3896736 EO 1.4.(c) EO 1.4.(g) P.L. 86-36

OCID:

SECRET

The Future of High Frequencies in Cryptology

Part I

N.C.GERSON

Editor's Note: Part II will follow in the next issue of Cryptologic Quarterly.

(S) Cryptology is now beset by many difficult problems at a time of curtailed funds and rapid technological innovations in communications (e.g., digital signaling, multiplexed transmissions of voice, data and documents, proliferation of compressed speech, increased COMSEC awareness, and global availability of cheap, sophisticated equipment). It is imperative to reexamine traditional operations and introduce concepts designed to meet challenges of the future in SIGINT's three main areas: intercept, analysis, and timely distribution of significant end product reports. This paper attempts to address only one portion of the first item: high frequencies (HF, 3–30 MHz). For SIGINT, HF is intensive in manpower and costly in maintenance. In other portions of the spectrum, operating funds may be smaller, but the initial capital investment is very high. The proportion of funds allocated to different spectral regions should consider the intelligence value of each region. This paper shows that HF still remains one of the most important contributors to SIGINT.

(S-CCO) High Frequency has been and will be an invaluable asset to SIGINT. It has provided intelligence of extreme value to the nation. Despite a shift of traffic to other circuits HF will remain as an effective, indestructible means of communications well into the future. The question facing SIGINT in an era of shrinking dollars and expanding requirements is that of introducing greater efficiencies into HF – in collection, analysis, and processing. The present system is too inflexible, both technically and geographically. It was not designed to confront merging communications techniques or geographically fragmented political targets. SIGINT for HF must make choices, some of which include greater use of ships, adaptive antenna arrays, and transportable advanced automated remoted sensors.

(S) The objective of this paper is to stimulate discussion on the future architecture of HF in relation to SIGINT. First an outline of the past value of HF will be presented and then an indication of the future SIGINT needs for HF. Critical evaluation is essential in order to optimize decisions on the allocation of cryptologic resources.

HISTORICAL

-(U)-HF has been employed for long-distance communications since its discovery by radio amateurs in the 1920s. Marconi's previous transmissions over long distances had been accomplished using Very Low Frequency (VLF, 3-30 kHz) or Low Frequency (LF,

Declassified and approved for release by NSA on 09-06-2011 pursuant to E.O. 13526

-SECRET

HANDLE VIA COMINT CHANNELS ONLY

SECRET

38967

7P**316** 86-36 EO 1.4.(q)

CRYPTOLOGIC QUARTERLY

30-300 kHz), which required high towers and high powers. At that time HF was unexplored by and was assigned to the radio amateurs until they demonstrated its usefulness.

(Uer)

• tija

UTILITY

(S) HF provides a simple, effective means for long-distance communications. It can be used by relatively untrained individuals (e.g., amateurs, terrorists, drug traffickers, and illegals). All equipments that use low power are readily available off the shelf at low cost. Present equipment, which can include encryption and spread spectrum, will become much more complex in the future. The trend in transmitter design is towards low-power bursttype emissions (fractions of a second). Should they materialize, these systems may cause a resurgence for HF communications but may cause great difficulties for the interceptor. The great limitation of HF systems is the variability arising from the dynamic ionosphere. Even with this deficiency, HF is effective, and it can be the primary means of communications for the Third World and illegals. It will always remain within any integrated communications systems of the great powers. Many examples can be cited (see Gerson, 1991), but only a few will be noted here.

SIGINT AND HF

(S CCO) SIGINT enlarges the definition of HF to 1-40 MHz and interacts with it in three areas: search, intercept, and target location via HF Direction Finding (HFDF).

(see Gerson, 1991). However, since the 1950s changes have occurred, i.e., proliferation of other communications systems of greater reliability and larger bandwidth. This change shifted some traffic to Very High Frequencies (VHF, 30–300 MHz), Ultra High Frequencies (UHF, 300–3000 MHz), and now optical systems.

(S.CCO) Despite the availability of new systems, HF communications persist and will never disappear. Crucial questions for SIGINT are these: "How much effort and resources should be devoted to HF in comparison with those for other frequency purposes?" "What is the proper mix of resources?" This paper attempts to provide an overall review of HF. However, it is imperative to consider the new threats (economic, military, fiscal, and political), the frequencies being used, and the potential intelligence to be derived. HF will be found to be at least as important in the near future as it has been in the past.

HANDLE VIA COMINT CHANNELS ONLY

FUTURE OF HIGH FREQUENCIES IN CRYPTOLOGY

EO 1.4.(c) EO 1.4.(q)

P.L. 86-36

-SECRET

SECRET

SIGINT VALUE

General

(S-CCO) It cannot be overemphasized too strongly that SIGINT must include HF (see Gerson, 1991). If anything, a greater proportional emphasis may be initially required. As one example, consider first the military threat. Prior to 1991 the Soviet Union was the only nation that could destroy the United States.

(Gerson, 1991). The disintegration of

the Soviet Union means that the communications and military capabilities of the new entities will not disappear but will be inherited by them

(S CCO) Third, consider the Third World and those outside the law terrorists and smugglers (drugs, arms, currency). For them HF use is increasing. They can use the new modulations, new services, and emerging developments becoming available in HF. It must be assumed that any dramatic movement from HF remains years away. Obviously, the sophisticated HF services will disperse throughout the world. As the sophistication of this technology increases, more complex systems will be introduced into HF and will be employed by civil and commercial entities in the emerging nations.

(S-CCO) Further, as a trend in communications was moving towards connectivity wherein a frequency continuum is used. Rapid switching allows messages to move over open lines; HF plays a vital role in this process. In short, SIGINT must monitor HF as well as, or even more than, other frequency bands.

S-CCOT Finally, even the United States itself has not abandoned HF.

Search

(S) National Security Council Intelligence Directive No. 6 assigns the mission of spectrum surveillance to NSA (all frequency bands: RF, IR, VIS, etc.). The value of HF search was demonstrated repeatedly during World War II. Although resources have since declined, HF research still remains invaluable.

DOCID: 3896736

SECRET

CRYPTOLOGIC QUARTERLY

(S-CCO) To fulfill its mission, the search operation must become much more efficient with greater use of transportable Remote Operations (ROF) or Collection Facilities automation and better-trained personnel.

HF Intercept

(S. CCO) Even, up to DESERT SHIELD/STORM, HF provided more valuable intelligence than any other frequency band. This condition arose because HF was extensively used for many communications.

(S-CCO) During the cold war most targets were Communist, necessarily fostering the establishment of many large HF intercept sites in the Northern Hemisphere,

SIGINT prudently concentrated on Soviet, Chinese, and associated targets whose formats and operations then became fairly well known. The attention given to other nations was modest in comparison.

(S-CCO) In practice, HF intercept and direction finding were combined at specific locations having large Circularly Disposed Antenna Arrays (CDAA). Mobile platforms (aircraft) were employed to complement the fixed sites.

(S-CCO) A series of painful experiences (Vietnam, Iran, Central America, Iraq, etc.), shattered the illusion of one tidy world, one concentrated threat, primarily military. Today additional concerns regarding economics, commerce, finance, narcotics, and politics bring new SIGINT targets, located in different and distinct geographic areas. (Most existing HF sites were not located for the new geographical threats nor equipped for the new HF technologies.

Target Location

(S-CCO) HFDF is still considered one of the best means for locating targets on the oceans. ______ This capability is obtained through the manpower-intensive operation of many large fixed sites. HFDF is also used to locate land targets and, to some extent, to steer intercept operators to their correct HF transmitter.

The topic

EO 1.4 EO 1.4 P.L. 8

of HFDF has been the subject of many studies over the years, but its concept, design, and operation have not changed significantly.

SECRET

48 HANDLE WA COMINT CHANNELS ONLY

FUTURE OF HIGH FREQUENCIES IN CRYPTOLOGY

(S-CCO) Many costly attempts were made to prove the accuracy of measured HFDF Lines of Bearing (LOB) and accuracies of the resulting fix, all without material success. Fix accuracies (about 100 km radius) are still considered unsatisfactory but acceptable. The inaccuracies stem from two factors: geometric dilution (a function of distance and crossing angle of the LOBs) and the unpredictable variability of tilts in the ionosphere that deflects HF rays out of the great circle plane. It is doubtful if the latter effects can be eliminated. A number of Single Site Location (SSL) systems exist. Again the changeable ionosphere limits location accuracies (commonly but erroneously assumed to be only about 10 percent of range).

(S-CCO) Several general comments should be made about geolocation accuracies. An accuracy within 100 km may be adequate for locating a ship somewhere on the high seas, but it may be completely unacceptable for tactical purposes. Accuracy requirements vary widely and depend upon the intended use. To "lay metal on a target" requires accuracies within meters. For HF rays returned from the ionosphere, such accuracies are unattainable. Obviously, LOBs in the wrong transmitter are worthless.

<u>(S CCO)</u> Inherent limitations of the existing HFDF network must be noted. It is aging, immobile, and manpower intensive. Using HF skywave, targets cannot be located within the skip distance or when "up and down" communications are used.

It is geographically inflexible, physically unwieldy, and becoming technically deficient. In addition, it has fulfilled its designated purpose for the political and military threats of the period. However, the time has come to reassess the SIGINT need of the entire system including cost, location, and innovation. Since SIGINT must maintain a capability for tactical and strategic target location and intercept, new sites, advanced equipment, new concepts, and different, smaller sites (ROFs) must be introduced.

Summary

896736

86-36

Τ. .

(S-CCO) During and after World War II, HF was an outstanding contributor to SIGINT in search, intercept, and target location.

However, while the world changed, the system did not. It remained essentially stagnant both geographically and technically. In the meantime, HF technologies advanced and political threats dispersed. For SIGINT, HF cannot disappear. It will always be useful and needed. Further, the global capital investment in HF is too large to be disbanded. With funds and resources declining, the SIGINT HF mission must become more efficient, automated, and flexible in order to maintain the orderly

DOC 1.4. (c) DOC 1.4. (c) BOC 1.4. (c)

SECRET

CRYPTOLOGIC QUARTERLY

prosecution of collection, search, and signal processing.

(S-CCO) In short, HF is a viable contributor to SIGINT. To meet impending technical and political challenges (strategic and tactical), operations must become more flexible (geographically and technically): Considering the importance of HF to SIGINT, the percentage of cryptologic funds devoted to it may initially increase not decrease. Smaller, more mobile automated and advanced facilities, transportable when necessary, must be implemented. Financing for the capital costs must be considered.

ADDITIONAL HF CONSIDERATIONS

(S-CCO) Some comments should be made about ionospheric predictions, which are employed in planning and, to some extent, in operating HF systems (e.g., communications, radar, or intercept). Predictions are based upon two main considerations: (a) ionospheric climatology (dependent upon location, time of day, year, and solar cycle) and (b) engineering factors (transmitter power, soil, antenna types, local noise environment, etc.). There are numerous prediction codes; all cumbersome, all inefficient, and many internally inconsistent. Nonetheless, for practical purposes, all provide about the same results.

(U) The DoD and NSA have applied considerable effort in attempts to improve the predictions, all with marginal, if any, success. A good portion of the problem lies in the fact that the ionosphere is a fluid whose physics and dynamics are not fully known. This fluid is controlled by the sun, whose changes still remain unpredictable. Until the forces influencing the state and movement of the ionosphere can be better defined, material improvements of the predictions will not be possible, irrespective of the funds applied.

(U) However, some studies of the ionosphere are warranted and necessary. The Arctic, in an age of fuel awareness, is destined to become a transportation and communications highway from North America over Siberia to Europe, Asia, and China. At present it also contains a military threat, where armed submarines roam the ocean depths and aircraft ply the polar skies. For communications, additional knowledge of the arctic ionosphere is needed. In an era of declining funds, efforts must be shared. Canada, which "owns the aurora," already has institutions (University of Alberta, University of Western Ontario, Communications Research Center, etc.) preeminent in studies of the polar and auroral ionospheres. Canada should be encouraged to assume full responsibility for investigating this region. Similarly, Australia should be encouraged to assume responsibility for examining the equatorial ionosphere.

(U) Further, within the United States, the DoD should amalgamate the disparate, overlapping, and sometimes wasteful efforts on "improving ionospheric predictions." The entire responsibility should be assigned to one triservice group, e.g., within the Air Weather Service (AWS), charged with generating, improving, and maintaining any and all prediction codes needed by the DoD (and NSA). DoD elements, connected via some

SECRET

FUTURE OF HIGH FREQUENCIES IN CRYPTOLOGY

networking scheme, requiring predictions would transmit queries to AWS and obtain instant responses. Past uncooperative, individualistic efforts have squandered resources and have distributed incompatible, deficient, prediction codes throughout the DoD. The waste must stop.

Ionospheric Disruptions

CID: 43896736

EO 1.4.(g) P.L. 86-36

÷.;

114

(S-CCO) A high-altitude nuclear detonation would disrupt the ionosphere for about an hour or less. The United States conducted tests in the Pacific to examine this effect during the 1950s. The Soviet Union, taking advantage of these "tests of opportunity," concluded that the ionosphere is self-healing under sunlight and returns to normal in about thirty to fifty minutes after the detonation.

The United States arrived at the opposite conclusion, that HF would be unusable. On the basis of SIGINT, however, U.S. views were later reversed. In summary, after a high-altitude nuclear detonation the ionosphere may be disrupted for a short period but not destroyed.

Technical Challenges

Fiscal Trends

0 1.4.(c) .L. 86-36

SECRET

EO 1.4.(c) EO 1.4.(g) P.L. 86-36

51 HANDLE COMINI CHANNELS ONLY

SECRET

CRYPTOLOGIC QUARTERLY

CONCLUSIONS

a. (S-CCO) From the past to the present, HF has been an outstanding contributor to SIGINT primarily because most communications of intelligence interest depended upon this means. This condition will prevail in the immediate future. 1.5

b. (S-CCO) Also in the past, most attention was prudently given to one generalized military threat, Communism, embodied by the Soviet Union, China, and their associates. The past, convenient, easily identified SIGINT focus has been shattered by several factors: emergence of new threats (military, economic, fiscal, narcotic, commercial) sprinkled around the globe, some dilution (not elimination) of the Communist threat, and the creeping introduction of sophisticated HF communications technology (not readily handled by existing SIGINT sites).

c. (S-CCO) HF search is a vital ongoing requirement. While it must be maintained it must become more efficient, i.e.

d. (S-CCO) Better-trained and more efficiently used manpower is essential for SIGINT sites. Manning by poorly trained individuals degrades search copy and other functions. Consideration must be given to (1) recruiting only individuals who first served a term as communicators and thus are trained in many skills required for SIGINT or (2) using

SECRET

SECRET

f. <u>(S-CCO)</u> a triad of shipborne ROFs whose positions are known through the Global Positioning System (GPS) could serve a crude local HFDF net concentrating on the crisis area of interest.

h. <u>(S-CCO)</u> Unless they are remoted, continued operation of the existing HFDF network is illusionary. It is technically inflexible and manpower intensive. It cannot handle geographically dispersed emergencies and advanced emerging technologies. Replacements of the same aperture are unlikely.

i. (S-CCO) For SIGINT, wideband communications trunks are essential to interlink sites and allow timely interchange of information.

j. -(S-CCO)_SIGINT sites should conduct periodic checks on internal system performance, e.g., antennas, noise, receivers.

k. (U) Ionospheric prediction services should be assigned to the Air Weather Service. Investigations in specific geographical areas (the Arctic, equatorial regions) could be assigned to Canada and Australia, respectively. Costs must be shared.

Acknowledgment

HD:1.43896736

	he author acknowledges the encouragement and stimulation provided by	
	Chief T3. Considerable thank	s also
go ti		and
	for their stimulating comments and assistance during the preparat	ion of
this	nanuscript. The author also expresses great appreciation to formed for a formed by the second s	or the

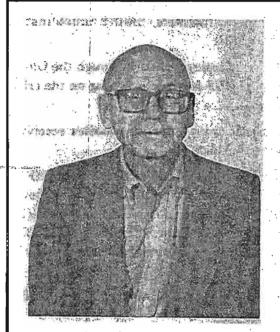
exceptional assistance provided throughout the course of this study.

P.L. 86-36

DOCID: 3896736

SECRET-

CRYPTOLOGIC QUARTERLY



(FOUO) Mr. Gerson, a physicist, has been with R6 since April 1988. Previously he had been with R5. He was one of the founders of the Air Force **Cambridge Research Laboratories (now** AFGL) and chief of its Ionospheric Physics Laboratory (1948-56). He was secretary of the U.S. Committee for the International Geophysical Year (IGY) (1953-57), secretary of its Executive Committee, vice-chairman of its Arctic Committee, chairman of its first two Antarctic committees, and a member of its Ionospheric and Rocketry panels. Mr. Gerson has served as consultant to ARPA; Lincoln Laboratory; Mitre **Corporation**; and Syracuse University Research Corporation. He has had over sixty scientific papers published in American and foreign journals.

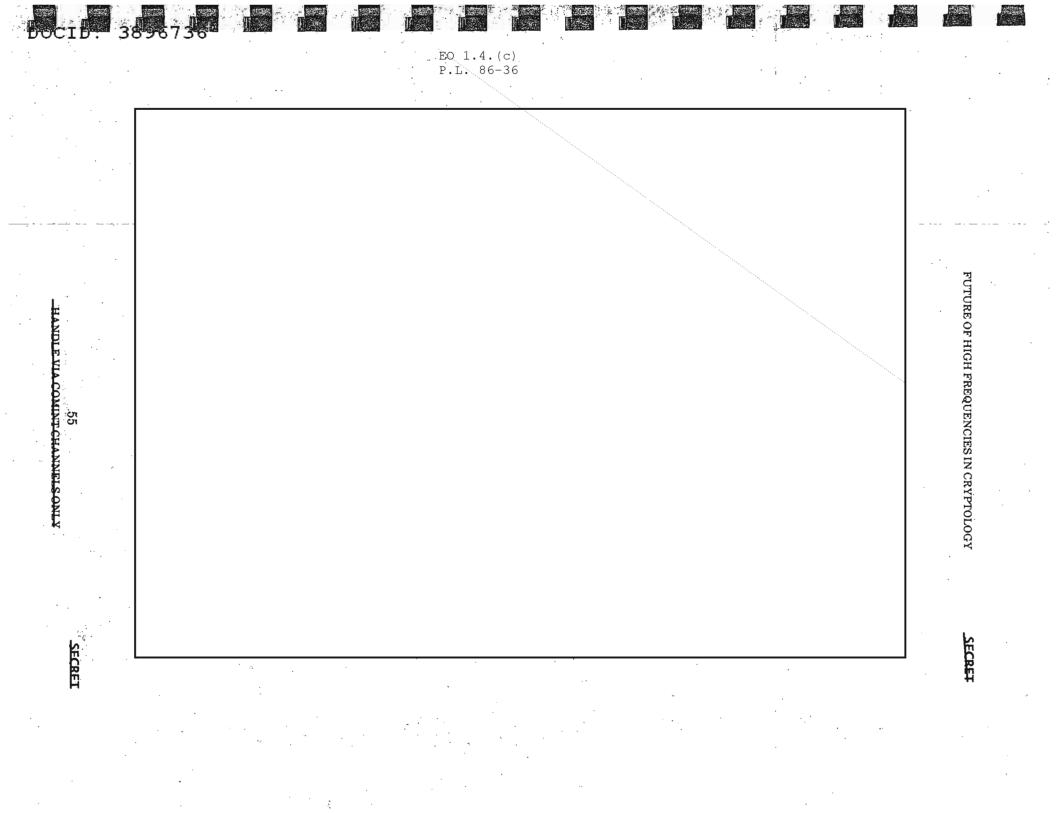
While serving on the U.S. National Committee for the IGY, he suggested transarctic submarine transit, wrote the report for the U.S. Antarctic Expedition, and selected the U.S. South Pole site. Mr. Gerson is the only Agency employee to have been sent to both the Arctic and Antarctic; his total TDY time in polar regions exceeds 48 months. A survey of his early accomplishments appeared in *Physics in Canada*, January 1984.

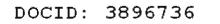
REFERENCES

(S-CCO) Gerson, N. C., 1991, The Future of High Frequencies in Cryptology, Part II, R6-TR-05-91.

- SECRET

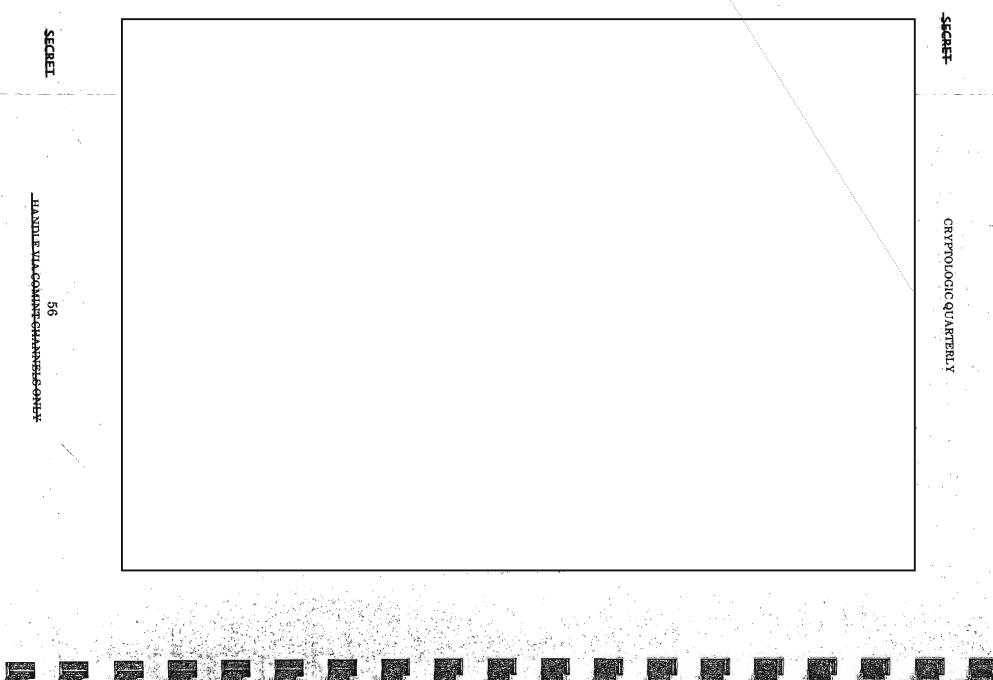
HANDLE VIA COMINT CHANNELS ONLY





AN ANT







57 Handle via comint channels only

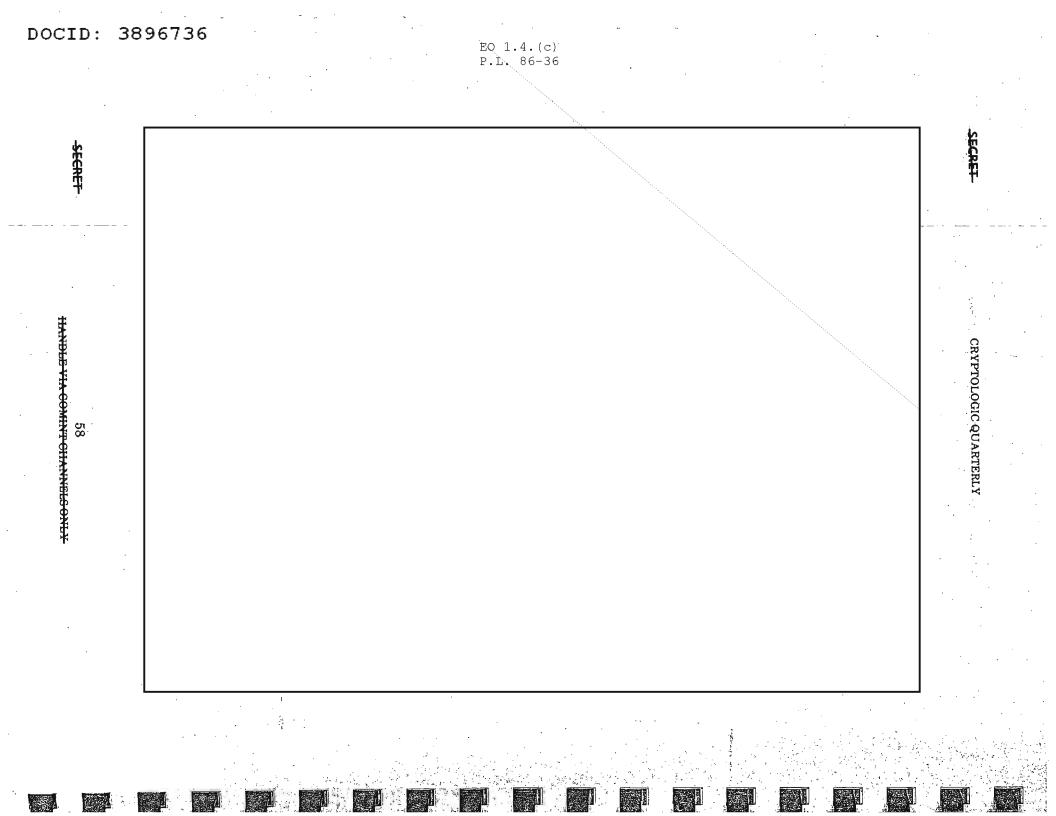
SECRET

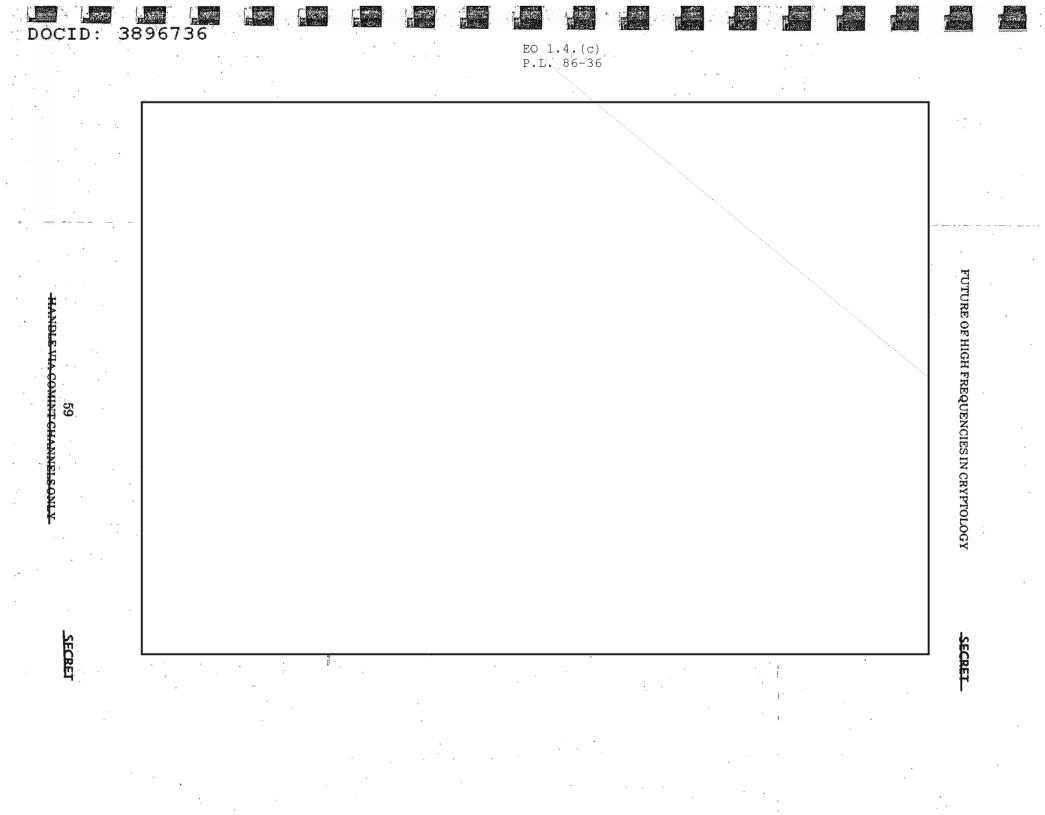
172



FUTURE OF HIGH FREQUENCIES IN CRYPTOLOGY

SECRET





1.4.(c) 0 1.4.(g)

₽.L. 86-36

ないとうないというなないとうと

「「「「「「「「「「「「「」」」」をいいていた。

TOP SECRET UMBRA

The Future of High Frequencies in Cryptology

Part II

N.C.GERSON

Editor's Note: Part I appeared in the Summer 1992 issue of Cryptologic Quarterly. (S-CCO) This paper continues and augments the discussion contained in Part I. It illustrates that High Frequency (HF 3-30 MHz) will remain as a valuable asset to SIGINT. Despite a shift of traffic to other circuit an effective indestructible means of communications well into the future. At a time of shrinking resources and expanding requirements, SIGINT must introduce greater efficiencies into collection, analysis, and processing. The present collection system is too costly, too geographically inflexible, and too technically deficient. It was not designed to confront merging technical sophistications or globally dispersed crisis areas. SIGINT must

EXECUTIVE SUMMARY

(S-CCO) High Frequency (HF), nominally 3-30 MHz, provides an effective communications medium over distances from kilometers to the antipode (20,000 km). To a good extent the choice of frequency is a function of range. Thus, for short distances the lower end and for long distances the higher end of the band are utilized. This fact is directly reflected in SIGINT target assignments: the army and Marine Corps concentrate on short-range battlefield communications transmitted below about 10 MHz, the navy on long range shore-ship communications above 15 MHz, and the air force on intermediate communications.

(S-CCO) Similar considerations apply to commercial and governmental communications: short-haul circuits operate at the lower frequencies and long-haul (usually diplomatic) at the higher. Groups beyond the law are likewise constrained by the same physics: Because of the availability of equipment, the latter groups may concentrate near the amateur bands.

(S-CCO) A number of practical factors ensure the continued viability of HF systems well into the future. First, the ionosphere is indestructible by man, although he may introduce perturbations usually persisting for less than an hour. For the great powers HF thus constitutes the ultimate backup. Second, for legitimate users (business, general

Declassified and approved for release by NSA on 09-06-2011 pursuant to E.O. 13526 103

(19)(c)(c) (19)

EO 1.4.(c) EO 1.4.(q)

P.L. 86-36 TOP SECRET UMBRA

CRYPTOLOGIC QUARTERLY

public, overt governmental, etc.) a large amortized capital plant already exists. It requires only maintenance and operating costs and, despite unpredictable disruptions caused by the sun, allows adequate communications most of the time.

(S-CCO) Illegitimate users (e.g., terrorists; smugglers of arms, currency, and drugs; and special military operators) find HF even more attractive. Smart equipments are already available on the open market. They are cheap, unobtrusive, and easily operated by untrained personnel from random locations. The equipment can embody features of covertness that challenge present SIGINT capabilities

Commonwealth of Independent States (CIS).

(S-CCO) It may be expected that the Third World will cling to their existing effective HF systems already available. Illegal and shadowy elements will tend to employ new sophisticated HF apparatus. The strong nations use both even as they upgrade internal communications onto optical fibers for COMSEC purposes.

(U) Conclusions – SIGINT Impact:

- a. (S-CCO) For seven decades HF has been an outstanding contributor to SIGINT primarily because most communications of intelligence interest depended upon this means. To a good extent this condition will prevail into the immediate future.
- b. (S-CCO) For four decades most attention was prudently given to one generalized military threat communism (embodied by the Soviet Union, China (PRC), and their associates).
- c. (S-CCO) Today this convenient, identifiable SIGINT focus has been shattered by the deterioration of communism and the emergence of new threats (military, economic, fiscal, narcotic, commercial) scattered around the globe.
- d.
- e. (S-CCO) Today HF usage by the decomposed Soviet Union, the Third World, and the PRC is firmly entrenched as an essential, effective communications medium. It is also the medium of choice for insurgents, smugglers, and illegals
- f. (S-CCO) With increasing responsibilities, decreasing funds, and fewer sites, SIGINT must introduce faster analyses and greater efficiencies. One obvious course lies in the use of transportable advanced Remote Operational Collection Facilities (ROFs), which include adaptive arrays, and rapid processing.
- g. (S-CCO) Search remains a vital, ongoing directed SIGINT requirement. It must
 - (1) incorporate rapid, automatic recognition techniques;
 - (2) introduce skilled personnel

(S-CCO) Strategic HFTL should utilize ROFs with their associated small arrays transported to areas of interest or placed aboard RF-quieted vessels (having small superstructures) traversing appropriate areas. (Three well-located ROFs constitute an HF Direction Finding (HFDF) net covering a specific area.) The position of ROFs or drones can be accurately determined using the Global Positioning System (GPS).

HIGH FREQUENCIES IN CRYPTOLOGY

EO 1.4.(c)

h. (S

i.

j.

k.

p.

q.

DOCID

(S-CCO) To improve efficiency, SIGINT sites must conduct periodic health checks on total system performance (e.g., antennas, noise, receivers). Such checks allow rapid identification of operational problems.

(U) All "ionospheric predictions" should be assigned to one triservice DoD entity (e.g., Air Weather Service) responsible for generating, updating, and maintaining all necessary DoD and NSA prediction codes. Answers could be provided on a clientserver basis.

m. (S-CCO) For some time the Third World will depend upon HF rather than costly satellite circuits for diplomatic and other traffic.

n. (S-CCO) To cover globally dispersed, technically advanced targets with reduced resources, SIGINT must implement automated equipments, interconnected by adequate bandwidth circuits and manned by better trained personnel. Commonality in processing HF, VHF, and UHF signals may be possible.

o. (S-CCO) Greater interoperability among the Cryptologic Services must be accelerated.

(S-CCO) With budgetary problems everywhere and the inexorable closure of many present sites, a greater interdependence among all Second Parties is essential.

(S-CCO) The continued operation of the present HFDF (including network is illusionary. The system is geographically inflexible, technically inadequate, and manpower intensive. It cannot handle geographically dispersed emergencies or advanced transmissions. Budgets cannot tolerate the large

105

DOCID: 3896741

CRYPTOLOGIC QUARTERLY

manpower costs. Replacements of the same size are unlikely; major dismantling is inevitable despite the advantages provided by these wide aperture CDAAs.

and the second

- - i ...

EO 1.4.(c) EO 1.4.(g) P.L. 86-36

r. (S-CCO) A large market for advanced HF systems and cellular telephones will emerge in Eastern Europe, the CIS, the PRC, and elsewhere.

.

the system the

SECRET UMBRA

INTRODUCTION

1.1. General

a state and the

(S-CCO) This paper continues the discussion on "The Future of HF in Cryptology, Part I." Part I attempted to illustrate the past tremendous exploits of HF as well as to show that it continues to be a major contributor to SIGINT. On the whole, Part I attempted to provide a brief tutorial and documentary on the past role of HF.

. . . .

(S-CCO) Part II, this paper, extends the discussion from the present to the future. It chronicles the 1991 views of the operational groups The text attempts to place some of these views in perspective.

(S-CCO) HF is so simple and efficient that it will continue to be used for communications well into the future. However, management must decide whether the value derived is commensurate with the cost. In any event, the present expensive, inflexible system must be replaced.

(S-CCO) At this time of rapid change, we should always remember that "eternal vigilance is the price of freedom."

(S-CCO) It is important to note that the nuclear potential of the former Soviet Union, the only nation that could destroy the West, has not yet vanished even though the potential for conflict has lessened. Also, an increasing number of nations have access to nuclear material. One irrational leader could concentrate sufficient ingredients aboard a cargo vessel, detonate it in a foreign harbor, and cause a Chernobyl-like disaster. こうないとうないない ちょうちょう ちょうちょう あいちょう

HIGH FREQUENCIES IN CRYPTOLOGY

TOP SECRET UMBRA

.

1.2. Radio Frequency Usage

(S-CCO) To place HF usage in perspective, several general comments may be made about practices in radio frequency (RF) communications. Frequencies below 100 Hz are employed for shore-submarine traffic, and between 10 and 60 kHz for long-haul naval traffic (including submarines). The primary users of these bands include the U.S., CIS, U.K., France, and the PRC; India and North Korea also may use this spectral region. With great power military tensions decreasing and with the availability of shore-ship links via satellite, the continued operation of these lower frequencies is not clear. Initial capital investment costs are high and construction times long.

(S-CCO) Frequencies above about 30 MHz normally propagate over geometric line-ofsight paths except during unusual meteorological conditions. They are not considered adequate for long distance circuits unless the total path is segmented to satisfy the line-ofsight criterion.

(S-CCO) HF can be used over paths both short and long. In contrast to the frequencies mentioned above and despite lesser reliabilities, HF is very effective and convenient. It is versatile, cheap, and simply operated. Terminals are not confined to specific locations. A rough guide to its performance is given in Table 1.

(SC) HF enciphered speech and data are usually intercepted at great distances from the target via skywave. Because of multipath and the dynamics of the ionosphere, HF propagation introduces considerable variability in the quality and reliability of the received signal. Generally the ratio of signal/noise for HF is smaller and much more variable than that for VHF, UHF, COMSAT, etc. Further, the probability of cochannel interference in the crowded HF spectrum is far greater than in other bands. From a cryptographic viewpoint, HF collection is not the optimum frequency of choice. However, as long as this band contains intelligence value, this traffic must be collected.

(SC) Collection must be maintained against unique signals not transmitted to other bands – e.g., (1) specific frequencies (to ensure continuity against outages on signals normally intercepted, (2) specific high-priority targets, and (3) to compare multiple streams of collected data. Further, melding the same HF intercepted at diverse sites enhances the resulting signal quality.

(SC) Insofar as HFDF is concerned, the order of priority is (1) more volume, (2) faster processing, and (3) increased accuracy. It is well known that as the Doppler spread on the received signal increases, so does the spread in measured angles and transit times of arrival. However, this fact may not separate bad from good bearings.

CRYPTOLOGIC QUARTERLY

RANGE (km)	MODE	DOPPL	ER (Hz)	MULTIPATH (ms)		
		MIDLAT	AURORAL SPREAD	MID LAT	AURORAL SPREAD	
0–50	GROUND WAVE	0	0	NONE	NONE	
0–300	UP_DOWN (NVIS)	< 1	< 20	≤ 2	4 1-1-1	
300-1000	SKYWAVE	1 - 2	≤ 60	~1		
1,0004,000	SKYWAVE	2-3	≤ 60	< 1	· · · ·	
> 5000	SKYWAVE	~ 3	≤ 60	· <1	·*************************************	

いいて いいたいしけいがい

 Table 1

 Factors Affecting HF System Performance

Note 1: Doppler: Midlatitude from layer movements:-Autoral from blob velocities Note 2: Multipaths merge with increasing distance

FUTURE COMMUNICATIONS USAGE

1

2.1. General 👋

(S-CCO) HF communications will remain in use for many reasons. Legitimate users have large, depreciated, capital plants. Illegitimate users can deploy advanced equipment available on the open market. New users in Eastern Europe and elsewhere have insufficient funds to implement other systems even as they consider moving to fiber or cellular systems.

· . ·

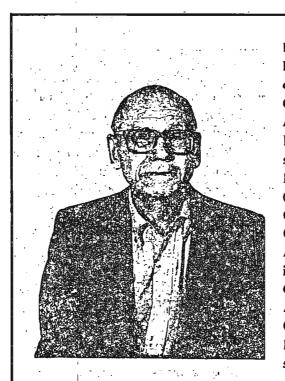
(S-CCO) For intelligence purposes, imagery cannot reveal plans made in boardrooms or staff meetings. COMINT and HUMINT become vital for deriving and confirming future trends and actions. HF currently is so effective that it will not soon be abandoned. SIGINT must follow.

2.2. The SIGINT System

(S-CCO) The present stations, located primarily in the Northern Hemisphere, provide an aperture of about 300m and a bearing measurement accuracy of about $2\pm$ degrees.

108

Operating costs are high and their long-term acceptability to host countries is unclear. Some geographic areas contain a high site density with unnecessary duplication. It is not evident that such site clusters are needed. The smaller arrays inherent in ROFs imply lower accuracies, but this deficiency may be reduced if ROFs are well located relative to their targets (i.e., some trade-off in accuracy is possible). Present site performance has been degraded by neglect of routine maintenance and unwise introduction of appreciable RF noise. ROFs must avoid these destructive conditions.



(FOUO) Mr. Gerson, a physicist, has been with W3 since July 1992. Previously he had been with R6 and R5. He was one of the founders of the Air Force **Cambridge Research Laboratories (now** AFGL) and chief of its Ionospheric Physics Laboratory (1948-56). He was secretary of the U.S. Committee for the International Geophysical Year (IGY) (1953-57), secretary of its Executive Committee, vice-chairman of its Arctic Committee, chairman of its first two Antarctic committees, and a member of its Ionospheric and Rocketry panels. Mr. Gerson has served as consultant to ARPA; Lincoln Laboratory; Mitre Corporation; and Syracuse University Research Corporation. He has had over sixty scientific papers published in American and foreign journals.

While serving on the U.S. National Committee for the IGY, he suggested transarctic submarine transit, wrote the report for the U.S. Antarctic Expedition, and selected the U.S. South Pole site. Mr. Gerson is the only Agency employee to have been sent to both the Arctic and Antarctic; his total TDY time in polar regions exceeds 48 months. A survey of his early accomplishments appeared in *Physics in Canada*, January 1984.

REFERENCE

- [1] (S-CCO) Gerson, N.C., The Future of High Frequencies in Cryptology, Part I. R6-TR-
- **04-91, 1991.**

TOP SECRET UMBRA CRYPTOLOGIC QUARTERLY

Appendix A and the second field of the second • . 1.1 HF and the Soviet Union L. Stringer & Walkerson Mathematical Later Science (Later Science) 5. . e. i 1. No. 1. ine ge $(1) [M_{ij}]_{ij} = \left\{ f_{ij} = -1 \right\} \left\{ f_{ij} = -1 \right\}$ · . · . · · . .. A1. PHILOSOPHY with presents to be able to the first of the

(S-CCO) It is a fundamental fact that major-world powers (those with global commercial and military interests) can exercise military Command, Control, Communications, and Intelligence (C³I) throughout the radio frequency (RF) spectrum.

(S-CCO) As technology improves, so will the ability to transmit faster using more complex HF systems. Illegitimate users will be attracted to these easily transmittable COMSEC systems. Legitimate users will remain with their amortized systems until cheap cellular systems become available. A2. FORMER SOVIET COMMUNICATIONS A2.1. Practice

> EO 1.4.(c) P.L. 86-36

いたない、 おおいろのです。 おいたいできたの、 あんだい、 ないです。

HIGH FREQUENCIES IN CRYPTOLOGY

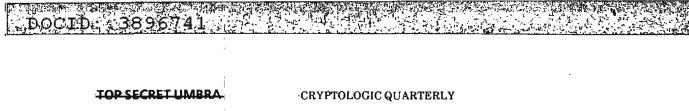
TOP SECRET UMBRA

A2.2. SIGINT Collection (S-CCO) HF search has been and will be invaluable. It is also a statutory requirement for SIGINT. It permits tracking the technical expansion and development of new. sophisticated HF or other systems.

(S-CCO) Another factor must be considered. The deployment of these advanced HF services will diffuse not only from military to civilian sectors but also globally from the Soviet Union (see Appendices B and C), allowing the SC advances to spread internationally.

(S-CCO) SIGINT must consider these technical innovations, which will be used even if military usage declines. It could be dangerous to ignore HF

.111





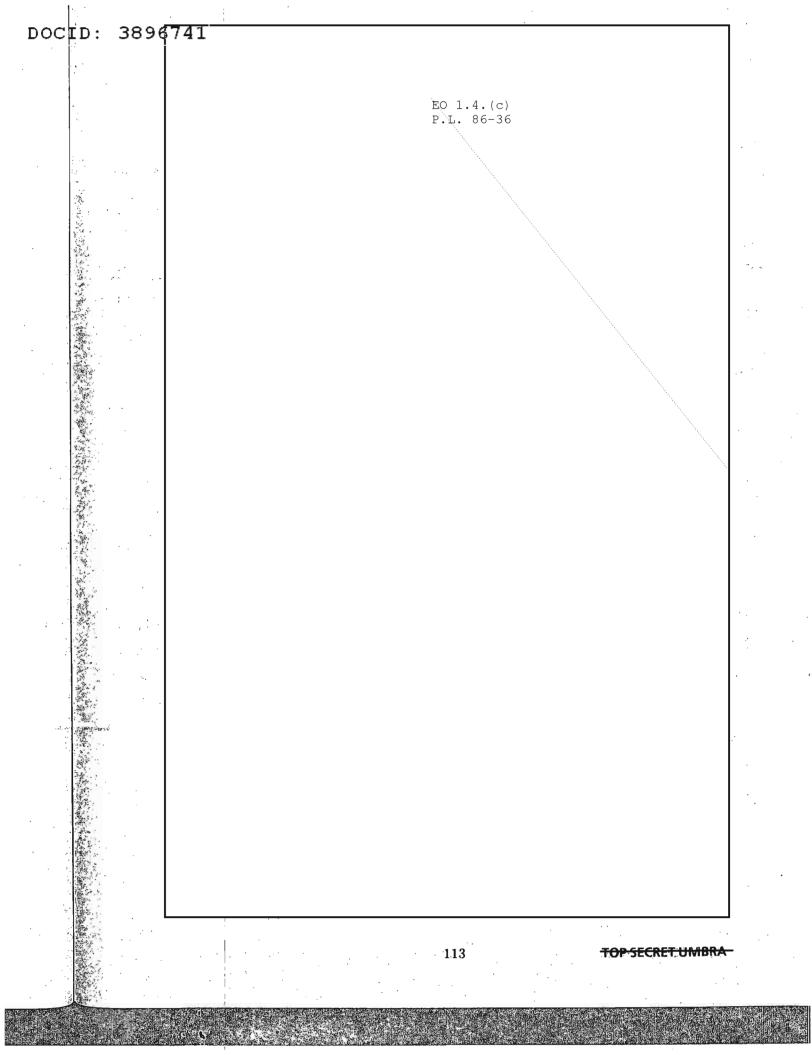
EO 1.4.(c) P.L. 86-36

1. A

.

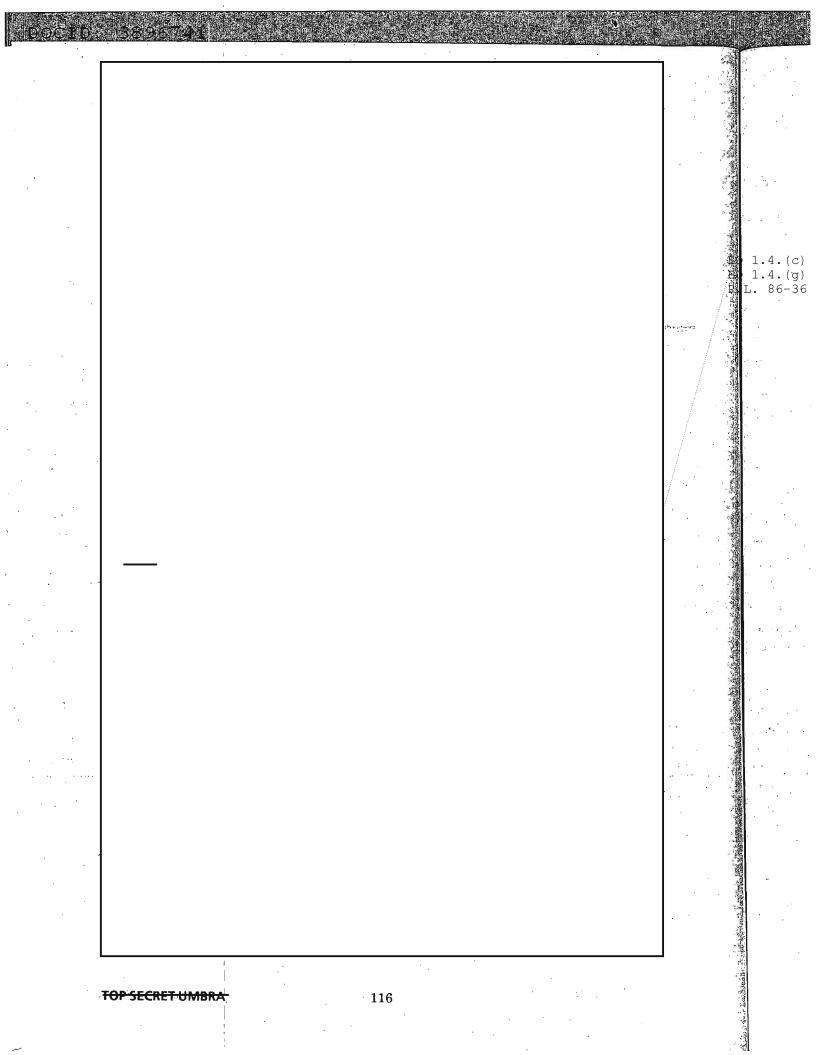
Sector and the sector of the

10457.16

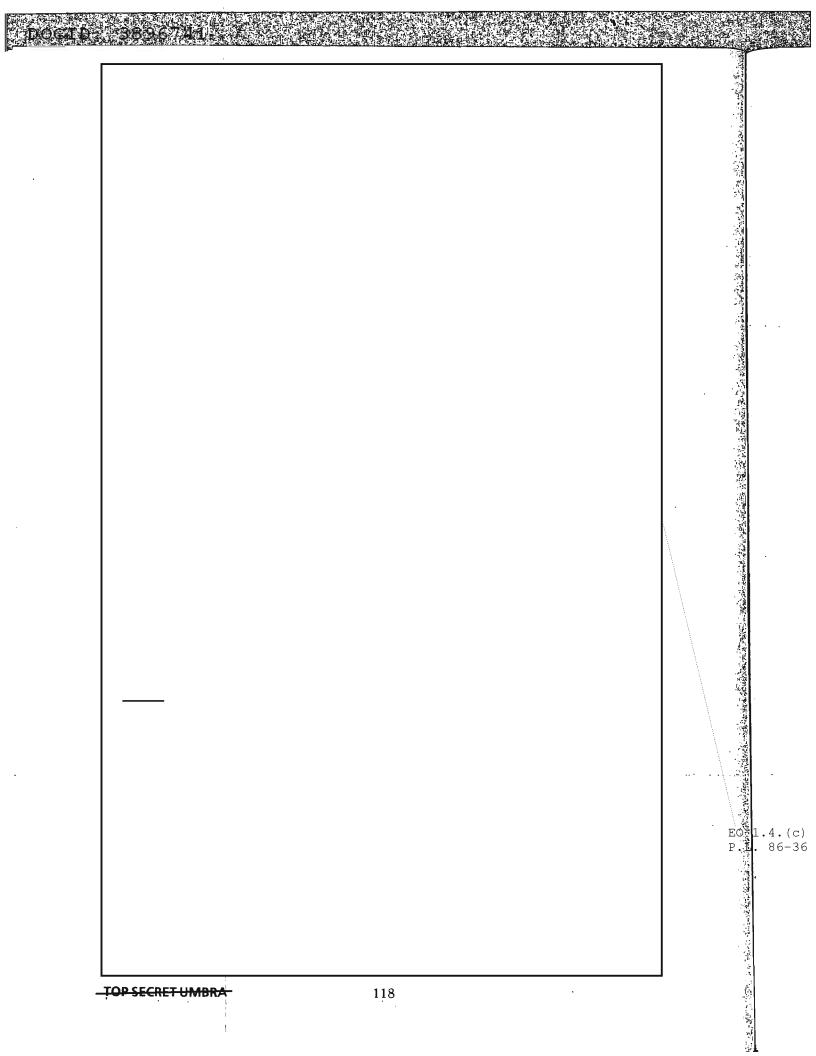


OCID: 3896741	
1	
	EG 1.4. P. t. . 86
	्र स्थान स्थान
	an fernanse i 11 mars
	a second s
	the second s
	are in the second
	्रा, गुरुषे मुख्य

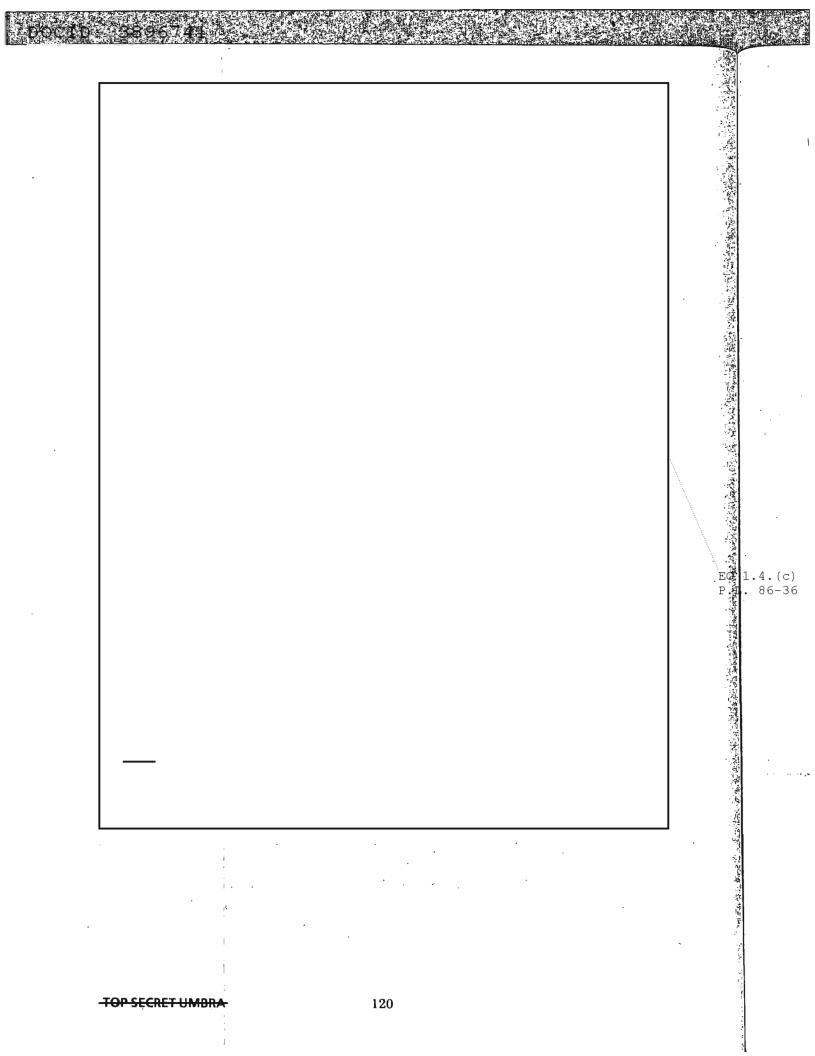
DOCID	: 38967	41			
					EO 1.4.(c) P.L. 86-30
د. محمد المحمد المحم محمد المحمد ا					
۲. ۱۹۹۵ - ۲۰۰۵ ۱۹۹۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵ - ۲۰۰۵					
	:				
	,				
	.•				
]



		ĘO 1.4
		P.L. 8
.: :		
5. 5		
- - - - - - - - - - - - - - - - - - -		
		·
1999 1999	en e	
	میں ہوتا ہوتا ہوتا ہوتا ہوتا ہوتا ہوتا ہوتا	· · · · · · · · · · ·
a Tayan Tanan Ang taona Ang taona An	an a	
и 		
15 A 1	117 TOP SECRET UMBRA	-



OCID: 38	96741	•					EO 1.4.(c P.L. 86-3
			HIGH FRI	EQUENCIES IN CF	RYPTOLOGY	TOP SECRET	UMBRA
							• ·
							-
	C3. DESEF		M,	$-1 = i_{1} + C = i_{1}$		nan Sud (Sud) Sud (Sud) Sud (Sud)	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
り 一つ し し し し し し し し し し し し し し し し し し							-
		4		. 110		TOPSECRET	
				119		TOP SECRET	-OWBIA-
						A TOP STATE	



DOCID	: 389674	1					
]
3							
							· .
						EO 1.4.0	(c)
						EO 1.4. P.L. 86-	-36
		. 8		· .			
		 		· · · ·			
				• .	· · · · · · ·		
	*					ų: 1. r. r. r.	• . * •
	e 		· · ·		-27 22	an an thair an thair An an tairt an thair An an tairt an thair an tairt	•
		· · ·	2	•		·	:.
			• .				
						· ·	• •
	5. 5. 1. 1.				. · · ·		
				121	TOP SECRET U	MBRA	
	793. 193				9 9		