SECRET NOFORN

OPERATIONS SECURITY UPDATE

APRIL 1985

Office of Origin:
HQ Electronic Security Command/DOOO
San Antonio, TX 78243-5000
Classified by: Multiple Sources
Declassify on: OADR

SECRET NOFORN

WARNING NOTICE:
Sensitive Intelligence
Sources and Methods
Involved (WNINTEL)

ELECTRONIC SECURITY COMMAND

* * * * * FOREWORD * * * * *

(U) The Operations Security Update is published aperiodically by HQ Electronic Security Command. It is intended for use by Air Force OPSEC program managers to assist in the development of local training materials, and promotion of the Air Force OPSEC Program. We encourage subscribers to submit articles, OPSEC poster ideas or comments to improve the publication. Local reproduction of the Update is authorized. Questions concerning the Update or submissions for future publication may be submitted to HQ ESC/DOOO, San Antonio, Texas 78243, AUTOVON 945-2112.

OPERATIONS SECURITY UPDATE - APRIL 1985

*** KEY PERSONNEL ***

Commander	BGen Paul H. Martin
Vice Commander	BGen Regis F.A. Urschler
DCS/Operations	Col John P. Lynch
Director, C3CM Operations	Col Robert D. Green
OPSEC Division	Col Marlin L. Logan
Editor	Mr. Joseph R. Folk

**** TABLE OF CONTENTS ***

NOCONTRACT

WARNING NOTICE: SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED (WNINTEL)

NOT RELEASABLE TO FOREIGN NATIONALS

ESC INK MESSAGE FOR 1985 (U)

EDITORS NOTE: The following information from our ESC INK folks appeared in their 201500Z Dec 84 weekly OPSEC Threat highlights message. Those personnel utilizing the INK Services are encouraged to submit their requirements for threat information IAW Para D.

A. (C) During 1984, we in the United States again saw further expansion of Communist Signals Intelligence collection capabilities. Year by year, hostile forces continue to increase the numbers and capabilities of intelligence collection platforms directly exploiting virtually all operations within U.S./Allied military forces.

B. (S/NF/WN) [redacted]

25X1

C. (S) Several other examples highlighted in INK weekly messages come to mind, but needless to say the USSR and its allies have been able to continue to gain and exploit significant information on U.S. military activities by completely overt intelligence collection methods. Given the closed door nature of Soviet Intelligence Services, we cannot completely fathom the scope and success of their operations.

D. (C) Therefore, only by continued vigilance and by taking cognizant actions, can we cope with ever improving enemy signals intelligence systems. Description of the threat, and its importance to Operational Security (OPSEC), must receive wide dissemination. Our goal in the coming year is to provide ever increasing detail on the deployment, actions, and capabilities of the hostile signals collection threat. In line with this goal we request your assistance in the coming year to aid in establishing requirements and priorities for evaluating all aspects of this hostile threat to our national security. Your priorities are our priorities.

WARNING NOTICE: SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED (WNINTEL)

U.S. MILITARY MEMBER POSSIBLY PROVOKED WHILE IN THE SOVIET UNION (U)

(U) A USAF NCO provided the following information concerning an Embassy support mission flown to Moscow on 13 Jun 84. The NCO served as a steward on the flight mission.

A. (U) The Embassy mission took off from Rhein Main AB, with AEROFLOT navigators on board, at approximately 1030L. The AEROFLOT navigators, as in past Moscow flights, did not converse with the airmen except to get something to eat or drink and just prior to entering Soviet air space talked with the pilot to advise him once he was in Soviet air space. Upon landing in Moscow, at approximately 1500L, the aircraft was downloaded and the Defense Attache office (DAO) contact officer took the crew through customs. Source had brought with him a video camera which the customs officials seized, saying he could pick up the camera the next day when they departed. After clearing through customs, the DAO contact officer took the air crew on a short tour of Moscow prior to taking them to a hotel. The crew checked in without any problems. In the past, the air crew had to stand in line with everyone else checking into the hotel, now there is a separate check in line for the air crews. After checking into the hotel the DAO contact took the crew to a restaurant in an out of the way area of Moscow. Upon arriving at the restaurant which was located on the second floor, they found the entrance door locked. The DAO contact officer finally got the attention of an employee in the restaurant and someone came down and unlocked the door to let them in. Source was the last in the door and the door was locked behind them. They lingered at the entrance for a moment and an unknown individual came to the glass door motioning source to come to the door. Source went to the door and the individual asked him in English if he was an American. Source told him he was. The individual then told source he (the individual) had to talk to him. At the same time the individual kept pulling a piece of paper up and down out of his coat pocket. Source did not know what the piece of paper was. Source then told the individual he could not talk to him and backed away going upstairs to the restaurant. Source then informed the DAO contact officer about the incident when the group was upstairs and the contact officer stated he had done the right thing by leaving. The DAO attended the dinner later and was briefed about the individual who approached the subject.

As the group exited the restaurant the individual was still outside the door and the DAO talked with the individual.

Source's group went back to the hotel for the night. Source and the rest of the crew checked out of the hotel at 0600L and went to the airport to prepare for the return trip. When they processed through customs, source's video camera was returned to him and did not appear to have been tampered with. The mission departed the airport at approximately 0930L with the AEROFLOT navigators on board. They did not converse with the aircrew and they got off the aircraft in Paris.

B. (U) OSI Comments: This report is provided to inform U.S. personnel of possible methods of Soviet provocation in order to better prepare them in the event they are faced with similar circumstances. A review of past incidents of similar nature indicated the U.S. person may have been a target of a provocation designed to either embarrass him or to place him in a compromising situation. Frequently, U.S. persons have been asked to do something which appears innocent on the surface but is illegal by law. A prime example of this would be to take any personal correspondence out of the country for Soviet persons; exchanging currency, trading of items such as clothes, books, magazines, or other objects; and to discuss politics which is prejudicial to the Soviet system. The actual intent of the Soviet in the above text is not known; however, whatever the intent, the U.S. person reacted most appropriately. (SOURCE: AFOSI)

* *

The following article provided by our ESC/IN office gives a prime example of Soviet methods of contacting U.S. military and DOD civilians who are associated with intelligence activities. Although the geographical area is Germany, the tactics employed by the Soviets are apt to occur in any Eastern Bloc country visited by U.S. personnel. The article stresses the need for education. Personnel must be made aware of how to cope with and report incidents of this nature.

* *

SOVIET ACTIVITY ON THE BERLIN-MARIENBORN AUTOBAHN (U)

A. (C) Members of U.S. Forces traveling over land from West Germany to West Berlin (or reverse), over 100 miles within East Germany, must use the limited access highway between Marienborn and West Berlin. Following processing of personnel and vehicle documents at the allied checkpoints, travelers proceed to the Soviet checkpoint. At the Soviet checkpoint, the travelers must dismount and show their travel orders and personal ID documents to the Soviet sentry. After a

Page Denied

F. (C) Conclusions about the Soviet modus operandi and the checkpoints are:

. . . There is a watch system to alert the checkpoint officer when one of his targets is due. Persons waiting in the shack for their paperwork are under some sort of observation.

. . . Soviet officers have a standing requirement to the sentry to identify Russian speakers or ethnic Russians determined by the name on the travel orders. An alert mechanism exists that enables the sentry to signal the shack (a burst of light).

. . . Soviet officers almost invariably probe for subjects capability to travel to East Berlin. Soviets modus operandi prescribes meetings in East Berlin if possible. Those who say they can't travel to East Berlin or who must travel in groups tend to be identified as intelligence personnel.

. . . Persons approached tend to be repeat travelers. The Soviets almost invariably ask about subjects frequency of travel.

. . . Soviet officers often give subjects a chance to show their amenability to repeat meetings.

G. (C) A profile of "Konstantin" based on descriptions provided during debriefing of U.S. Army personnel reveals that he is a 30 year old Lieutenant, who speaks with a Moscow accent and speaks good German and English. He is in his third year of a five year tour. He claims to be the commander of a "translation platoon" in Magdenburg, East Germany. His wife likes western fashions. He is well spoken and has a well polished delivery. He is alert and quick to respond. Friendly rather than pushy, and in general, quite well suited for the role assigned to him.

H. (C) Subjects most likely to be approached can be male or female. "Konstantin" seems to speak more freely with females and doesn't hide his marital status. Those who travel alone after having made three or more trips in the past, those who drive an eye catching car, those having a Russian appearing name on the travel orders and those showing an interest in the literature (Soviet) on the table are likely to be approached. Other indicators for an approach are assigned to a security or intelligence unit, officer or senior NCO, and enlisted linguists from a SIGINT unit on assignment in West Berlin versus West Germany.

I. (C) Some lessons learned indicates that the awareness program needs to be fine tuned. Some people did not report promptly because they did not think it was important. Others failed to report promptly because they feared trouble from U.S. authorities, such as being banned from further travel in their vehicle. Many people did not know how to cope with the approach. Some became hostile while one agreed immediately to meet with the Soviet in principle. "Would you meet me for dinner in East Berlin?" The U.S. Service member replied, "sure, anytime." Personnel with Russian and German language capabilities should not flaunt their skills. Personnel with Russian or Eastern European names should be briefed. School teachers tend to travel frequently and should be briefed as a group.

J. (C) The 24 approaches reported equate to an average of one per week during the survey period. Even when one considers the other approaches to the British, French, or U.S. Air Force personnel, this is not a heavy workload for "Konstantin." It must be assumed that he has approached others who have not reported. Soviet checkpoint personnel are obviously under orders to produce leads. These approaches are bold, they are made in the face of a known allied counter intelligence program and they are often directed against intelligence personnel or others of higher rank who would be likely to report such approaches to authorities. This indicates that the Soviets are enjoying some measure of success and that checkpoints are their most readily available conduit into our ranks. There is a clear and present danger that "Konstantin" or one of his colleagues will succeed in contacting a naive, malleable or gullible prospect.

K. (C) CITD comment: The Marienborn-West Berlin highway is unique to U.S. forces and allies in West Berlin and provides a controlled environment for Soviet intelligence activities. A good briefing and awareness program about the checkpoints will alert U.S. personnel traveling on the highway of possible approaches by Soviet intelligence personnel. The above study points out that "Konstantin" could possibly succeed in his mission as a result of some approaches not reported to authorities.

SOURCE: CDR USAITAC

* *

SOVIET ACCESS TO WESTERN COMPUTER NETWORKS THROUGH SWEDISH COMPUTER CONFERENCE SYSTEM (S/NF/WN/NC)

Source for this report is the director of a computer communications department at a U.S. Academic Institution.

A. (S/NF/WN/NC) [redacted]

25X1

Page Denied

[redacted] 25X1

D. S/NF/WN/NC) [redacted] 25X1

* *

ELECTRONIC DATA PROCESSING SECURITY (U)

The following article indicates some of our allies are concerned over our computer vulnerability and are taking steps to counter hostile exploitation.

(S/NF/WN/NC) As of Oct 84, Electronic Data Processing (EDP) Security has become a major concern to most foreign countries as well as to the United States in both governmental and private sectors. Data Security Systems have taken on a new importance due to computer networking and prolification of personal computers that have individual data storage capacities. (Source Comments: The move to National Security Standards and National EDP Security networks will take place in Japan and Western Europe prior to occurring in the U.S. This is due to the governmental or institutional characteristics of Japan and Western Europe. Government organizations and large institutions are in a stronger position than private or commercial computer users to agree on security standards and requirements and to work towards the development of such standards.)

(S/NF/WN/NC) [redacted]

25X1

(S/NF/WN/NC) The Japanese Diet committee or security has also tasked the ministry of finance to develop a bank to bank data security network. However, the ministry of finance is encountering some difficulties with the Ministry of International Trade and Industry (MITI) and the Ministry of Posts and Telecommunications. There appears to be a turf battle developing among these three Japanese government organizations. MITI and Ministry of Posts and Telecommunications believe that the national data security network should include not only encryption of bank transactions, but should also include encryption of voice and executive correspondence. (SOURCE: CIA)
S/NF/WN/NC

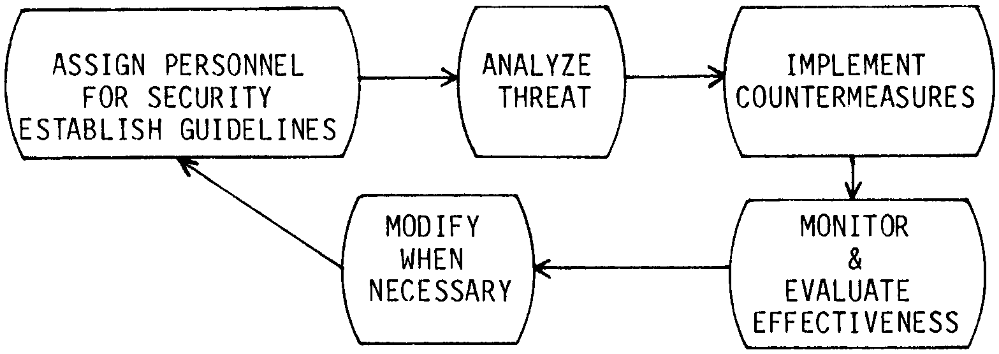
* *

OPERATIONS SECURITY FOR SMALL COMPUTERS (U)

EDITORS NOTE: The following article submitted by 1Lt Evelyn Rockwell of our OPSEC Education Branch creates an interesting approach to small computer security. The author, presently serving as an 8031 Intelligence Officer, has an extensive background in computer programming. She is a fully qualified 5135b, having previously served as a Small Computer Systems Analyst for Air Training Command.

(U) The recent growth of small computers throughout the Air Force has created a new problem for Operations Security Managers. During the mid-1970's and early 1980's when small computers were coming into general Air Force use, many bases acquired first one computer, then another, and another.... TAC has the CROMENCO, ATC the Burroughs

XE500, and the Air Force Data Systems Design Office has recently acquired the Z-100 and Z-150 for Air Force-wide use. This is in addition to the IBM's, WANGS, APPLES, TRS-80s, and numerous others already on inventory. How does the average OPSEC Officer/NCO handle the micro-explosion? Absolute security in the average Air Force office is unlikely and probably not necessary. But not making any attempt to minimize the risks is inviting trouble. To begin, let's look at a modified OPSEC process for microcomputers as a cyclic function.


ASSIGN PERSONNEL FOR SECURITY ESTABLISH GUIDELINES
ANALYZE THREAT
IMPLEMENT COUNTERMEASURES
MONITOR & EVALUATE EFFECTIVENESS
MODIFY WHEN NECESSARY

If we consider the modified OPSEC process for small computers as a simple application of common sense, each step of the process is easy to analyze. Let's consider the process step by step:

a. ASSIGN PERSONNEL FOR SECURITY & ESTABLISH GUIDELINES - This should always be a person familiar with the software and preferably has an office close to the hardware. A person familiar with the equipment will be better able to assess needs and establish guidelines. He should be able to develop a list of authorized users, and insure that only those personnel use the equipment. He must know enough about the hardware to realize if it is being harmed, or if the software is being tampered with. Once he has established a list for security and/or established user guidelines, it will be his responsibility to insure that they are adhered to. One word of advice here, make sure your security person has enough rank to make his policies stick! Use common sense here. The two striper in the office may be your "computer-whiz kid"; however, if the average grade of operator is E-7 or higher the Airman may initially need a considerable amount of support from you, or his supervisors to ensure the necessary procedures are enforced. If you go to the trouble of assigning a security person, then don't defeat your program before you start.

Step 1 - Select a qualified person to develop your security, establish your guidelines and protect your office investment - a small computer.

b. ANALYZE THREAT - What is small computer threat? Are you looking for people in trench coats stealing classified secrets off your high-tech devices? If you are, you're probably looking for a problem that doesn't exist, or is beyond the scope of this paper. The average office in CONUS is not going to have an alien agent problem in their midst (check with your local OSI), however, if you are running unauthorized classified on your computer you may have a very real TEMPEST problem. You could even have a problem with classified trash or the release of unclassified EEFI.

Consider your office trash, within the United States, the majority of offices never worry about what goes in the trash, but let's look at where the trash goes. First, there is the maid that takes it to the dumpster, then there is the dumpster that sits unwatched until the truck comes to take it to the dump. From the dump it could go anywhere. One California base contracted all of its paper waste to be sold as scrap to Thailand. The paper was compressed, boxed, and shipped by the ton straight to Thailand. Let's hope it was all "unclassified."

And what about the physical threat? Is your computer in a high traffic area? How easy would it be for that just counseled Airman to "snip" the keyboard cord, or what about that Field Grader who doesn't think the no coke, no smoke rule applies to him. If you have important operational plans, programs, or procedures on your TEMPEST approved Z-150 or unclassified information on your B-25 you could have an Operational Security problem. Your mission could be slowed down or stopped by your dependence on one information device and failure to protect it.

Then there is the "accidental" threat areas. Do you have procedures to insure that all disks are "backed up" with copies stored in separate areas. Are the storage areas safe from extreme heat, cold, humidity, or magnetic effects? A floppy disk set next to a telephone can be ruined by one incoming call. When the phone rings, a strong magnet is initiated which will scramble your electronically stored information.

Step 2 - Consider your threat from three angles: Hostile Agent Threat; Physical Threat; Accidental Threat.

c. Implement Countermeasures - This takes us to the countermeasures area. Once you have defined your threats, know how to counteract them. If you have already prepared for a problem, your operations will not suffer if the problem can be countered quickly and efficiently.

Step 3 - Be prepared for a threat problem, and know how your operations might be affected and can be corrected before a problem arises.

d. MONITOR AND EVALUATE EFFECTIVENESS. No program will be successful if it remains static. Your program must be a dynamic process, just as your personnel change, your program can change. Consider the everyday office considerations of moving furniture. Maybe when the computer first arrived it had a dedicated spot safe in a quiet corner. Due to office space realities, it now must be moved next to a busy hallway. Your physical security needs have changed. What about office personnel? When the computer first arrived maybe there was a little hostility toward the device. It was new, and meant change to procedures that were familiar and, above all, not well understood. Maybe the small computer is more accepted now, with less need for constant surveillance and more room for creativity on the part of your users. "Accidents" should be less likely and there should be room for more trust. The small computer can be a great office tool. Let your people use it as such.

Step 4 - Monitor your program and make sure it stays effective.

e. MODIFY WHEN NECESSARY - This takes us to our final stage. Don't be afraid of change. You got the computer for the office - use it, but don't forget to protect it.

Step 5 - Learn from experience. If your program fails, make it work; if it works, make it better.

That's the OPSEC Small Computer process in a nutshell - five easy steps. You won't find it in any regulation, and the IG will not be there to make sure you use this exact process (they do inspect for other items). But, the Air Force does expect you to keep your small computer system safe from threat and operationally secure. Order copies of, and become familiar with: AFR 300-3, Management of Small Computers; AFR 300-13, Safeguarding Personal Data on Automated Data Processing Systems; and AFR 700-10, Information System Security. This may not be the process for you. Design your own OPSEC system. Implement it and stay with it. Remember, if you don't who will?

* *

THE HUMINT THREAT (U)

This article was produced by the Air Force Office of Special Investigations to acquaint Air Force OPSEC Officers with the nature and scope of the threat to the resources for which they have protective responsibility.

25X1

Page Denied

Next 1 Page(s) In Document Denied

requests by U.S. officials in the PRC.

7. (U) Since there are no travel restrictions for East European officials, no closed areas for PRC officials, and since Soviet Officials travel through "closed" areas with special permission, virtually no section of the U.S. is immune from visits by hostile intelligence officers. In addition, there are no travel restrictions on Soviet or PRC tourists, exchange students, or employees of the UN Secretariat.

e. (U) Illegals

1. (S) [redacted]

25X1

2. (S/NF) [redacted]

25X1

3. (C/NF) Since 1973 when the Soviet Union reduced immigration restrictions, especially for Soviet Jews desiring to resettle in Israel, the Soviet immigration population in the U.S. increased dramatically - - by over 20,000 in 1980 alone. The SIS have not overlooked this influx of well-educated and talented Soviet-born immigrants as a cover for infiltrating intelligence operations.

4. (S/NF/WN) [redacted]

25X1

f. (C) The intelligence role of the Soviet Journalists.

Soviet journalists abroad for the most part represent TASS, the Soviet Wire Service; the Novosti Press Agency; Pravda, the CPSU daily; Izvestia, the official government daily; and the State Committee for Television and Radio broadcasting. While their journalistic productivity is less than impressive, in the collection of information, they have notable advantages. Since they are not official representatives of the Soviet Government, their travel in non-communist countries is normally not subject to the restrictions imposed on members of official Soviet missions. They are particularly valuable in the Soviet intelligence effort since their overt role as collectors of information is readily accepted. Many of the Soviet foreign news correspondents assigned abroad may be intelligence officers.

g. (S) Communist-nation visitors to U.S.: In 1955 the United States and the Soviet Union began discussion leading to what has become known as the East-West exchange program (EWEP). While the first agreement under the EWEP was signed in 1958, the program witnessed dramatic growth beginning in 1972. Summit conferences that year spawned a series of educational, cultural, commercial and scientific/technical agreements which brought increasing numbers of communist-nation visitors to the United States. Between 1978 and 1980, the number of communist-country commercial and cultural visitors almost doubled (from more than 14,000 to about 28,000). PRC student presence increased almost five fold between 1979 and 1980 (from about 950 to 4,600). The tourist influx from some communist countries almost tripled from 1979 to 1980. These increases, coupled with a parallel growth in communist-nation official presence, provided the USSR an unprecedented opportunity to exploit its access in the U.S. for intelligence purposes.

h. (U) Students

1. (S) [redacted]

25X1

2. (S/NF) [redacted] They are

25X1

interest as are the details of school job requirements and hiring practices.

3. (S/NF) Three academic fields accounted for most of the 1980-81 Soviet applicants' courses of study: Computers (18 students), microelectronics (11), materials processing and manufacturing (8). Because of the large number enrolled in scientific and technological fields of study, it is obvious their primary objective is to learn as much as possible about advanced Western technology.

i. (U) Merchant Ships

1. (S) There is increasing evidence that Soviet Merchant Ships (merships) engage in intelligence collection activities. The tremendous size and worldwide deployment of the Soviet Merchant Fleet offers a significant maritime intelligence collection potential. State control of this fleet makes it relatively easy for the ships to be tasked with a maritime intelligence role. As of Jan 80, the Soviet ocean-going merchant fleet consisted of about 1800 ships. The Soviet fishing fleet numbers in excess of 3800 units. Augmenting the commercial fleet is a vast special service fleet that includes ice breakers, ocean salvage ships, dredges, and training and scientific units. The extensive trade routes followed by these merchant vessels provides a means of surveillance in areas far removed from the ordinary coverage of other surveillance systems.

2. (S) [redacted]

25X1

etc.

h) (S) Reporting on Soviet Emigres.

c. (U) Western Visitors to USSR.

1. (S) [redacted]

25X1

2. (S) [redacted]

25X1

3. (S/NF/WN) [redacted]

d. (U) Soviet Trade Activities Abroad

1. (S/NF) [redacted]

25X1

2. (S/NF) [redacted]

WARNING NOTICE: SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED (WNINTEL)

NOT RELEASABLE TO FOREIGN NATIONALS

3. (C) [redacted]

25X1

4. (S) Soviet trade activities abroad also include the work of inspectors dispatched to western countries to inspect and receive industrial equipment and materials purchased by Soviet trade organizations. These inspectors may make short trips abroad or may actually be assigned to a factory in the west where the equipment is being produced for the Soviet customers.

5. (U) Soviet trade representatives such as those described above have a significant advantage over personnel assigned as official staff members at Soviet diplomatic establishments. Commercial employees are not normally subject to the travel restrictions imposed upon diplomatic personnel.

e. (S/WN) Scientific Conferences and Symposia:

Both the KGB and GRU recognize the collection potential represented by conferences, symposia, conventions and congresses sponsored by Western professional and scientific societies. According to a U.S. intelligence agency, while Soviet intelligence officers do not expect to collect classified information, such meetings are regarded as opportunities to identify targets (personnel, materials, projects, industrial firms, governmental agencies, new scientific or technological developments, etc.) for future exploitation. In addition to face-to-face contact with Western scientific and technical personnel, these events afford access to reports, speeches, papers, and technical publications which may not otherwise be easily obtainable by the Soviets. Access to meetings is often obtained by joining the sponsoring society.

f. (C) Trade Fairs, Exhibits, and Air Shows:

Opportunities to collect scientific and technical data at events open to the public attract the interest of, and attendance by, Soviet Intelligence Officers, co-optees and agents. For example, Director of the KGB First Chief Directorate (responsible for collecting and analyzing scientific data) is reported to maintain special task forces which operate at international trade fairs. Air shows, in particular, attract attention as lucrative targets. Not only do such shows provide an opportunity to scrutinize the latest in Western aviation technology, but they also enable the Soviets to gather sales brochures and other literature. These shows also provide an opportunity for face-to-face contacts with aviation personnel possessing direct access to the latest Western aviation developments. The Farnborough Air Show in the United Kingdom, the Paris Air Show, the Hannover Air Show in West Germany, and the Japan International Air Show invariably attract Soviet Visitors.

g. (C/NF/WN) Patents and Licenses:

Soviet pursuit of Western technology increasingly involves the acquisition of Western patents and licenses. According to a Soviet immigre, it became apparent after the mid-1970's that even by producing Soviet prototypes based on single items of Western equipment - - acquired illegally or by purchase - - the USSR was still at least several years behind the West. Foreign technology presented by patents and licenses needed to be obtained, even at great expense. For this reason, the all-union association (V/O) responsible for export and import of patents was established to acquire high-technology patents from abroad. Patent services were also created in all government ministries and departments. The number of Soviet personnel involved in patent services reportedly almost doubled from 1970 to 1976.

h. (U) Open Sources

1. (U) A major source of information continues to be publications available in the public domain. In addition to newspapers, magazines, technical and academic journals, maps, industrial and trade promotional literature, corporate directives and reports, and congressional publications, Soviet institutions and representatives systematically obtain American official and private publications, from organizations such as the National Technical Information System (NTIS).

2. (U) The NTIS bibliographic data file consists of hundreds of thousands of summaries of technical documents prepared by major federal departments and agencies, including the Department of Defense. The Soviets are estimated to collect over 80,000 documents yearly from NTIS. Although NTIS has curtailed its response to overt Soviet requests, the use of third parties as requesters is anticipated.

i. (U) Hostile Intelligence Targeting of USAF Personnel

1. (U) During 1981, 894 USAF personnel in the CONUS made reports of contacts responsive to AFR 205-57, "Reporting and Investigating Espionage, Sabotage, Terrorism and Subversion." The majority of contacts reported represented a minimal intelligence threat to the USAF, i.e., solicitations to subscribe to Soviet magazines, Ham radio contacts, correspondence with relatives living

behind the Iron Curtain, etc. In more than 200 incidents, defense-related information was solicited from USAF personnel by unauthorized individuals and organizations.

[redacted]

2. (U) Requests for information were occasionally received telephonically or by mail; however, the overwhelming majority of requests were made during a personal contact in which the requester approached the USAF member and initiated a conversation.

3. (U) Most incidents involved young, first-term airmen in the grades of E-1 through E-4. The individuals approaching USAF members represented both sexes and several racial groups. They range in age from the late teens into the sixties, and many appeared to be U.S. citizens.

4. (S) Some unauthorized requests for information may have represented mere curiosity on the part of the requester or were otherwise attributable to a motive not necessarily inimical to USAF security. AFOSI analysis, however, disclosed that most of the inquiries fell within the parameters of known hostile intelligence collection requirements directed against the USAF.

5. (C) Frequently the timing of the questions corresponded with some significant activity such as an exercise, deployment, alert, ORI, etc. In some instances, AFOSI analysis was able to correlate the time frame of the request or content of specific questions with other known hostile intelligence activities targeting the USAF installation or activity involved.

j. (C) This article describes some of the dimensions and complexity of the intelligence threat posed by Communist-Nation Intelligence Services, particularly those of the Soviet Union, to an Air Force target. A clear knowledge of the threat is essential before effective countermeasures can be undertaken. Although OPSEC activities in the Air Force vary, there is a need for aggressive "awareness" programs and effective countermeasures tailored to individual units/situations. (SOURCE: AFOSI)

* *

HUMINT THREAT TO SECURE AUTOSEVOCOM FACILITIES (KY-3) (U)

(U) A recent message from HQ USAF/SIT (quoted below), emphasizes the HUMINT threat to our secure AUTOSEVOCOM facilities. As the preceding HUMINT article states, the Soviet Intelligence Services and

their BLOC representatives seek classified information, scientific and technical data and endeavor to identify targets for future exploitation. A prime target of the Soviets is U.S. cryptography.

1. (S) Ensuring the integrity of keying material against possible exploitation by hostile agents is a vital consideration in the maintenance of a viable COMSEC posture. The National Security Agency has noted an alarming increase in COMSEC insecurities resulting from the loss of two-person integrity of AUTOSEVOCOM Wideband key cards. Although the circumstances of reported COMSEC insecurities differ, the principle cause of the COMSEC insecurities appears to be the same:

[redacted]

A. (U) Lack of awareness and sensitivity on the part of users to the importance to the national security of the COMSEC keying material they handle.

B. (U) The need for stringent compliance with prescribed physical security safeguards.

25X1

[redacted]

[redacted] 25X1

* *

The following article by Mr. Pat Martin, HQ ESC/CSI appeared previously in our October 1983 edition of the OPSEC Update. We feel the information is worth repeating.

<u>COUNTERINTELLIGENCE</u> (U)

(U) Counterintelligence is an often misunderstood term both inside and outside the USAF. In order to understand counterintelligence as a term and a practical and integral aspect of OPSEC, a knowledge of the intelligence threat posed by adversary intelligence services is necessary.

(U) Intelligence gathering activities currently directed against the United States Air Force are multifaceted. They can generally be divided into two categories: Technical collection efforts (i.e. SIGINT and IMINT) and human collection (HUMINT). Although vast quantities of information can be collected through technical collection efforts, adversary intelligence services have demonstrated time and time again that human acquired information is considered the most reliable indicator of the true workings and details of any specific event. Human collection, while often difficult to initiate, can be specifically targeted, can be extremely difficult to detect, can remain hidden until required (the "sleeper agent"), and can be relatively inexpensive to sustain. The human collector, if properly trained, can also re-direct his/her efforts to meet the needs of the situation and can often provide collateral information while working a specific target. With proper cover and documentation the human agent can penetrate the most secure areas by obtaining employment and gaining trust. If such long term preparation is not considered feasible, the adversary intelligence service can attempt recruitment of an employee in place through monetary or ideological persuasion. All of the factors which make the human so valuable to any system can also be made to work against the system we are trying to protect.

(U) One hypothetical example can be given to further illustrate the benefit of HUMINT. Let us assume that ALPHA AFB, anywhere, has recently acquired the F-25 weapons system. Operational elements have determined that day to day sortie generation is susceptible to technical exploitation and have thus ordered that "look-down-shoot-down" radar capability be exercised only during specific and randomly selected times. With strict compliance it is felt that this should severely limit technical intelligence collection against the system. After repeated attempts to establish technical collection against the F-25, an adversary intelligence service concludes ALFA AFB must receive priority HUMINT collection. An assessment of ALFA and its environs is made and the following scenario is created. Local intelligence officers assigned to diplomatic and quasi-diplomatic establishments are instructed to activate their contacts in the local civilian population who cater to the entertainment needs of ALFA AFB personnel. These contacts are to begin collecting information on personnel who are engaged in excessive drinking, gambling and socializing with members of the opposite sex. They are also instructed to be alert for those military members interested in selling goods from ALFA's BX and commissary. Anger, disgruntlement, and ideological naivete' were also to be reported. After some frustrating false leads, an avionics technician is identified. Through careful targeting and patient waiting, the reward finally comes. The adversary intelligence service obtains the complete tech order of the radar. Cost? Time and $5,000.00 paid to the technician for "services provided."

(U) What does the OPSEC manager have at his/her disposal to combat the HUMINT threat? The Air Force Office of Special Investigations. Through AFOSI's counterintelligence efforts, the OPSEC manager can insure his units receive AFR 205-57 briefings (Reporting and Investigating Espionage, Sabotage, and Terrorism), be placed on distribution for Intelligence Information Reports (IIRs) outlining significant counterintelligence and terrorist - threat charges affecting his unit/base, and arrange for specialized AFOSI counterintelligence efforts to work the problems relating to security and protection of significant systems or events. In accordance with AFR 55-30, the OPSEC manager can request a multi-disciplined counterintelligence (MDCI) threat estimate for OPSEC planning. This threat description currently includes the HUMINT threat and the SIGINT threat as provided by HQ ESC/INKC. The OPSEC manager may also contact the AFOSI MAJCOM rep to his/her command for assistance. AFOSI has currently placed MAJCOM reps at HQ MAC, HQ SAC, HQ AFSC, HQ TAC, HQ ESC, and USCENTCOM. Officers assigned to these commands can offer assistance in OPSEC planning in the area of counter-HUMINT and anti-terrorism. They can also provide assistance in understanding MDCI threats and their value in command level OPLANS and CONPLANS.

(U) Effective OPSEC cannot become a reality unless the OPSEC manager makes full use of all resources. AFOSI is charged with Air Force counterintelligence and MDCI responsibilities under AFR 23-18. Know your experts in AFOSI.

TEMPEST AND YOU (U)

(C) TEMPEST is an unclassified short name for the study and control of electromagnetic emanations which can be used to "read" classified information. Emanations are the result of any electrical process either natural or manmade. Lightning strikes and your automobiles spark plugs are examples of natural and manmade electrical processes which are easily detectable on your AM or FM radio. The problem begins when classified information is processed electrically and the information leaves a "fingerprint" on the emanation which can be detected and broken back to the original text. In many cases, the detected emanation is no more difficult to decipher by the trained operator than the word puzzles you find in the Sunday paper.

[redacted]

(S) How do we control something which is the natural result of using electricity? The only thing we can do is minimize those signals or if that is not sufficient, contain them. The efforts of the designer, installer and operator are needed to minimize signals. The designer can use several methods to aid him. The most important is low-levels of current and voltage. The lower these levels, the lower the energy of the emanation, and the harder it is to detect. Grounding is very important for both the designer and installer. A good ground will conduct many undesirable signals into the world's biggest conductor, the earth itself, where they cannot be recovered. When all else fails, it is necessary to encase, or shield, the offending component or equipment to prevent leakage of the emanation. Shielding is undesirable because it is difficult to maintain its integrity and it usually requires operational restrictions. These methods will usually reduce the emanation to a level that is only detectable a short distance away from the source and is easily protected by the Control Space.

(S) The emanation, if still detectable in the immediate area, will impress itself on any antenna that is available. Telephone lines, conduits, water pipes, air conditioner ducts or any other metal structure can act as the antenna, and then conduct the emanation out of the Control Space on any conductor which is attached. Conducted emanations from a weak emitter can travel many miles when the radiated emanation may only travel a few meters.

(C) There are two ways to prevent conducted emanations. The first is to keep all conductors outside the Control Zone. This is not always easy to do, and in some cases may be impractical. A filter or an isolator may be used to stop emanations from being conducted out of the Control Zone. Filters allow desirable signals to pass, and block undesirable signals while isolators block all signals.

(U) So, what can you do to help? Just being aware of your TEMPEST responsibilities is a big help. Anytime classified information is or will be processed electrically, TEMPEST must be considered. If you are involved in buying or leasing equipment, you should be aware of all Air Force policies regarding TEMPEST, and you are responsible for including TEMPEST requirements in the contract. Maintenance personnel who install or maintain this equipment are charged with maintaining the TEMPEST integrity of all the equipment they service.

(S) Be alert to open cabinet doors or broken wires. A broken shield or a bad ground can ruin several thousand dollars worth of TEMPEST modifications. Also, be aware of the separation requirements between RED equipment (which is used to process classified information) and BLACK equipment (which should never be used to process classified information). The administrative telephone is the worst offender. It makes an excellent antenna, and has a conductor which extends far beyond the bounds of any control space.

(U) The best place to go for TEMPEST information is to your local TEMPEST Officer and/or NCO. They have the answers to your questions, or know how to get those answers.

(C) You are encouraged to contact them with all your questions. Trying to correct a TEMPEST problem as an afterthought is much more costly in time and money, and exposes our carefully guarded classified information to easy and safe interception.

SOURCE: ESC TEMPEST Office, 1Lt Hackett.

* *

COMINT THREAT TO U.S. AUTOVON AND GERMAN BUNDESPOST TELEPHONE NETWORK (U)

(C/NF) The purpose of this article is to reveal the extensive and sophisticated effort that the Warsaw Pact has dedicated to the collection of information from the highly lucrative, and vulnerable, U.S. AUTOVON and West German Bundespost telephone system. Thousands of AUTOVON calls are made daily by European assigned personnel. Although reminders warning against discussion of classified information are posted on all military phones, Communications Security (COMSEC) monitoring of AUTOVON lines has disclosed that classified information, or information considered hazardous to National Security, is discussed openly over AUTOVON phone lines. These discussions provide Warsaw Pact intelligence services with valuable and sensitive data.

(4) (S/NF) AEROFLOT, the Soviet National Airline, is possibly being used to monitor AUTOVON communications. In Oct 83, three AEROFLOT flights deviated from scheduled takeoff and approach paths to overfly the U.S. Army military facility in Livorno, Italy. This facility consists of an ammunition storage area, a depot area, and the Altano AUTOVON switching center. One of these aircraft was an AN-12 CUB -- a type suspected of conducting covert SIGINT collection.

(5) (S/NF) The Chief Intelligence Directorate of the Soviet General Staff (GRU) has technical service elements established in Soviet legal residences throughout the world. These technical service elements conduct continuous COMINT collection against U.S. Communications, to include the AUTOVON network. In Central Europe, COMINT collection occurs at the Soviet trade mission in Brussels, Belgium, the Soviet Embassy in Luxembourg, the Soviet Embassy in Bonn, and probably the Soviet trade mission in Cologne. Exploitation targets include format messages such as Emergency Action Messages (EAM) passed on AUTOVON channels from the CINCEUR, and phone conversations between military personnel both in Europe and the U.S.

(6) (S/NF) At the SMLM facility in Frankfurt, two 19-element Yagi Ultra High Frequency (UHF/Very High Frequency (VHF) antennas are pointed towards the Donnersberg and Geldberg, West Germany, AUTOVON switching centers. Intercept of communications emanating from these centers would allow access to a large amount of unencrypted AUTOVON circuits. On 10 Mar 77, a SMLM vehicle from Frankfurt was detailed less than 100 yards from the V Corps Mobile Tactical Command Post (CP). Signal Security (SIGSEC) monitoring of USAREUR phone lines reflected a 4 Mar 84 conversation in which the Corps Tactical CP was indicated to be "700 meters south of the 3rd Armored Division at or near NB414133." There is a possibility the SMLM could have had foreknowledge of the CP location as a result of the AUTOVON monitoring.

(7) (S/NF) Microwave communications intercept sites are located throughout East Germany and Czechoslovakia along the West German border. The site at Brocken, East Germany, maintained by an unidentified Soviet SIGINT brigade subordinate to HQ GSF6, is a major Soviet intercept facility tasked with the monitoring of Bundespost and U.S. AUTOVON telephone communications. This site is perfectly placed for the intercept of telephone calls transmitted via microwave links physically located within West Germany.

(8) (C/NF) A former senior lieutenant with the Czechoslovak 7th Radio Regiment, a major COMINT organization tasked with radio intercept of CENTAG communications, disclosed that the most lucrative intelligence was derived from monitoring of the U.S. AUTOVON network. He was assigned to an intercept company at Cerchov, Czechoslovakia, intercept site monitoring on a daily basis the super high frequency

(SHF) AUTOVON switchboard of the U.S. VII Corps.

(9) (C/NF) The 78th Radio Center, a regimental size COMINT collection unit subordinate to the Czechoslovak ministry of National Defense is responsible for the intercept of troposcatter communications between USAREUR and the U.S. Army Berlin Brigade. This intercept of AUTOVON communications transmitted via microwave is conducted at Dylen and Cerchov. Parabolic antennas are used for this intercept.

(10) (C/NF) West German Intelligence/Security Services are well aware that Soviet Bloc nations intercept telephone calls made both within West Germany and between West Berlin and West Germany. An official of the Bonn government stated that long distance calls transmitted via microwave are intercepted by the Soviet Bloc using special equipment and then analyzed with the help of sophisticated computers. West German governmental telephone communications are a high intercept target for HOIS.

(11) (C/NF) In an effort to limit the success of this monitoring activity, the Bonn government has replaced their conventional telephone cables with fiber-optic cables for their official telephone communications. This will minimize the effect of electromagnetic "bleeding" from the cables making hostile intercept much more difficult.

(12) (S/NF) Since the early 1970s, high emphasis has been placed on the intercept of microwave channels owned and operated by the West German Bundespost and leased by the U.S. and West German military. Targets for this intercept include the telephone exchanges at Frankfurt, Kaiserslautern, Munich, and possibly Augsburg. The exploitation of AUTOVON links serving U.S. Corps and division elements, as well as individual units fielding Theater Nuclear Force (TNF), Readiness, exercise plans/results, equipment capabilities, and operational limitations.

(13) (S/NF) HOIS also monitor selected AUTOVON circuits carried over U.S. communications satellites. The Defense Satellite Communication System (DSCS) is the principal Super High Frequency (SHF) SATCOM system providing communications among DOD users. The DSCS is responsible for maintaining AUTOVON satellite communications servicing some 130 globally deployed earth terminals. The Soviet Union and other Soviet Bloc nations intercept DSCS Communications Satellites (COMSATS) carrying AUTOVON communications.

(14) (S/NF) Of the nine GRU military associated satellite intercept facilities located in the Soviet Union, the site at Vicak USSR, is believed to be tasked with the exploitation of AUTOVON communications carried by the Atlantic DSCS II Satellite. A 16.5 meter parabolic antenna is used to intercept the DSCS. DSCS

communications are also probably intercepted at the Lourdes Central SIGINT complex near Torrens, Cuba. The KGB maintains satellite intercept sites in the Soviet Union for the intercept of commercial satellite signals not associated with the U.S. military.

(15) (S/NF) The East Germans and the Poles are also believed to possess satellite intercept sites used to monitor U.S. AUTOVON communications between West Germany and the continental U.S. The Czechoslovakian 78th Radio Center also monitors satellite communications in the range of 200 to 400 MHZ and eight GHZ. The Soviets primarily use the Soviet Intelligence Collection Ship (AGI) fleet for mobile COMSAT intercept. Many AGI's are assessed to be capable of intercepting signals in the range of 15 KH3 to 100 GH3, easily covering all DSCS frequencies.

(16) (C/NF) Conclusion. At this time, U.S. AUTOVON and West German Bundespost telephone circuits are being consistently exploited for their intelligence value since the reliance on these communications are critical to USAREUR in both peace and war. There is little doubt that HOIS will continue to heavily monitor these circuits. The only methods available for ensuring AUTOVON/Bundespost security from hostile monitoring activities would be to bulk encrypt all communications emanating from the major switching centers or to provide speech encipherment devices at all line terminals (telephones). In the case of the AUTOVON network, this is not feasible in the near future and is cost prohibitive. With regard to the Bundespost system, the cost of total network encryption could not be justified by the West German government based on the philosophy that the Bundespost is a public, as opposed to a military, communication network.

(17) (S/NF) A recent defector assigned to a major Czechoslovakian SIGINT unit stated his organization collected their most valuable data by monitoring the phone calls of U.S./NATO flag officers. Since this is the case, it would be appropriate to supply these personnel with speech encipherment devices in lieu of, or attached to, their telephones. A likely candidate for this device would be the STU-2M recently developed by NSA. An addition of more AUTOSEVOCOM terminals throughout the USAREUR command would also help to eliminate the need to "talk around" classified information when a secure telephone is unavailable.

(18) (C/NF) The HOIS capability to intercept, process and glean intelligence from the AUTOVON or Bundespost networks is formidable. This capability represents a serious threat to USAREUR and will become an even greater threat in the future as more U.S. military telephone lines are leased from the Bundespost. At the present time, HOIS can accurately determine USAREUR's readiness posture, operational deficiencies, organization, exercise plans/results, and the complete status of the TNF force. The HOIS acquisition of more

sophisticated intercept equipment and large scale computers obtained through western technology transfers, will increase USAREUR's vulnerability to hostile collection derived from the monitoring of AUTOVON/Bundespost telephone circuits and poses an even greater threat to Operations Security throughout the command.

SOURCE: CINCUSAREUR - Extract from ESC OPSEC Highlights Message 231500Z Feb 85.

* *

SOVIET MILITARY ATTACHE TRAVEL IN THE U.S. (U)

The following article was extracted from a U.S. Army Intelligence and Threat Analysis Center Intelligence Brief. It provides a synopsis of Soviet Military attache travel within the United States during 1980-83, and a summary of their overt collection activities.

A. (S) As the "main enemy" of the Soviet Union, the U.S. is subjected to pervasive intelligence targeting by the Committee of State Security, or KGB, and the Ministry of Defense's Chief Directorate for Intelligence or GRU. Collection efforts to satisfy this targeting range from legal and overt to illegal and clandestine. This article will provide insight into the intelligence threat posed by one type of Soviet Intelligence Collection Activity: Overt collection by Soviet Military Attaches (SMA) during travel in the U.S.

B. (S) SMA travel in the U.S. from their Washington DC Embassy base during the period 1980-83 showed little significant change from travel performed in prior years. Travel was invariably in pairs with at least one attache having experience traveling in the U.S. Neither rank nor service affiliation seemed to bear on who was paired with whom.

C. (S) Because of the frequency and numbers of SMA and other Soviets who travel the Washington DC - New York City corridor, routine monitoring has been very limited. Information on this route of travel is not included.

D. (S) SMA's generally use Soviet-owned vehicles for travel to destinations that lie within about 500 miles of Washington DC. One exception to this rule was an April 1982 trip when they made a round trip drive to Fort Lauderdale FL from Washington DC. The normal mode of travel is public transportation, usually flying to a base city and then using local airlines, buses, or taxies for shorter trips. SMA's are not permitted to rent vehicles. The SMA's have deviated from the schedule outlined in their travel requests only twice in the past three years. Once they deviated and drove by the Pratt and Whitney Plant in Hartford CT and once they had to remain overnight in Chicago IL because of a cancelled airline flight.

E. (S) While traveling by car, the SMA's make numerous stops for food, refueling, picture taking, and driver changes. They are usually safe and careful drivers, having been stopped for speeding only twice in the past three years. When traveling by air, they check their suitcases but never their attache cases. They are also careful to avoid having their cameras x-rayed at airport security check points.

F. (S) While traveling, the SMA's invariably carry at least one, and often two, attache cases, which never leave their possession. They also have at least one, and often two, 35mm cameras. They carry what appears to be a normal amount of luggage for the trip to be undertaken. Despite this, they have been observed wearing the same clothing for a four-five day period with a resulting strong body odor.

G. (S) Hotel or motel accommodations are made for SMA's in advance. They tend to stay at moderately priced national chain motels. Upon registration, they identify themselves as Soviet diplomats. If asked, they will admit to being Soviet military officers although they always travel in civilian clothing. About half the time they eat their meals in their rooms, combining Russian canned goods they have brought with them with bread, fruit, and vegetables acquired in a local grocery. When they do eat out, it is usually at an inexpensive place and the meal usually consists of pizza or hamburgers. They very often drink beer with both lunch and dinner and usually consume one or two bottles of vodka in their room at night. They will occasionally invite someone they meet by chance in the halls or dining room of the motel to come to their room for drinks. The drinking and conversation often lasts until early in the morning. These guests are always male. On one occasion, the guest was an FBI undercover agent.

H. (S) The SMA's have made a total of 10 or 11 major trips each year for the past three years. On each of these trips, the SMA's usually spend one or two nights in different cities on their scheduled itinerary.

I. (S) The daily routine of the SMA's while on a trip does not vary greatly. They visit the local chamber of commerce, telephone company, library, book stores, and sometimes a museum, amusement park or art gallery. They acquire information on local employers, maps, a local telephone directory, and any other available information. Most of the material is available free, but the Soviets will pay for the material if required. If the material is not for sale, they will copy it whenever possible. In libraries at state capitols and state universities, the Soviets will sometimes spend hours obtaining materials of a statewide nature. They seem especially interested in heavy industry, power companies, port facilities, and transportation networks.

J. (S) The SMA's have been observed taking a large number of pictures during their trips. Often they appear to be merely photographing local tourist attractions. Some of the photography appears to be designed to include microwave towers, radio relay antennas, or local government-related communications antennas in the background. At other times, the SMA's purposely walk to an otherwise insignificant building or areas and carefully position each other for a photograph. This latter type of photography may have any of several purposes: To spot and record suspected surveillants, to provide a mix of general subjects among overt intelligence subjects in case the film gets into the hands of strangers who would otherwise turn it in to U.S. authorities, to get non-mission related photos for family or friends, or, possibly to support mensuration of Soviet overhead photography.

K. (S) The SMA's are avid collectors of overt information at nearly every city visited on their itineraries. Examples of information collected include:

Local telephone directories

Local and statewide business directories

Local, state, and regional maps

Directories of research facilities

Guides to sources of information which businessmen and researchers can use as references

Marketing Information

Data on local, state, and regional industries

Economic profiles of areas visited and manufacturing guides

Relocation packets providing local area information, e.g., housing, schools, churches, recreation facilities, and employment

Listings of industrial firms

Directories from colleges and universities

Copies of unclassified military manuals, dealing with basic military subjects, that are available in university libraries.

Photographs of landmarks, buildings, and other areas of political, economic, or historical interest.

Local chamber of commerce, Federal Information Center, and State Information Center handouts of all types.

Local newspapers, especially those that contain items relating to area military bases or prominent Defense contractors.

Environmental Impact Statements

Zip Code Directories

Adult Education Programs.

Directories of electronic and light assembly manufacturing plants.

Data on Florida ports and International Airports, facilities, docks, tide tables, and warehouses.

Directories of research facilities which provide mailing addresses.

Published items on the MX missile program.

Directories published in 1982 and 1983, of military commanders, public affairs officers, protocol officers, and secretaries (provides lists of individuals by rank, area of assignment, and telephone number).

Who's Who in business and professions.

Department of Defense or local directories of military officers.

L. (S) [redacted] 25X1

Attempts to detect and identify surveillants.

Great attention to detail in positioning attache cases which could indicate possible short range agent communication activity.

libraries, and tourist areas.

Brief trips to certain areas where the only observed activity was a telephone call from a public telephone booth.

Unexplained, unprovoked periods of apparent tension or great nervousness.

Frequent checking of watches.

Non-typical periods of inactivity in parks or extended stays in restaurants or movie theaters.

Suspicious activities of unknown individuals in the immediate vicinity of SMA's.

M. (S) [redacted]

25X1

* *

IMAGERY INTELLIGENCE (U)

A multidiscipline threat utilized by Hostile Intelligence Services is Imagery Intelligence (IMINT.) This article explains a few of its capabilities.

(U) The importance of imagery interpretation was demonstrated effectively during WWII, Korea, and the Cuban crisis. In WWII, military experts found that almost eighty percent of the intelligence was derived from aerial photography. Imaging sensors can collect information over otherwise inaccessible areas. This is perhaps their most important military advantage. The imagery is a permanent record of the detail within the sensor field of view, and provides a first-hand impression of the target to the expert qualified to interpret it, though he may be many miles distant. The imagery is unprejudiced and reproducible; it can be studied and restudied for various purposes by different users. It can be compared, detail by detail, with other imagery of the same area to provide comparative intelligence. Imagery may be used to map or chart an area as to geographic and cultural detail, and to provide beach and coastal information as well as bottom conditions in the shore area. It can sometimes provide detailed data on shore water depths, but it cannot confirm deep-water soundings. Sensor imagery can provide much detailed military information, such as strength and disposition of enemy forces and general terrain features of areas under his control.

CAPABILITIES:

(U) ... Imagery interpretation provides an accurate and extensive source of information relative to the strength, disposition, and activities of the enemy in areas not readily accessible to ground observers.

(U) ... It provides extensive and detailed information regarding the enemy's installation and equipment and general terrain features of areas under his control, such as vegetation, soil, beaches and water depths.

(U) ... It provides a means of detecting errors in bombing, and data from which recommendations can be made for improvement in operational techniques.

(U) ... It furnishes indications, as in bomb damage clearance and reconstruction studies, of the enemy's evaluation of the importance of damage inflicted on him.

(U) ... It provides target data for operational use, such as annotated plans of enemy installations.

(U) ... It can usually detect and see through camouflage designed to confuse the aerial observer or attack pilot. In addition, it makes possible an evaluation of friendly camouflage techniques.

(U) ... It provides highly accurate information for the preparation and revision of maps and charts.

(U) ... It provides checks on the accuracy of reports from other intelligence sources covering visible objects or activities.

(U) ...It provides a means for assessing the physical effectiveness of geographic and cultural detail, and to provide beach and coastal information as well as bottom conditions in the shore area. It can sometimes provide detailed data on shore water depths, but it cannot confirm deep - water soundings. Sensor imagery can provide much detailed military information, such as strength and disposition of enemy force and general terrain features of areas under his control.

* *

USSR: TECHNOLOGY TRANSFER (U)

A. (S/NF/NC) The Soviet Bloc is using United Nations Programs to gain Western technology. Reportedly, the Soviet Union will use $20,000 of the United Nations Education and Scientific Cooperation Organization (UNESCO) funds to establish a pilot project on microcomputers for their polytechnic schools. Undoubtedly, key features of computer hardware/software, as well as know-how and experience, will flow from the schools to be used in military applications. Normally, UNESCO funds are intended to help transfer new technology to developing countries; however, because a Soviet is directing the microcomputer pilot project, Soviet acquisition of funds was assured.

B. [redacted]

25X1

OPSEC UPDATE - APRIL 1985

COMMENTS:

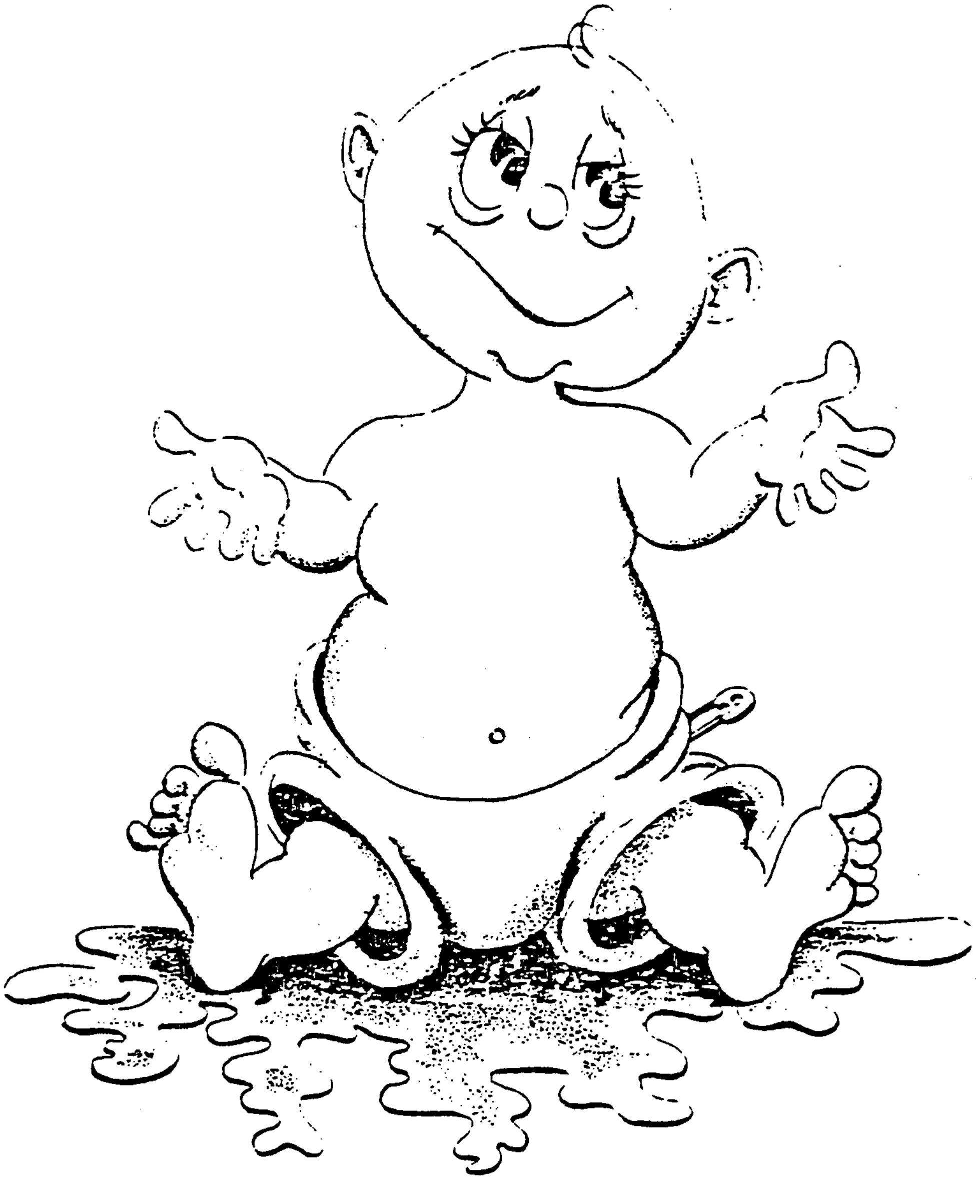
ATCH 1

HQ ESC/DOOO
ATTN: OPSEC UPDATE
SAN ANTONIO, TX 78243-5000

ATCH 1A

Stop those leaks!

[redacted]



OPSEC

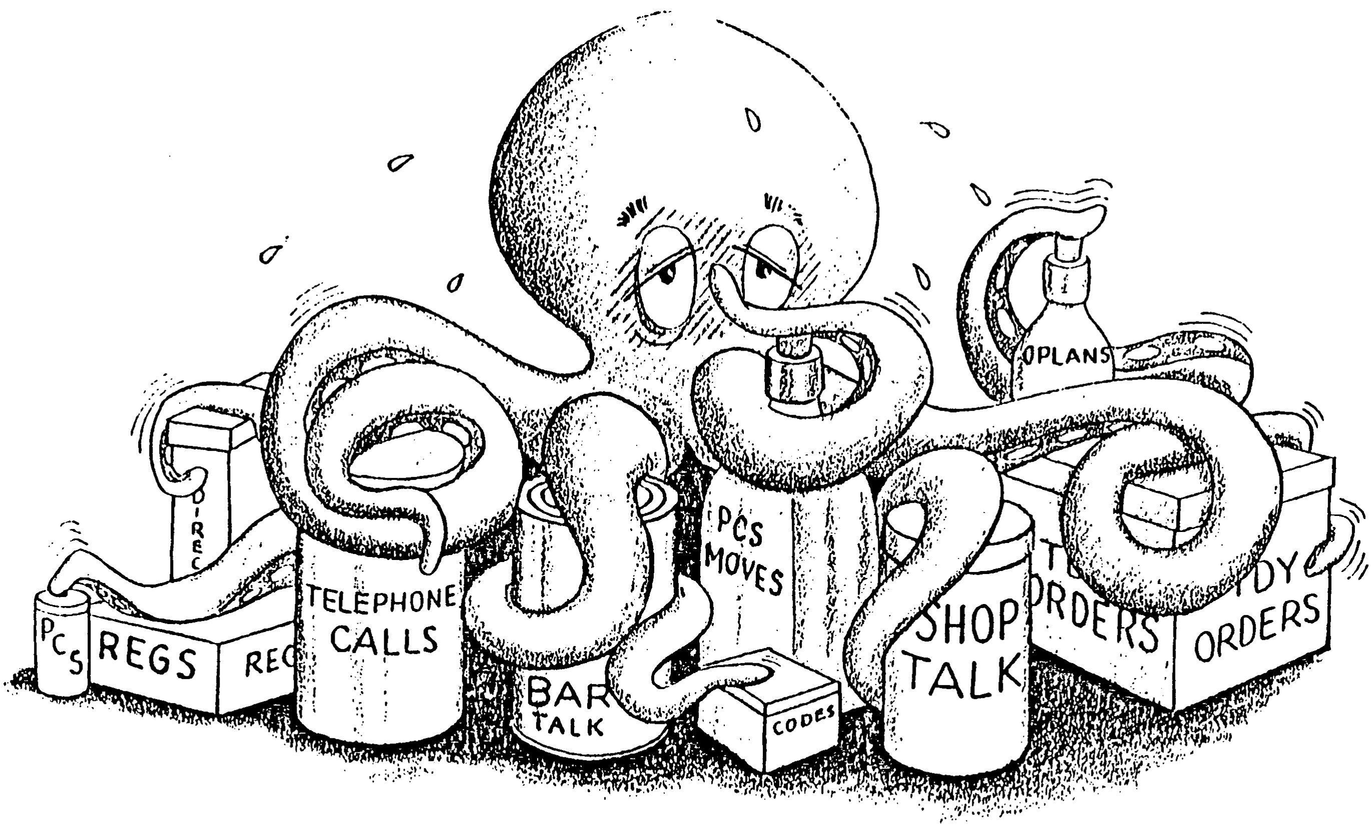
YOUR OPSEC OFFICER IS:

ATCH 2

DON'T let the Cat out of the Bag!

OPSEC YOUR OPSEC OFFICER IS:

ATCH 3



ATCH 4

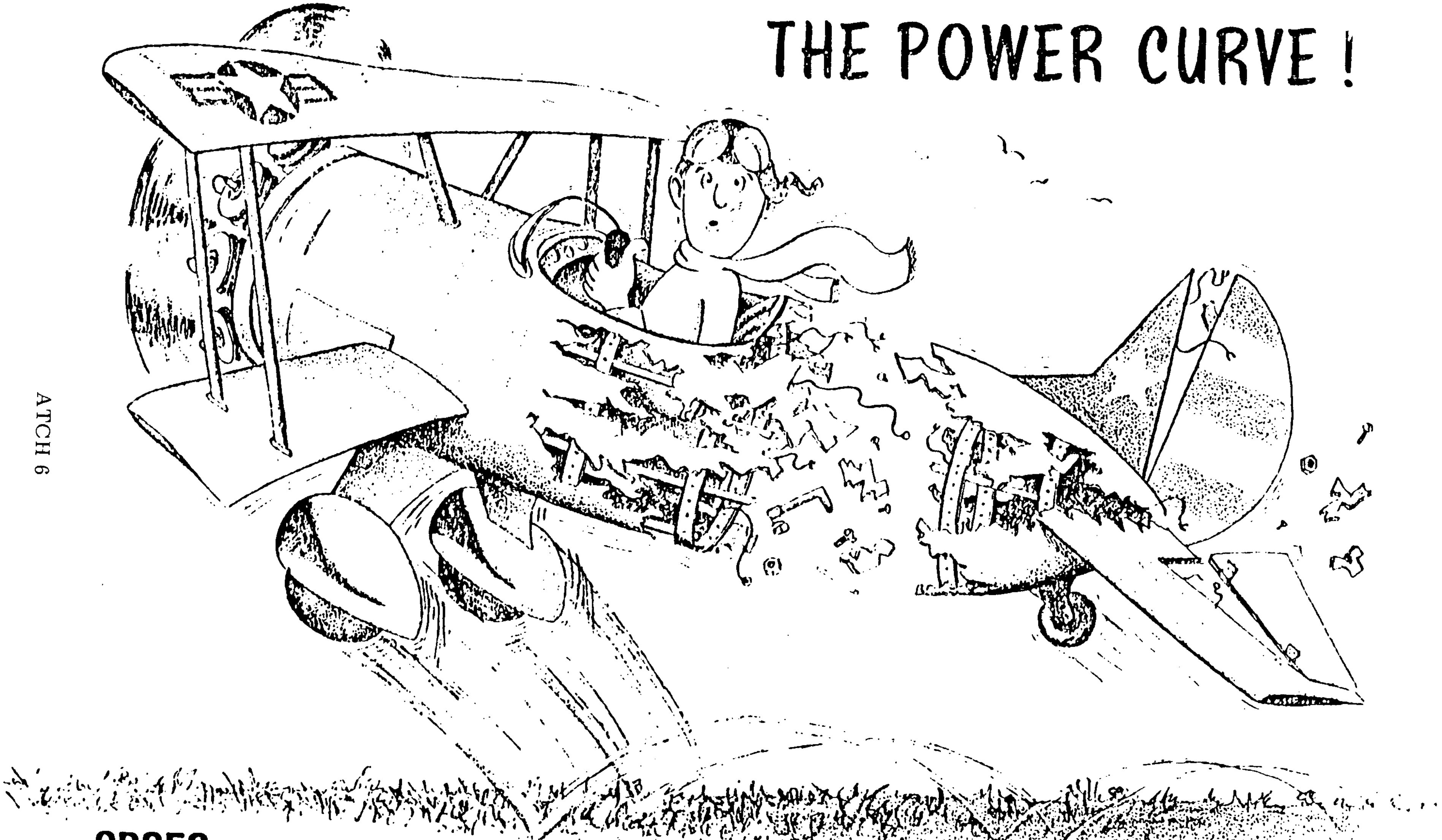
KEEP THE LID ON EVERYTHING!

OPSEC **YOUR OPSEC OFFICER IS:**

CAN YOUR OPERATION WEATHER THE STORM?

OPSEC YOUR OPSEC OFFICER IS:

OPSEC: DON'T GET BEHIND THE POWER CURVE !



OPSEC YOUR OPSEC OFFICER IS:

ATCH 6

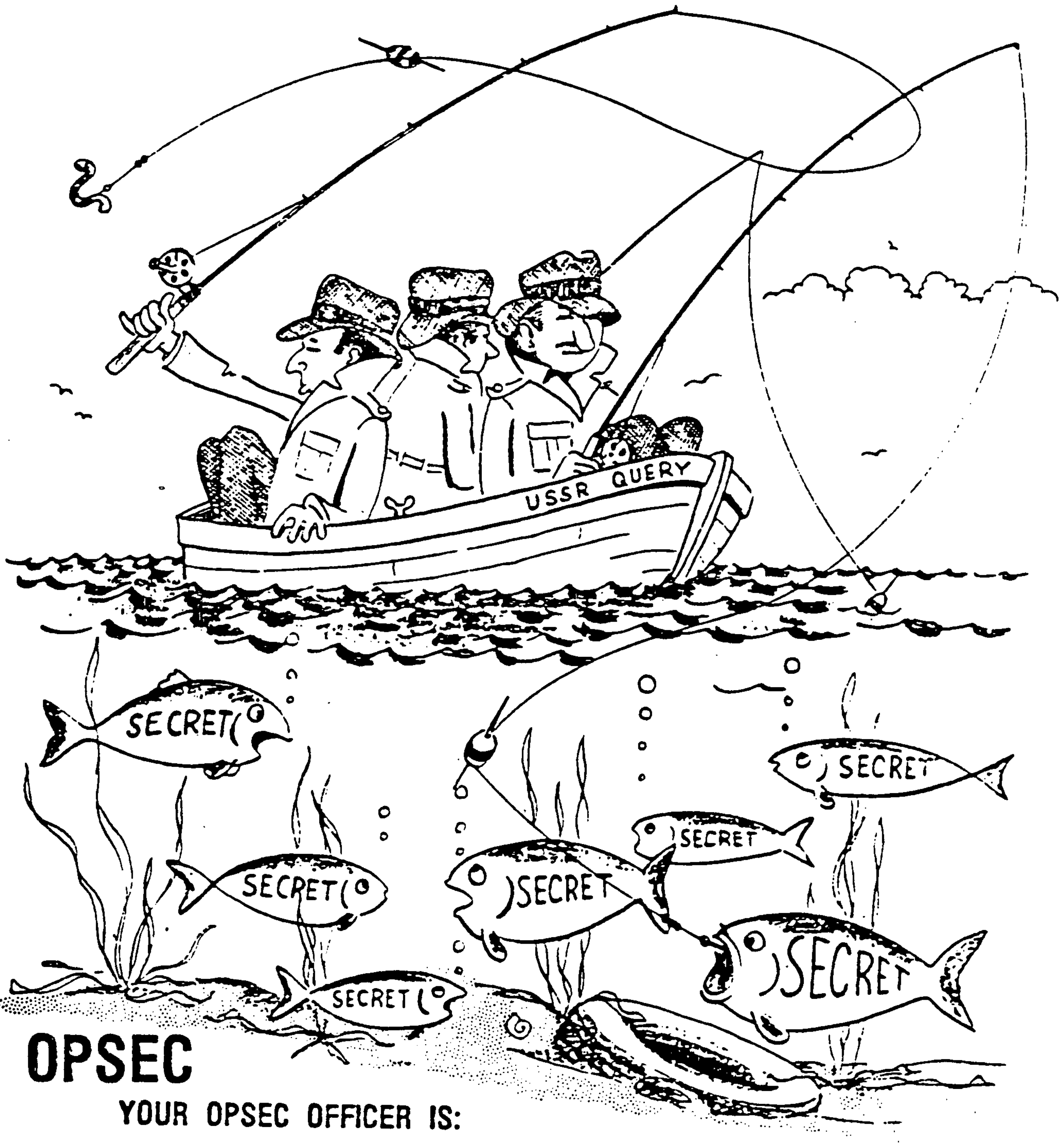
ARE YOU THE MISSING LINK IN OPSEC?

OPSEC

YOUR OPSEC OFFICER IS:

ATCH 7

SHHH! SOMEONE'S FISHING!

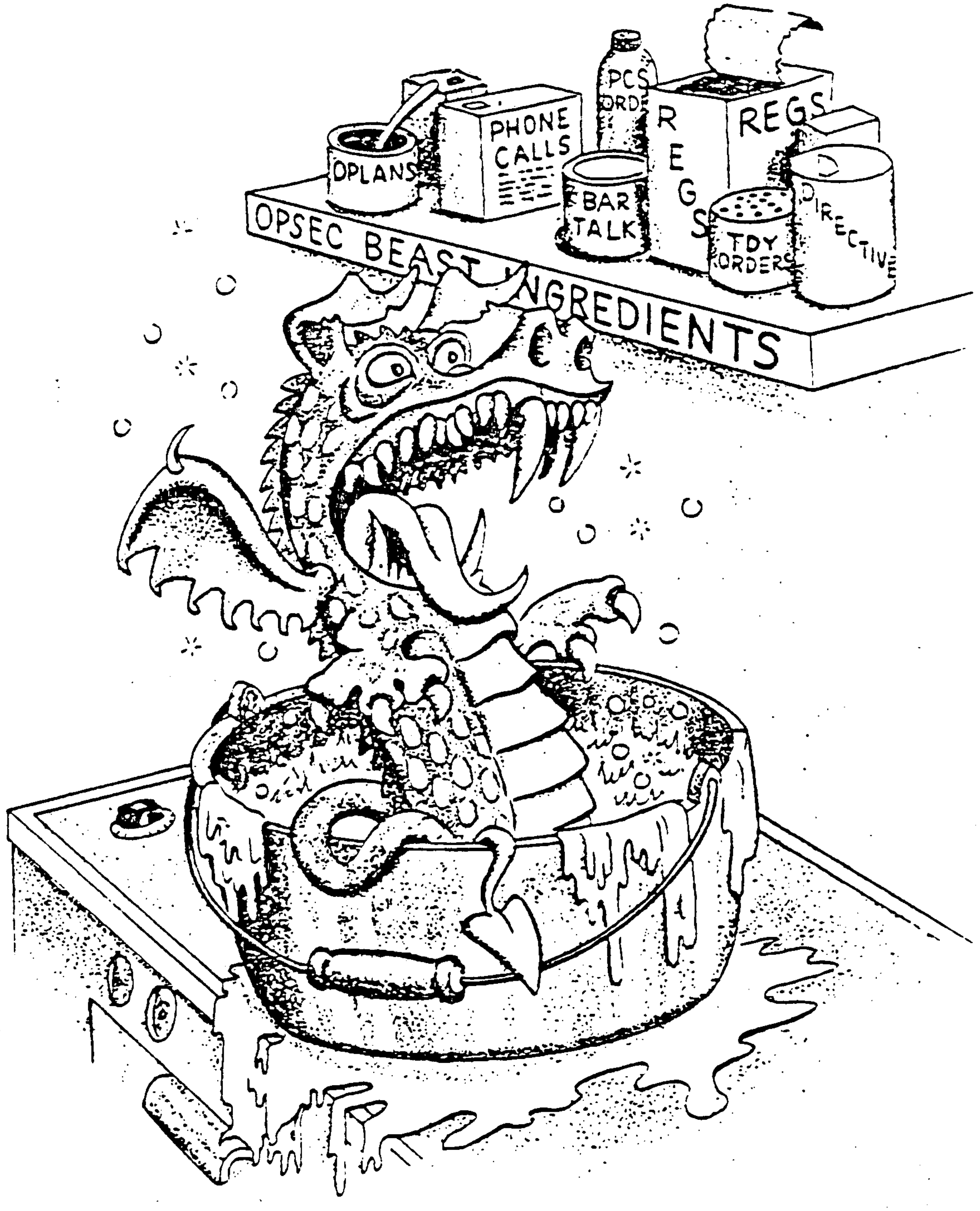


OPSEC

YOUR OPSEC OFFICER IS:

ATCH 8

ARE YOU "BREWING UP" AN OPSEC *BEAST?*



OPSEC YOUR OPSEC OFFICER IS

ATCH 9

A	S	Q	C	O	N	C	E	A	L	M	E	N	T	R	S	W	V	T	E
O	M	O	R	B	L	R	A	C	M	S	R	U	W	O	I	A	N	T	R
M	E	T	H	O	D	S	M	R	A	E	M	C	O	N	O	I	N	D	C
T	D	V	I	W	O	G	D	N	R	E	H	O	I	F	D	I	E	W	O
L	I	T	P	A	C	D	I	A	H	B	I	E	O	A	M	N	V	H	U
C	A	M	O	U	F	L	A	G	E	T	L	P	R	U	S	D	U	K	N
I	W	A	W	C	L	A	B	U	S	A	Z	E	H	G	U	A	G	H	T
T	L	S	I	G	I	N	T	Z	U	T	W	F	T	L	S	W	J	F	E
E	D	K	W	B	R	M	O	S	A	C	P	H	O	T	I	N	T	I	R
N	J	I	E	C	P	C	I	O	A	K	M	M	D	O	G	O	B	G	I
G	Q	N	R	E	S	V	T	O	P	S	E	C	O	T	S	H	I	J	N
A	H	G	F	A	T	E	F	Z	Q	E	N	O	L	A	E	L	I	N	T
M	P	D	T	I	M	E	L	V	R	C	O	M	S	E	C	D	B	T	E
O	R	A	W	H	N	V	H	E	F	U	E	I	K	G	S	R	L	O	L
R	A	D	I	A	T	I	O	N	N	R	T	N	L	C	H	E	D	M	L
T	E	L	S	B	O	D	W	L	P	I	L	T	H	R	E	A	T	T	I
C	O	I	T	T	D	A	S	F	B	T	H	B	E	F	P	N	O	S	G
E	L	S	E	C	C	N	J	S	T	Y	L	E	C	V	I	O	P	F	E
L	R	C	P	S	I	C	T	U	O	L	E	V	I	S	I	N	T	N	N
E	E	F	I	N	W	I	D	W	L	I	C	D	C	L	M	A	M	U	C
D	E	S	D	F	O	R	C	E	S	B	T	E	L	E	P	H	O	N	E

FIND THESE OPERATIONS SECURITY RELATED WORDS ABOVE. WHAT DO THEY MEAN?

EEFI
TIME
OPSEC
ELINT
STYLE
MEDIA
ELSEC
EMCON

COMSEC
SIGINT
COMINT
RADINT
VISINT
FORCES
THREAT
VISUAL

SIGSEC
HUMINT
PHOTINT
METHODS
MASKING
SECURITY
TELEPHONE

CAMOUFLAGE
CONCEALMENT
INTELLIGENCE
ELECTROMAGNETIC
COUNTERINTELLIGENCE
RADIATION

ATCH 10

************************** OPSEC DISTRIBUTION ***********************

FILE NAME: DISTRO1   DATE OF PRINTING: 24 APRIL 85

1	ADDRESSEES	0	2	*DMAAC/SOFA*	2
3	1ST CEG/RBOO	2	4	2AD/INS1	2
5	2BMW/DOC	2	6	2 WS/SQ	2
7	3AF/ESO	2	8	3ACCS/DOF-B	2
9	3D AIR DIVISION	2	10	5TH AF/INS	2
11	5TH AF/DOP	2	12	7TH WEATHER WING	2
13	8AF/DOXF	2	14	8AF/INS	2
15	9TH AF/INS	2	16	9 STRAT RECON WING	2
17	9 STRAT RECON WING/IN	2	18	10 TWR/INS	2
19	12TH AF/DOXE	2	20	12TH AF/INS	2
21	12 ABG/XPR	2	22	13TH AF/DOY	2
23	15AF/DOXM	2	24	15AF/INS	1
25	16 AF(INS)	2	26	16TH SURVEILLANCE SQ	1
27	17 SURS/IOA	2	28	178CF(SFT)/DC	1
29	20 MWS/DOS	2	30	21 AF/INS/STOP 11	2
31	23NR/AD	2	32	30 WEATHER SQ/DOX	2
33	31 ARRS/CC	2	34	33 ARRS	2
35	38 ARRS/CC	2	36	39 ARRW/DOI	2
37	40 TACG/IN	2	38	41 ARRS/CC	2
39	41 CAMS/CC	2	40	41 RWR/DO	2
41	41 RWRW/INS	2	42	41 ECS/DOI	2
43	42NDBW/DO	2	44	53WRS/CC	2
45	54 WRS	2	46	55 WRS/CC	2
47	60 MAWG/INS/STOP 6	2	48	62 MAW/DOXC	2
49	71 ARRS/CC	2	50	100/119 TCF/DOT	2
51	102 ARRS	2	52	121 TFW/DOX	2
53	140 TAW/DOX	2	54	165 TAG/DOI	2
55	185 TAS	2	56	304 ARRS/DOI (AFRES)	1
57	317 TAW/DOT	2	58	416MMS/MAWSM	2
59	435 TAW/INS	2	60	437 MAW/DOXF	2
61	443 MAW/DOXC	2	62	497 RTG/INS	2
63	601TCW/FS	2	64	931 AFREFG/DOI	2
65	1605 MAC SQ	2	66	1883D ISS	2
67	1901 ISG/SP	2	68	1905 ISS	2
69	1915 ISS/KT	2	70	1954 RADAR	1
71	1965 ISG	2	72	1974 ISG/TPA	2
73	1985 ISS/ASC/SSR	2	74	2045 ISG	2
75	2049 ISG	2	76	2130 ISS	2
77	2152 ISS	2	78	2160 ISS/ATC	2
79	2189 ISS/DONA	2	80	3246 TEST WG/CCU	2
81	3270TTCP/TTGE	2	82	3395 TTG/TTEOOAF	2
83	3902 ABW/XP	2	84	7113 SAS (USAFE/INCES)	2
85	AFCC/DET 6	2	86	AFDSCP/SCP	2
87	AFTC/XRO STOP 31	2	88	AFWL/INS	2
89	AMD/RDI	2	90	JOINT LIAISAON DET	2
91	ARMED FORCES STAFF	2	92	SURVEY SECT. SHAPE	2

ATCH 11

93	FLEET AIR KEFLAVIK	2	94	US FORCES CARRIBBEAN	2
95	COMMANDER IN CHIEF US	2	96	DEFENSE COMM AGENCY	2
97	DET 257 AFTAC	2	98	DET 1 2046 ISG	2
99	DET 1 AFCOS	2	100	DET 1 USAF TAWC/DA	2
101	DET 10 5 WS/CC	2	102	DET 2 SPACE DIVISION/ENI	2
103	DET 23 17 WS/CC	2	104	DET 3 23 AF/DA	2
105	DET 75/ 7 WEATHER WG	2	106	DET 9 37 ARRS	2
107	DIA	2	108	DIA/OS-1C	2
109	DOD C3CM JTF/IN	2	110	ELECTRONIC SYS DIV/INS	2
111	FAA ISD/ACS-300	2	112	FEMA REGION 6	2
113	AFWAL/GLXPS	2	114	FTD/SP	2
115	HQ 129 ARRS	2	116	HQ 137/TAW	2
117	HQ 166TAC GP	2	118	HQ 2187 ISG/SP	2
119	HQ 22AF/LGRSS	2	120	HQ 25 IFAVO	2
121	HQ 2ND WEATHER WING/DOX	2	122	HQ 306 STRAT WG/INS	2
123	HQ 314AD/INS	2	124	HQ 3AF/XN	2
125	HQ 4AF/DO (AFRES)	2	126	HQ 834 AIRLIFT DIV.	2
127	HQ 914 TAC AIRLIFT GP (AFRES)	2	128	HQ AAC/DOY	2
129	HQ AAC/INS	2	130	HQ AD/INS	2
131	HQ ADCOM/INXS	2	132	HQ AF GLOBAL WEATHER CENTRAL	2
133	HQ AFAFC/LGVS	2	134	HQ AFCC/DOY	2
135	HQ AFCC/SIMS	2	136	HQ AFCC/XORIA	2
137	HQ AFCOMS/IGS	2	138	HQ AFDSDC/SCP	2
139	HQ AFESC/DEOP	2	140	HQ AFFSC/DOEP	2
141	HQ AFIS/INOI	2	142	HQ AFIS/INOI	2
143	HQ AFIS/INSC	2	144	HQ AFIS/INSD	50
145	HQ AFISC	2	146	HQ AFISC/IGAK	2
147	HQ AFLC LOC/XOWW	2	148	HQ AFMCD/SP	2
149	HQ AFOSI/IVOA	2	150	HQ AFOSI/IVOX	2
151	HQ AFOSP	2	152	HQ AFOSP/SPI	2
153	HQ AFOSP/SPO	2	154	HQ AFRES/DOXE	2
155	HQ AFRES/DOXX	2	156	HQ AFSC/TEOX	2
157	HQ AFSC/INS	2	158	HQ AFTAC/DOR	2
159	HQ AFTPC/CK	2	160	HQ AFTPC/IC	2
161	HQ AMD/RDI	2	162	HQ ATC/XPR	2
163	HQ AWS/DOJR	2	164	HQ MAC INS/INO	2
165	HQ MAC/DOOAS	2	166	HQ PACAF/INS	1
167	HQ SAC/DOCCO	2	168	HQ SAC/DOR	2
169	HQ TACOPS/INO	2	170	HQ SPACE COMMAND/DOCE	2
171	HQ SPACE DIVISION	2	172	HQ SPACE DIVISION	2
173	HQ SPACECMD/DOCE	2	174	HQ TAC/DOXC	2
175	HQ TAC/SIS	25	176	HQ USAF/XOEO	42
177	HQ USAFE/DOFF	2	178	HQ USAFE/DOFF	2
179	HQ USAFE/INS/INST	2	180	HQ USAFERC/CC	2
181	HQ USCENTCOM/CCJ3-OC	2	182	JOINT CRUISE MISSLE PROJECT	2
183	JOINT SPECIAL OPERATIONAL	2	184	LANTIRN TEST TEAM	2
185	NAFCOS (8AF)/DOXT	2	186	NGB/XOX	2
187	NSA C/O SIE	2	188	NSA-F61	2
189	NSA/S-15	2	190	NSA/S112	2
191	NSA/S114	2	192	OHIO ANG	2
193	OJCS/NEACP	2	194	PACAF/DOXZ	2
195	PACOPS/DOX	2	196	SPACE DIVISION/CSI	2
197	SPACE DIVISION/INS	2	198	SPECIAL SECURITY OFFICER	2
199	USAF INTL REP (USAFINREP FM)	2	200	USAFE ELF 1 CMD/INS	2

ATCH 12

201 HQ ADCOM/J3CE	2	202 HQ DSOC	2
203 HQ USCINCLANT	2	204 HQ USEUCOM	2
205 HQ USREDCOM	2	206 HQ USSOUTHCOM	2
207 JEWC	2	208 JEWC/CDC	2
209 OJCS/J1	2	210 OJCS/J3/J33	2
211 USCENTCOM	2	212 USCINCLANT (J625)	2
213 USCINCPAC J316	2	214 USECENTOCM	2
215 CI DETACHMENT	2	216 DCA	2
217 DEFENSE NUCLEAR AGENCY	2	218 DIS	2
219 FAA	2	220 FEMA	2
221 INSTITUTE-DEFENSE ANNALYSIS	2	222 JS DEPT OF JUSTICE	2
223 LOS ALAMOS NL	2	224 NASA HQ DOD AFFAIRS DIV.	2
225 NR DIRNSA FMDE 1522 NRC	2	226 US DEPT OF ENERGY	2
227 US DEPT OF STATE	2	228 HQ ESA	2
229 HQ ESE	2	230 DET 1 HQ ESE/SP	2
231 HQ ESP	2	232 OLYO HQ ESP/5AF	2
233 HQ ESS	2	234 HQ EST	2
235 DET 1 HQ EST	2	236 DET 2 HQ EST	2
237 DET 3 HQ EST	2	238 OLTB HQ EST	2
239 OLTS. HQ EST	2	240 6903 ESG	2
241 6906 ESS	2	242 6910 ESW	2
243 6911 ESG	2	244 6912 ESG	2
245 6913 ESS	2	246 6915 ESS	2
247 6916 ESS	2	248 6917 ESG	2
249 6918 ESS	2	250 6920 ESG	2
251 6922 ESS	2	252 6924 ESS	2
253 6931 ESS	2	254 6940 ESW	2
255 6947 ESS	2	256 DET 1 6947 ESS	2
257 6948 ESS	2	258 6949 ESS	2
259 6945 ESS	2	260 6950 ESG	2
261 6952 ESS	2	262 6960 ESW	2
263 6960 SPS	2	264 6964 CPSS	2
265 6981 ESS	2	266 6985 ESS	2
267 6988 ESS	2	268 6990 ESG	2
269 6990 ESG	1	270 6993 ESS/DOGA	2
271 6994 ESS	2	272 DET 1 6994 ESS	2
273 8075 ESS (AFRES)	2	274 3480TTG/TTM1	2
275 3480TTG/TTM2	2	276 3480TTW	2.
277 AFCSC	2	278 AFEWC	2
279 JEWC	2	280 HQ ESC/CC	1
281 HQ ESC/AC	1	282 HQ ESC/AD	1
283 HQ ESC/DA	1	284 HQ ESC/DC	1
285 HQ ESC/IE	1	286 HQ ESC/DO	1
287 HQ ESC/DOC	1	288 HQ ESC/DOO	1
289 HQ ESC/DOQ	1	290 HQ ESC/DOS	1
291 HQ ESC/DOT	1	292 HQ ESC/DOZ	1
293 HQ ESC/DP	1	294 HQ ESC/HC	1
295 HQ ESC/HO	1	296 HQ ESC/IG	1
297 HQ ESC/IN	1	298 HQ ESC/LG	1
299 HQ ESC/PA	1	300 HQ ESC/SP	1
301 HQ ESC SPI	1	302 HQ ESC/XP	1
303 1TFW/DO	5	304 3TFW/IN	5
305 4TFW/DO	5	306 8TFW/IN	5
307 9AF/DOX	5	308 10 AF/R/DOX	5

ATCH 13

309	15ABW/DOX	5	310	18TFW/DOT	5
311	23AD/DOX	5	312	23TFW/DO	5
313	24COMPW/DO	5	314	24AD/DO	5
315	25AD/DOE	5	316	26 AD/DOX	5
317	27TFW/DOO	5	318	31TFW/DO	5
319	33TFW/DO	5	320	35TFW/DO	5
321	37TFW/DO	5	322	49TFW/DO	5
323	51TFW/IN	5	324	56TTW/DO	5
325	57FWW/DO	5	326	58TTW/DO	5
327	67TRW/DO	5	328	102 FIW/IN	5
329	108TFW/DO	5	330	113TFW/DO	5
331	116TFW/DO	5	332	117TRW/DO	5
333	121TFW/DO	5	334	122 TFW/DO	5
335	123 TRW/DO	5	336	128 TFW/DO	5
337	131 TFW/DO	5	338	132 TFW/DO	5
339	140 TFW/DO	5	340	144 FIW/DO	5
341	174TFW/DO	5	342	301 TFW/DO	5
343	325 FWW/DO	5	344	326AD/DOT	5
345	347TFW/DO	5	346	354TFW/DO/IN	5
347	355TTW/DO	5	348	363TFW/DO	5
349	366TFW/DO	5	350	374TAW/DOX	5
351	388TFW/DO	5	352	405TTW/DO	5
353	419 TFW/DO	5	354	432TFW/DOC	5
355	434TFW/IN/DO	5	356	435TFW/CCA	5
357	442TFW/DO	5	358	474TFW/DO	5
359	475ABW/OTF	5	360	479TTW/DO	5
361	482TFW/DO	5	362	507TAIRCW/DO	5
363	552AWACD/DOX	5	364	602 AIRCW/DO	5
365	831AD/CCE	5	366	832AD/CCE	5
367	833D CSG/SPOM	5	368	833AD/CCV	5
369	833AD/IGO	5	370	833AD/IG	5
371	836AD/CCE	5	372	5540SW/CC	5
373	HQ 20TFW	5	374	HQ AFI/DO	5
375	SE ROCC INTELL FACILITY/	5	376	USAFADWC/DO	5
377	USAFSO/DO	5	378	USAFTAWC/DOO	5
379	USAFTAWC/DOX	5	380	USAFTFWC/CS	5
381	HQ AFOTEC/CVO	2	382	HQ AFOTEC/TEF	1
383	DET 1 AFOTEC	1	384	DET 2 AFOTEC	1
385	DET 3 AFOTEC	1	386	DET 4 AFOTEC/TSE	1
387	DET 5 AFOTEC	1	388	OL-AC AFOTEC	1
389	OL-AE AFOTEC/OTEA	1	390	OL-AF AFOTEC	1
391	OL-AI AFOTEC	1	392	AFOTEC ICBM	1
393	OL-AN AFOTEC	1	394	OL-AS AFOTEC	1
395	OL-AT AFOTEC	1	396	OL-AW AFOTEC	1
397	OL-AW AFOTEC	1	398	OL-AY AFOTEC	1
399	OL-BA AFOTEC (AF/LE)	1	400	OL-BC AFOTEC	1
401	OL-BF AFOTEC	1	402	OL-BW AFOTEC	1
403	OL-BT AFOTEC	1	404	OL-DD AFOTEC	1
405	HQ 1 CEVG/RBOO	2	406	DET 1. 1CEVG	2
407	DET 2. 1CEVG	2	408	DET 4. 1CEVG	2
409	DET 5. 1CEVG	2	410	DET 7. 1CEVG	2
411	DET 8. 1CEVG	2	412	DET 9. 1CEVG	2
413	DET 10. 1CEVG	2	414	DET 11. 1CEVG	2
415	DET 12 1CEVG/RBO	2	416	DET 14 1CEVG	2

ATCH 14

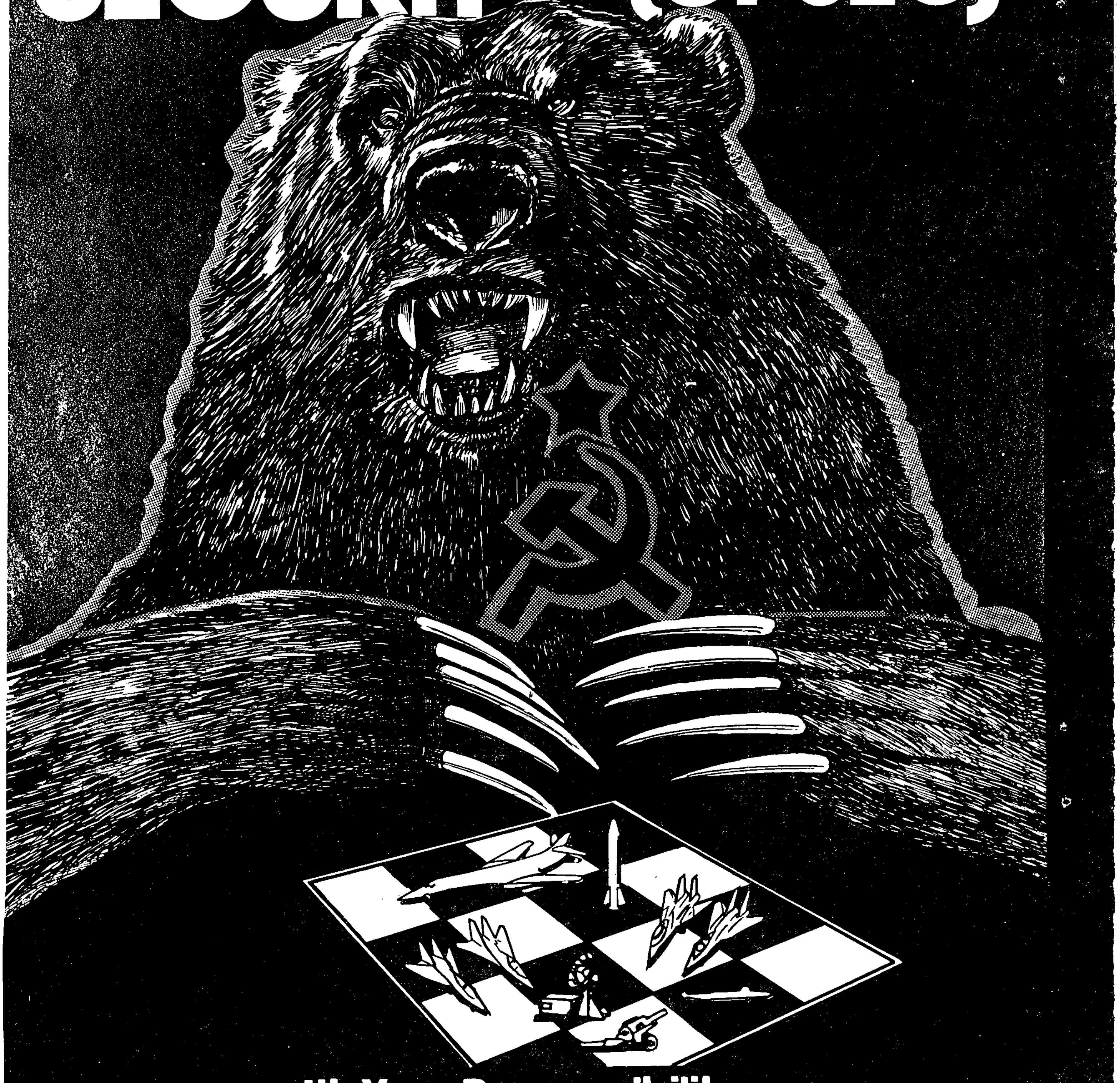
417	DET 16 1CEVG	2	418	DET 24 1CEVG	2
419	AFOSI DIST 1	1	420	AFOSI DET 102	1
421	AFOSI DET 106	1	422	AFOSI DET 109	1
423	AFOSI DET 110	1	424	AFOSI DET 111	1
425	AFOSI DET 140	1	426	AFOSI DISTRICT 4	1
427	AFOSI DET 403	1	428	AFOSI DET 411	1
429	AFOSI DET 412	1	430	AFOSI DET 413	1
431	AFOSI DET 414	1	432	AFOSI DET 440	1
433	AFOSI DISTRICT 5	1	434	AFOSI DO5 OL-D	1
435	AFOSI DET 509	1	436	AFOSI DET 512	1
437	AFOSI DET 514	1	438	AFOSI DET 515	1
439	AFOSI DET 516	1	440	AFOSI DET 518	1
441	AFOSI DET 540	1	442	AFOSI DISTRICT 7	1
443	AFOSI DET 707	1	444	AFOSI DET 709/CC	1
445	AFOSI DET 710	1	446	AFOSI DET 711	1
447	AFOSI DET 712	1	448	AFOSI DET 716	1
449	AFOSI DET 717	1	450	AFOSI DET 721	1
451	AFOSI DET 740	1	452	AFOSI DO7 OL-E	1
453	AFOSI DO7 OL-F	1	454	AFOSI DISTRICT 8	1
455	AFOSI DET 810	1	456	AFOSI DET 811	1
457	AFOSI DET 812	1	458	AFOSI DET 813	1
459	AFOSI DET 814	1	460	AFOSI DET 815	1
461	AFOSI DET 816	1	462	AFOSI DET 840	1
463	AFOSI DISTRICT 10	1	464	AFOSI DET 1001	1
465	AFOSI DET 1008	1	466	AFOSI DET 1012	1
467	AFOSI DET 1014	1	468	AFOSI DET 1016	1
469	AFOSI DET 1018	1	470	AFOSI DET 1040	1
471	AFOSI DISTRICT 11	1	472	AFOSI DET 1101	1
473	AFOSI DET 1103	1	474	AFOSI DET 1108	1
475	AFOSI DET 1110	1	476	AFOSI DET 1114	1
477	AFOSI DET 1117	1	478	AFOSI DET 1140	1
479	AFOSI DISTRICT 13	1	480	AFOSI DET 1302	1
481	AFOSI DET 1306	1	482	AFOSI DET 1312	1
483	AFOSI DET 1313	1	484	AFOSI DET 1314	1
485	AFOSI DET 1340	1	486	AFOSI DISTRICT 14	1
487	AFOSI DET 1401	1	488	AFOSI DET 1402	1
489	AFOSI DET 1404	1	490	AFOSI DET 1405	1
491	AFOSI DET 1406	1	492	AFOSI DET 1407	1
493	AFOSI DET 1408	1	494	AFOSI DET 1440	1
495	AFOSI DISTRICT 18	1	496	AFOSI DET 1801	1
497	AFOSI DET 1802	1	498	AFOSI DET 1803	1
499	AFOSI DET 1810	1	500	AFOSI DET 1811	1
501	AFOSI DET 1812	1	502	AFOSI DET 1815	1
503	AFOSI DET 1816	1	504	AFOSI DET 1817	1
505	AFOSI DET 1840	1	506	AFOSI DISTRICT 19	1
507	AFOSI DET 1901	1	508	AFOSI DET 1902	1
509	AFOSI DET 1904	1	510	AFOSI DET 1905	1
511	AFOSI DET 1910	1	512	AFOSI DET 19 OL-C	1
513	AFOSI DET 1940	1	514	AFOSI DISTRICT 20	1
515	AFOSI DET 2001	1	516	AFOSI DET 2004	1
517	AFOSI DET 2006	1	518	AFOSI DET 2007	1
519	AFOSI DET 2010	1	520	AFOSI DET 2011	1
521	AFOSI DET 2040	1	522	AFOSI DISTRICT 21	1
523	AFOSI DET 2101	1	524	AFOSI DET 2102	1

525	AFOSI DET DET 2103	1	526	AFOSI DET 2104	1
527	AFOSI DET 2105	1	528	AFOSI DET 2140	1
529	AFOSI DISTRICT 42	1	530	AFOSI DET 4201	1
531	AFOSI DET 4203	1	532	AFOSI DISTRICT 44	1
533	AFOSI DISTRCT 45	1	534	AFOSI DET 4502	1
535	AFOSI DET 4503	1	536	AFOSI DET 4504	1
537	AFOSI DET 4506	1	538	AFOSI DET 4507	1
539	AFOSI DET 4540	1	540	AFOSI DISTRICT 46	1
541	AFOSI DET 4606	1	542	AFOSI DET 4607	1
543	AFOSI DET 4640	1	544	AFOSI DISTRICT 62	1
545	AFOSI DISTRICT 62 OL-B	1	546	AFOSI DET 6202	1
547	AFOSI DET 6203	1	548	AFOSI DET 6204	1
549	AFOSI DET 6205	1	550	AFOSI DET 6206	1
551	AFOSI DET 6207	1	552	AFOSI DET 6208	1
553	AFOSI DET 6209	1	554	AFOSI DET 6210	1
555	AFOSI DET 6240	1	556	AFOSI DISTRICT 68	1
557	AFOSI DET 6801	1	558	AFOSI DET 6802	1
559	AFOSI DET 6803	1	560	AFOSI DET 6804	1
561	AFOSI DET 6805	1	562	AFOSI DET 6806	1
563	AFOSI DET 6807	1	564	AFOSI DET 6808	1
565	AFOSI DET 6809	1	566	AFOSI DISTRICT 69	1
567	AFOSI DET 6901	1	568	AFOSI 69-OA	1
569	AFOSI DET 6903	1	570	AFOSI DET 6905	1
571	AFOSI DET 6940	1	572	AFOSI DISTRICT 70/IVOE	1
573	AFOSI US EMBASSY (D-321)	1	574	AFOSI OL-G	1
575	AFOSI RA OL-L	1	576	AFOSI RA OL-M	1
577	AFOSI DET 7008	1	578	AFOSI DET 7010	1
579	AFOSI DET 7011	1	580	AFOSI DET 7013	1
581	AFOSI DET 7014	1	582	AFOSI DET 7024	1
583	AFOSI DET 7028	1	584	AFOSI DET 7030	1
585	AFOSI 7031	1	586	AFOSI DET 7032	1
587	AFOSI DET 7033	1	588	AFOSI DET 7034	1
589	AFOSI DET 7040	1	590	193D MIL INT	EL
591	400 MP P.W. CAMP	2	592	CDR TRADOC	2
593	USSASSD BERLIN	2	594	USASSD MUNICH	2
595	470TH MI GROUP	2	596	USASSC USARERU	2
597	COMMANDER	2	598	USASSD BELVOIR	2
599	USASSD WHITE SD	2	600	COMMANDER USASSD HANCOCK	2
601	HQ 1ST BN 209TH FA NYARNG	2	602	HQ DA (DAMI-CIC)	2
603	HQ USA MATERIAL DEVELOPMENT	2	604	HQ USAINSCOM	2
605	HQ VII CORPS	2	606	HQ XVIII ABN CORPS	2
607	HQS 7TH SIGNAL COMMAND	2	608	SECURITY SPT DET/INSCOM	2
609	US ARMY COMBINED AREA CTL	2	610	3482 TTS/INAF	2
611	BRAVO COMPANY - 104TH MI BN	2	612	CINCPACFLT (N334)	2
613	CINCUSNAVEUR 811	2	614	CO 2ND RADIO BTN	2
615	CO3 CORPS	2	616	USASSD BRAGG	2
617	COMMANDER NSG COMMAND/G123	2	618	FITRON ONE ZERO THREEE	2
619	TEWC 33	2	620	USN MCB 74	2
621	6MR 2DMD FMF	2	622	FCTCLANT	2
623	HQ 25TH COMBAT AVIATION BT	2	624	HQ NAV MAT. MAT 098	2
625	MILITARY SEALIFT COMMAND	2	626	NAVAL AIR TEST CENTER	2
627	NIS DIRECTOR	2	628	NSGA OPS 35	2
629	OPNAV (OP-944)	2	630	USCINCLANT	2
631	USN MOBILE CONST. BAT. 74	2			

----->>>>>>>>>>>> TOTAL # OF COPIES REQUIRED: 1379

ATCH 16

Don't Make His Job Easier
OPERATIONS SECURITY (OPSEC)



It's Your Responsibility.

Distribution: F

AFVA 55-3
14 December 1984