS

LEGEND:

★ – SOVIET EMBASSY OR LEGATION
▲ – SOVIET TRADE DELEGATION
■ – OTHER SOVIET DELEGATION
SMLM – SOVIET MILITARY LIAISON MISSION
SIA – SOVIET INTELLIGENCE ADVISORS
○ – RU OPERATIONAL BASES (MILITARY INTELLIGENCE SERVICE)
● – KGB OPERATIONAL BASES (CIVILIAN INTELLIGENCE SERVICE)



(C) Figure No. 39

agent operations designed to provide routine information on USAREUR OB. These operations, although considered low-level because of the unrefined handling and targeting techniques involved, do contribute to Soviet holdings.

(b) The East German Intelligence Services (EGIS) controlled 65 percent of all neutralized agents reported during 1960 as being directed against USAREUR. The massiveness of EGIS operations is also indicated by the 1,847 agents neutralized in West Germany from January to October 1960, a figure which represented 86 percent of total apprehensions. The extremely high level of activity, which is at least partially attributable to operational advantages of the EGIS, currently represents the most important threat to USAREUR. Based on estimates of total agent activity, approximately 13,500 East German agents probably received assignments for completion in West Germany during 1960. Although the percentage of those who had military or specific USAREUR targets cannot be substantively estimated, it is possible that at least 3,000 had such missions. Many of the East German agents were Communist functionaries who were primarily concerned with Party missions and collected intelligence information only as a secondary objective. While most such agents are not of direct concern to USAREUR, they do represent a pool of espionage agents who may be directed at any target. The majority of known EGIS operations of specific USAREUR interest are low-level observation missions against installations and units. Such missions include OB targets, counterintelligence EEI, spotting/assessing of personnel and employees, observation of maneuvers and procurement of unclassified publications. A portion of low-level operations is also preparatory in nature, such as obtaining employment with USAREUR, locating bars frequented by military personnel and establishing residence in areas where USAREUR forces are concentrated. While most EGIS missions are categorized as low level, they do have the ability to answer basic hostile EEI and cannot be dismissed as unimportant threats. The great number of low-level EGIS operations has suggested that the basic purpose may be to saturate and immobilize Western defenses. While this would undoubtedly serve hostile interests, virtually all agents have had valid missions which do answer enemy EEI and should not, therefore, be considered other than actual collection operations. During 1960 the EGIS also demonstrated an ability to establish and conduct

high-level penetrations as well as to control unusually productive agents who had only limited access. Such sources included agents within West German federal ministries and major Allied military headquarters as well as newspaper reporters who exploited opportunities to visit USAREUR activities. The volume of information of intelligence value collected by EGIS agents undoubtedly constitutes the majority of all Soviet Bloc collection efforts. While the EGIS rely primarily on low-level agents, based on easy access to the USAREUR areas, and on innumerable recruitment opportunities, the over-all threat must be rated as extremely high.

(c) Ranking only behind the Soviets and East Germans in volume of agent activity are Czech Intelligence Services (CIS) operations as indicated by the 33 agents neutralized in 1960 and identified as being directed against USAREUR. Most of these operations were targeted against intelligence activities. The threat of CIS operations is, however, not limited to defensive operations. CIS cases exposed in 1960 included sophisticated approaches to USAREUR personnel and a penetration of the West German Parliament and defense committee which was neutralized only after six years. Well-contrived recruitment operations, which are usually based on threats to relatives in Czechoslovakia, pose a particular threat. Other approaches are predicated on appeals to ethnic ties or on blackmail or financial gain. Employees and personnel with Czech backgrounds are particularly vulnerable to such inducements. In general these operations are skillfully contrived. Many CIS operations are also conducted with unusually advanced modus operandi which include high agent payments, efficient communication systems and consideration of agent security. The most important CIS case of 1960, the penetration of the West German Parliament (see paragraph 2c(6) below), definitely established the Czechs as an important threat to USAREUR interests.

(d) The Polish Intelligence Services (PIS) again accounted for only a limited number of operations directed against USAREUR. However, the 16 cases in 1960 represented an increase in cases over 1959. Two factors, exploitation of USAREUR personnel and a widespread system of legal residencies, increase the threat to USAREUR. Known PIS activity in 1960 emphasized operations against Western intelligence with secondary emphasis on OB and other military missions. This emphasis in targeting reduces the

number of cases of direct USAREUR interest. Cases involving approaches by the PIS have been limited and usually confined to personnel who have relatives in Poland or a connection with a Polish legal residency in the West. The number of known cases against USAREUR is, however, considered less than is consistent with PIS capabilities and missions.

(e) Other Satellite and the Yugoslav intelligence services represent only a minor threat as indicated by the level of known activity and type of targets. In general these services also concentrated on counterintelligence missions. The one Hungarian case reported in 1960 involved the successful penetration of an intelligence operation. The Rumanians showed some interest in emigré groups and general military targets, but the primary mission remained penetration of Western intelligence. This type of targeting is in accordance with the capabilities and principal interests of these countries. The relatively limited intelligence resources of the minor Satellites must be first employed on defensive missions designed to neutralize antiregime activities. This again is based on Soviet Bloc preoccupation with internal security. The primary threat to USAREUR from minor Satellite operations is the possibility that USAREUR personnel will be recruitment targets. Those with relatives or other ties to Satellite countries are often considered exploitable by hostile services, particularly when travel behind the Iron Curtain or contact with a legal residency in the West presents a relatively secure means of approach.

(2) Communist Subversion

(a) The subversive element of primary interest in the USAREUR area is the illegal Communist Party of West Germany. Certain activities of the East German Party also directly concern USAREUR because of East German control of Communist organizations in West Germany. Control and necessary aid for the Party and subordinate front groups are provided by the internal Communist system, both directly from Moscow and through a system of international front groups which coordinate activities of the national organizations. As a whole the Communist Party in West Germany presents only a limited threat compared with the hostile intelligence services, since the majority of Communist effort is not specifically directed against NATO.

Only as part of general anti-NATO, anti-atomics propaganda campaigns have USAREUR forces been directly attacked. Even such campaigns have been isolated, relatively limited and ineffective. The more important threat of the Communist Party in West Germany is the potential capability to serve as an espionage or sabotage organization.

(b) The threat of the Communist Party would be particularly important if it were to be used extensively as an espionage apparatus. Some reports of individual Party members being recruited as agents or of lower echelon organizations collecting information have been received during the past year. However, these reports have not been numerous enough to suggest that the Party organization as such is being directed into general clandestine activity. The classic Soviet separation of the Party and espionage has been generally observed. Exceptions to this rule normally represent uncoordinated activity by overzealous individuals. However, it must be accepted that Communists are required to report through Party channels on their employment and other subjects which can be exploited as propaganda issues. In certain instances such reporting will provide information of intelligence value.

(c) The West German Party also represents a potential source of sabotage agents or, as an organization, an element able to provide cover, intelligence and other support to Soviet Bloc sabotage groups dispatched into the USAREUR area. However, no confirmed reports of sabotage training or planning have been received. Communist elements can be expected during 1961 to avoid illegal activities, such as involvement in sabotage or espionage, which could be used as a basis for governmental repression. The desire to avoid further governmental action lessens the direct threat of the Party for clandestine activity.

(3) Sabotage

Hostile-directed sabotage is considered a major threat to USAREUR interests only immediately before or during hostilities. Certain hostile intelligence services, elements of Soviet Bloc armies and a limited number of Communists have a current capability to launch sabotage attacks which would interfere with USAREUR operations. However, friendly forces would be able to contain such attacks while suffering only a minimum of loss.

Materiel destroyed or damaged could be replaced. Such action would also lead to appreciable improvement in security defenses. The results of current sabotage activity would, therefore, not serve Soviet Bloc objectives. Under a continuing Cold War situation, primary hostile interest will be directed toward recruitment and training of personnel within the Soviet Bloc, developing plans for wartime operations, and collecting target information on USAREUR vulnerabilities to sabotage. Sufficient espionage missions were reported during 1960 to establish hostile interest in determining the defenses and weaknesses of USAREUR and civilian facilities which are essential to wartime operations. Typical of such missions were those to locate unprotected power cables and points where explosives could be introduced and to determine the number, reliability and position of guards. Such activity, while not an immediate threat, does provide the enemy with a basis for damaging attacks at a later date. Based on defector statements and recent EEI, targets of primary hostile interest include advanced weapons, supply depots, communication facilities and road nets.

2. (S) Espionage, Subversion and Sabotage Activity

a. The Soviet Intelligence Services (SIS)

(1) Status and Capabilities

(a) The two Soviet services of direct interest to USAREUR are the Intelligence Directorate (RU) of the Main Intelligence Directorate (GRU) of the Soviet General Staff and the Committee for State Security (KGB). The RU has the mission of collecting information on imminence of hostilities, Western OB and scientific-technical data. The KGB is responsible for the security of the USSR at home and abroad, including security of the Soviet Armed Forces. Two departments within the KGB are of particular interest, the Foreign Intelligence Directorate (INU) which conducts positive and counterintelligence operations abroad, and the Armed Forces Counterintelligence Directorate (UKR) which is responsible for the security of the Armed Forces including the Group of Soviet Forces, Germany (GSFG).

(b) Approximately 400 to 600 RU officers and enlisted men are assigned in East Germany. World-wide strength

is unknown, but RU staff members are assigned to Soviet legal residencies abroad and to the Soviet Military Liaison Missions (SMLM) in West Germany. East Germany is the principal operational area from which covert operations are conducted against USAREUR. Operational bases are located in East Berlin, Erfurt, Schwerin, Magdeburg and Leipzig. The majority of personnel are assigned to the operational base in East Berlin. Other operational bases in East Germany reportedly each have a strength of approximately 40 officers and enlisted men. The RU operational base in Erfurt apparently operates primarily against USAREUR forces located in central West Germany. The operational areas of the other bases have not been conclusively established but probably are analogous to locations in East Germany, with the exception of the East Berlin base which conducts operations against targets throughout West Germany and Western Europe. In addition to the operations units, an RU staff element is assigned to GSFG Headquarters at Wuensdorf. This group is responsible for the collection and analysis of intelligence information and does not conduct covert operations. It is, however, presumably responsible for staff direction of the operational elements in cooperation with GRU headquarters in Moscow.

(c) The over-all strength of the INU of the KGB is unknown, but it is larger than that of the RU. Its strength is based principally on the broader collection responsibilities of the INU which collects not only military but political and economic intelligence. In East Germany, however, INU strength is believed to be less than the RU. This is due to the existence of the GSFG and the opposing NATO forces which creates a special need for military intelligence concerning forces in Germany and western Europe, a function which the RU can best satisfy. The number of SIS operations against USAREUR which are attributed to the INU is less than the number known to have been conducted by the RU. INU personnel are assigned to Soviet legal residencies in West Germany and Western Europe and to trade delegations and Soviet business enterprises abroad.

(d) The total strength of the UKR of the KGB also is unknown but is undoubtedly large, based on Soviet preoccupation with the loyalty of their armed forces. It is improbable the Soviets would economize on attempts to keep the armed forces free of Western influences and to prevent defections, particularly in the GSFG which, by virtue of its proximity to the West, requires greater vigilance from