The Future of High Frequencies in Cryptology

Part II

N. C. GERSON

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

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 circuits [redacted] HF will remain 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 [redacted]

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

DOCID: 3389674

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

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 [redacted] These features may also find favor in China and the 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. [redacted]

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 [redacted]

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 [redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36
DOCID: 3896741

h. ~~(S~~

i. ~~(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).

j.

k. ~~(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.

l. (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 client-server 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.

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

q. (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

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

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

INTRODUCTION

1.1. General

~~(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 [redacted] The text attempts to place some of these views in perspective. [redacted]

~~(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.

EO 1.4.(c)
DOCID: 3896741

[redacted]

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-of-sight 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-of-sight criterion. [redacted]

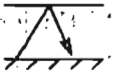
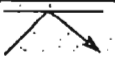
~~(S-CCO)~~ HF can be used over paths both short and long. In contrast to the frequencies mentioned above and despite lesser reliabilities, HF is very effective and convenient. It is versatile, cheap, and simply operated. Terminals are not confined to specific locations. A rough guide to its performance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

Table 1
Factors Affecting HF System Performance

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

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

FUTURE COMMUNICATIONS USAGE

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± degrees.

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.

Appendix A

HF and the Soviet Union

A1. PHILOSOPHY

~~(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 (C^3I) throughout the radio frequency (RF) spectrum.

[redacted]

~~(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

[redacted]

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

DOCID: 3896741
P.L. 86 36

[redacted]

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. [redacted]

~~(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. [redacted]

DOCID: 3896741

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

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

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

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

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

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

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

C3. DESERT SHIELD/STORM

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

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