

PB264447

PB264447

NTIS

One Source. One Search. One Solution.

STUDY OF VULNERABILITY OF ELECTRONIC COMMUNICATION SYSTEMS TO ELECTRONIC INTERCEPTION. VOLUME I

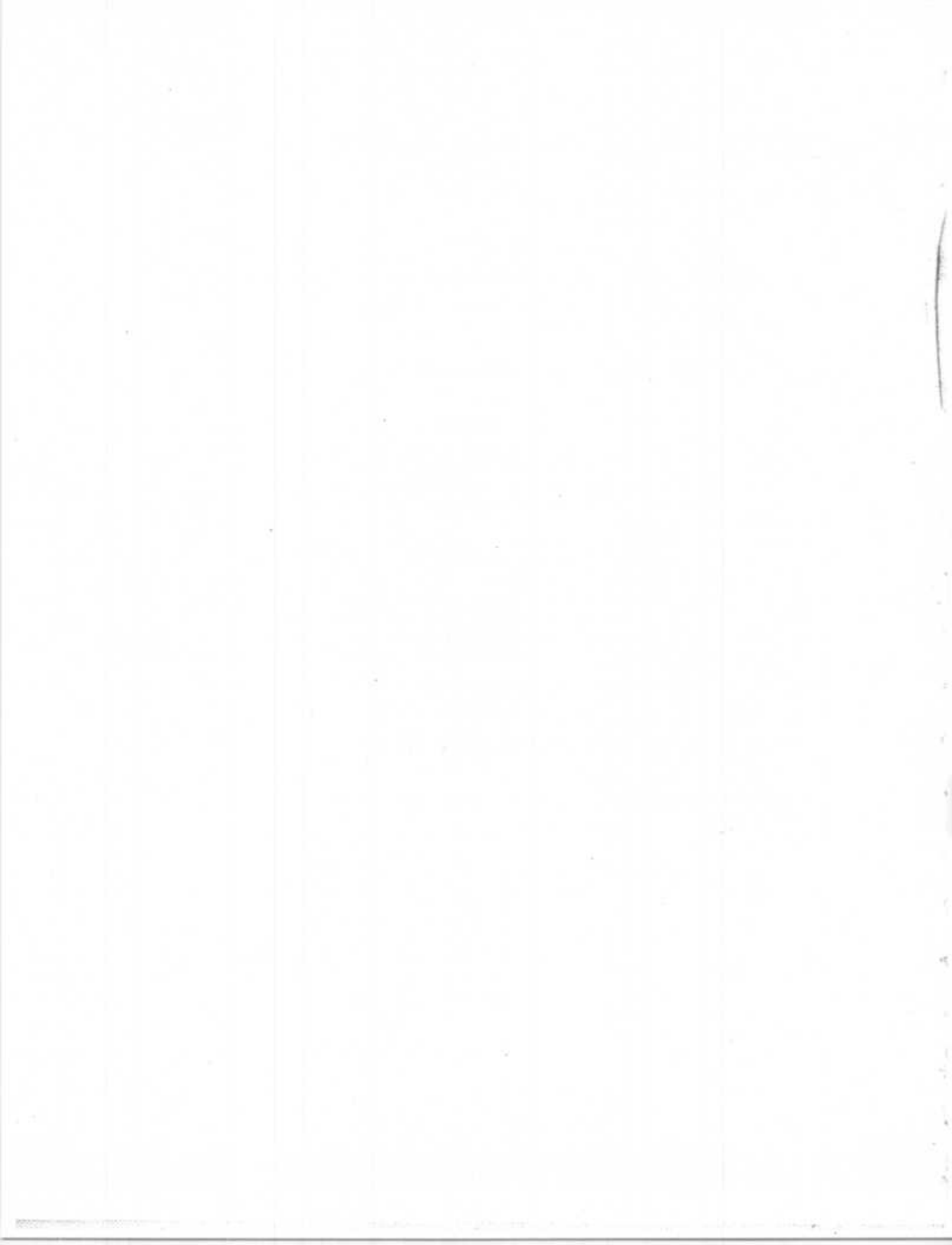
MITRE CORP., MCLEAN, VA. MATREK DIV

JAN 1977



U.S. Department of Commerce
National Technical Information Service

BIBLIOGRAPHIC DATA SHEET		1. Report No. OTP 77-06 (c)	2.	3. Recipient's Accession No. 38-264-447
4. Title and Subtitle Study of Vulnerability of Electronic Communication Systems to Electronic Interception - Vol. I			5. Report Date January 1977	
7. Author(s) C. W. Sanders, G. F. Sandy, J. F. Sawyer A. Schneider			8. Performing Organization Report No.	
9. Performing Organization Name and Address The MITRE Corporation METREK Division 1820 Dolley Madison Blvd. McLean, Virginia 22101			10. Project/Task/Work Unit No.	
			11. Contract/Grant No.	
12. Sponsoring Organization Name and Address Office of Telecommunications Policy 1800 G Street, N.W. Washington, D.C. 20504			13. Type of Report & Period Covered	
			14.	
15. Supplementary Notes				
16. Abstracts This report is a summary of the findings of a study performed for the Office of Telecommunications Policy, Executive Office of the President by the MITRE Corporation, to investigate the vulnerability of commonly available electronic communications to unauthorized interception. Common and specialized carrier and privately-owned communications system were studied. Various forms of communication such as analog and digital communications carried by dedicated service and switched service systems were analyzed. The transmission modes considered were terrestrial and satellite microwave systems, mobile radio systems and wire and cable (multi-pair and coaxial) systems. The capability required to target a specific person's or corporation's communications and extract the information content of these communications was addressed.				
17. Key Words and Document Analysis. 17a. Descriptors Electronic Communications Systems Electronic Interception Frequency Division Multiplex (FDM) Common Carrier Specialized Carrier Satellite Microwave Systems Multi-pair Coaxial Targetting Telecommunications Terrestrial				
17b. Identifiers/Open-Ended Terms				
17c. COSATI Field Group				
18. Availability Statement Unclassified			19. Security Class (This Report) UNCLASSIFIED	21. No. of Pages
			20. Security Class (This Page) UNCLASSIFIED	



ABSTRACT

This report is a summary of the findings of a study performed for the Office of Telecommunications Policy, Executive Office of the President, by The MITRE Corporation, to investigate the vulnerability of commonly available electronic communications to unauthorized interception. Common and specialized carrier and privately-owned communications systems were studied. Various forms of communication such as analog and digital communications carried by dedicated service and switched service systems were analyzed. The transmission modes considered were terrestrial and satellite microwave systems, mobile radio systems and wire and cable (multi-pair and coaxial) systems. The capability required to target a specific person's or corporation's communications and extract the information content of these communications was addressed.

FOREWARD

This report consists of two volumes. Volume I presents the general findings and conclusions of the study. Technical details supporting the findings of Volume I are presented in appendices in Volume II.

TABLE OF CONTENTS

	<u>Page</u>
LIST OF ILLUSTRATIONS	vii
LIST OF TABLES	ix
GLOSSARY OF ACRONYMS	x
GLOSSARY OF TERMINOLOGY	xii
 1.0 INTRODUCTION	 1
2.0 OBJECTIVES	1
3.0 SCOPE	1
4.0 ASSUMPTIONS	2
5.0 METHODOLOGY	3
6.0 GENERAL DEFINITIONS	7
6.1 Communication System Definition	7
6.2 Definition of Electronic Interception of Communications	13
7.0 STUDY CONCLUSIONS	15
7.1 Conclusions Relative to the Acquisition of Communication Signals from Various Transmission Media	15
7.1.1 Penetration of Wire and Cable Systems	15
7.1.2 Reception of Microwave Radio Communications	17
7.2 Conclusions Relative to Targeting Correspondents Within Within Networks	18
7.2.1 Conclusions Relative to the Public Telephone Switched Network	18
7.2.2 Conclusions Relative to Dedicated Service Networks	20
7.3 Citizens Band and Public Service Band Radio	21
8.0 SUMMARY OF FINDINGS	23
8.1 General Characteristics of Electronic Common Carrier Systems	23
8.1.1 Public Switched Service Networks	23
8.1.2 Dedicated Service Networks	32

TABLE OF CONTENTS (Concluded)

	<u>Page</u>
8.1.3 Mobile Radio Systems (Public Service and Citizen Band Radio)	43
8.2 Vulnerability of Electronic Communications Systems	45
8.2.1 Vulnerability of Communications Systems as a Function of Transmission Media	45
8.2.2 Effects of Multiplexing and Signaling on Communications Interceptability	97
8.2.3 Vulnerability of Communication Systems as a Function of the Network Type	113
8.2.4 Information Extraction	147
9.0 SUMMARY OF INTERCEPTOR EQUIPMENT CHARACTERISTICS	154

LIST OF ILLUSTRATIONS

<u>Figure Number</u>		<u>Page</u>
1	Segment of Public Direct Distance Dialing Network	8
2	Distribution Plant Cable Hierarchy	9
3	Identification of the Elements of Electronic Interception	14
4	Illustration of Bell System Switching Plan	25
5	MCI System Map	36
6	Nationwide Transmission Network	39
7	Distribution Plant Cable Hierarchy	49
8	Subscriber Loop Intercept Arrangements	55
9	Trunk Circuit Intercept Arrangements	62
10	Azimuthal Directivity Gain Pattern for AT&T Horn-Reflector KS-15676 at 4 GHz for Vertical (Open) and Horizontal (Shaded) Polarization	76
11	Equipments Configuration for Signal Acquisition of Terrestrial Microwave Systems	79
12	Terrestrial Microwave: Bi-Directional Reception of Telephony-Loci of Potential Reception Sites	80
13	Terrestrial Microwave: Bi-Directional Reception of Telephony-Loci of Potential Reception Sites	81
14	Terrestrial Microwave: Bi-Directional Reception of Telephony-Loci of Potential Reception Sites	82
15	Terrestrial Microwave: Bi-Directional Signal Acquisition of Telephony-Loci of Potential Interception Sites	84
16	Terrestrial Microwave: Bi-Directional Signal Acquisition of Telephony-Loci of Potential Interception Sites	85

LIST OF ILLUSTRATIONS (Concluded)

<u>Figure Number</u>		<u>Page</u>
17	Terrestrial Microwave: Bi-Directional Signal Acquisition of Telephony-Loci of Potential Interception Sites	86
18	Equipment Configuration for Acquisition of Satellite Systems Signals	92
19	Use of Subscriber Earth Station for the Unauthorized Telephony Signal Acquisition	94
20	Direct Distance Dialing Network	116
21	Public Direct Distance Dialing Network with PBX Added	127
22	TWX Teletype Switched Network	132
23	Telex Switched Network	135
24	Composite Information Extraction Functional Block Diagram	148

LIST OF TABLES

<u>Table Number</u>		<u>Page</u>
I	Microwave Frequency Bands	73
II	Terrestrial Microwave Equipment for Bi-Directional Signal Acquisition of TD-2 Telephony	78
III	Satellite Microwave Equipment for Bi-Directional Signal Acquisition of FDM-FM Telephony, Estimation of Costs	91
IV	A Summary Comparison of Transmission Media in Terms of Their Interceptability Characteristics	96
V	Major Bell System Carrier Systems	
	Short Haul	99
	Long Haul	100
VI	Interception Equipment Characteristics	157

GLOSSARY OF ACRONYMS

A/D	Analog-to-Digital
ASCII	American Standard Code for Information Interchange
AT&T	American Telephone and Telegraph
BCD	Binary Coded Decimal
BER	bit error rate
CB	Citizens Band
CCIS	Common Channel Interoffice Signaling System
CCITT	International Telegraph and Telephone Consultative Committee
CO	Central Office
COMSAT	Communications Satellite Corp.
DAC	Digital-to-Analog Converter
DATRAN	Data Transmission Co.
DCC	Digital Communication Console
DDC	Data Channel Controller
DDD	Direct Distance Dial
DDS	Digital Data System
DEMUX	Demultiplex
DUV	Data Under Voice (AT&T)
DSBSC	Double Sideband Suppressed Carrier
DSBTC	Double Sideband Transmitted Carrier
EDS	Electronic Data Switching
EO	End Office
FDM	Frequency Division Multiplex
FM	Frequency Modulate
FSK	Frequency shift keyed
FCC	Federal Communication Commission
EMP	Electromagnetic Pulse
INTELSAT	International Telecommunications Satellite Co.
ISCS	Information Services Computer System
ITU	International Telecommunications Union
MF	Multi-frequency
NACK	Non-acknowledged
PAM	Pulse Amplitude Modulation
PBS	Public Broadcasting Service
PBX	Private Branch Exchange
PC	Primary Center
PCM	Pulse Code Modulation
PIC	Plastic Insulated Conductor
PSH	Phase Shift Keyed
RC	Regional Center
SBS	Satellite Business Systems
SC	Sectional Center
SCC	Satellite Communication Controller
SF	Single Frequency
SNR	Signal-to-Noise

GLOSSARY OF ACRONYMS (Concluded)

SSBSC	Single Sideband Suppressed Carrier
SSBTC	Single Sideband Transmitted Carrier
STP	Signal Transfer Point
TC	Trunk Circuit
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TDR	Time Domain Reflectometry
TELEX	Western Union Switched Teletype Network
TTY	Teletypewriter
TWX	Public Switched Teletypewriter Network
VFCT	Voice Frequency Carrier Telegraph
VSWR	Voltage Standing Wave Ratio
WATS	Wide Area Telephone Service
WESTAR	Western Union Communications Satellite System

GLOSSARY OF TERMINOLOGY

Acquisition, signal	- The first phase of interception including the penetration of the wire or multi-pair cable or coaxial cable or the reception of radio frequency energy and the signal processing required to obtain a signal simple enough to be usable by the next stage in interception process (information extraction).
Alarm	- Audible, visual or teleprinter notification received in a central office to inform maintenance personnel of equipment problems or other anomalous conditions in the telephone plant.
Amplifier	- A device which accepts a signal at its input and delivers an enlarged version of that signal at its output.
Analog-to-digital (A/D)	- The conversion of a signal from an analog form to a digital form.
Annunciate	- To automatically display (either audibly or visually) the existence of some condition, such as an alarm.
Antenna	- The portion of a radio system which radiates or collects electromagnetic energy. When connected to a radio transmitter, electromagnetic energy is radiated. When connected to a radio receiver, electromagnetic energy is collected.
Auxiliary (repeater) huts	- Small above-ground structures constructed at fixed intervals along cable routes to house the repeaters for coaxial or multi-pair cable carrier systems.
Azimuthal	- Pertaining to angular measurement in a horizontal plane progressing in a clockwise direction around an observer's horizon.
Backbone (route)	- The primary physical route utilized by a specialized common carrier (usually a terrestrial microwave radio route).

GLOSSARY OF TERMINOLOGY (Continued)

- Backbone, network - The main segments of a communications network used to interconnect the network nodes.
- Baudot code - A code used primarily for the low speed transmission of teletype characters where each character is represented by five binary elements which are preceded by a "start" element and followed by a "stop" element.
- Binary coded decimal (BCD) - The representation of decimal numbers obtained by encoding each decimal digit into the corresponding binary number.
- Bit - A binary (either a one or a zero) digit.
- Bit error rate (BER) - In digital transmission, the ratio of the number of erroneous bits received to the total number of bits transmitted.
- Bits-per-second (bps) - The total number bits transmitted or received in a second.
- Bit stream - The serial presentation of a set of binary bits.
- Bridge - To connect the terminals of a two-terminal device or transmission line to two corresponding conductors of a cable/wire pair without permitting the conductors to electrically contact each other.
- Bridge-tap - A cable or wire pair which has been bridged to another cable or wire pair.
- Bugging - The act of implanting an electronic listening device, usually small and concealed, for the purpose of the unauthorized monitoring of audible communications.
- Cable, multi-pair - An assemblage of paired, color-coded conductors within a protective sheath. In communications, each wire pair is twisted in order to reduce noise pickup and inter-pair interference.

GLOSSARY OF TERMINOLOGY (Continued)

- Cable carrier system - A multiplex system designed specifically for application to cable pairs. Such a system enables one or two pairs to carry a number of telephone conversations simultaneously.
- Cable, coaxial - A medium through which a very large amount of information (e.g., many hundreds of voice channels) can be transmitted. A coaxial cable consists of one or more coaxial tubes. Each tube consists of an inner conductor and an outer (coaxial) conductor.
- Call - The action performed by a calling party, or the operations necessary in making a call, or the use made of a connection between two stations.
- Cable closure, encapsulated - A cable appearance used on buried cable routes to enclose interconnections between wire pairs.
- Carrier - a) The wave (or frequency) upon which the information to be transmitted over a communications system is impressed (modulation of the carrier).
b) A company which provides communication services.
- Carrier-to-noise ratio (C/N, CNR) - The ratio of the carrier signal magnitude to the noise signal magnitude in a given medium or system, usually expressed in dB.
- CENTREX - A telephone company private branch exchange (PBX) service which permits direct inward dialing to the extensions of the PBX by DDD subscribers. CENTREX service is usually furnished by allocating a part of a DDD switch in a central office for the exclusive use of the customer.

GLOSSARY OF TERMINOLOGY (Continued)

Channel	- In communications, the whole or a portion of a communications medium specifically assigned for the transmission of electronic signals. For example, a tube in a coaxial cable as a whole is regarded as a communications channel. On the other hand, the electromagnetic bandwidth may be subdivided into a set of frequency bands each of which is also considered to be a communications channel.
Circuit	- An electronic path between two or more points. A circuit consists of all communications equipment and media needed to provide the path.
Coaxial cable	- (See - cable, coaxial.)
Coaxial pair	- (See - pair)
Coaxial tube	- (See - cable, coaxial)
Coaxial cable carrier	- A multiplex system designed to provide a large number of two-way voice channels on coaxial tubes.
Code	- A representation of a set of quantities by a corresponding set of binary numbers; also, a representation of one set of binary numbers by another set of binary numbers.
Coil, induction	- A number of turns of wire wound around an iron core used to modify the signal characteristics of communications cables.
Coil loading	- A small induction coil inserted periodically in cable circuits for the purpose of reducing cable loss and making it relatively independent of frequency.
Communications, electronic	- (a) Electronic equipment used to transmit information from point to point through various media or (b) the information transmitted.
Communication	- The transferring of information in any form whatsoever.

GLOSSARY OF TERMINOLOGY (Continued)

- | | |
|----------------------------|--|
| Communication system | - The transmission equipment and media required to accept an input signal at one point and deliver a faithful reproduction of the input signal (called the "output" signal) at another point. |
| Complexity of installation | - Electrical, mechanical or positioning requirements for use of the interception equipment which would not be commonly available. |
| Complexity of operation | - The degree of operator involvement (and skill) necessary for successful intercept operation. |
| Concentrator | - A device having more inputs than outputs that (a) associates each input with one output at any given time on a first-come first-serve basis or (b) multiplexes several inputs into one or more combined output(s). |
| Conductor | - An insulated metallic path for carrying electrical signals within a cable; one-half of a wire pair. |
| Conduit | - A pipe-like or ducted structure used to enclose one or more underground cables. |
| Conduit boxes | - Small boxes inserted between conduit sections on underground cables for the purpose of making the cable pairs available for splicing. |
| Contactor | - A sensing device used on pressurized cable that closes a switch (to operate an alarm in the central office) when the cable pressure drops below a preset threshold. |
| Contents | - When used with respect to a specific communication, the information obtained from the communication itself that concerns the substance or meaning of the communication. |
| Cryptographic | - Pertaining to the transformation of information to conceal its actual meaning by means of a secret process or code. |

GLOSSARY OF TERMINOLOGY (Continued)

Data	- Basic elements of information which can be processed or produced by a computer usually expressed as coded sequences of binary digits.
Data processor	- An electronic or mechanical device for handling information (data) in a sequence of operations.
dBi	- The gain of an antenna whereby the output power ratio is referred to the power which would be radiated by a perfectly omnidirectional (isotropic) antenna.
dBm	- A unit of measurement of power given by the formula $10 \log \frac{P_1}{P_0}$ where "log" is the common logarithm; P_0 is one milliwatt; and P_1 is the power being measured expressed in milliwatts.
dBW	- A unit of measurement of power given by the same formula as above except that P_0 is one watt and P_1 is the power being measured expressed in watts.
DC signaling	- The process of transmitting supervisory signals and dial pulses over cable circuits by means of dc voltages or currents.
Decode	- To translate a coded sequence of binary numbers back into its original uncoded form.
Dedicated circuit	- A telephone, telegraph, or data circuit consisting of equipment and channels which are used exclusively by a specific subscriber.
Dedicated cable plant	- Cable plant having no multiples or bridge-taps. If bridging is required, dedicated plant is bridged at the central office.

GLOSSARY OF TERMINOLOGY (Continued)

Demodulator	- A device which recovers the information originally impressed on a carrier by the modulating signal.
Demultiplexer	- A device which recovers the separate channels from the multiplexed signal usually by the process of demodulation.
Detectability	- The ease with which an interceptor can be detected by any agency or means.
Detector, signal	- The device or system that converts a modulated signal to a useful form. Usually refers to last or lowest stage of demodulation.
Dial	- The act of informing an adjacent central office switch as to the destination of a call being placed. Dialing may be accomplished by a rotary dial or a Touch-tone dial on a telephone; or a multi-frequency (MF) transmitter in a central office.
Dial pulses	- DC pulses or two-tone pulses passed from a customer to a machine, or from machine to machine, representing the digits of the destination number of the dialed call.
Digital (signal)	- A quantity whose variation as a function of time is discontinuous and whose amplitude can take on discrete values only.
Digital transmission	- A communications system specifically designed for the transmission of digital data.
Directivity	- The property of an antenna that causes it to radiate or receive more energy in some directions than in others.
Downlink	- The electromagnetic radiation path from a radio relay satellite transmitter to an earth station receiver.

GLOSSARY OF TERMINOLOGY (Continued)

- | | |
|----------------------------|--|
| Earth station | - That portion of a communications satellite relay system located on the ground and which connects the satellite relay system to terrestrial communications systems. |
| Effectiveness | - The repetitive success in intercepting a communication given the proper functioning of the intercept equipment. |
| EIRP | - The effective electromagnetic power radiated by an antenna, usually expressed in dBm or dBW. |
| End office | - The local central office containing the switch to which DDD subscribers are connected is called the end office. It represents the lowest level in the DDD hierarchy. |
| Encapsulated cable closure | - (See - Cable Closure, encapsulated.) |
| Error rate | - (See - Bit error rate (BER).) |
| Exchange | - One or more central offices with associated plant and stations in a specified area. |
| Extraction, information | - The phase of interception that deals with the translation of targeted communications to ascertain their substance or meaning (e.g., decoding data formats). |
| Facilities, transmission | - The radio systems, multiplex systems, and multiplex channels to which a communications circuit is assigned; a particular type of transmission medium such as a coaxial or radio facility. |
| Final trunk group | - A trunk group through which a DDD call will be routed if all high usage trunk groups are unavailable. |
| Frame (TDM) | - In time division multiplex (TDM) systems, the total elapsed time (or number of bits) between the beginning of a particular time slot in the multiplexed bit stream and the next time the same time slot appears in the bit stream. |

GLOSSARY OF TERMINOLOGY (Continued)

Frequency	- The number of recurrences of a periodic phenomenon in a unit of time specified in "Hertz". In electromagnetic radiation it is the number of maxima or minima that the electromagnetic wave passes through in a second.
Frequency agility	- The ability to rapidly and continually shift the frequency to which a transmitter or receiver is tuned.
Frequency division multiplex (FDM)	- A process whereby a number of individual channels is stacked by translating each channel to a different frequency.
Frequency modulation (FM)-	The process of impressing information on a carrier by continuously varying the frequency of the carrier in accordance with the instantaneous value of the modulating signal.
Frequency shift keying (FSK)	- The process of impressing digital information on a carrier by changing the carrier frequency in discrete steps (used for the transmission of digital data).
Full duplex	- Refers to the ability to transmit information in both directions simultaneously over a communications circuit.
Gain (G)	- The ratio of the power output of a device to the power input, usually expressed in dB. $G = 10 \log \frac{P_2}{P_1}$ where P_2 is the output power expressed in any convenient units, and P_1 is the input power expressed in the same units.
Gigahertz (GHz)	- Frequency expressed in billions of Hertz.
Group, FDM	- Twelve voice channels multiplexed together as a basic unit occupying a band from 60 to 108 khz.

GLOSSARY OF TERMINOLOGY (Continued)

- Group, trunk - The complete set of trunks interconnecting two switching machines.
- Half-duplex - Refers to the ability to transmit information in only one direction at a time over a communications circuit.
- High-usage trunk group - A trunk group which bypasses one or more switching centers of the final call routing path.
- Horn-reflector (antenna) - A large coneshaped microwave antenna having high gain and directivity used for various Bell System microwave radio systems, such as TD2, TH, TM, and TJ.
- Impedance - A property of electrical circuits which resists the flow of alternating current when an alternating voltage is applied to the circuit.
- Induction coil - (See - coil, induction.)
- Information - Any intelligence whether verbal, telemetry or alphanumeric which can be transmitted over a communications system.
- Information extraction - (See - extraction, information.)
- Inter-toll - Between toll offices; e.g., an inter-toll trunk links two different toll offices.
- Intercept equipment - All equipment necessary to target and acquire the contents of a specific communication.
- Interception - The term, as used in this document, refers to the entire set of processes employed to monitor communications between correspondents and extract their information content. Interception includes: signal acquisition, targeting, and information extraction.

GLOSSARY OF TERMINOLOGY (Continued)

Intercept	- The ability to target correspondents and acquire the contents of their communication and includes the acquisition of such contents by simultaneous transmission or recording.
Interceptability	- The ease with which a specific communication can be intercepted.
Interceptor	- One who practices unauthorized interception.
Kelvin, degrees ($^{\circ}\text{K}$)	- Temperature measured on a scale using the same divisions as the Celsius (Centigrade) scale, but with the zero point established at -273°C .
Kilobits per second (kbps)	- Data transmission rate in thousands of bits per second.
Landline	- Any ordinary communications circuit or channel confined to the continental United States. This term is often used to distinguish an ordinary telephone facility from high frequency, very high frequency, or ultra high frequency mobile communications.
Line signal	- In any communications system, the signal applied directly to the transmission medium whether cable or radio.
Loading	- The addition of lumped inductances to a cable at periodic intervals to decrease its loss and make it relatively independent of frequency.
Loading coil	- (See - coil, loading.)
Lobe, antenna	- One of the areas of greater transmission signal strength in the gain pattern of a directional antenna. The area with the greatest signal strength is known as the "major" lobe - and the others are "minor" lobes.

GLOSSARY OF TERMINOLOGY (Continued)

Long-haul	- This term refers to a multiplex system having a maximum permissible length greater than 150 miles.
Loss (L)	<p>- The ratio of the power input to a device (or medium) to the power output (or receiver) expressed in dB.</p> <p>$L = -10 \log \frac{P_1}{P_2}$ where P_1 is the power input and P_2 is the power output. Both P_1 and P_2 must be expressed in the same units.</p> <p>P_1 is less than P_2 for positive L.</p>
Machine, switching	- A processor-controlled device for making telephone connections automatically without the assistance of manual operators.
Main station	- A telephone station that has a distinct call number and a direct connection to a central office.
Medium, transmission	- The physical path through which signals actually travel. For example - microwave uses free space as a medium. Multipair and coaxial cable are other media.
Megabits per second (Mbps)	- Data transmission rate expressed in millions of bits per second.
Message service	- A direct dial (switched) service whereby the subscriber is billed on a time-of-use basis.
Message switching	- This refers to the switching of teletype-writer and other low-speed record data communications.
Metallic pair	- Any two-conductor wire or cable pair (including coaxial cable).
Microwave	- Electromagnetic radiation in the frequency range of 1 to 18 GHz.

GLOSSARY OF TERMINOLOGY (Continued)

Mixer	- Equipment to effect the non-interfering combination of signals originating on two separate paths.
Mobile (station)	- A station for radio communications intended to be used while in motion or during halts at unspecified points.
Mobile (service)	- A service of radio communications between mobile and land stations, or between mobile stations.
Modem	- Contraction of words "modulator-demodulator". A device used to adapt digital signals for transmission over communications circuits and to reconstruct the original digital signals from the received signal. Used synonymously with term "data set".
Modulation	- To impress a signal upon a carrier by making the amplitude, phase or frequency of the carrier vary in accordance with the amplitude of the impressed signal.
Multipair cable	- An assemblage of six or more wire pairs contained within a cable sheath.
Multiplex	- Pertaining to or designating a system of simultaneous transmission of two or more independent signals on the same circuit.
Multipoint	- Refers to a communication circuit or network having three or more subscribers connected simultaneously.
Network, dedicated	- A communications network provided for the exclusive use of the subscribers.
Network, switched	- A network where the subscribers have dedicated lines to the switches but the trunks between switches may or may not be dedicated to any particular subscriber.
Noise	- Any unwanted disturbance or spurious signal within a communications system which has the potential of modifying the intelligence of the transmitted signal.

GLOSSARY OF TERMINOLOGY (Continued)

- Noise figure - A number which characterizes the noise added to a communications system by a communications device (e.g., an antenna or a receiver). It may be expressed in decibels or as an equivalent "noise temperature" in degrees Kelvin.
- Noise temperature - (See - "Noise figure".)
- Office, central - The structure which houses telephone switching machines, transmission and maintenance equipment. A central office may contain any one or all three types of equipment.
- Optical fiber (systems) - Communications systems which transmit intelligence by modulating light (or infra-red) beams through silica fibers.
- Oscillator - An electronic device which generates alternating currents at frequencies determined by the properties of the electronic components within the device.
- Pair - Two conductors that carry communication signals in a wire or cable. These conductors are usually twisted about each other throughout the length of the cable except in the case of coaxial cable or open wire systems. There are usually many pairs in a multipair or coaxial cable.
- Paging - To summon a particular person by announcing his name over a public address system, by sound using his uniquely coded call signal or by selectively calling him on a pocket radio receiver which announces the call by emitting an alerting signal.
- Penetration - The act of accessing the signals carried on multipair or coaxial cable systems.
- Phase-shift keying (PSK) - The process of impressing digital information on a carrier by changing the electrical phase of the carrier frequency in discrete steps (used for the transmission of digital data).

GLOSSARY OF TERMINOLOGY (Continued)

- | | |
|-------------------------------|--|
| Plant | - All assets including buildings, equipment, cable, radio towers, etc., used in furnishing communications services. |
| Plant, inside | - Plant items contained within the confines of central offices and other structures. |
| Plant, outside | - Plant items outside of central offices and customer premises. |
| Plug (pressure) | - A device inserted in pressurized cable to isolate pressured sections. Plugs are usually bypassed and used only in isolating cable leaks. |
| Polarization | - The state of an electromagnetic wave such that the vibrations assume a definite form. The paths of the vibrations (all perpendicular to the direction of travel of the wave) may be straight lines, circles or ellipses. |
| Pre-emphasis | - The selective amplification or attenuation of the frequency components of a signal. |
| Preferred trunk group | - The first choice for call routing among high usage trunk groups. |
| Primary center | - The switching center positioned between the toll center and the sectional center along the final routing in the DDD hierarchy. |
| Private branch exchange (PBX) | - A private telephone switching system located on the premises of a business and requiring an attendant to complete most incoming calls. |
| Probe (coaxial) | - A device designed for the acquisition of the signal being carried by a tube of a coaxial cable. |

GLOSSARY OF TERMINOLOGY (Continued)

- Pulse amplitude modulation (PAM) - The process of sampling an analog signal with a sequence of narrow pulses. The resultant PAM sequence has the same repetition rate as the sampling sequence but the amplitude of each pulse is proportional to the amplitude of the analog signal at the moment each sample is obtained.
- Push-to-talk - A process by which a user can transmit his communication only during the time he is holding a push button down or operating a switch. Push-to-talk circuits are usually half-duplex but not always.
- Radio carrier system (microwave) - The multiplex equipment and microwave radio equipment required to implement a channel of a microwave radio system.
- Radio frequency (rf) - Any frequency at which electromagnetic radiation can be propagated.
- Ready-access enclosure - A cylindrical container suspended from aerial cable or attached to poles for the purpose of enclosing splices, cable terminals, or other miscellaneous apparatus.
- Receiver - (a) That portion of a communications system that converts electromagnetic radiation into an electronic signal suitable for demultiplexing, detection, etc.
(b) A telephone receiver converts electric currents at audible frequencies into soundwaves.
- Record - (a) To register sound by an electronic, mechanical or other device in a manner that will permit its reproduction.
(b) A type of communications service whereby the received message is in type-written form.
- Regional center - The switching center located at the top of the DDD hierarchy (above sectional center) along the final call routing path.

GLOSSARY OF TERMINOLOGY (Continued)

- Repeater, cable - An amplifier, usually located in central offices, used on non-carrier or carrier circuits to maintain adequate signal strength along the length of the cable.
- Repeater, coaxial - A wideband amplifier located in central offices and manholes to maintain adequate signal strength along the length of high capacity coaxial cables.
- Repeater, radio - A microwave transponder located at appropriate intervals along radio routes to maintain line-of-sight transmission between transponders and maintain adequate signal strength along the length of the route.
- Repeater station - In general, any type of structure that contains repeaters.
- Reperforator - A device for producing punched teletype-writer tapes from:
(a) local keyboard transmissions;
(b) incoming teletype messages;
(c) other punched tapes.
- Ring current - 20 Hz AC at a maximum 150V peak and usually having -48VDC superimposed. The combined AC/DC signal level is about 200 Volts peak. This current is inserted on subscriber loops to ring subscriber phones.
- Ring generator - A generator for producing 20 Hz ringing current. These vary greatly in peak voltage and maximum ringing current.
- Route, cable (physical) - The actual physical right-of-way over which a multipair or coaxial cable is installed. Repeater stations are located at fixed intervals along such a route.
- Route, radio (physical) - The actual physical radio path over which a microwave transmission is directed. Microwave towers equipped with antennas and repeater stations will be located at appropriate line-of-sight intervals along such a path.

GLOSSARY OF TERMINOLOGY (Continued)

- Route, circuit - Telephone circuits are said to be routed through certain multiplex systems and cities without regard for physical routing.
- Satellite, communications- A device put into orbit around the earth outside of the atmosphere for the purpose of being visible from intercommunicating points when communications are desired. Satellites usually consist of transponders, antenna, telemetry, beacon transmitters, transponder controls, stabilizing equipment, and solar power cells. Many satellites are put into synchronous orbits where they remain constantly visible to all intercommunicating points. Other satellites, not in synchronous orbits, are visible only for fixed periods of time.
- Sectional center - The switching center along the final routing of a call located between the regional center and the primary center in the DDD hierarchy.
- Sheath, cable - A cable's protective outer covering.
- Short-haul - This term refers to multiplex systems whose maximum permissible length is 150 miles.
- Signal - A physical quantity such as current, voltage, or power whose fluctuations carry the intelligence of a transmitted communication.
- Signal strength - The amplitude of the physical quantity (i.e., current, voltage, power) which is represented as the "signal".
- Signal-to-noise ratio (SNR, S/N) - The ratio of the amplitude of the intelligence-bearing signal to the amplitude of the noise signal being generated by the system transmitting the intelligence.

GLOSSARY OF TERMINOLOGY (Continued)

- | | |
|---------------------|---|
| Specialized carrier | - A communications company organized specifically to perform a specialized communications service such as data transmission (e.g., DATRAN) or private line voice and data (e.g., MCI). |
| Splice | - A physical joining together of two cable pairs to form a continuous electrically conducting path. |
| Splice case | - A cylindrical enclosure designed to contain splices, cable terminals or other miscellaneous apparatus. |
| Switch | - (See - machine, switching.) |
| Switched connection | - The temporary interconnection of two or more communications circuits or trunks either manually or automatically for the purpose of providing communications between their extreme ends. |
| Switching machine | - (See - machine, switching.) |
| Subscriber | - A customer who purchases or subscribes to a communications service. |
| Tandem office | - A central office which houses a tandem switch. |
| Tandem switch | - A switch, having no direct subscriber connections used to interconnect toll-centers or end-offices, or toll centers and end-offices. |
| Tap | - A two-terminal, non-interfering bridged connection to a two-terminal device or to the two conductors of a cable pair. |
| Tap, bridged | - (See - bridged-tap.) |
| Tap, wire | - The use of a tap or bridged connection to accomplish unauthorized interception of communications. |

GLOSSARY OF TERMINOLOGY (Continued)

- Targeting - That phase of interception which deals with the pinpointing of useful information by zeroing in on the communications of specific individuals, groups of individuals, or organization. Targeting can range from a low degree (random snooping) to pinpointing a specific piece of information.
- Telecommunications - Electronic communications systems and practices that permit the communication of intelligence.
- Telegraph - Low speed data transmission ranging from about 5 bps to 300 bps.
- Telemetry - The transmission of specific measurements or signal levels by means of any of a large number of AM, FM, or digital transmission processes. Most modern telemetry systems employ A/D conversion and digital transmission.
- Teletype - Low speed data transmission ranging from 35 baud to 300 baud. Although originally aimed at teletypewriter transmissions the term "teletype" has almost become synonymous with "telegraph".
- Terminal (lug) - A terminal is a metal lug or other binding post used to tie down a metallic conductor (one-half of a cable pair).
- Terminal, communications - A wide variety of telephones, consoles, PBX's, data transmission or other communications devices used to terminate one or more telephone circuits.
- Terminal housing - A metallic box or container used to enclose terminal (lug) mounting strips for the purpose of terminating or interconnecting cable pairs.
- Terrestrial - An earth-bound radio system as opposed to a satellite radio system.

GLOSSARY OF TERMINOLOGY (Continued)

Test set	- Any of a large variety of telephone sets ranging from simple non-dial telephones to battery powered telephones equipped with ringing generators normally used by telephone company maintenance personnel for testing telephone circuits.
Time division multiplex (TDM)	- A process whereby the information originated by a number of subscribers is separated from each other in time and added together to be impressed on a single carrier frequency (usually, but not necessarily, used in the transmission of digital data).
Toll	- (a) A charge made for a connection beyond an exchange boundary; (b) by extension, any part of the telephone plant, circuits, or service for which toll charges are made.
Toll center	- A switching center situated between the end office and the primary center along the final call route of the DDD hierarchy.
Toll-free	- A call or service for which no toll charges are required.
Toll office	- (See - Toll center.)
Transducer	- A device used on more modern pressurized cable systems to make continuous pressure measurements.
Transmission medium	- (See - medium, transmission.)
Transmitter, radio	- The equipment used to generate an rf carrier, modulate this carrier with intelligence, and feed the modulated carrier to the transmitting antenna.
Transmitter, telephone	- The microphone inside the handset that converts sound waves into audio frequency electrical waves for transmission over telephone lines.

GLOSSARY OF TERMINOLOGY (Continued)

- | | |
|-------------------|---|
| Transponder | - A radio receiver-transmitter combination which receives an rf signal, amplifies it and retransmits the signal, usually at a different rf carrier frequency. |
| Trunk circuit | - A telephone circuit interconnecting two switches or PBX's. |
| Trunk group | - (See - group, trunk). |
| Tube, coaxial | - A communications medium consisting of an inner conductor strung with polyethylene discs around which is wrapped a copper outside conductor (tube). The outside conductor is then spirally lapped with steel tape. |
| Uplink, satellite | - The transmission path between the transmitting antenna at an earth station and the receiving antenna on the satellite. |
| Voice band | - The set of all frequencies between 300 and 3400 Hz. |
| Voice bandwidth | - The difference between the highest frequency and the lowest frequency of the voice band (3100 Hz). |
| Voice channel | - The portion of a communications medium assigned for the transmission of a voice signal. |
| Waveguide | - A communications medium consisting of a hollow conducting tube within which electromagnetic waves are propagated through a dielectric medium. |
| Wavelength | - The physical length of an electromagnetic wave as it propagates down a transmission line, through a waveguide, or through free space. |

GLOSSARY OF TERMINOLOGY (Concluded)

- | | |
|---------------------|---|
| Wire | - One or two pairs of electrical conductors within a common cover to form a communication path. |
| Wire carrier system | - A multiplex system designed to work on wire pairs. |
| Wire, open | - Single conductors (both insulated and uninsulated) strung individually on telephone poles. |

1.0 INTRODUCTION

This report presents the results of The MITRE Corporation's study for the Office of Telecommunications Policy addressing the vulnerability of electronic telecommunication systems to electronic interception. The general definition of the term "electronic interception" as used in this study includes the acquisition of the signals, the targeting of correspondence and the extraction of the contents. The purpose of the study is to provide the technical basis for determining the need for and nature of legal safeguards relative to protection of information privacy.

2.0 OBJECTIVES

The objectives of this study are:

- a. To establish the technical capabilities required to implement electronic interception,
- b. To assess the degree of vulnerability of electronic communication systems to electronic interception, and
- c. To determine the detectability of attempts to perform electronic interception.

3.0 SCOPE

In general, the study addresses commonly used electronic communication systems including common and specialized carrier communications and privately-owned systems. Resources did not permit every possible aspect of these systems to be considered. It was necessary to be selective and pragmatic and cover the most likely examples of these systems. However, various forms of communication, including analog and digital, and types of systems, such as dedicated and switched services, were analyzed. The transmission modes considered were terrestrial and satellite microwave systems, mobile radio systems, and wire and cable (coaxial and multi-pair) systems. Wave-guide systems were not addressed since they are only experimental and may

never be employed in an operating system. In the distant future many of the present electromagnetic transmission systems are likely to be replaced by optical fiber systems. These also have not been addressed in this study. However, it is safe to say that the implementation of optical systems will introduce a whole new technology that will have a significant deterring impact on the unauthorized interception of communications.

The specific equipment types selected for analysis are nominal representatives of large classes of systems. For example, the most common components used to implement a specialized carrier microwave system are analyzed. The study addresses the capability required to target a specific person's or corporation's communications and to extract the message content as well as signaling information that identifies sets of correspondents. Also the study addresses both acquisition of systems specifically designed for intercepting telecommunications and the use of systems acquired for legitimate purposes but subverted for use in unauthorized interception.

The study does not address the vulnerability of special government networks such as the Federal Telephone System or the Department of Defense AUTOVON System. Of course, many of the analyses could be applied to these systems as well.

4.0 ASSUMPTIONS

The ease with which private communications can be intercepted is a strong function of the knowledge and skill of the interceptor and the availability of intercept equipment as well as the opportunities available to him to perform the interception without being detected. All of these requirements are met by maintenance personnel and others employed by the common carrier. In addition, free access to the common carrier's premises could be used by a knowledgeable

interceptor to subvert the common carrier's own equipment to assist him. The probability that an employee will be caught is strongly dependent on security measures taken by the common carrier and nearly impossible to assess without a very detailed and lengthy investigation. It is therefore assumed that an interceptor does not have access to a common carrier's switching systems offices.

Free access to the premises of the target of the interception (the person or organization whose communications are to be intercepted) would also simplify the task of the interceptor. Since this capability is dependent on the security measures taken by the target, it is assumed that the interceptor does not have access to the premises of the target.

It cannot be assumed that the interceptor has a limited knowledge of the common carrier's system, the target or the availability of equipment, or that he has a limited set of skills. While the need for particular knowledge and skills is used to evaluate the difficulty of the interceptor's task, this study has assumed that the interceptor has or can acquire the required knowledge and skills.

5.0 METHODOLOGY

The approach taken was to determine the minimum capability required to intercept communications. A key element of this approach was determining the minimum signal strength required:

- a. To acquire voice communications with sufficient intelligibility to understand the substance of the conversation.
- b. To acquire digital data information with an acceptable error rate (e.g., 1 in 10^5) such as to permit extraction of pertinent information, and
- c. To acquire sufficient signaling information from a network to identify the destination of calls from or to specific subscribers.

For radio systems, including microwave, satellite and mobile radio, the approach was to determine the minimum required antenna, receiver, and signal processing equipment combinations necessary to acquire the desired signals with the required signal strengths as a function of direction relative to and distance from communication system radiating antennas. In some cases, a range of interceptor capabilities were considered.

For cable and wire, the specific means for acquiring the signal energy were identified and the appropriate configuration of signal processing equipment was determined.

As indicated above, all communication carriers use a large variety of equipment types. Therefore, for this study, classes of communication equipment representative of major portions of the telecommunication carrier industry were selected. All the systems selected are capable of handling analog or digital information. The following systems and their characteristics were selected for analysis during this project.

TERRESTRIAL MICROWAVE SYSTEMS

<u>System</u>	<u>Characteristics</u>
AT&T	Multi-channel common carrier, switched and dedicated voice and data service
Western Union	Dedicated voice service, switched and dedicated data service and teletype service
MCI	Dedicated voice and data service
DATRAM	Switched and private line data service
Privately-owned	Dedicated voice and data circuits

SATELLITES

<u>System</u>	<u>Characteristics</u>
COMSAT/AT&T/GTE	Common Carrier Service, 4 and 6 GHz frequency bands
WESTAR	Dedicated service, possible subscriber-owned earth stations, 4 and 6 GHz frequency bands
Satellite Business Systems	Dedicated digital service, many small earth stations on subscriber premises, 12 and 14 GHz frequency bands
INTELSAT	International Common Carrier, many foreign-owned earth stations, 4 and 6 GHz frequency bands

CABLES AND WIRE

<u>System</u>	<u>Characteristics</u>
Coaxial Cable	Frequency division multiplexed circuits with carrier signals
Multi-pair Cables	Frequency- or time-division multiplexed circuits or many voice bandwidth circuits
Wire	Frequency- or time-division multiplexed circuits or single voice bandwidth circuit

MOBILE RADIO

<u>System</u>	<u>Characteristics</u>
AT&T and Private Radiotelephone Systems	Common and private telephone service
Police, Fire, Taxi, Marine, and Citizens Band Radio	Public service Radio Systems

The sources of information used in this study include:

- a. Interviews of carrier industry personnel,
- b. Discussions with federal government representatives such as members of the FCC staff,
- c. FCC application filings,
- d. Published system specifications and standards, and
- e. Vendor catalogs and discussions with vendors.

It should be noted that this study did not assess interception of communication other than those carried by electronic communications systems. (e.g., it did not address hidden microphones or other forms of "bugging".)

6.0 GENERAL DEFINITIONS

This section presents a general description of "electronic communication systems" and their components and a definition of "electronic interception" identifying all the elements of the interception process. These descriptions and definitions are given to provide an introduction to terminology used in the report and a basis for the discussion of the vulnerability of electronic communications systems to electronic interception.

6.1 Communication System Definition

Figure 1 presents a segment of a common carrier telephone system. The system can be considered as consisting of three major categories of equipment; the distribution plant that connects telephones or other terminals to the end offices, the switching systems located in the end offices and toll centers and the trunks that interconnect the switches in those end offices and toll centers. The equipment within the end offices and toll centers is frequently referred to as "inside" plant and distribution system and trunks as "outside" plant.

Figure 2 presents a segment of the distribution plant and indicates the hierarchical nature of its structure. The connection between a subscriber's telephone and the end office, also known as a central office, is a pair of wires called a local loop or a subscriber loop. A large number of local loops will leave the central office in the form of a main feeder cable containing as many as 100 pairs of wires (also called wire-pairs). As shown in Figure 2, the wire-pairs are then fanned-out through branch feeder cables and distribution cables and finally end as a drop or service wire entering a residence or a business. The cables carrying more than six wire-pairs are referred to as multi-pair cables. There are many "appearances" present along the wires and cables.

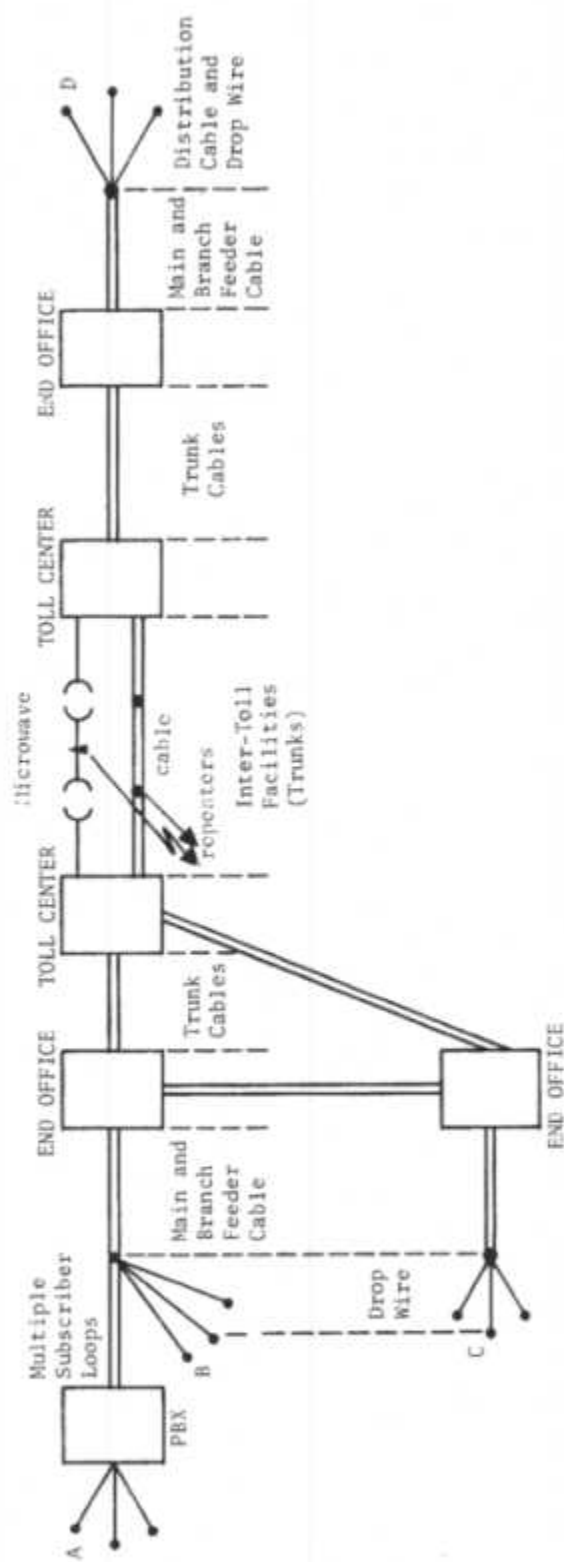


FIGURE 1
SEGMENT OF PUBLIC DIRECT DISTANCE DIALING NETWORK

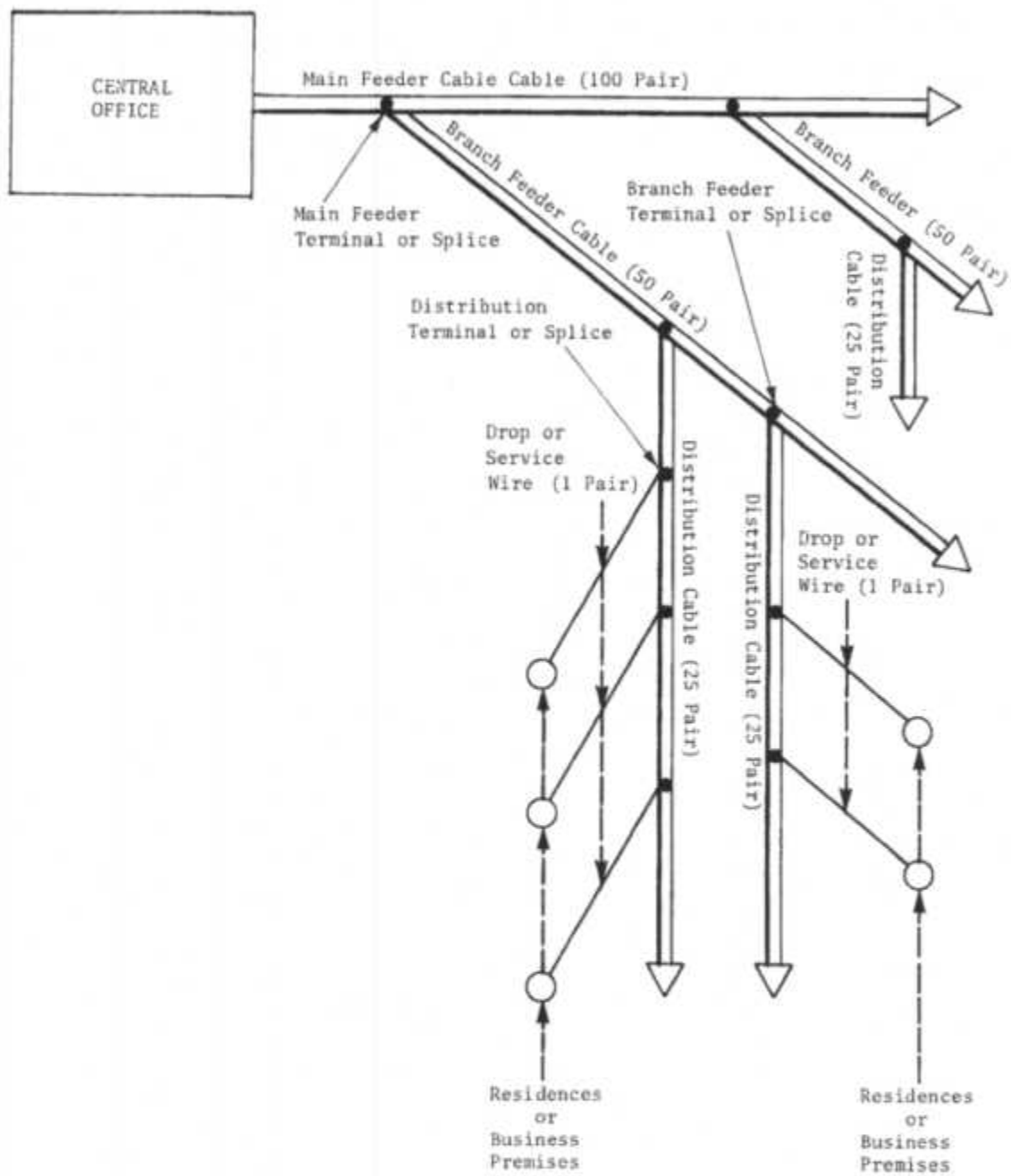


FIGURE 2
DISTRIBUTION PLANT CABLE HIERARCHY

"Appearances" are points where segments of wire and cable are connected together for various purposes. These include splice cases, terminal enclosures and terminal housings.

Referring again to Figure 1, cables connecting the switches in end offices with switches in other end offices or toll centers also contain many pairs of wires known as trunk circuits. Each pair of wires may carry a single conversation or several conversations simultaneously through the use of a process called multiplexing.

Toll center switches are interconnected by toll trunk circuits. Many trunk circuits may be carried simultaneously over microwave radio systems, coaxial cable systems, or multi-pair cable systems. As with wire systems the technique of multiplexing is also used with toll trunk circuits to transmit a large number of conversations over the same medium simultaneously.

In the case of long-haul communications, the transmission facilities are frequently shared by a large number of trunk circuits between many toll centers. The number of channels carried by a microwave system or a coaxial cable system may be as high as 10,000. Of this number, 50 to 100 might be dedicated to carrying traffic between a specific pair of offices. This portion allocated to a pair of offices is known as a "trunk group".

There are two basic types of multiplexing processes referred to above: frequency division multiplexing (FDM) and time division multiplexing (TDM). FDM is a process whereby a number of individual channels share a common transmission medium by translating each channel to a different frequency. TDM is a process whereby a number of individual channels share a common transmission medium by transmitting samples of each channel in a different time slot. Systems employing multiplexing are

frequently called "carrier" systems. In contrast, those carrying a single channel are referred to as "non-carrier" systems.

Several kinds of wire and cable are used in telecommunications systems. In addition to the insulated wire pairs and the multi-pair cables there are the coaxial cables referred to above and "open-wire". Briefly, coaxial cables consist of many tubes. Each tube consists of a center metal core conductor surrounded by an insulating material which, in turn, is surrounded by an outer metal conductor. As indicated above, multiplexing is used to send many conversations over the coaxial cable simultaneously.

Open-wire refers to insulated or uninsulated single conductors strung on the cross arms of telephone poles. This can be found in many places throughout the public network and is used for both local loops and short-haul trunks.

Wire and cable plant may be typed according to the three methods of physical installation. These are:

- (a) Aerial wire and cable - wire and cable attached to a pole or the cross-arms of a pole,
- (b) Buried cable - cable buried directly in the ground,
- (c) Underground cable - cable placed in underground conduits.

Communication services are provided for the public by "common carrier" companies. Common carriers provide a number of kinds of services. Two of these are the public telephone switched service and dedicated or "private line" services. With private line service, the carriers provide a customer with circuits dedicated to that customer's use only. The dedicated service can range from a single circuit between two points to an entire network including central office switching dedicated to a single customer's use.

Common carrier companies can be classified according to the types of communication services that particular companies are authorized by the Federal Communications Commission to provide. A large number of companies are interconnected with the AT&T Long Lines Company to form the public telephone switched service, the Direct Distance Dialing (DDD) network. The same carriers can provide dedicated ("private line") circuits for non-switched voice or data service. One carrier is authorized to provide domestic switched teletype service and some are authorized to provide switched data network services. Some carriers, frequently referred to as "specialized carriers", provide only leased "private line" services, (e.g., MCI).

Also shown in Figure 1, subscribers may have a Private Branch Exchange (PBX) on their own premises for serving a number of telephones within those premises. The PBX may be connected with the public switched network by means of local loops or may be connected to a dedicated service network or both.

Switched service networks make use of "signaling" systems to control the operations of the network. The signaling systems pass requests for establishing connections and information regarding the status of portions of the network (e.g., busy signal).

This brief discussion has focused principally on telephone service to illustrate some of the terminology used in the telecommunication industry. It is well known that the same transmission facilities are also used for the transmission of teletype, data and television and to provide a variety of types of service. Further explanations of terms used in this study are given either in the glossaries or within the text as appropriate.

6.2 Definition of Electronic Interception of Communications

The term "electronic interception" is defined to include the acquisition of the electronic signals, the targeting of correspondence by specific individuals or organizations and the extraction of the information contents. Figure 3 presents a diagram of the elements of the interception process. The nature of signal acquisition varies with the transmission media being used to carry the electronic signals. That is, acquiring signals from wire may require little more than attaching intercepting wires. Cable requires additional effort to penetrate the sheath. Acquisition of radio signals, of course, involves radio reception.

Targeting refers to the acquisition of communication signals between specific individuals. In some portions of the study report, targeting is defined as having a range, from essentially non-targeting, i.e., random snooping to full targeting, i.e., the acquisition of a specific individual's communications. In the case of random snooping, an interceptor might be interested in randomly sampling communications between particular regions such as between groups of commodity exchange dealers.

The last element of interception is the extraction of information. This might be as simple as listening to a telephone conversation or as difficult as decoding data that has been scrambled either to achieve some degree of privacy or for some other reason.

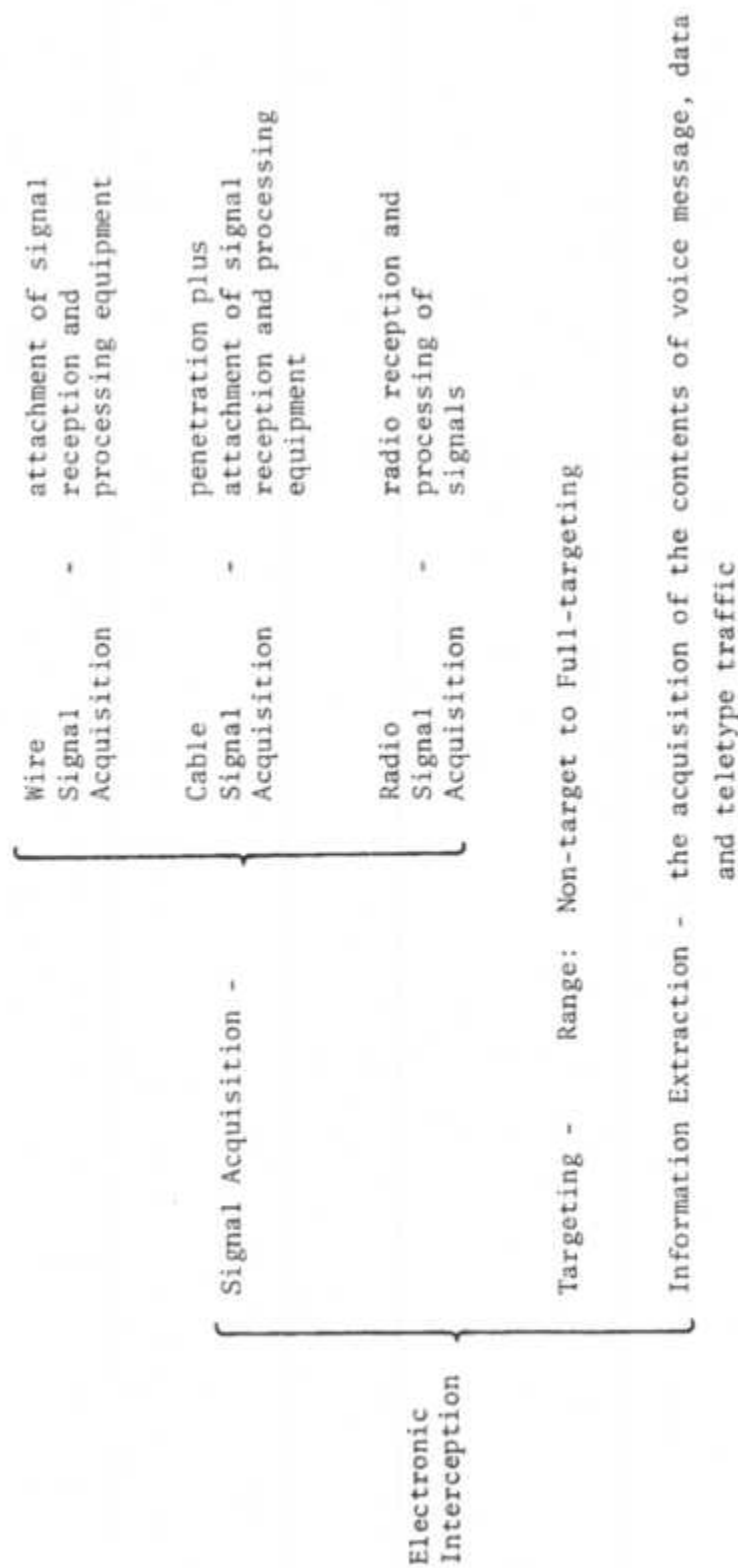


FIGURE 3
IDENTIFICATION OF THE ELEMENTS OF ELECTRONIC INTERCEPTION

7.0 STUDY CONCLUSIONS

In general the study found that intercepting electronic communications is a function of the kinds of transmission media employed, the kinds of networks formed using the media and the kinds of services provided by the common carrier networks (i.e., switched or dedicated). Therefore the study conclusions are categorized according to these findings.

7.1 Conclusions Relative to the Acquisition of Communication Signals from Various Transmission Media

7.1.1 Penetration of Wire and Cable Systems

(1) Penetration of open-wire systems for communications interception is easily accomplished with the aid of inexpensive equipment. Open-wire systems consist of uninsulated wire strung on poles above ground and can be tapped with simple alligator clips.

(2) Penetration of aerial multi-pair cable for communications interception is easily accomplished with the aid of inexpensive equipment. The outer sheath of the cable is easily cut through and individual wire pairs stripped of insulation. Subscriber loop cables and most short haul cables have many appearances which are neither locked nor alarmed and to which a wire tap can be easily installed. Some cables are pressurized but pressure alarms for this type of cable are easily defeated.

(3) Penetration of buried multi-pair cable for communications interception is easily accomplished with the aid of inexpensive equipment. The location of the cable is readily identified by telephone company markers. Cable is readily dug up. Buried cable has fewer appearances than aerial cable but is less frequently pressurized. The outer sheath of the cable is easily cut through and individual wire pairs stripped of insulation. The risk of visual detection of the wire tap can be reduced by connecting wires through a trench extended to a remote point and burying the tap and extension wires.

(4) Underground multi-pair cable is not as vulnerable to penetration as aerial or buried cable (but still relatively easy to tap). The location of the cable is readily identified by telephone company markers. Cable is readily dug up (although buried more deeply). Access to the cable requires cutting through conduit in addition to penetrating the cable. Underground cable has frequent appearances but appearances are in manholes or buried conduit boxes. Extension of the wire tap from a manhole to a remote point is more likely to be discovered than the extension of buried cable wire tap.

(5) Coaxial cable must be penetrated in order to intercept communications. It is unlikely that adequate signal levels can be acquired by inductive methods to intercept communications carried by a coaxial cable.

(6) Coaxial cable is very difficult to penetrate without setting off alarms or seriously degrading the performance of the system (both detectable by telephone company maintenance personnel). The copper outer conductor of each coaxial tube in the cable is usually covered with a spiraled layer of steel tape. The coaxial tubes are enclosed in a sheath consisting of lead and possibly other materials. A considerable length of cable would have to be exposed in order to separate the tubes. Each tube is pressurized and connected to a very fast-reacting pressure alarm. A specialized precision tool would be required to puncture the steel tape and copper outer conductor, seal the resultant hole instantly and insert a probe near the center conductor. The precision tool could easily cause an electrical disturbance detectable by telephone company personnel.

The only other means of penetrating a coaxial cable system is at repeater manholes or auxiliary huts. Most manholes and all auxiliary huts have burglar alarms which are extended by telemetry to telephone company offices. Manholes and repeaters are securely locked against intrusion and are pressurized as well.

7.1.2 Reception of Microwave Radio Communications

(1) Communications over terrestrial microwave systems are easily received. Usable microwave radiation is available to the interceptor as far as five to ten miles from a repeater.

(2) The antenna and radio receiver portion of a terrestrial microwave intercept system will cost at least 100 times as much as a single wire tap device.

(3) Communications over satellite microwave systems are easily received. Areas available to the interceptor of satellite down-link radiation vary from several tens of thousands of square miles (for spot beams) to the entire continental U.S. and adjacent oceanic and land areas (for most domestic satellites) to nearly a full hemisphere (for the INTELSAT global beam).

(4) The antenna and radio receiver portion of a satellite microwave intercept system will cost at least 700 times as much as a single wire tap device.

(5) Microwave radio intercept equipment can be readily hidden. The principal form of detection of radio intercept activities is physical surveillance. The principal observable would be the intercept antenna. The interceptor can make use of a number of innocent-appearing structures such as apartment, houses, sheds, barns or a specially out-fitted van to house his entire monitoring station. All equipment except the antennas could be readily hidden or disguised in most structures. The intercept equipment (including the antenna) could also be "hidden" by adding the intercept receiving equipment to legitimate antenna installations such as a subscriber-owned earth station for use with a domestic satellite, a radio astronomy station or manufacturing plants which build and test radar and/or radio antennas. INTELSAT earth station equipment in one country could also be used to intercept traffic between two other countries.

7.2 Conclusions Relative to Targeting Correspondents Within Networks

The conclusions relative to networks and services are grouped according to whether they relate to the Public Switched Telephone Network or to Dedicated Service Networks.

7.2.1 Conclusions Relative to the Public Telephone Switched Network

(1) The optimum place to intercept communications over the public telephone switched network is the subscriber loop. The subscriber loop is the only place in the network where all communications of the target can be intercepted. The subscriber loop consists of open wire or single-pair wire or multi-pair cable which is readily and inexpensively penetrated. With few exceptions, carrier systems are not employed. Minimal precautions are necessary to avoid detection by telephone company office equipment. Visual detection can be minimized by judiciously selecting the time and place for making the wire tap and by remoting the monitoring station to a safe hiding place.

(2) Targeting communications between two specific individuals or organizations in two different toll areas by intercepting communications carried on trunk circuits of medium to high density routes is a formidable task. Trunks connecting two toll switches (called a trunk group) will usually be divided among two or more physical routes. Medium and high density routes will carry many times the number of trunks and other circuits as the number of trunks in the trunk group of interest. There may be several routes which are possible candidates for carrying the trunk group of interest, spread over hundreds of miles. Although techniques exist for determining most or all of the trunks belonging to the trunk group of interest, the total number of trunks to be individually tested can be overwhelmingly large.

The interceptor's job is further complicated by the fact that the candidate routes may be either radio, coaxial cable or multi-pair cable, each requiring different types of equipment to intercept the communications.

For example, a trunk group between two representative toll centers, each located in a medium-sized city might consist of 40 trunks divided among 2 or 3 physical routes out of 4 or 5 possible candidate routes involving 1 or 2 radio routes, 1 or 2 coaxial routes and a multi-pair cable route. The total cross-section of the candidate routes might vary from 10,000 to 40,000 trunks at different places.

(3) The signaling associated with switched networks can be used to determine when a particular circuit is being used and to identify the party being called. Signaling is used by the switching machines to determine when a subscriber has his instrument "off-hook", to determine the identity of the particular subscriber being called and to tell other machines what interconnections are desired.

(4) Access to the Common Channel Interoffice Signaling System (CCIS) would allow the interceptor to be more selective in targeting conversations between two individuals or organizations. If CCIS is fully implemented as now visualized, a signaling network will be established that will carry all signaling information over circuits completely separate from the trunks carrying the communications between two parties. The information transmitted will include the dialed number (destination), the calling number (origination) and the identity of the particular trunk to be used for the call.

(5) If the CCIS is fully implemented as now visualized, the interceptor may have difficulty in locating the particular CCIS circuit carrying the signaling information associated with the targeted individuals or organizations. The fully implemented CCIS would have its own network, completely independent of the public telephone switched network (except for the originating and destination

offices). Therefore, the CCIS circuits carrying the signaling information of interest may appear on a completely different physical route than the circuit carrying the targeted communication. For example, the interceptor's task would be particularly difficult if the routes carrying the communication of interest are radio or multi-pair cable routes but the circuits carrying the signaling information are routed on coaxial cable.

7.2.2 Conclusions Relative to Dedicated Service Networks

(1) In most cases, the optimum place to intercept communications carried by dedicated service networks is the "local loop". Subscribers to dedicated network services that share transmission facilities with the public telephone switched network are connected to the dedicated service by a local loop between the subscriber's premises and a telephone central office that is similar to the loop used for connection with the public telephone switched network. Subscribers to dedicated network services provided by the specialized carriers are connected to the dedicated service by a circuit that is leased from the local public telephone switched service carrier and runs between the subscriber's premises and the entry point to the specialized carrier facilities. The circuit leased from the public telephone switched service common carrier is routed through the public telephone central office. The segment of the circuit from the subscriber's premises to the central office is similar to a telephone local loop and, therefore, is an optimum point for intercepting communications.

(2) Locating the physical routes of circuits of dedicated network services which share transmission facilities with the public telephone switched network is more difficult than locating the routes of dedicated network services provided by the specialized carriers. The diversity of possible routes that can be taken and the number of trunks to be monitored is much greater for the circuits sharing the public telephone network facilities.

(3) Finding the dedicated circuits of a particular subscriber to the services of a specialized common carrier is relatively easy. There are relatively few routes available.

(4) Interception of subscriber communications relayed by the WESTAR satellite is relatively easy. WESTAR traffic is entirely private line service.

(5) It would have been moderately difficult to intercept traffic (either private line or switched service) carried on the DATRAN backbone network (now discontinued). The DATRAN signal was scrambled before transmission. Each subscriber's communication was digitally encoded before being time division multiplexed by DATRAN. However, a knowledgeable person could break both the scramble code and the subscriber's code. Since DATRAN has only one switch to provide the switched service, the interceptor's task is not significantly different from that required for the intercept of communications using a dedicated service.

(6) If Satellite Business Systems (SBS) implements a satellite relay system as proposed, it will be difficult to intercept the communication of some subscribers. SBS plans to offer cryptographic devices to subscribers desiring the service.

7.3 Citizens Band and Public Service Band Radio

(1) Transmissions over citizens band and public service band radios are easily received and the information extracted. Inexpensive receivers covering these bands are available from retail outlets.

(2) Targeting of specific individuals using CB radios is difficult. However, targeting specific classes of individuals (e.g., truck drivers) or types of communications (e.g., distress calls) can be more easily accomplished. Specific individuals may use any of the channels assigned to this band (40 channels as of

1 January 1977). However, communications of certain classes of individuals or types of communication tend to be broadcast on certain prearranged channels.

(3) Targeting of specific mobile radio telephone subscribers is moderately easy. Individual mobile telephone units are usually equipped with very few channels.

(4) Targeting of organizations (e.g., police, fire, ambulance services) using public service radio is moderately easy. These organizations use relatively few frequencies, each of which is usually assigned for a specific use.

(5) It is practically impossible to detect the interception of traffic on citizens band or public service band radio if the interceptor wishes to hide the fact. Possession of these receivers is quite common and they are used for legitimate purposes.

8.0 SUMMARY OF FINDINGS

This section summarizes the analyses of the vulnerability of electronic communication systems. The detailed analyses are contained in the appendices in Volume II of this report.

The summaries of the analyses are preceded by brief descriptions of the general characteristics of the common carrier networks and the services provided. The descriptions provide some of the background and a part of the basis for the analyses. Additional descriptive material is provided within the analytic sections themselves. The amount and level of detail of descriptive material is limited to that necessary to support the analyses.

8.1 General Characteristics of Electronic Common Carrier Systems

The common carriers provide several different kinds of switched and dedicated (private line) service. Public switched service refers to the ability of any subscriber to be connected quickly (within seconds) to any other subscriber within a public switched network.

The best known service of this kind is provided by the public telephone network offered by the Bell System together with the independent telephone companies. Dedicated service refers to the provision of one or more full or part-time circuit(s) for the exclusive use of the subscriber between specific points of interest to him. Another service offered consists of a number of private line circuits terminating in customer switching arrangements whereby the subscriber is provided a switched network for his exclusive use.

8.1.1 Public Switched Service Networks

There are three general categories of public switched service: Message service (voice and data which can be carried over regular voice channels); teletype; and data (which may carry voice after analog-to-digital conversion).

8.1.1.1 Public Distance Dialing Service

Within the U.S., the largest public switched service network is the Direct Distance Dialing (DDD) network, of which the Bell System is the largest portion, consisting of the AT&T Long Lines Department and the associated local operating companies. Nearly all independent companies (approximately 1800) in the United States are tied into the Bell System and therefore must be compatible with it.

Within the Bell System, the local operating companies are the primary interface with nearly all subscribers. They procure, install and maintain the facilities for nearly all traffic between subscribers within their individual areas. AT&T Long Lines provides the facilities for communication over long distances between different local operating companies, although some direct routes are established between adjacent operating company areas without going over AT&T Long Lines facilities.

Within the Bell system, a hierarchy of switching centers has been established. An illustration of this plan is shown in Figure 4. The centers and end offices shown represent switching machines (as opposed to physical buildings). In fact, two or more switching centers may be collocated in the same physical building. Subscribers are connected to end offices (also known as central offices) by subscriber loops (also known as local loops). End offices and other centers are interconnected by trunk circuits. Subscriber loops may terminate at single telephones or data sets or at private branch exchanges (PBXs). Single telephones or data sets connected to a subscriber loop are sometimes called main stations. The collection of trunk circuits between any two switching machines are called trunk groups. The collection of subscriber loops terminating at a private branch exchange (PBX) are sometimes referred to as a PBX trunk group. Trunk groups may involve very long or very short physical distances. Further, a trunk

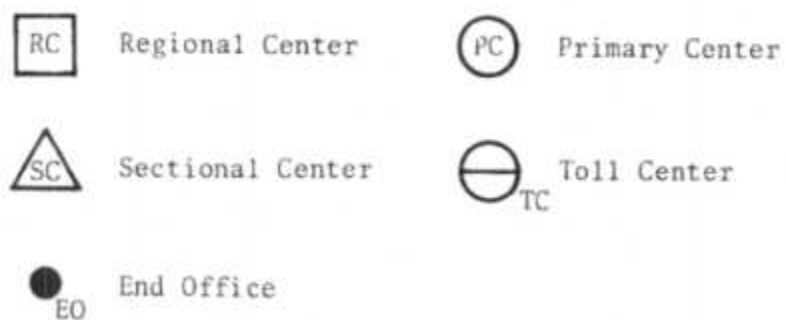
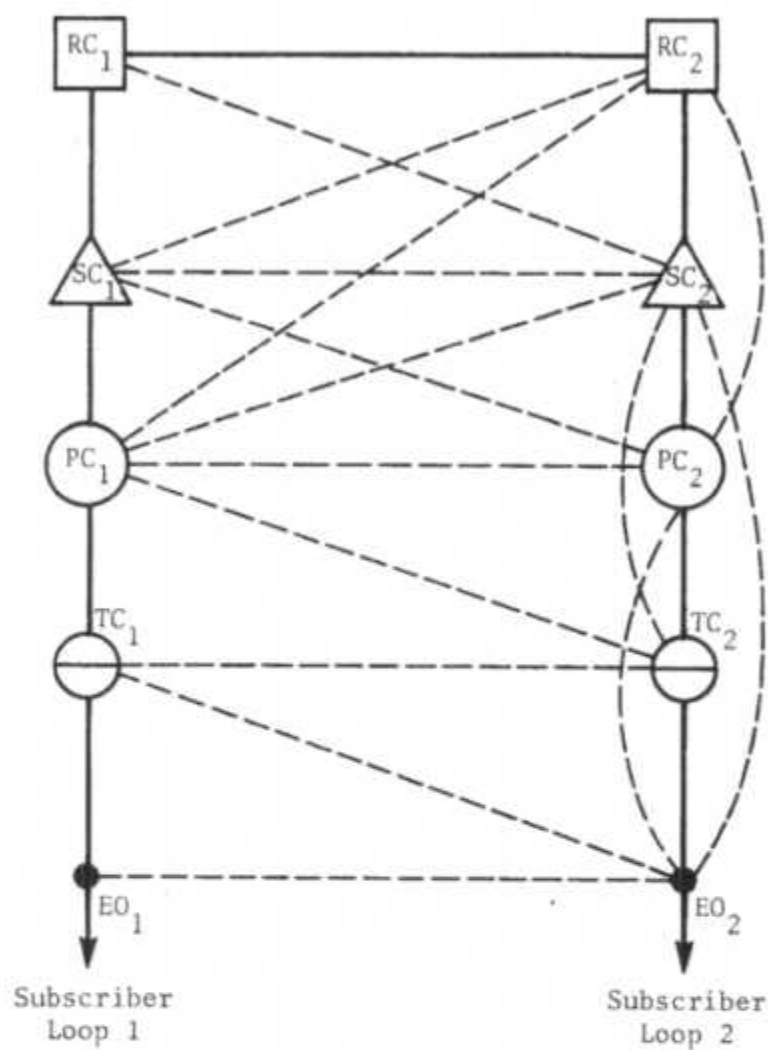


FIGURE 4
ILLUSTRATION OF BELL SYSTEM SWITCHING PLAN

group connecting two centers is defined as including all connections between them, independent of the physical route taken by individual trunks. The trunk group circuits may, in fact, be divided among several physical routes.

The dashed lines in Figure 4 represent high usage trunk groups and the solid lines represent "final" trunk groups to be used only when all other paths are fully loaded. For example, a subscriber loop terminated at EO_1 calling a subscriber loop terminated at EO_2 would normally be routed on the high usage trunk group directly connecting EO_1 and EO_2 . If all trunks on this route are being used, the subscriber's circuit will be switched to the final trunk group to TC_1 . If all trunks on the final trunk group are also busy, the subscriber will hear an interrupted trunk busy tone to indicate that his call cannot be completed at this particular time.

Assuming the subscriber is connected to a trunk in the final trunk group to TC_1 , two high usage trunk groups are available to connect him to subscriber 2's end office (a direct route to EO_2 or a route via TC_2 to EO_2). One or the other will have been designed to be the first choice (for example, it may be the most economical route). If all trunks are busy, the other high usage trunk group will be tried. Only if both of these trunk groups are busy will the final trunk group to PC_1 be tried. The same principle applies at all higher centers in the hierarchy. Of course, Figure 4 is only illustrative of the principles involved. Actual trunking plans will depend on the traffic patterns for a particular area. For example, some lower class offices do not have high usage trunk groups (dashed lines in the figure) but have only a final trunk group.

Not shown in Figure 4 is a switching center known as a tandem office. In metropolitan areas having a large number of end offices, the direct connection of every end office to every other end office could result in a very large number of trunk groups. In this case, it may be more economical to establish a more or less centrally located switching center to which each of the local end offices and toll centers are connected via tandem trunk groups. A tandem office does not eliminate all trunks between end offices, but does significantly reduce the number of trunks required.

The following examples of high-usage trunk groups and physical route cross sections between representative end offices located in large, medium and small cities may serve to indicate the magnitude of the effort required to intercept communications over the public switched network. Trunk group sizes include only long haul trunks. Additional trunks and branch feeder cables can be expected at numerous places along the routes.

Example #1: An end office in a large city to an end office in another large city.

At least four physically separate routes link the two large cities. The four routes have a total cross section of at least 49,000 trunks (2 radio and 2 coaxial cable routes) in a sample cross section and at least 62,000 trunks (1 radio and 3 coaxial cable routes) in another. The first choice routing from a specific end office in the first city to a specific end office in the second city consists of a high-usage trunk group (approximately 200 trunks) between the end office and a primary center in the first city; a high-usage trunk group (approximately 50 trunks) between the primary center in the first city and a toll center in the second city routed over two physical routes between the two cities; and a high-usage trunk group (approximately 100 trunks) between the toll center and the specific end office in the second city.

Example #2: An end office in a large city to an end office in a medium-sized city.

At least six physically separate routes link these cities. The routes have a total cross section of at least 67,000 trunks over 8 routes (4 radio, 3 coaxial cable and 1 multipair cable) in a sample cross section and at least 85,000 trunks over 7 routes (3 radio, 3 coaxial cable and 1 multipair cable) in another. The first choice routing from a specific end office in the large city to a specific end office in the medium-sized city consists of a high-usage trunk group (approximately 250 trunks) between the end office and a primary center in the large city; a high-usage trunk group (approximately 60 trunks) between the primary center in the large city and a sectional center in the medium-sized city routed over two physical routes between the two cities; and a high-usage trunk group (approximately 110 trunks) between the sectional center and the specific end office in the medium-sized city.

Example #3: An end office in medium-sized city to an end office in another medium-sized city

The number of physically separate routes linking these two cities ranged from two to five. The routes have a total cross section of at least 10,000 trunks over 2 routes (1 radio and 1 coaxial) at a sample cross section, at least 27,000 trunks (2 radio routes) at a second cross section, at least 47,000 trunks (3 radio routes) at a third cross-section, and at least 33,000 trunks over 5 routes (2 radio, 2 coaxial cable, and 1 multi-pair cable) at a fourth cross section. The first choice routing from a specific end office in the first city to a specific end office in the second consists of a high-usage trunk group (approximately 50 trunks) between the specific end office and a sectional center in the first city; a high-usage trunk group (approximately 40 trunks) between the sectional center in the first city and a regional center in the second city routed over three physical routes; and a high-usage trunk group (approximately 30 trunks) between the regional center and the specific end office in the second city.

Example #4: An end office in a medium-sized city to an end office in a small city

The number of physically separate routes linking these two cities ranged from three to five. The routes have a total cross section of at least 20,000 trunks over 5 routes (2 radio, 2 coaxial cable and 1 multipair cable) in one sample cross section, at least 12,000 trunks over 3 routes (2 radio and 1 coaxial cable) at a second cross section and at least 24,000 trunks (3 radio routes) at a third cross section. The first choice routing from the specific end office in the medium-sized city to the specific end office in the small city consists of a high-usage trunk group (approximately 50 trunks) between the end office and a sectional center in the medium-sized city; a high usage trunk group (approximately 30 trunks) between the sectional center in the medium-sized city a sectional center in the small city routed over two physical routes; and a high-usage trunk group (approximately 100 trunks) between the sectional center and the specific end office in the small city.

A variation of switched service called WATS (Wide Area Telephone Service) is provided by AT&T. One or more access lines are provided the subscriber from his location to a toll center near him. Beyond this toll center, the regular switched distance dialing network is used.

8.1.1.2 Teletype Switched Service Network

The present teletype switched network provided by Western Union in the U.S. consists of an integration of the historically separate telegram, cablegram, TWX and TELEX services, and the addition of some new services such as teleprinter computer service (called "InfoMaster") and mailgram. In addition, subscribers to private line teletype service have access to the entire integrated teletype switched network. "Infocom" is a separate private line record system with switches at

New York City, Mahwah, N.J., Atlanta, San Francisco and Chicago. It can access "Infomaster" via switches at Middleton, Va. and Bridgeton, Mo.

Essentially, ISCS is a message-switching store-and-forward computer system that accepts and records messages, releases the caller from the line, then forwards the message to its destination on an immediate or selectively deferred basis.

The TWX and TELEX services are real time dial-up services. These networks were left intact as separate networks but interconnected via the ISCS. Both TWX and TELEX are connected to overseas carriers and provide real time dial-up services via these carriers. Cablegram service was made available to all subscribers by connecting the ISCS to gateways serving overseas carriers. Telegram service from and to public offices is implemented by connecting each public office to the ISCS (eliminating the reperforator network). TELEX, TWX and teleprinter subscribers as well as Western Union public offices and centralized telephone bureaus (accessible by toll-free telephone call) can originate Mailgram messages to be transmitted over the teletype switched network. ISCS forwards traffic to teleprinter terminals installed at selected post offices across the country. Routing of Mailgrams to the appropriate post office is accomplished by use of Zip Code. Post office personnel remove mailgram messages from the teleprinter, insert them in envelopes and place them in mailbags for delivery. All post offices are not equipped with teleprinters. However, the selected post offices are strategically located so that any other post office can be reached by regular overnight postal service.

TWX is usually transmitted using the ASCII (American Standard Code for Information Interchange) digital code and operates at 100 words per minute (110 bps). Some TWX machines operate at 45 bps

and use the Baudot code. TELEX is transmitted using the five-level Baudot code and operates at 66 words per minute (50 bps). Teletype communication from Western Union public offices to the Middleton, Va. switching center operates at 110 bps but communication in the opposite direction is at 75 bps. Communication from the centralized telephone bureaus to the Middleton, Va. or St. Louis switching centers is at 2400 bps. Overflow traffic going to Middleton or St. Louis is routed to the other at 56 kbps. The ISCS has the capability of making the code and speed conversions necessary between these two systems as well as conversions between these and other standard codes such as BCD (Binary Coded Decimal).

Another addition to the switched network known as Electronic Data Switching (EDS) is to be cut over in the near future. The initial switch is located in New York City. Although the initial service will be an extension of the TELEX network, it is planned to provide the capability to expand the service to accept traffic at a variety of data speeds and codes. Time division multiplex will be used and the individual circuits do not have to be synchronized with each other or the switch.

All TWX switching machines are located on telephone company premises, although it is expected that Western Union will build and operate its own TWX switching machines on its own premises in the next few years. The present switching hierarchy consists of three levels. The lowest (tertiary) level consists of 72 offices, each of which homes on a next higher (secondary) level office. The 69 secondary offices have a limited amount of interconnectivity by means of high usage trunks. The highest (primary) level consists of 10 offices, all of which are interconnected. About 85% of the trunks between TWX switches are dedicated trunks. The other 15% operate via the

Direct Distance Dialing telephone system. TWX local loops use one TWX channel per voice channel. TWX trunks sometimes use six TWX channels per voice channel.

The TELEX hierarchy consists of concentrators (multiplexers) at the lowest level and two levels of switching centers. Each concentrator is associated with a secondary or primary level switch. There are 18 secondary level offices with varying degrees of interconnectivity between them. The nine high (primary) level switches are fully interconnected.

Subscribers to TWX or TELEX service may be connected directly to any of the switches in their respective hierarchies. Some TWX subscribers are connected to the TWX network via concentrators.

8.1.1.3 Switched Data Network

Although DATRAN has gone out of business, the DATRAN network is included in this report because it is representative of a form of telecommunication service optimized for data transmission. DATRAN provided inter-subscriber switched service via one switch located near Chicago (Brunswick, Ill.). This dial-up service used the ASCII code format for communicating the address of the called party to the switch. A privacy feature was offered whereby a subscriber provided DATRAN with a list of other subscribers lines which were allowed to call him. Calls to such a subscriber, made by subscribers not on the destination party's privacy list, were denied by the switching system.

8.1.2 Dedicated Service Networks

8.1.2.1 Network Structures and Services

Dedicated (or private line) service is a service whereby the common carrier provides one or more circuits for the exclusive use

of the subscriber. The service may be provided on a part time or full time basis. Many variations are available. These range from a single point-to-point circuit to an extensive multi-point network. A switching capability may be provided allowing the subscriber selective calling within his private network. The Federal Telephone System (FTS) and AUTOVON are switched dedicated networks provided by the common carriers which provide the public television switched network. Some non-government enterprises provide their own or lease switches (PBX or Centrex) to obtain multipoint switched dedicated networks. The common carrier provides the individual circuits and a means for relaying signaling information between switching machines. Other enterprises do not have switched networks, even for multipoint dedicated service (e.g., DATRAN's dedicated service).

In the latter case, the communication may be simply broadcast to all receiving stations or (particularly for data service), the identity of the called party is included in the message and each receiver is set to recognize which messages are intended for it. Common carriers may provide dedicated service to other common carriers whereby switched service, if provided, is furnished by the other carrier (e.g., INTELSAT provides only dedicated services and only to other common carriers).

Full time private line circuits tend to remain on the same set of facilities for relatively long periods of time. AT&T has estimated that one private line circuit may remain on the same physical route for two or three years, although there are areas, such as those undergoing plant modernization, in which the physical routing of a private line circuit might be changed with an average frequency of several months.

8.1.2.2 Examples of Dedicated Service Networks

Dedicated services are provided by the same common carriers that provide the public telephone switched service and also by a number of specialized common carriers that offer only dedicated service.

8.1.2.2.1 Dedicated Service Networks Sharing Facilities with the Public Telephone Switched Network

The common carriers that jointly provide the public telephone switched service also use these same facilities to provide dedicated services. The services essentially share transmission media such as microwave radio communications systems and satellites. The types of service offered include voice, television, data and teletype.

The dedicated services provided can range from a single circuit connecting two locations to a complete telephone network with full switched telephone service among a set of specific locations. Examples of the latter are the Federal Telephone System and the Department of Defense AUTOVON system. A common arrangement is the provision of dedicated circuits among a number of specific locations with switching services provided by the subscriber leasing the dedicated lines.

The teletype service offered by the public telephone switched network carriers differs from that offered by Western Union, the teletype common carrier in that the public telephone switched network carriers may provide only dedicated teletype service. The teletype signal may be applied directly to a regular voice channel or special equipment may be added to convert the teletype signal to a frequency-shift keyed (FSK) signal or to frequency division multiplex (FDM) several FSK signals for transmission over regular voice circuits.

A special digital service is provided by the Bell System which permits a subscriber to transmit digital information without conversion of the digital signal to an analog format. This service is provided by the Bell System's Digital Data System (DDS). The DDS consists of short haul transmission systems such as the T1 and T2 systems and a long haul microwave radio system known as Data Under Voice (DUV). Digital multiplexers using time division multiplex (TDM) techniques are used to combine the digital information from a number of subscribers requiring low or medium-speed digital services into one high speed digital bit stream for transmission over the short haul and/or long haul digital facilities.

8.1.2.2.2 MCI

A map of the MCI system is shown in Figure 5 (Courtesy of MCI Telecommunications Corporation). A combination of their own and leased facilities provides MCI with a coast-to-coast terrestrial microwave facility. MCI provides only private line service of which 85% is voice traffic. The rest is data (2400 to 9600 bps) in voice channels except for a small amount of teletype traffic. The microwave baseband signal consists of a frequency division multiplex (FDM) system with 4 kHz voice channel spacing. The baseband signal is used to frequency modulate (FM) a radio carrier frequency for transmission.

Data is carried over the regular 4 kHz voice channels using commercially available modems (2400 bps to 9600 bps) or the subscriber can supply his own. Teletype data is frequency division multiplexed and uses a two-tone FSK for each teletype circuit.

Subscribers are connected to the route by means of dedicated circuits leased from the local telephone company.



8.1.2.2.3 DATRAM

DATRAM provided an all digital backbone service between Chicago, St. Louis, Kansas City, Tulsa, Oklahoma City, Dallas and Houston. They had connections via the AT&T-supplied digital data service (DDS) to 26 other cities across the country. One DDS channel operated at a data rate of 1.544 Mbps (T1) and the remainder operated at 56 kbps. DATRAM provided their subscribers with a digital communication console (DCC) which connected the subscriber's digital lines to the local DATRAM office via a telephone company 4-wire, full duplex loop. Seventy-two percent of their traffic was private line, either multipoint full-period service or point-to-point full-period service. The remainder was switched (dial-up) service as discussed above. Many private line services were routed through the Brunswick switch using permanent non-switchable connections at the switch.

The backbone-carried data was at 44.66 Mbps in a 30 MHz bandwidth by means of an 8-phase phase-shift-keyed (PSK) modulation technique. The useful bit-rate for carrying subscriber traffic was 43.008 Mbps. The remainder was used for local and system-wide control, activity reporting and maintenance.

The first level of multiplex boosted the data rate to 56 or 168 kbps. DDS at 56 kbps and the first-level multiplex outputs were combined by the second-level multiplexer to produce data rates of 1.344 or 2.688 Mbps. Standard T1 digital data (via bit rate converters) and the second-level multiplexer outputs were combined by the third-level multiplex to produce a data rate of 21.504 Mbps. The fourth-level multiplexer was contained in the eight-phase PSK modem which could combine two 21.504 Mbps bit streams. First-level multiplexers were installed at distant cities in order to TDM local subscriber data rates (mostly 4800 bps or 9600 bps, although lower and higher data

capacity could have been provided up to 56 kbps) for transmission by the telephone company. The New York City office added a second-level time division multiplexer to bring the New York-to-Chicago channel rate up to the T1 data rate for the telephone company-supplied DUV link between these two cities.

Data was scrambled in the data sets or line drivers and again by a scrambler in the PSK modem. The purpose of the scramblers was to randomize the bit patterns in order to minimize the occurrence of single-frequency power peaks on the local loops and microwave links.

8.1.2.2.4 Western Union

Western Union provides dedicated voice, television, data and teletype service in addition to the switched teletype (dial-up) service discussed above. Western Union transmission facilities consist of a nationwide terrestrial microwave network (some cable is used in and near cities), the Westar satellite system and a few local teletype loops. (Nearly all local distribution is via the telephone carrier for the area). Figure 6 is a map showing the terrestrial microwave network and the location of the Westar earth stations.

Most of the present terrestrial microwave transmission facilities use frequency division multiplex with a 1200-voice channel capacity per radio channels. Various schemes are being considered for implementing a time division multiplex capability.

The Westar satellite provides dedicated message and television service for all 50 states. Each satellite has 12 transponders. The current traffic is all voice channel (4 kHz) traffic. Each transponder has a capacity for 1200 one-way voice channels using FDM/FM or

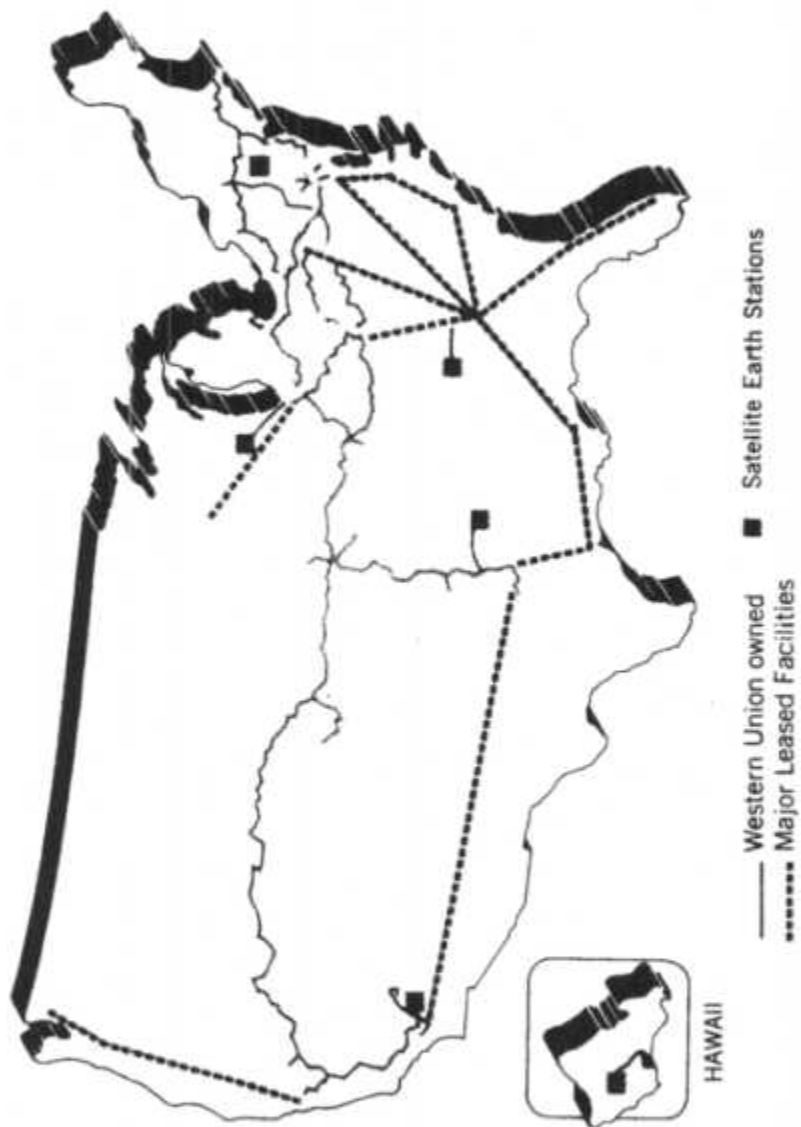


FIGURE 6
NATIONWIDE TRANSMISSION NETWORK

one television channel using FM modulation or up to 50 Mbps using PSK modulation. Teletype service is provided by FDM multiplex with frequency-shift-keyed (FSK) modulation into a voice channel. A second service offered is FDM/FM multiple access whereby a number of separate rf carriers would share a transponder. In the case of two carriers per transponder, each rf channel is capable of supporting 360 one-way voice channels. A third service offered is a TV receive-only capability to individual subscribers whereby the receive terminal could be located on the subscriber's own premises. The Public Broadcasting Service (PBS) will make use of this service and will provide their own earth stations (both transmit and receive). Yet another service is the provision of a "Transportable" earth station which can be set up anywhere within their earth coverage area.

8.1.2.2.5 INTELSAT

INTELSAT provides international dedicated service. Unlike other carriers, INTELSAT owns only the satellites. Earth stations are owned by the communication carriers in the individual countries although INTELSAT specifies earth station requirements which must be met by the carriers and provides additional advice and assistance as appropriate.

TV service is provided by splitting a 36 MHz channel into two 17.5 MHz TV channels. Digital service is provided on a single channel/carrier basis at a data rate of 64 kbps using a 4-phase PSK modulation. About 80% of the traffic is standard FDM/FM channels. Subscribers have a wide choice of bandwidths. Available bandwidths range from 2.5 to 36.0 MHz, providing from 24 to 1092 one-way voice circuits.

8.1.2.2.6 COMSTAR Satellite System

The COMSTAR satellite system will provide a domestic dedicated service similar to that provided by INTELSAT for international service.

The earth stations are owned by the local common carriers (AT&T and GTE). Service is to be provided to all 50 states and Puerto Rico.

Except for some private line service for the U.S. government, the satellites will act as relays for the public telephone switched network. Each satellite will have 24 transponders (12 active at any one time). Each transponder will be capable of handling 1200 one-way voice channels using FDM/FM or one NTSC color TV signal using FM modulation or one 64 Mbps data channel using a TDM/PSK multiplex/modulation technique.

AT&T earth stations are located at Hawley, Pa., Woodbury, Ga., Hanover, Ill; and Three Peaks, Cal. The GTE earth stations are located at Homosassa, Fla., Triunfo Pass, Ca; and Sunset, Hawaii.

8.1.2.2.7 Satellite Business Systems

Satellite Business Systems (SBS) is a consortium composed of COMSAT, IBM and Aetna. SBS proposes to provide private line switched service (voice, data and image) to private business and government agencies. Each subscriber will control his own intra-company network via earth stations on or near the premises of the various locations with which the subscriber wishes to communicate. All earth stations will be owned and maintained by SBS and access restricted to SBS employees only.

Data will be transmitted in bursts at a rate between 40 and 50 Mbps. A maximal-length code linear feedback shift register will be used to randomize the bit patterns in order to minimize the occurrence of single-frequency power peaks. The randomizer could be replaced (at the option of the subscriber) with cryptographic devices to provide higher levels of privacy or information security.

Each earth station will be provided with a satellite communications controller (SCC). The SCC provides the subscriber with interfaces (known as ports) for voice and data. Voice traffic will be analog-to-digital converted and both voice and data will be compressed by taking advantage of pauses which occur naturally. The bit error rate (BER) for the basic system is being designed to provide for good voice quality. Since data generally requires a lower bit error rate than voice, forward error correction techniques will be used to provide the transmission quality required for data. The SCC will also provide the necessary signaling functions as well as assembly of the individual inputs into the burst to be transmitted and disassembly of the received bursts into the components to be delivered to the various output ports. The sequence by which inputs will be assembled into the burst will be variable, depending on a priority system as well as the time of arrival to each input port.

The particular technique to be used for transmission is called time division multiple access (TDMA) with demand assignment. The TDMA technique consists of assigning time slots to each earth station within the overall fixed frame length (the basic repetition period required to accommodate all time slots). All timing is referred to the satellite. A variation of this technique is being considered by SBS. Instead of time slots being assigned on an earth station basis, time slots would be assigned the group of ground stations making up a particular subscriber's network. The subscriber would subdivide his time slot into many small time slots and could dynamically change the assignment of the small slots in response to the changing traffic patterns on his own network. Demand assignment refers to the ability of a subscriber to temporarily increase his network capacity by requesting (and receiving) an extra time slot set aside by SBS in their overall frame for such purposes. Of course, as time goes on,

it is expected that a particular subscriber may outgrow the capacity of his assigned time slot. In this case, SBS would assign him an additional time slot which might not be contiguous with his existing time slot.

8.1.3 Mobile Radio Systems (Public Service and Citizen Band Radio)

A number of public service agencies, private businesses and individuals use mobile radio communication systems that operate in the Public Service Radio Bands (30 - 50, 147 - 174, and 450 - 470 MHz). The principal public service users are police, fire, ambulance and marine radio operators. Private business system users include, among others, transportation companies, hospitals, medical professionals and taxi services. Many people use Citizens Band Radio (27 MHz band) for a variety of applications such as mobile communications for large farming operations.

Mobile radiotelephone operators provide service to those who do not want to operate their own networks, although many users own their own mobile radio equipment. Mobile radio telephone services (one-way paging as well as two-way voice services) are provided by many independent companies in addition to the regular telephone companies. All companies use the Public Service Radio bands. Specific channel (frequency) assignments are made by the FCC. Any one radiotelephone company will usually be assigned several channels in order to provide the capability to handle several conversations simultaneously. The location and operating characteristics of base stations must be approved by the FCC. Several base stations may be operated by a single company in a single metropolitan area in order to provide effective service out to a range of 20 to 25 miles from the metropolitan center.

A subscriber may have either half-duplex (push-to-talk) or full duplex service. An individual subscriber's radiotelephone set will usually have a capability to access at least two channels.

The radiotelephone company interconnects with the local telephone company either manually by means of an operator and switchboard or automatically by means of a direct dial access.

8.2 Vulnerability of Electronic Communications Systems

This section summarizes the analyses of the vulnerability of electronic communication systems to electronic interception. The detailed analyses are presented in the appendices in Volume II of this report.

The presentations of the analyses summarized are grouped according to the following four categories:

- a. The analyses of the vulnerability of the communications systems as a function of the transmission media employed,
- b. The analyses of the effects of multiplexing and signaling on interceptability,
- c. The analysis of the vulnerability of the communications systems as a function of the network types, and
- d. The analysis of the effort required to extract information from communications traffic.

8.2.1 Vulnerability of Communications Systems as a Function of Transmission Media

This section is generally divided into two basic parts. The first discusses the vulnerability of wire and cable communications systems and the second, radio systems. The part on radio systems covers the analyses of terrestrial and satellite microwave systems and the citizens band, mobile telephone and public service radio systems.

8.2.1.1 Wire and Cable Communication Systems

The discussion of wire and multi-pair cable communications systems begins with a discussion of the physical characteristics of wire and cable systems. This is followed by analyses of the vulnerability of "non-carrier" and "carrier" wire and multi-pair cable communications systems and "carrier" coaxial cable systems. The section closes with a discussion of the detectability of attempts to intercept communications over wire and cable systems.

8.2.1.1.1 Physical Characteristics and Vulnerability of Wire and Cable Plant

This section presents a description of wire and cable construction and installation techniques, the construction of subscribers' local loops using wire and cable and an assessment of the vulnerability of the wire and cable plant to the penetration necessary to acquire signals.

(1) Relative Vulnerability of Cables as a Function of the Type of Installation

Wire and cable plant may be typed according to the three primary methods of physical installation. These are:

- (a) Aerial wire and cable - wire and cable attached to a pole or the cross-arms of a pole;
- (b) Buried cable - cable buried directly in the ground;
- (c) Underground cable - cable placed in underground conduits.

All three types of cable have their advantages and disadvantages from the point of view of the interceptor. Although one type might be more conveniently penetrated than another, the risk of being observed during the penetration may be greater. Some of the advantages and disadvantages are described below:

(a) Aerial Wire and Cable - Aerial wire and cable are by far the most easily penetrated of all three types. Besides being exposed to inductive (placing a coil of wire around or very close to a wire to intercept the magnetic field induced along the wire by the information signals passing through the wire) or "surgical" penetration (cutting through a cable, stripping the insulation and connecting wires), there are numerous "appearances" such as suspended or pole-mounted terminal housings, splice cases and ready access enclosures. All of these appearances are neither locked nor alarmed and present opportunities for convenient and speedy tapping. The aerial conductors may be insulated wire or uninsulated wire (also known as "open wire") or cables. The only drawbacks to the penetrator

are that aerial cable is pressurized much more frequently than the other types and attempts at unauthorized monitoring may be readily visible.

(b) Buried Cable - Buried cable seems to be the second most easily accessed type and perhaps may be more convenient for establishing long-term monitoring points than other types. Buried cable has fewer appearances than any other type but it is less frequently pressurized than the others. In fact, common carriers have, of late, taken to burying "filled" cable, which cannot be pressurized. Filled cable is usually equipped with "encapsulated cable closure" appearances containing splices, loading coils, and terminals. The encapsulated closures are slightly less convenient for ready monitoring than the older types of terminal housings inasmuch as they contain filler compound which must be removed before the pairs can be tapped.

Since buried cable is often neither pressurized nor protected by conduit, it can be accessed anywhere along its length by digging a hole where a surgical penetration can be performed. The fact that such a hole can be dug, the tap made, and the entire installation reburied, makes the arrangement ideal for the establishment of permanent, undetectable monitoring points in isolated areas. However, it should be noted that older buried cables were frequently brought above-ground to terminal housings for the purpose of splicing and to provide future access points for cable branching, expansion and distribution. Consequently, in many older routes, the convenience of terminal exposure is provided on buried cable.

(c) Underground Cable - Underground cable is not as vulnerable along its entire length as aerial or buried cable. Underground cable does have frequent splice, loading coil and terminal appearances in manholes and conduit boxes positioned periodically along its length. It does not seem to be practical to extend

a monitoring pair from a manhole tap to a more conveniently located listening post, especially since underground cable lies mostly under city or suburban streets and its appearances are frequently collocated with other utilities. A monitoring station could conceivably be kept in a manhole, but the interceptors would be seen entering and leaving which presents a significant risk of discovery. However, there are many scenarios for monitoring this type of plant. In the past, penetration of underground cable has been perpetrated under the guise of public works or utilities projects.

(2) Distribution System Cable Hierarchy

In addition to the means of physical installation described in the last few paragraphs, subscriber loop cable can be categorized according to its place in the distribution plant hierarchy. Figure 7 is a diagram of the cable hierarchy.

The outside plant portion of a subscriber loop is bounded on one extremity by the point at which the wire enters the subscriber's residence and on the other by the point where the loop cable is connected to the central office (CO) cable. Figure 7 identifies the elements of the subscriber loop. These are as follows:

<u>Loop Section</u>	<u>Cable Element</u>
(a) From Residence to the Distribution Terminal	Drop Wire (Aerial)* Service Wire (Buried)*
(b) From the Distribution Terminal to the Branch Feeder Terminal	Distribution Cable Distribution Wire*

* "Wires" are defined here as one or two twisted conductor pairs within a single insulated covering (no sheath).
"Cables" or "Multi-pair cables" are defined as aggregates of six or more twisted conductor pairs within a single sheath.
"Coaxial cable" refers to an aggregate of coaxial pairs or "tubes" within a single sheath. A coaxial cable may consist of a single tube.

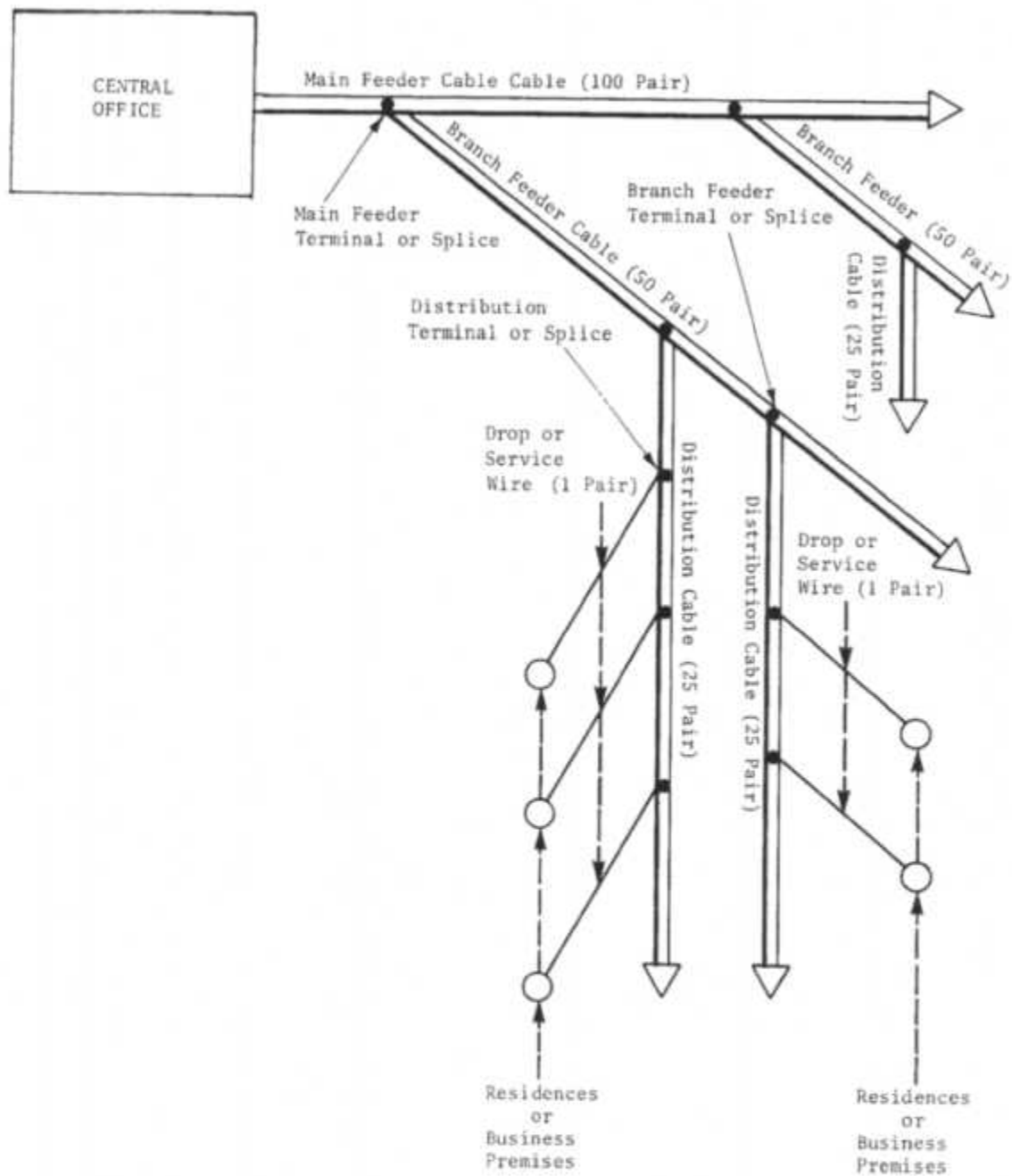


FIGURE 7
DISTRIBUTION PLANT CABLE HIERARCHY

- | | |
|--|---------------------|
| (c) From the Branch Feeder Terminal
to the Main Feeder Terminal | Branch Feeder Cable |
| (d) From the Main Feeder Terminal
to the Splice in CO | Main Feeder Cable |

Distribution cable is the part of the outside plant to which the customer's drop or service wire is directly connected. Feeder cables interconnect distribution cable with the CO. Main feeder cables are high capacity backbones into major service areas. The branch feeders connect the distribution cables to the main feeder.

In some cases not all elements of the cable hierarchy need be present. Main feeder cables can serve as both main and branch feeders. In smaller telephone companies, or in rural areas, main or branch feeder cables may serve as distribution cables for those portions most distant from the CO.

(3) The Construction of Subscriber Loops

A subscriber loop can consist entirely of a single type of plant, such as aerial cable, or it can be made up of all three types in tandem. In fact, most loops are rarely constructed of only one type of facility; this results in additional appearances at transition points.

A cable carrying subscriber loops may also contain inter-switch trunk circuits, private line circuits and cable carrier systems. This might make the job of locating a specific subscriber loop in a multi-pair cable a little more time-consuming.

(4) Cable Appearances

Each type of outside plant may have anywhere from a very few to a multitude of "appearances" where the individual cable pairs are brought out of their bundle within splice cases, terminal

housings or other types of terminal enclosures. Such appearances may occur in manholes, in conduit boxes, suspended from messenger cables, mounted on poles, mounted at the surface of the ground, attached to the walls of buildings, or buried in the ground. Cable appearances represent convenient points where the interceptor can access individual pairs without using surgical techniques.

Cable appearances may be inserted at any of the following locations along a route:

- a. subscriber distribution points;
- b. cable/wire route junctions (main and branch feeder junctions, branch and distribution cable junctions);
- c. junctions between buried/underground and aerial cable;
- d. cable loading* points;
- e. cable splice points;
- f. potential (not in use) subscriber distribution or cable junction points;
- g. pole or manhole mounted repeater points;
- h. any additional points necessary to ensure a maximum appearance separation of 5000 feet along the cable route.

Individual telephone companies may not adhere consistently to the above uses of appearances and most will deviate from them on nearly every route (especially in rural areas), but the above types of cable appearances are represented in the literature as "good outside plant construction practice." Of late, Bell has been cutting down on the number of above ground appearances in their new plant.

* Points along the length of a cable at which inductive coils are placed in order to improve system performance for voice traffic

When terminal housings, terminal enclosures, ready-access enclosures, splice cases and the like, are viewed in the context of unauthorized interception, they appear as weak spots in the communications network, because none of these enclosures are locked or otherwise purposely protected from illegal entry. They are all fastened shut with simple fasteners that can be removed with readily procurable tools.

(5) Pressurized Cable

The hazards that water, or even moisture, present to pulp- and paper-insulated conductors are a major maintenance problem. In order to prevent water and moisture from adversely affecting service, the Bell System pressurizes almost all of its non-filled cables. The non-Bell telephone companies tend to pressurize mainly their pulp- and paper-insulated cables.

High capacity coaxial cable routes are always pressurized on a per-tube basis. In fact, in most high capacity coaxial systems, even the repeaters are hermetically sealed and pressurized.

Pressurization of cable presents a problem to would-be penetrators, second only to burglar alarms, inasmuch as most pressurized systems have "contactors", or other transducers, spaced out along the cable that automatically inform central office maintenance forces when the cable has been significantly breached. However, not all types of cables respond identically to punctures. For example, pulp- or paper-insulated cables respond very slowly and it is estimated that if a point of entry is judiciously chosen, the central office would not know of a large puncture in less than 4 hours. Plastic-insulated conductor (PIC) cables require at least a half hour and coaxial cables less than that. However, not all PIC and coaxial routes are engineered for minimal contractor/transducer spacing so in some cases the times would be longer.

Not only would the location of a puncture need to be judiciously selected but the time must also be carefully planned because there is a "reaction" time involved. The reaction time is the interval between the time the central office forces learn of the leak and the time maintenance people reach the location of the leak. This study estimated that for an interceptor with knowledge of the maintenance philosophy commonly in use by telephone companies, the proper choice of the place (halfway between contractors) and the time (Friday night) of penetration could result in at least 70 hours of uninterrupted monitoring time on all but coaxial routes. The general thrust of cable maintenance philosophy in most organizations is to put off costly cable repairs for as long as possible (if service is not interrupted) and accomplish such repairs on a routine or scheduled basis.

It is important to point out that cables can be plugged, and equipment and sections by-passed, leading to the following viable possibilities for a would-be interceptor to avoid detection while penetrating a cable:

- (a) Existing by-pass valves at plugs could be shut and the cable pressurized from a portable source during penetration.
- (b) A permanent penetration could be installed by inserting plugs at both sides of the cable breach and bypassing it with a valve and tube arrangement. The technique for doing this is well documented, and the proper tools are readily available.
- (c) The penetrator, with specially designed tools, could breach the cable, insert monitoring attachments, reseal and repressurize the cable before the central office detects a significant pressure drop (for pulp- and paper-insulated cables).

There are any number of similar tactics that, when coupled with judicious selections of time and place, would render detection impossible.

Many pressurized cables are not alarmed at all, making them particularly vulnerable to unauthorized monitoring.

8.2.1.1.2 Vulnerability of Non-Carrier Wire and Multi-Pair Cable Systems

The analysis of the vulnerability of non-carrier wire and multi-pair cable systems begins with an analysis of the subscriber loop plant and is followed by an analysis of the vulnerability of non-carrier trunk cables.

Vulnerability of Subscriber Loop Plant

The results of this study indicate that in nearly all cases, the subscriber loop outside plant is the optimum place for an interceptor to practice unauthorized monitoring. For example, in order to intercept a single voice conversation carried over a wire or cable pair, one needs only some wire terminated with alligator clips, a battery powered amplifier with a high input impedance, and a set of headphones (or at most a recorder) as depicted in Figure 8. (Additional strategies and equipment arrangements for intercepting signals other than voice communications are described in Section 8.2.3.) There are four primary reasons for this conclusion:

- (a) The subscriber loop outside plant is composed of highly accessible, non-carrier cables or wire-pairs;
- (b) As one moves from the central office towards the subscribers, the number of wire-pairs contained within each cable of the distribution plant diminishes, making it easier to target individual stations;
- (c) The inexpensive taps can consistently yield very high signal-to-noise ratios permitting the accumulation of more usable information;

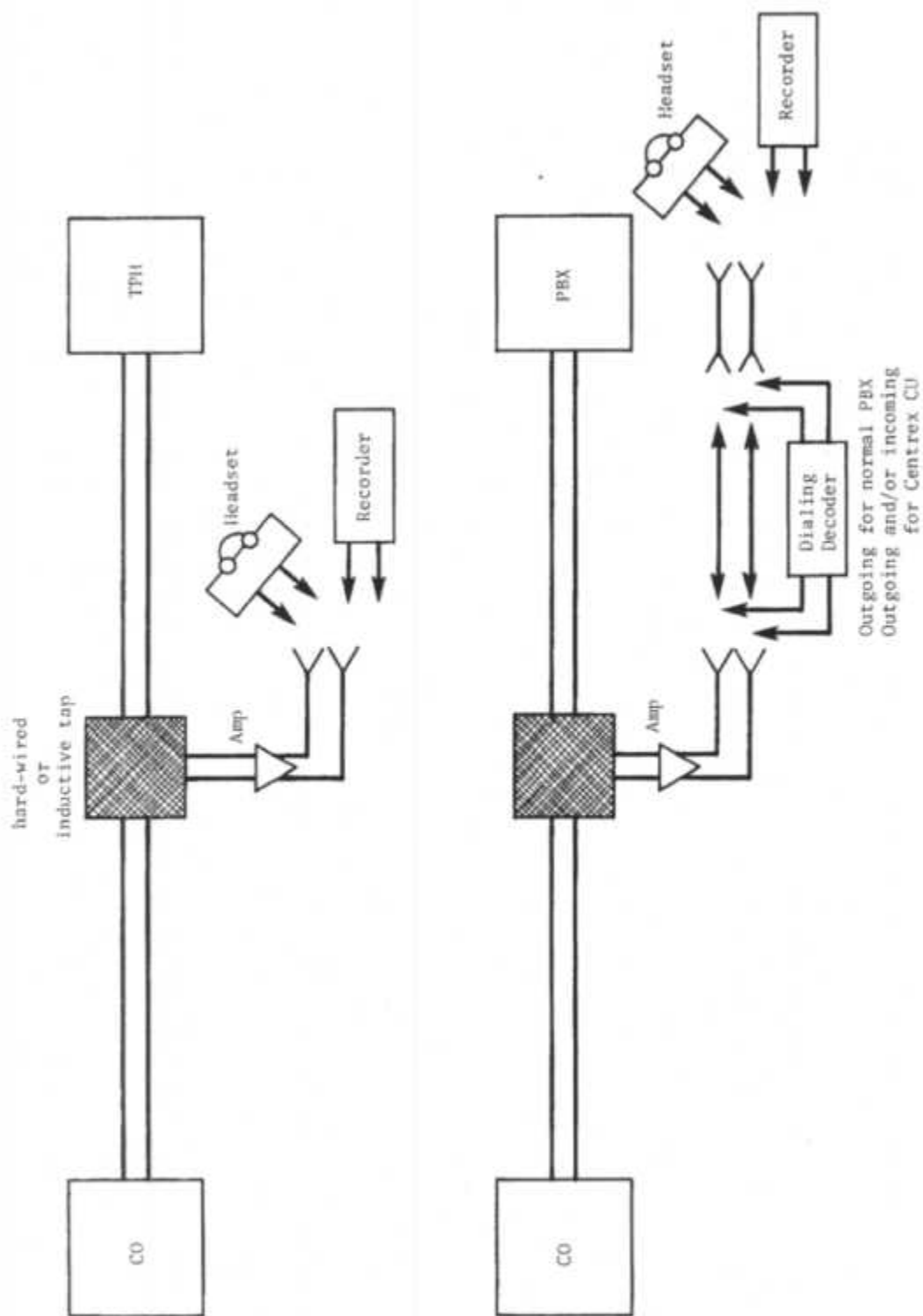


FIGURE 8
SUBSCRIBER LOOP INTERCEPT ARRANGEMENTS

- (d) The unique assignment of wire-pairs to specific subscribers or premises permits easy targeting of individuals, or at least narrowing down the communications traffic to that of a small group of individuals.

It is envisioned that continuous taps of aerial wire would not be continued as "man on the pole" arrangements. Rather a long, unobtrusive wire pair (or pairs) would be run from the tap point to a vehicle, structure, or other convenient hiding place where the interceptor could carry-out the monitoring unnoticed. Taps have even been run to public telephone booths for dialed-up connections to a well equipped listening post.

The practice of multipling,* which results in several lengthy intentional taps being appended to many loops, creates opportunities for monitoring a subscriber loop at a location far removed from the customer's premises. Thus interception at a multipling bridge-tap or along the cable or wire connected to the bridge-tap would minimize an interceptor's exposure. The interceptor could, by means of logical step-by-step procedures, trace the distribution cable to multipling points and sequentially check the local count to determine whether the pairs of interest were multiplied. He could then establish his tap on a point remote from the customer premises if the pairs were indeed bridged.

*Multipling: Either the intentional placing of multiple junction points along a subscriber loop wire-pair for the convenience of serving future subscribers or the residual junction points resulting from previous service connections along the wire-pair which have not been disconnected (the practice of multipling creates multiple accesses to a single line).

In a broader sense, the term "multipling" refers to the practice of making the same cable wire-pairs available at a sufficient number of points (without necessarily making any physical connections) to provide for multi-point service, party line service, and potential subscriber changes with minimal cable rearrangement. In this report, "multipling" always refers to the physical connections (known as a bridge-tap), and the "count", or "home count", is the general plan or pattern used in a "home" area to maintain consistent pair designation and usage between the CO and the subscriber.

The fact that similar count patterns are used in most telephone companies means that an interceptor having expertise in the color identification of cable pairs and the philosophy of the count patterns could trace a subscriber line through numerous cable appearances. He could start at the subscriber's drop wire and work toward the feeder cables, or vice versa.

The use of "tracer" calls* to the subscriber and the subsequent application of low level tracer tones would permit an interceptor to locate a subscriber's pair anywhere in the entire subscriber loop plant. This tracing would be done for the purpose of locating unused bridge-tap, or cable appearances remote from the subscriber's premises, in order to monitor at an inconspicuous location, or to change one's location if detection became imminent.

Although some subscriber loop pairs bear carrier systems, rather than individual voice conversations, the percentage of such plant

* Tracer calls are calls (usually brief) made purposely to a subscriber station and marked with a distinctive signal so that interceptors can scan through pair appearances to locate the specific pair receiving the call.

is rather small and the interception of those communications requires only a demultiplexer in addition to the simple apparatus mentioned previously.

Vulnerability of Non-Carrier Trunk Circuits

The above discussion of the vulnerability of subscriber loop circuits is generally applicable to non-carrier trunk and toll cables as well. The only significant differences are:

(1) There are usually many more pairs in a trunk/toll cable than in subscriber branch feeder and distribution cables (although sometimes trunks are routed through main and branch feeder cables).

(2) There are fewer above ground appearances because most trunk/toll cable is the buried type outside of cities and the underground type within cities. By the same token, the vulnerability of long stretches of buried cable in isolated areas presents opportunities to interceptors. However, some of the fastest reacting, most modern computerized gas pressure alarm systems are installed on trunk/toll cables.

(3) There are few bridge-tap access points on the trunk/toll plant.

(4) Long trunk/toll cable routes can often be traced cross-country by a well-manicured right-of-way, frequent signs warning the public of the cable's presence, and occasional repeater huts (because some of the pairs are usually dedicated to a multiplex system). Repeater huts are equipped with open-door alarms that inform the central office maintenance personnel when the hut has been entered. A few medium length toll routes are composed exclusively of thick aerial cables which also can be easily traced from pole to pole.

(5) The trunk circuits in such routes are not usually dedicated to any specific subscriber, but rather interconnect switching machines and are used as described in Section 8.1.1. This means, of course, that, except for random snooping, a signal-decoding capability must accompany the more prosaic monitoring amplifiers/headsets mentioned above. Accordingly, trunk selecting and monitoring arrangements would probably be several times more costly than the equipment required to intercept communications on subscriber loops.

To summarize, the interception of communications on multi-pair trunk cables is somewhat more costly and complicated than the interception of communications on subscriber loop cable because of the larger numbers of pairs encountered, more sophisticated alarm systems, and signaling decoding problems. However, because of the exposure of long stretches of buried cable in isolated areas and the lack of the visibility that accompanies attempts on subscriber loop plant, it is concluded that it would be easier to install permanent taps without detection providing reasonable efforts were made to spoof the gas pressurization system.

8.2.1.1.3 Vulnerability of Carrier Wire and Multi-Pair Cable

Cable-carrier trunk circuits fall into the following categories:

- a. short-haul systems (within urban areas) using frequency division multiplex (FDM) and time division multiplex (TDM),
- b. long-haul systems (between urban areas) using frequency division multiplex (FDM), and
- c. carrier subscriber loop circuits

The multi-pair cables used with the short-haul systems are usually specially treated wire-pairs of main feeder cables and branch feeder cables. Hence, most of the conclusions regarding the accessibility of short-haul systems are similar to those expressed

under "Vulnerability of Non-Carrier Wire and Multi-Pair Cable Systems." The peculiar problems pertaining to the "trunk" character of these circuits are similar to those addressed in the section "Vulnerability of Non-Carrier Trunk Circuits". The only additional attributes to be addressed are as follows:

- (1) Demultiplexers must be added to the interception equipment discussed above in order to access a single voice channel.

- (2) High-frequency wide-band line repeaters are occasionally inserted in the longer multiplexed routes. TDM systems such as T1-carrier need regenerative repeaters every 6000 feet. These repeaters are sometimes installed in central offices but more often, of late, have been mounted in manholes. These repeaters present additional appearances for potential communication interception.

The long-haul cable-carrier trunk communications ride on pairs which are subject to the same considerations posed for long-haul non-carrier trunk circuits except for the increased complexity resulting from the demultiplexing requirement, as stated in items (1) and (2), above. Circuits on long-haul systems are more likely to be carried by FDM systems equipped with line repeaters.

In summary, the interception of communications on short-haul and long-haul cable-carrier trunk circuits is somewhat more costly and complex than non-carrier trunk circuits because of the demultiplexing equipment required. However, long-haul cable carrier trunk interception is similar to the long-haul non-carrier trunk interception in that long stretches of buried cable in isolated areas present abundant opportunities for sophisticated, virtually non-detectable incursions where relatively permanent taps could be established.

One decisive drawback for the interceptor is that greater expertise must be exercised in the design and application of penetration devices because the wideband FDM/TDM signals are easily affected by bridged devices. An inexpert attempt at monitoring could affect the signal in such a way that either central office alarms would be activated or service would actually be degraded or interrupted.

Figure 9 is a block diagram depicting the tapping of both carrier and non-carrier cable trunk circuits.

Carrier subscriber loop circuits will not be covered here since only a small portion of the telephone loop plant is involved. The problems encountered in intercepting communications on carrier loop plant resemble those posed in intercepting communications over carrier wire and multi-pair cable trunk circuits.

8.2.1.1.4 Vulnerability of Carrier Coaxial Cable

Approaches to intercepting communications on coaxial cable differ markedly from those previously addressed for wire/multi-pair cable communications. Even the tap methodology calls for a considerably different approach. The clamp-on inductor and the soldered/alligator-clipped connection which can easily be used for acquiring communications signals on wires are not suitable for the tapping of coaxial cable tubes.

The standard coaxial cable used with what is called the L4 System consists of 20 coaxial tubes spiraled around 47 wire pairs (19 and 16 gauge) and 10 non-paired conductors (19 gauge). The 47 pairs and 10 conductors serve as the cable core. The 20 coaxial tubes and the wire core are enclosed in a lead-polyethylene-paper (lepeth) sheath. Each coaxial tube consists of a .1003 inch copper center

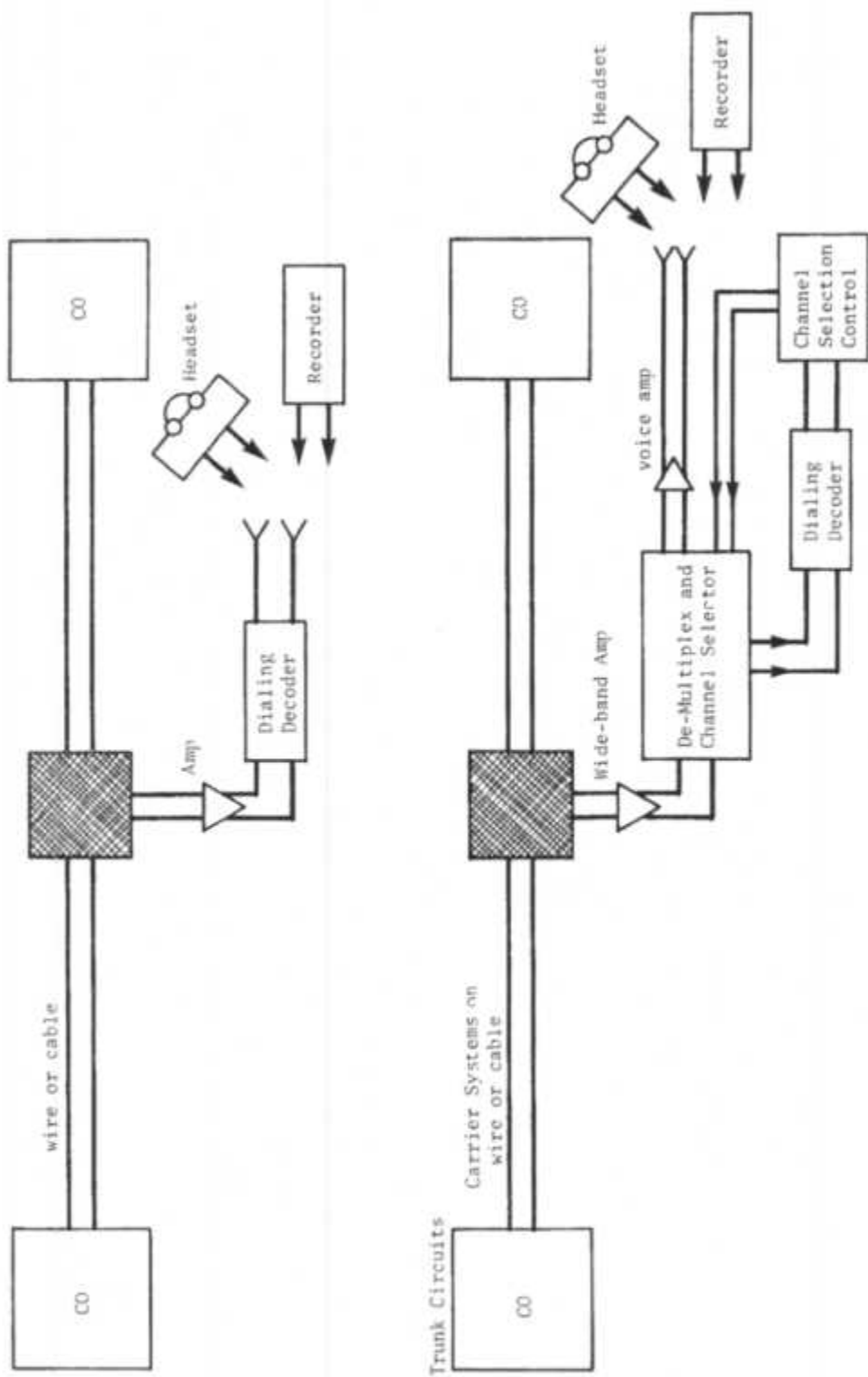


FIGURE 9
TRUNK CIRCUIT INTERCEPT ARRANGEMENTS

conductor which acts as the hub for a string of polyethylene discs spaced one inch apart, longitudinally along the cable. The discs are surrounded by a copper outer conductor which is a tube closed longitudinally along the cable. The copper outer conductor is covered with a spiraled layer of steel tape.

The signal is transmitted as a high frequency voltage difference between the center conductor and the copper outside conductor. In general, repeaters on coaxial systems are spaced between 1 and 4 miles apart, depending on the system in use. The repeaters are powered by DC voltage on the center conductor of each coaxial tube. This voltage can be as high as several thousand volts.

The cable is pressurized and has a fast-acting gas pressurization alarm system which quickly reveals any significant cable punctures. Actuation of the alarm results in crews being immediately dispatched to determine the cause.

When acquiring communications signals from a coaxial system it is impossible to elicit any meaningful signals (except at the repeaters) without first opening the lead sheath and separating the individual tubes. Studies have shown that the amount of loss the information bearing signal suffers when measured by induction coils on the outside of the steel tape is too large to yield a usable signal-to-noise ratio.

At present, too little is known about the noise level on the copper outer conductor (after the steel tape is peeled off) to determine whether useful signal-to-noise ratios can be achieved using physically manageable induction coils. Outer conductor noise is a complex signal resulting from the periodic common grounding of all the outer copper conductors plus spurious

earth currents. The loss that the information signal suffers, when measured by a reasonably sized induction coil on the outside copper conductor is quite large although it still may be usable. However, the total useful signal-to-noise ratio is determined by the complex conductor noise currents. Making the use of this technique for interception is highly questionable.

An alternative method would involve the development of a specialized precision tool which would puncture the steel tape and copper outer conductor, seal the resultant hole instantaneously so that gas pressure would be maintained, and insert a probe near or onto the center conductor to directly tap the signal without shorting the repeater power supply to ground. This would probably yield an extremely high signal-to-noise ratio. Great care would have to be exercised in the design and use of this device because of possible adverse effects on the gain-frequency response of the cable. Such effects would be noted at the central offices.

Another approach to interception involves entry into the repeater manhole or auxiliary hut and monitoring directly on the test jacks of the repeaters. This would present difficulties to the penetrator because some of the manholes and all the auxiliary repeater huts have burglar alarms which are extended by telemetry to responsible central offices whose forces react immediately after an incursion. In addition the manholes and repeaters are securely locked against intrusion. The entire cable/repeater/apparatus case system is pressurized and the individual apparatus case must be isolated before the twin test jacks can be accessed. Accordingly, it appears that only a very sophisticated approach backed up with considerable expertise would permit monitoring at coaxial cable repeater points.

High capacity coaxial cable systems utilize wideband signals which can be very easily degraded by poorly designed or inexpertly used monitoring equipment. In this event, the degree of degradation can vary between triggering of pilot* alarms to interruptions to service so that a high level of expertise must be exercised in the design and use of coaxial interception equipment.

A total coaxial cable interception equipment complement would consist of:

- (1) Digging, cable entry and tube spreading tools;
- (2) Specialized tapping and tube sealing or plugging and bypass devices;
- (3) Wideband amplifiers and demultiplex equipment;
- (4) Trunk signaling decoders;
- (5) Voice channel amplifiers and monitoring (or recording) devices;
- (6) Van or other listening/recording post;
- (7) An optional microprocessor controller.

The total cost of these devices would probably be at least a couple of orders of magnitude greater than the simple subscribers' loop intercept equipment.

Entry at a repeater would eliminate items (1) and (2) but greater expertise and sophisticated station entry gear would be required. The penetrator is also limited by available space in the manhole and lack of commercial AC power.

* Pilot signals are single-frequency waveforms transmitted outside the frequency bands occupied by voice channels in multiplex systems for the purpose of sensing system gains, automatic adjustment of repeater gains, synchronizing demodulation processes, etc.

It is concluded that it is far more difficult and hazardous to monitor a coaxial cable route than a multi-pair cable route or any other communications media.

8.2.1.1.5 Interceptor Detectability

Interceptors of cable communications systems will be subject to exposure by several different modes of detection, such as:

- (1) Being observed during installation or use of the tap;
- (2) Accidentally activating system alarms;
- (3) Having tap arrangements discovered during telephone company testing deliberately aimed at such disclosures;
- (4) Having tap arrangements discovered as a result of accidental system degradation resulting from the use of poorly designed or inexpertly applied interception devices.

Visual Detection

The risk of being visually detected will be greatest in urban or suburban areas where larger numbers of people are on hand to observe the penetration. There are a number of factors which will influence the degree of risk at any given time, such as:

(1) The public's attitudes in general regarding communications security (i.e., Has anything happened recently to increase awareness of such security?).

(2) The attitudes of specific groups regarding communications security (e.g., industries which have the most to lose from breaches in security may make their employees more aware of potential interception activities). This would make the risk a function of the location of the penetration and require the interceptor to remote himself as quickly as possible (e.g., by the use of multiplying bridge-taps or other tap extensions to secure listening posts).

(3) The skill with which an interceptor can disguise or cover his activities and camouflage his listening post (or perhaps remove it to a remote location).

(4) The level of alertness exhibited by telephone company personnel and the law enforcement agencies (also a function of training and social climate).

(5) The type of communications plant involved in the penetration (e.g., aerial cable vs. penetration in a manhole).

On the other hand, in rural or isolated areas it is probable that the interceptor could establish a very elaborate and sophisticated cable listening post with little risk of accidental detection. This is not to say that there is no risk of detection, since cable routes are patrolled by telephone company personnel, and when confronted time after time with a structure or ground disturbance of an even slightly anomalous nature, the maintenance forces may gradually become aware of the existence of a listening post. Again, this is a function of personal attitude derived from experience, training and social climate regarding the subject of communications security.

Activation of System Alarms

(1) Intrusion Alarms

Auxiliary repeater huts and certain repeater stations in manholes along cable- and coaxial-carrier routes are alarmed to prevent unauthorized intrusion. Maintenance forces react quickly to inform law enforcement authorities at the slightest hint of unauthorized entry. It is probable that these alarms could be defeated by some combination of sophisticated entry equipment and penetrator expertise, but the alarms make what might appear to be a very convenient monitoring point (the carrier system repeater) somewhat less attractive.

(2) Gas Pressure Alarms

All high capacity coaxial cables and a significant percentage of multipair cables are pressurized. When a penetrator punctures or opens a pressurized cable, eventually an alarm will be set off in the central office maintenance center followed by the dispatching of maintenance forces to repair the cable.

The older cable routes are equipped with devices which activate when the pressure reaches a low threshold. It is impossible to ascertain what is happening on such a route until the pressure at a contactor falls below the threshold value (unless accurate observations of the gas flow are made at the point where the gas is fed to the cable). This system can be easily spoofed by interceptors in a number of ways as described in the previous discussion of pressurized cable.

The newer cable routes (especially in the Bell System) are equipped with transducers. The outputs of the transducers may be fed to computerized systems which not only are programmed to alarm at variable thresholds but can also pinpoint the location of a breach in the cable by processing the pressure gradients measured across several transducers as a function of time. These systems can be set to react more quickly than the contactor type systems. However they also can be spoofed by the methodology described in the discussion of pressurized cable. In any event, coaxial cable systems show pressure losses at transducers much more quickly than multi-pair cable systems, hence, they must be treated more gingerly by prospective interceptors.

(3) Power System Alarms

The repeaters of most modern carrier systems are powered remotely from central offices over the cable pairs of multi-pair cables or the center conductors of coaxial tubes. Anything which significantly disturbs the values of these circuits/voltages immediately triggers an alarm in a responsible central office. Thus a penetrator who inadvertently shorts a pair or central conductor to ground would immediately inform the central office of an anomalous condition. In coaxial systems, even a resistance imbalance on one of the two tubes (transmit and receive) used to close the power loop can trigger a power system alarm.

(4) Pilot Alarms

On multiplex systems it is quite easy to perturb the gain-frequency response of the system by bridging an improper impedance across the pair or the coaxial tube. If excessive loss is created at a pilot frequency, an alarm associated with the respective pilot will be triggered.

Deliberate Testing to Detect Interception Apparatus

There are a number of tests which can be done deliberately to disclose the presence of unauthorized connections to cable pairs or coaxial tubes. The degree of effectiveness of such testing depends on the sensitivity of the telephone company test equipment and the expertise exercised in the design and use of interception devices.

(1) Capacitance testing - Tests exist to determine whether a given pair has the correct allotment of capacitance associated with it.

(2) Resistance-to-ground and resistance unbalance test equipment, such as the Wheatstone Bridge, can be used to detect any anomalous resistances with respect to ground or resistive unbalances in either conductor of a pair.

(3) Frequency response - A system frequency response can be used to determine the presence of bridged impedance anomalies on both multipair and coaxial cable systems.

(4) Voltage standing wave ratio (VSWR) or impedance vs. frequency measurements can be used for the same purpose as (3). Time domain reflectometry (TDR) apparatus can also be used to pinpoint the location of an anomaly on coaxial cable.

(5) Deliberate scanning of non-automatic (non-annunciated) gas pressure contactors.

(6) Deliberate scanning of telemetry systems to check for existence of masked intrusion alarms.

Detection of Interception Apparatus Through System Degradation

The most obvious examples of system degradation resulting from the application of interception apparatus are gross reductions in transmitted signal level when excessively low impedances are bridged onto a pair, and the introduction of high noise levels into a system when unbalanced apparatus is bridged to a pair.

More subtle effects are involved when an impedance which varies as a function of frequency is connected to a cable pair or coaxial tube. Such an impedance can leave some frequencies of the wideband carrier signal unaffected and introduce excessively high losses at other frequencies.

Most FDM carrier systems have "line pilots" which are frequencies transmitted along with the information signals to check on the cable losses at each pilot frequency across the carrier band. The use of the frequency-sensitive bridging apparatus described above can have two effects:

- (1) Excessive losses introduced by the bridged interception equipment at frequencies where there are no pilots can disastrously degrade service without triggering alarms at the terminal; and
- (2) Excessive losses introduced by the bridged interception equipment at frequencies where there are pilots can cause the pilot alarms in the terminal to operate.

Effect (1) will, after a time, result in the isolation of the degradation and eventually a crew will be dispatched to correct the trouble. Effect (2) will result in a quick isolation and a crew will be dispatched almost immediately to repair the trouble. In either case, the discovery of the interception point is imminent.

The situation is analogous in digital systems with a somewhat different detection mechanism involved. Frequency sensitive anomalous impedances bridged to a cable pair will cause distortion sufficient to make pulses unrecognizable at the terminals or at regenerative repeaters. The loss of even occasional pulses will produce "bipolar violations" in the received signal which will trigger an alarm. Degradation of the line signal can also result in noticeable noise being introduced into the voice channels of the system.

As mentioned above, any accidental shorting of the power system will cause an alarm.

In summary, multiplex systems are particularly sensitive to improperly designed interception equipment or the inexperienced utilization of equipment. It is rather easy to affect line pilots in FDM systems resulting in an alarm or producing service degradation. Degrading the digital line signal results in noise in the voice channels as well as alarms from bipolar violations.

Coaxial cable is the most easily perturbed medium of all because of the very broad frequency bandwidths such systems carry, and because of the high voltages for powering repeaters which appear on the inner conductors of the coaxial tubes. For these reasons tapping coaxial cable systems outside of the repeater stations probably is not viable.

8.2.1.2 Radio Systems

This study has analyzed three basic types of radio communication systems: (1) terrestrial microwave systems, (2) satellite microwave systems and (3) citizens band, mobile telephone and public service radio. A summary of the analyses of each of these types of systems

is presented in the following sections. As indicated previously, detailed technical analyses are given in the appropriate appendices in Volume II of this report.

8.2.1.2.1 Microwave Radio Systems

Radio systems described as microwave systems are so-called because the radio frequencies at which they operate have very short wave-lengths. Both terrestrial microwave systems and many satellite systems use the same radio frequencies. The frequency bands most often employed for multichannel terrestrial and satellite communications extend from about 1 GHz to 15 GHz, the microwave radio frequency band. The frequencies within this band have been allocated to different services by the International Telecommunications Union (ITU) for international circuits and by the FCC/IRAC* for national circuits in the U.S. The principal band allocations are summarized in Table I. It is apparent from the table that microwave communication systems are employed by the common carriers, private users, and federal/local governments. The table also shows that certain frequency bands are shared by both terrestrial and satellite systems, e.g., 3.7 - 4.3 GHz and 5.925 - 6.425 GHz.

Terrestrial microwave systems relay traffic from point-to-point by employing line-of-sight transmission paths with repeaters spaced about 40 km apart. The transmission losses associated with such systems are principally those due to the geometric spreading of the transmitted radiation (the so-called free-space loss). The radio systems operate with transmitter powers of about 1 - 10 watts and receiver noise figures of about 5 - 10 dB. The antenna systems generally employ parabolic reflectors or parabolic-horn reflectors having directivity gains of about 40 dBi.

* Interdepartment Radio Advisory Committee

TABLE I
MICROWAVE FREQUENCY BANDS

<u>Band</u>	<u>GHz</u>	<u>Band Center Frequency</u>
Government	1.710 - 1.850	1.780
Operational Fixed	1.850 - 1.990	1.920
STL ¹	1.990 - 2.110	2.000
Common Carrier	2.110 - 2.130	2.120
Operational Fixed	2.130 - 2.150	2.140
Common Carrier	2.160 - 2.180	2.170
Operational Fixed	2.180 - 2.200	2.190
Operational Fixed (TV Only)	2.500 - 2.690	2.595
Common Carrier (incl. Space)	3.700 - 4.200	3.950
Government	4.400 - 5.000	4.700
Common Carrier (incl. Space)	5.925 - 6.425	6.175
Operational Fixed	6.575 - 6.875	6.725
STL ¹	6.875 - 7.125	7.000
Government	7.125 - 7.750	7.435
Government	7.750 - 8.400	8.075
Common Carrier	10.700 - 11.700	11.200
Operational Fixed	12.200 - 12.700	12.450
CATV ² - STL ¹ (CARS) ³	12.700 - 12.950	12.825
STL ¹	12.950 - 13.200	13.075
Government	14.400 - 15.250	14.825

¹ Studio Transmitter Link

² Community Antenna Television

³ Community Antenna Relay Service

Satellite systems also relay traffic from point-to-point by employing line-of-sight transmission paths. However, in contradistinction to terrestrial relay systems, a set of transponders synchronously orbiting the earth at an altitude of about 36,000 kilometers, is sufficient to relay traffic between any two points within the United States. Satellite system earth stations are usually characterized by large steerable parabolic antennas having diameters in excess of 20 meters and "directivity gains" of about 55 dBi. Earth station transmitter radiated power is typically about 1 kilowatt and receiver operating noise figure about 0.5 dB. The satellite transponder, literally the weak link in the relay system, typically radiates only about 1 watt of power through an antenna with a directivity gain of only about 20 dBi and has a receiver operating noise figure of about 10 - 14 dB.

Definition of Radio Signal Acquisition

"Radio signal acquisition" refers to the reception and subsequent demodulation (detection) of a radio frequency (r-f) carrier by an unauthorized receiver with a fidelity and/or accuracy commensurate with the successful extraction of the information transmitted. The reception of an r-f carrier necessarily requires the erection of an antenna for the conversion of the electromagnetic (radio) waves into electrical signals suitable for demodulation by the receiver; the assurance that demodulation will be accomplished with a "fidelity and/or accuracy commensurate with the successful extraction of information" requires not only the selection of the parameters determining receiving system performance but implicitly requires the identification of appropriate quantitative fidelity and/or accuracy performance objectives. Performance measures of fidelity and/or accuracy depend upon the character of the information transmitted: for analog information (e.g., FDM telephone, television) the usual performance measures (of fidelity) are test-

tone signal-to-noise ratios (SNR) at the demodulator output; for digital information the usual performance measure (of accuracy) is the bit-error-rate (BER).

Acquisition of Signals from Terrestrial Microwave Systems

The susceptibility of terrestrial microwave systems to r-f signal acquisition is engendered by the inadvertent (and, often, unavoidable) radiation of electromagnetic energy in directions other than toward the intended terrestrial receiver. Most of the unintentional radiation arises as a result of the non-zero angular width of the main antenna lobe which is directed toward the intended receiver and the inadvertent radiation from side- and back-lobes. The antenna gain pattern, which describes the directivity characteristics of the radiation, depends upon the antenna type (e.g., parabolic reflector, horn-reflector, lens, horn, or dipole), the r-f carrier frequency and the polarization. The azimuthal dependence of the AT&T horn reflector antenna KS-15676, the predominant type employed by the Bell System, is illustrated by the antenna gain patterns of Figure 10.

To assess, quantitatively, the vulnerability of terrestrial microwave systems to clandestine signal acquisition, the Bell System TD-2 microwave system has been selected as an illustrative target which typifies common-carrier, switched voice service. This particular microwave system is employed by the AT&T for nearly 60 percent of all Long-Lines circuit-km. The equipment configuration employed for r-f signal acquisition will be determined by the interceptor's resources and performance objectives; it may be custom-engineered or off-the-shelf equipment. The former includes receivers with component sub-systems specifically engineered for unauthorized signal acquisition as well as those jury-rigged from old parts and/or test equipment; the latter includes receivers available commercially through purchase or acquired through theft.

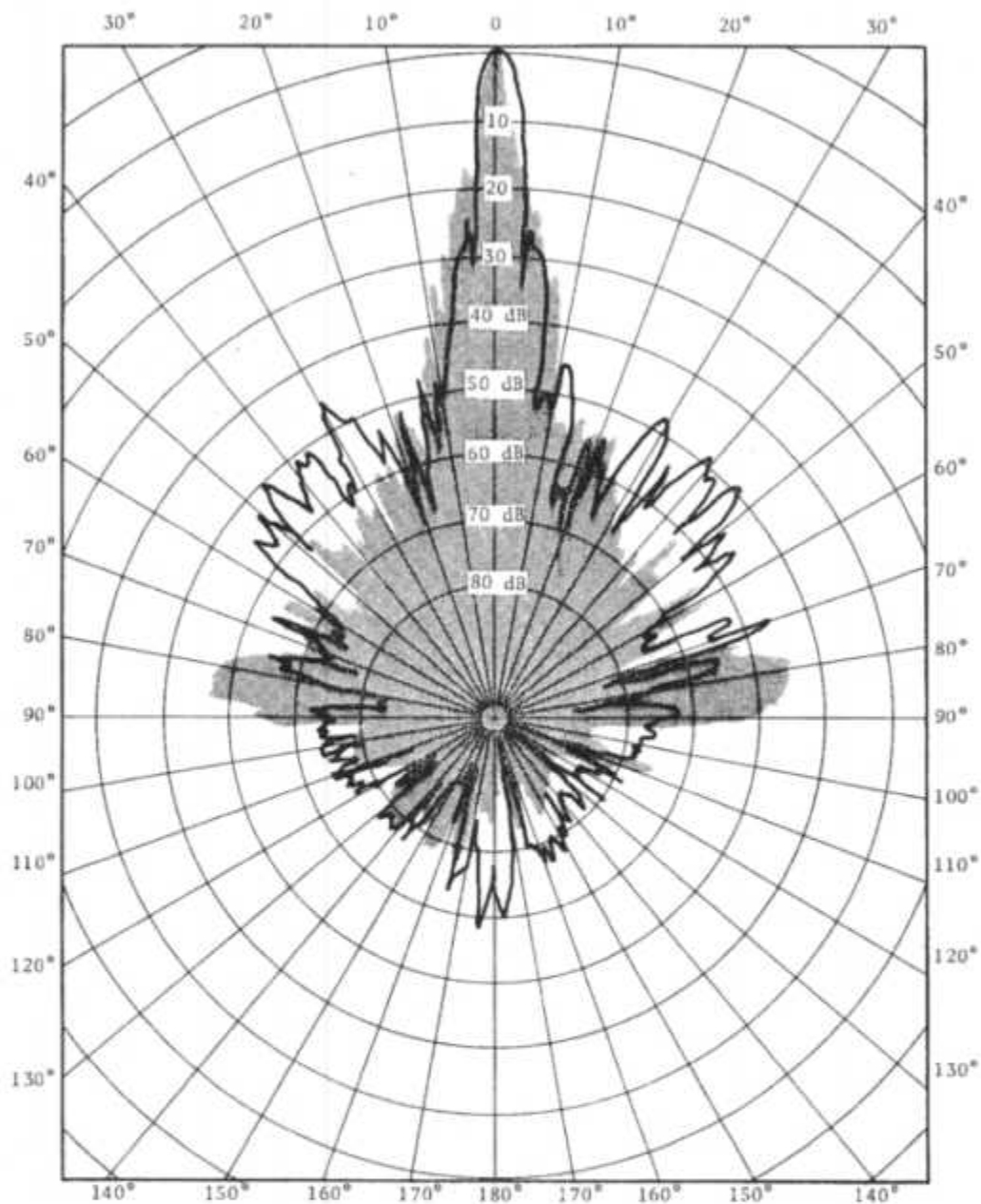


FIGURE 10
 AZIMUTHAL DIRECTIVITY GAIN PATTERN FOR AT&T HORN-REFLECTOR
 KS-15676 AT 4 GHz FOR VERTICAL (OPEN) AND HORIZONTAL (SHADED)
 POLARIZATION

A reasonable upper-bound on the vulnerability of the target system can be derived by assuming that an interceptor employs an equipment complement equivalent in performance to that normally employed by the target. For the assessment of TD-2 vulnerability, the analysis below assumes for such an equipment complement a TD-2 radio receiver (available, for example, by purchase from Collins or by theft from Western Electric) and a 10-foot diameter parabolic reflector antenna. Two other signal acquisition equipment complements were also employed to assess TD-2 vulnerability: (a) a TD-2 radio receiver and a standard gain horn (instead of the 10-foot paraboloid), and (b) a compact surveillance receiver and standard gain horn. The salient technical parameters and costs characterizing these three equipment configurations are summarized as Cases I, II, and III in Table II. A generic block diagram, valid for all three acquisition equipment complements is shown in Figure 11.

Presented in Figures 12 through 14 are the loci of signal reception sites within which an interceptor's antenna can be located to acquire successfully the bi-directional telephony of a TD-2 system. Each of these figures corresponds to a different repeater site spacing (d_S) of the TD-2 system: 30, 40, or 50 kilometers. In each of the figures, loci are presented for each of the three acquisition equipment configurations described in the previous paragraph and identified in Table II. In all figures, the antenna heights of the targeted system repeaters at sites A and B (h_A and h_B) and the antenna height of the reception site (h_I) are assumed to be 50 meters. That is, the acquisition site is assumed to be essentially in line-of-sight of the repeater sites. The terrain roughness is assumed to be gently rolling with only a 20 percent probability that the hilltop-to-valley height (Δ_h) exceeds 90 meters. The r-f carrier frequency (f) is assumed to be 4 GHz. In all cases, the received signal is assumed acceptable if the carrier-to-noise ratio (CNR) exceeds 10 dB and the signal-to-noise ratio (SNR) exceeds 20 dB.

TABLE II
TERRESTRIAL MICROWAVE EQUIPMENT FOR BI-DIRECTIONAL
SIGNAL ACQUISITION OF TD-2
TELEPHONY

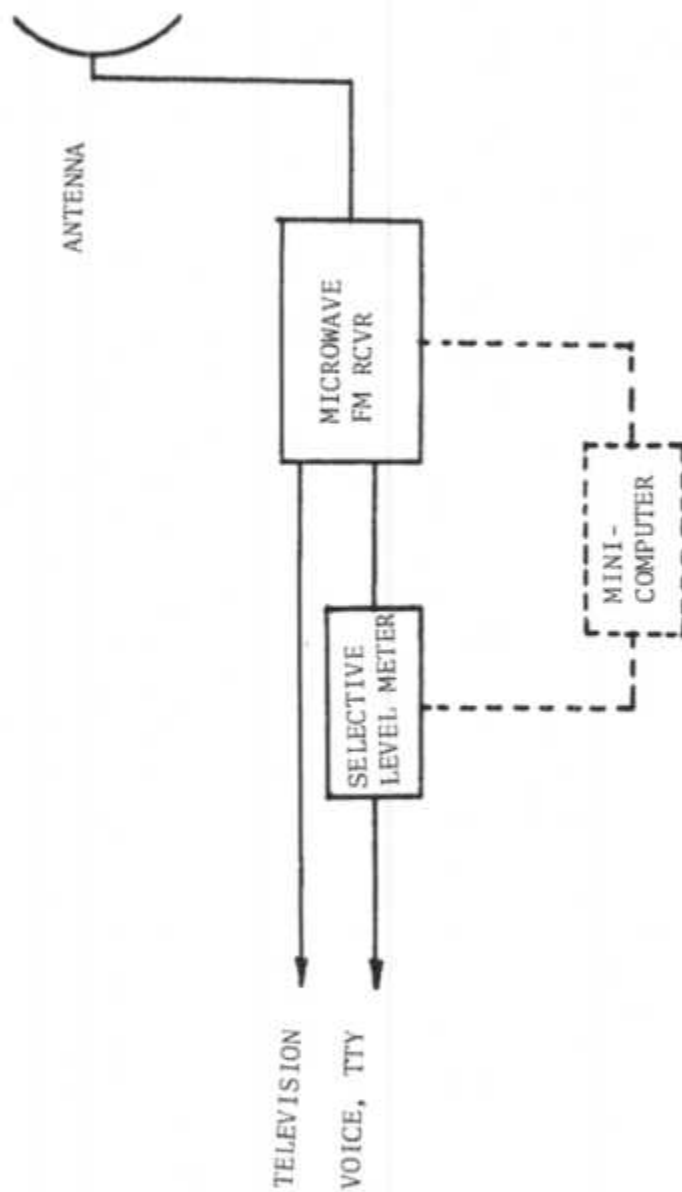
Estimation of Costs

CASE	RECEIVER		ANTENNA			SYSTEM COST*
	TYPE	NOISE FIGURE	TYPE	SIZE	GAIN	
I	TD-2	7.5 dB	Parabolic	10' dia.	39.5 dBi	\$30K**
II	TD-2	7.5 dB	Horn	4-3/4" x 6-3/8"	16.5 dBi	\$25K**
III	Surveil- lance	20.0 dB	Horn	4-3/4" x 5-3/8"	16.5 dBi	\$60K

NOTE: Minicomputer controlled scanning capability would increase the above cost estimates by about \$10K

* System costs include selective level meter with single-sideband (SSB) detector.

** Receiver cost includes custom modification of TD-2 to achieve tuning capability.



NOTE: Dashed lines denote optional automatic control functions

FIGURE 11
EQUIPMENTS CONFIGURATION FOR SIGNAL ACQUISITION OF TERRESTRIAL MICROWAVE SYSTEMS

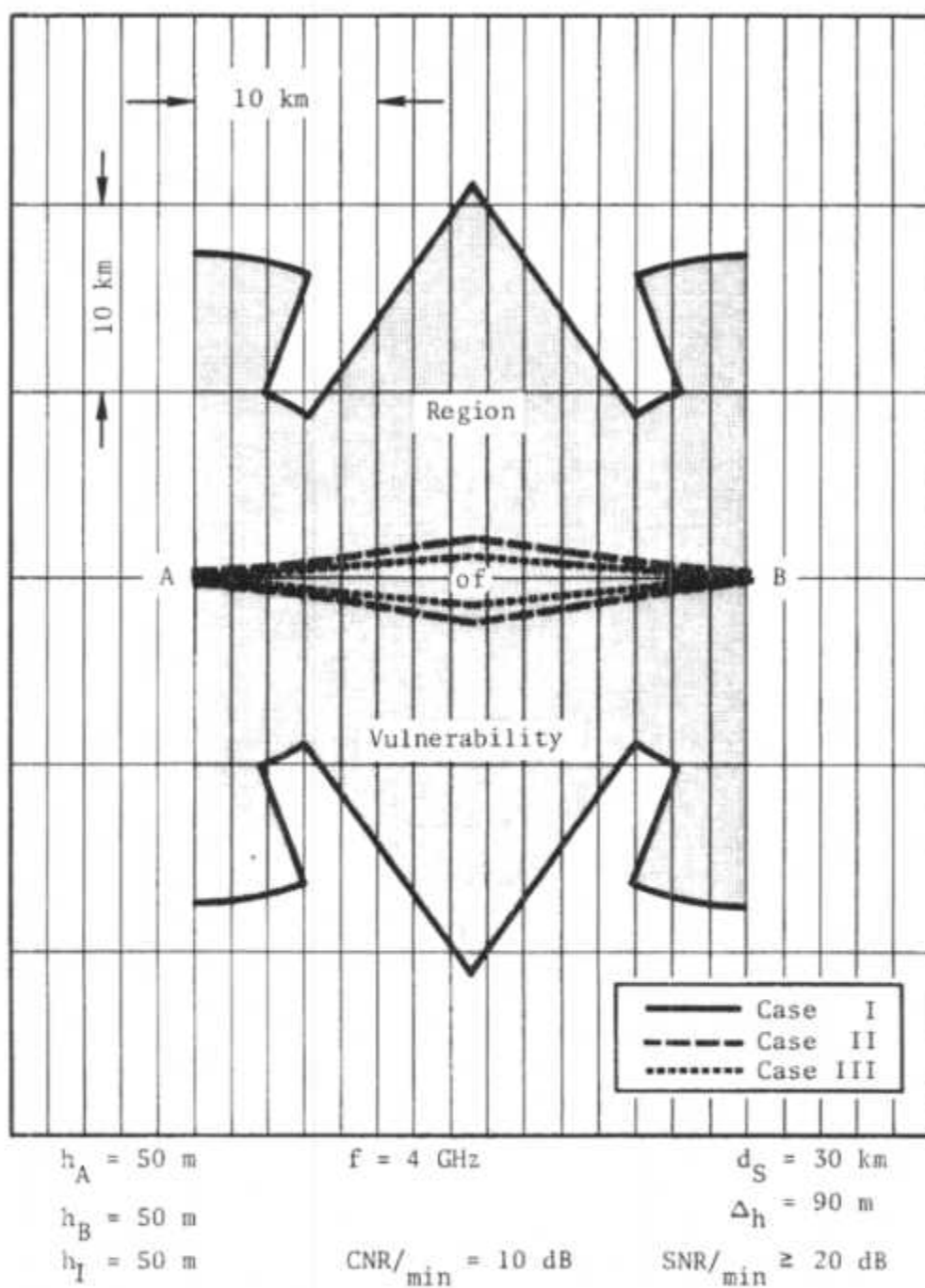


FIGURE 12
TERRESTRIAL MICROWAVE: BI-DIRECTIONAL RECEPTION OF TELEPHONY-
LOCI OF POTENTIAL RECEPTION SITES

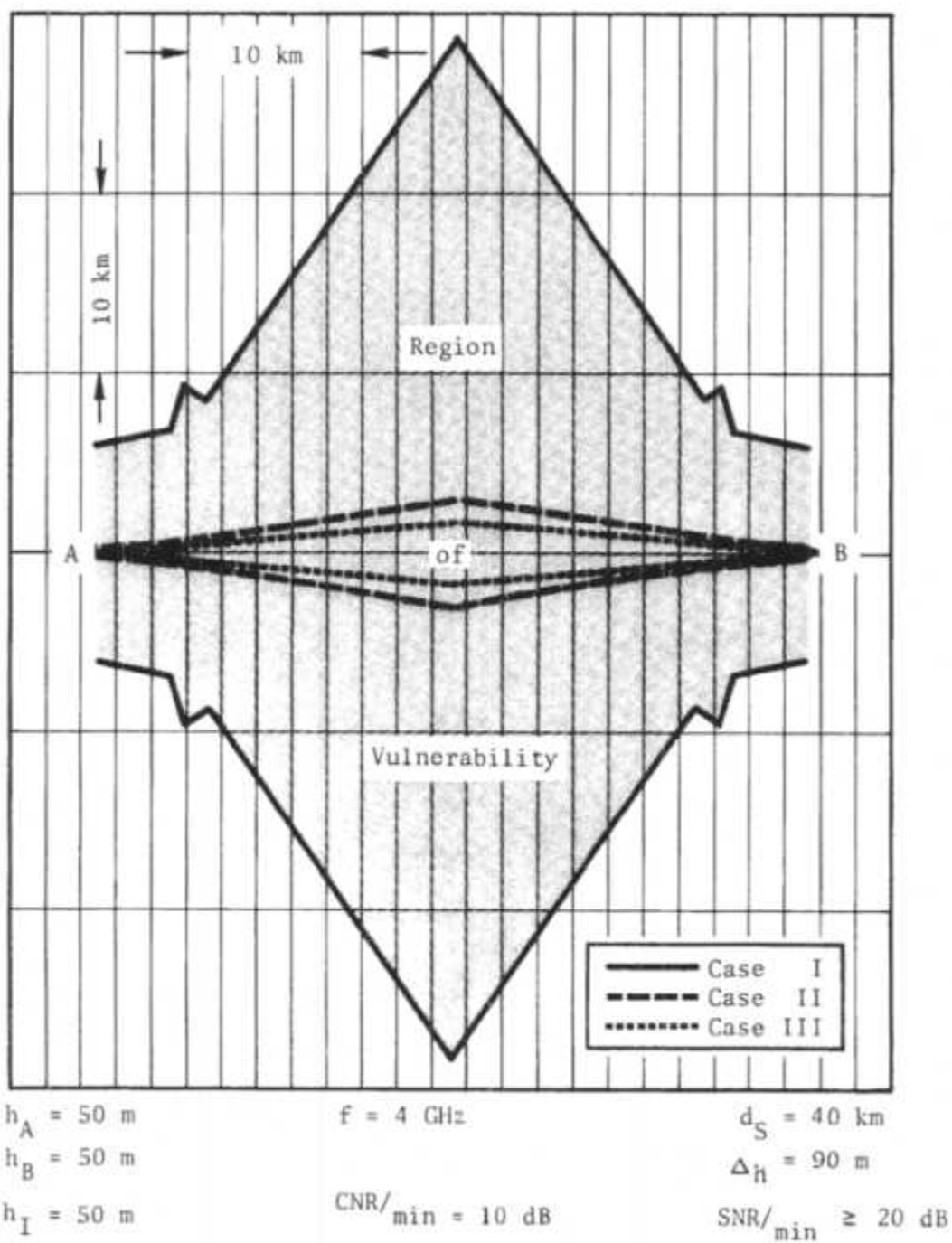


FIGURE 13
TERRESTRIAL MICROWAVE: BI-DIRECTIONAL RECEPTION OF TELEPHONY-
LOCI OF POTENTIAL RECEPTION SITES

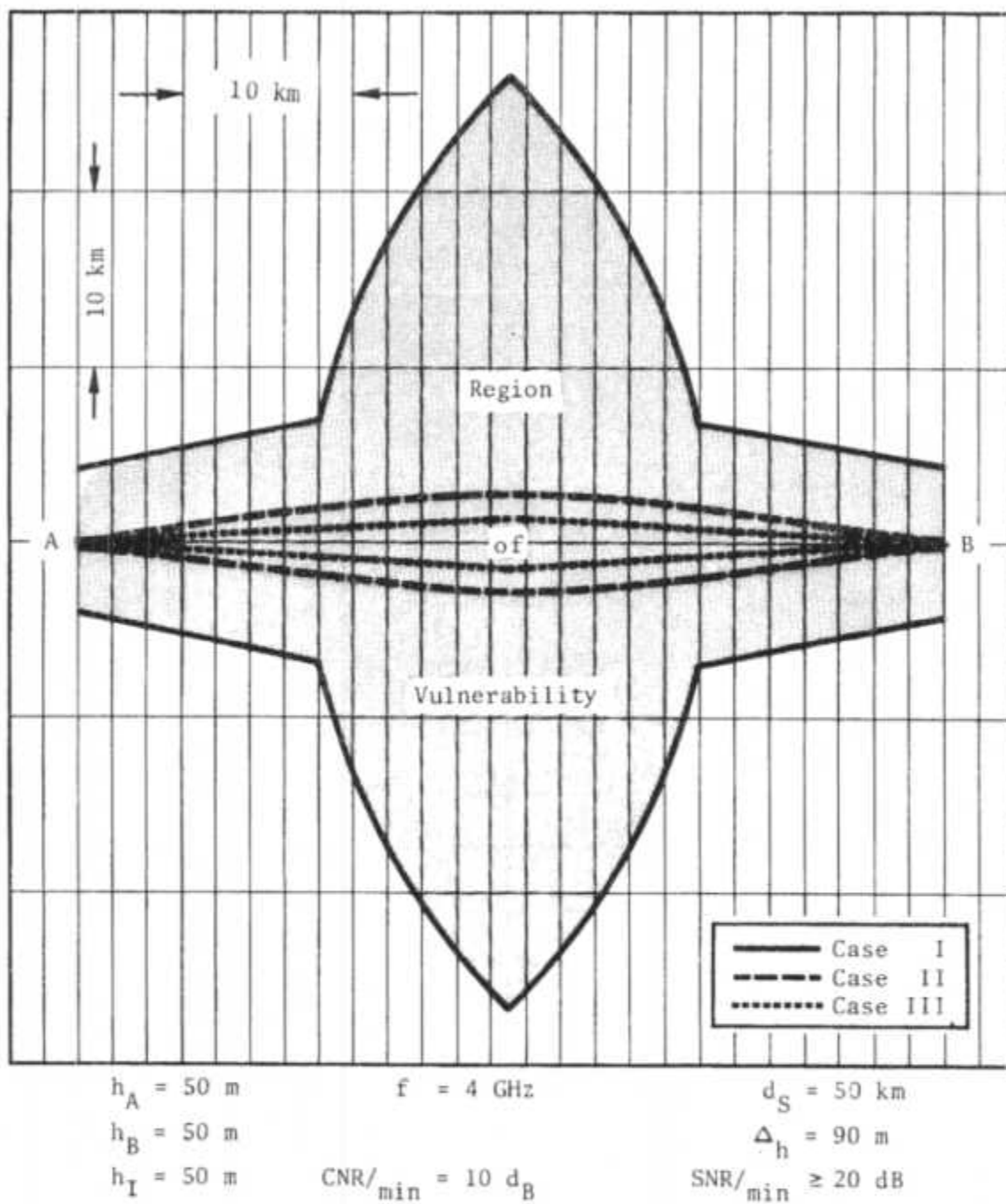


FIGURE 14
TERRESTRIAL MICROWAVE: BI-DIRECTIONAL RECEPTION OF TELEPHONY-
LOCI OF POTENTIAL RECEPTION SITES

It is apparent from these figures that with high quality reception equipment (i.e., equipment quality comparable to that of the target system), the target TD-2 microwave system appears vulnerable to signal acquisition even if the interceptor's antenna is as much as 20 km from the line-of-sight right-of-way. For poorer quality reception equipment, the target TD-2 system is vulnerable to signal acquisition only along the line-of-sight right-of-way and within a small region about the repeater site.

The loci of reception sites for the successful acquisition of bi-directional traffic which, for the poorer figures-of-merit, lie in the vicinity of the target system repeater are described in further detail by Figures 15 through 17. For these loci, propagation loss is due only to free-space geometric spreading of the radiowaves. Consequently, these loci are independent of the antenna heights, h_A , h_B , and h_I so long as unobstructed, line-of-sight transmission path can be achieved. Within this constraint, the loci will also apply to the case of a nearby receiver located in a mobile van.

On the basis of the vulnerability analysis for the reception of TD-2 system signals, it may be concluded that, with a receiving equipment complement comparable in quality to that of the target terrestrial microwave system, an interceptor's receiving antenna need not be located directly along the target system's line-of-sight right-of-way or even within a few kilometers of the repeater terminal in order to acquire a signal with the fidelity and/or accuracy commensurate with successful extraction of the information. Although the validity of this conclusion is, strictly speaking, predicated upon the assumption of the illustrative example, the parameters assumed are sufficiently typical of all terrestrial microwave systems.

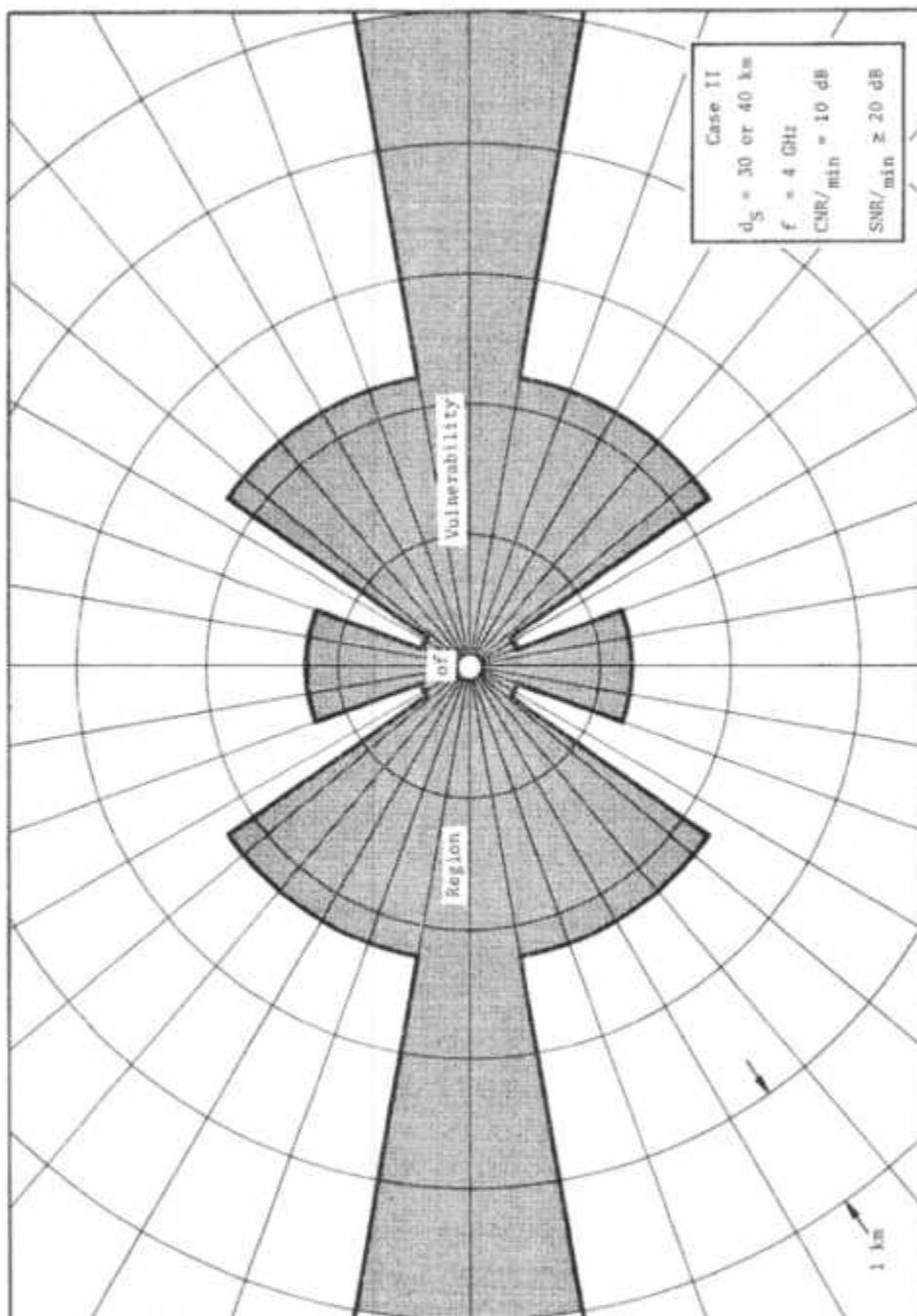


FIGURE 15
TERRESTRIAL MICROWAVE: BI-DIRECTIONAL SIGNAL ACQUISITION OF TELEPHONY –
LOCI OF POTENTIAL INTERCEPTION SITES

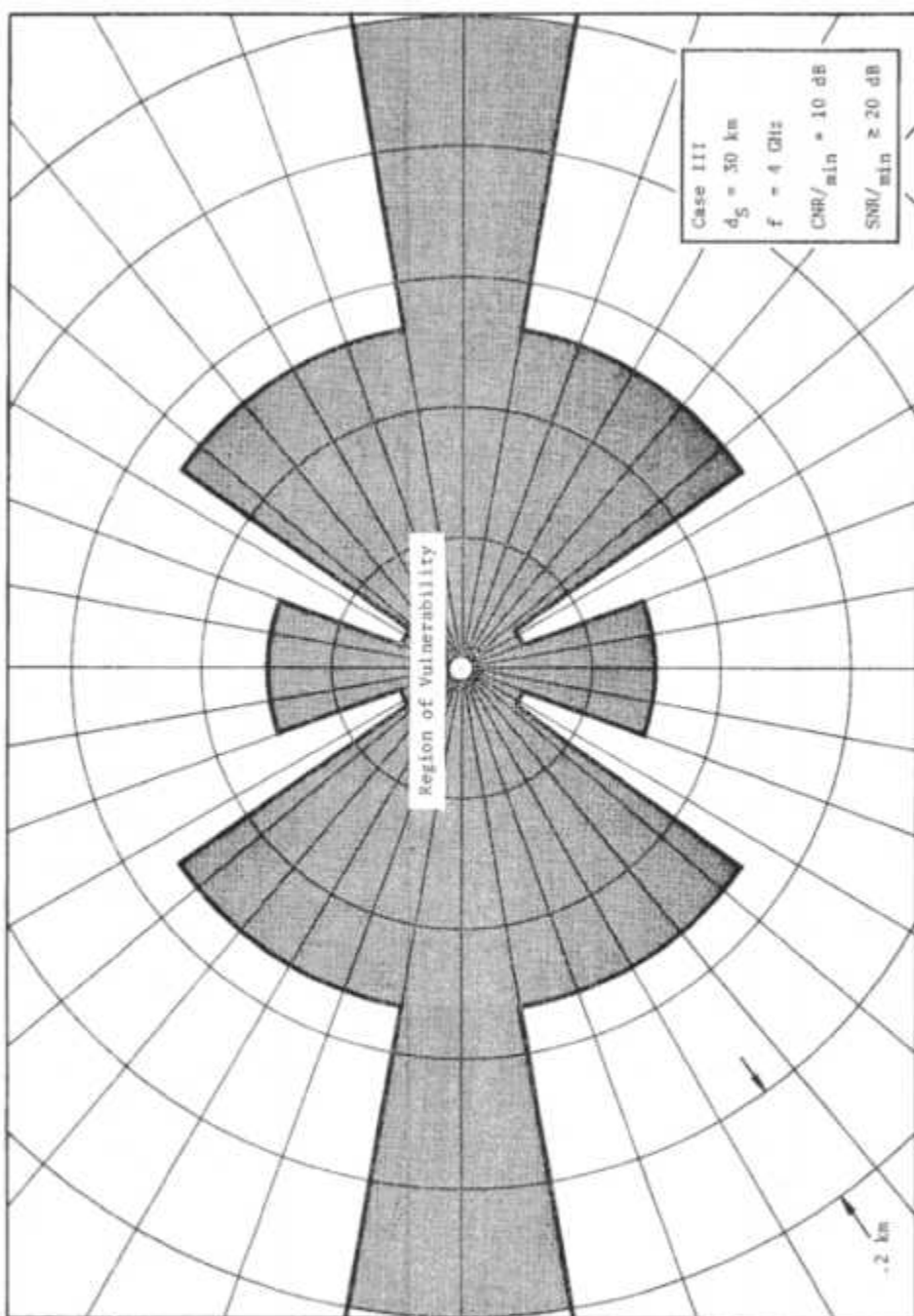


FIGURE 16
 TERRESTRIAL MICROWAVE: BI-DIRECTIONAL SIGNAL ACQUISITION OF TELEPHONY –
 LOCI OF POTENTIAL INTERCEPTION SITES

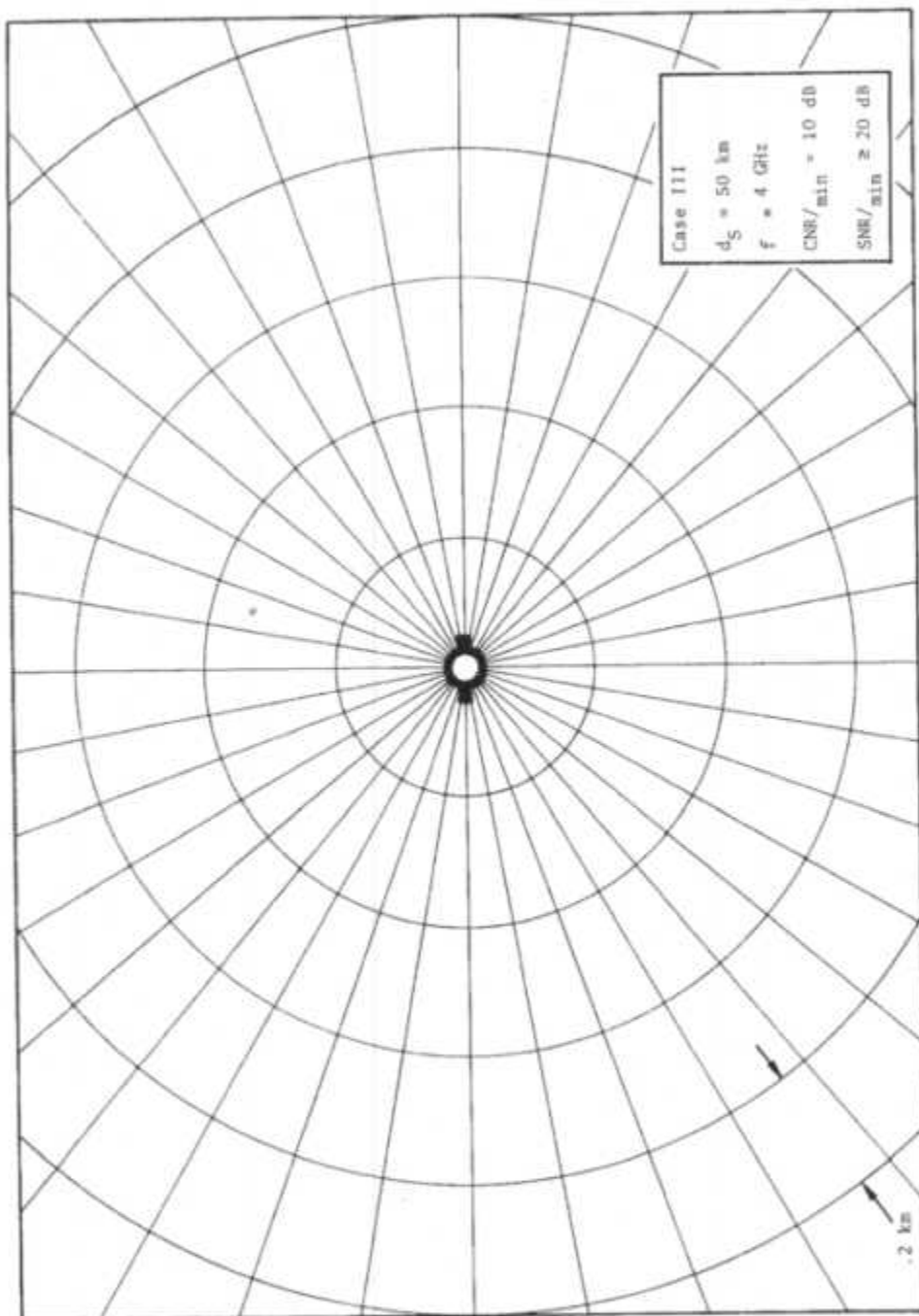


FIGURE 17
TERRESTRIAL MICROWAVE: BI-DIRECTIONAL SIGNAL ACQUISITION OF TELEPHONY -
LOCI OF POTENTIAL INTERCEPTION SITES

The two technical parameters impacting most strongly upon the vulnerability of a terrestrial microwave system to unauthorized r-f reception are the interceptor's receiver noise figure and antenna gain. With a high quality (i.e., low noise figure) receiver the interceptor's antenna can be significantly removed from the vicinity of the repeater towers; such receivers can be bought commercially or stolen from the target system's equipment inventory. Although the latter source has the advantage of ensuring equipment compatibility between the target system and interceptor, it introduces certain difficulties in tunability. More specifically, most AT&T microwave systems employ multiple carrier frequencies; the systems employing the TD-2 use up to 12 r-f channels: 10 are available for carrying traffic, the remaining 2 are reserved for spares. For a particular link the interceptor's equipment must be capable of receiving any one of these 12 r-f channels and so must be "frequency agile." However, off-the-shelf TD-2 receivers are fixed frequency receivers -- the frequency being determined by a crystal oscillator. To change frequency it is necessary to change crystals; clearly, this solution is not acceptable to an interceptor who will, in most cases, not know a priori which of the r-f channels is carrying the targeted traffic. Further, most microwave equipment includes pre-selection waveguide filters. These filters must be tuned manually by adjusting set-screws in the waveguide feeder connecting the antenna to the receiver. This, too, is unacceptable to an interceptor. However, alternatives are available. Continuously tunable Gunn oscillators and YIG (Yttrium-Iron-Garnet) waveguide filters could be retrofitted into the equipment, although not without cost, time, or sophisticated technical assistance. Surveillance receivers, although usually frequently agile, are considerably more expensive and less sensitive (i.e., higher noise figures). Test equipment,

too, can be configured for unauthorized signal acquisition. The principal difficulties in employing test equipment are its high cost, the absence of r-f pre-selection, and low r-f sensitivity.

Acquisition of Signals from Common Carrier Satellite Systems

The acquisition of signals from a common carrier satellite communication system may be exemplified by considering INTELSAT IV. This satellite, which employs frequency-division-multiple-access (FDMA) to achieve multi-carrier FDM-FM transponder operation, typifies the configuration of all satellite systems employing U.S. earth stations with the exception of that proposed by Satellite Business Systems (SBS). However, the SBS system, which will employ digital modulation and time-division multiple-access (TDMA), is not expected to be operational until 1981.

Nearly all of these satellite systems, which typically require earth stations with G/T ratios* in excess of 30 dB/°K, employ large steerable antennas with diameters in excess of 10 meters. The cost and size associated with building and controlling such a structure probably precludes its procurement by any unauthorized interceptors. A smaller antenna system with diameter less than 5 meters used in conjunction with sophisticated low-noise receiving equipments would seem much more acceptable in spite of a probable decrease in reliability.

* The gain-to-temperature ratio is a commonly used figure-of-merit for satellite receiving systems based upon the receiving antenna gain, G, and the receiving system effective input noise temperature, T.

The INTELSAT IV satellite communication system achieves a G/T of 40.7 dB/°K with a standard earth station configuration consisting of a 30 meter diameter steerable parabolic reflector antenna and a system noise temperature of about 78°K. The cost of such an antenna structure, (reportedly about \$1,500,000) appears prohibitive for any but the most determined interceptor. However, several alternative earth station configurations are available which could result in significantly reduced costs in implementation and construction although not without decreased reliability and increased maintenance. For example, instead of employing a nitrogen-cooled (77°K) parametric amplifier, a helium-cooled (4°K) parametric amplifier could be employed to reduce the receiving system noise temperature from 78°K to about 50°K. Further, an interceptor could eliminate the margin requirement for equipment degradation and rain and accept the increased outage time and reduction in time availability. Finally, an interceptor could employ a threshold extension applique-unit to reduce the FM discriminator threshold and so increase the sensitivity of the receiving system. The sum improvement due to the introduction of the helium-cooled parametric amplifier, the elimination of the system margin, and the use of threshold extension is about 7.7 dB. If this improvement factor is used only to reduce the antenna size, the antenna diameter can be reduced from 30m to about 12m. The reported cost of a 12-meter diameter steerable earth terminal antenna is about \$600,000.

The discussion above is applicable to all down-link traffic relayed by the satellite transponder including the low traffic density (up to 132 voice channels), global-beam, standard r-f carriers which are, potentially, the most difficult to receive. Considerably more vulnerable to reception, however, are the so-called expanded global-beam carriers which provide greater-than-standard traffic densities within standard bandwidths and the standard spot-beam carriers. For both of these carrier types the INTELSAT IV

satellite transponder employs effective radiated powers which are at least 7.3 dB above the effective radiated powers employed for standard global-beam carriers. At the expense of poorer received quality, the interceptor can employ this 7.3 dB in conjunction with the previously realized 7.7 dB advantage to further reduce the earth station antenna diameter to about 5-meters. The cost of a 5-meter diameter steerable earth station antenna is about \$20,000.

The equipment configurations required for successful signal acquisition of r-f transmissions employing either global- or spot-beam satellite transmitting antennas with either standard or expanded traffic are summarized in Table III. In the table Cases I and II refer, respectively, to: (I) He-cooled parametric pre-amplifier, microwave receiver, and steerable 12-meter antenna; and (II) He-cooled parametric amplifier, microwave receiver, and steerable 5-meter antenna. A generic block diagram, valid for both configurations, is shown in Figure 18.

Satellite systems are also vulnerable to interception through the use of authorized subscriber-owned earth stations for the unauthorized reception of the traffic of other subscribers. For example, an INTELSAT earth station in one country could be employed to receive and demodulate r-f carriers intended for INTELSAT subscribers of other countries. This capability is available since the low-noise parametric amplifiers employed for most subscriber earth stations are nearly always broad-band (500 MHz) and therefore are capable of receiving the entire frequency band allocated to space communications. Following amplification by the parametric amplifiers, the r-f carriers can be separated by filtering and the signals targeted for interception passed to a conventional microwave receiver for demodulation. Since the frequency assignments of subscribers are changed only infrequently, a crystal-controlled, fixed-frequency microwave receiver would appear

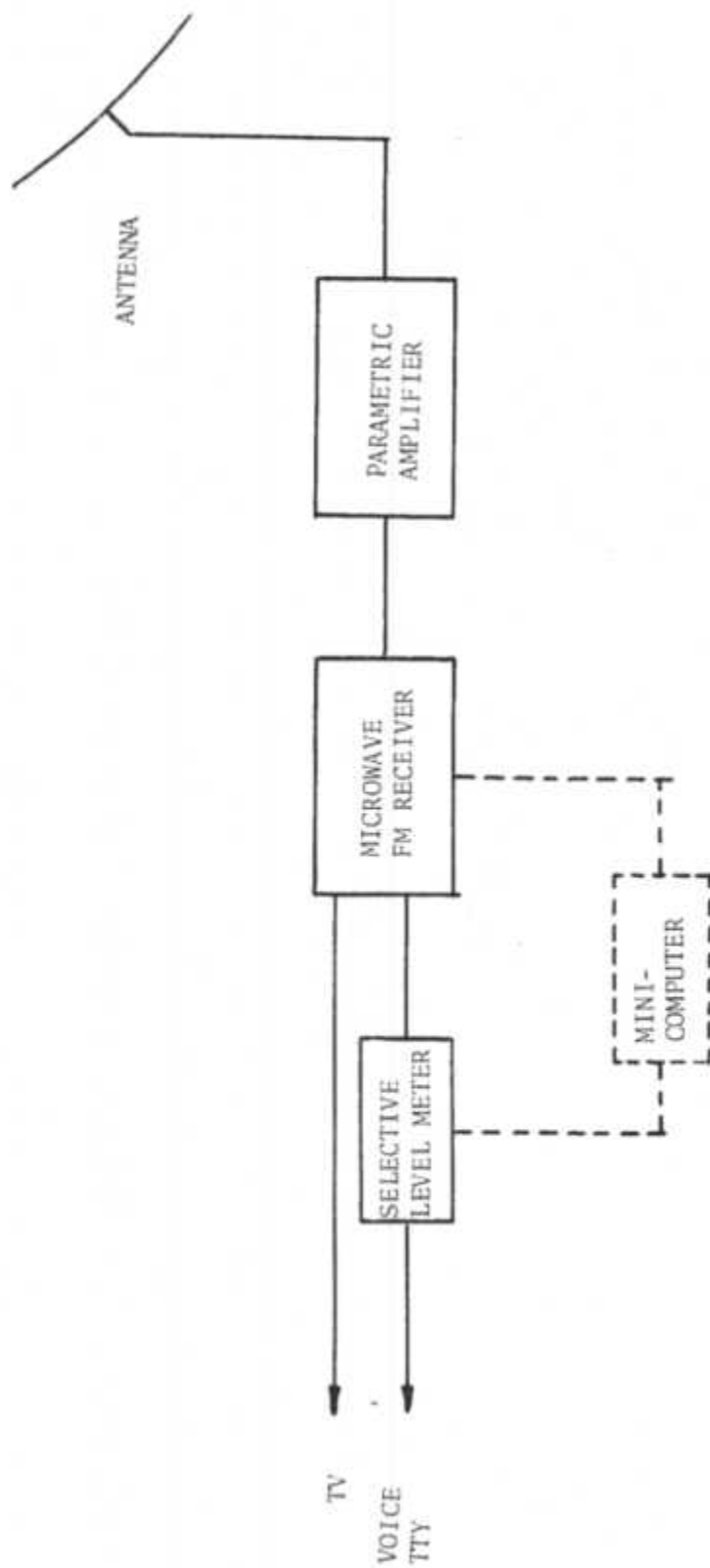
TABLE III
SATELLITE MICROWAVE EQUIPMENT FOR BI-DIRECTIONAL
SIGNAL ACQUISITION OF FDM-FM TELEPHONY
ESTIMATION OF COSTS

CASE	RECEIVER SYSTEM		ANTENNA		COST**
	TYPE	OPERATING N.F.	DIAM- ETER	GAIN	
I	He-Paramp	0.7 dB	12 m	51.5 dB	\$700 K
II *	He-Paramp	0.7 dB	5 m	43.5 dB	\$110 K

NOTE: Minicomputer controlled scanning capability would increase the above cost estimates by about \$10K

*Manually Steerable Antenna Mount

**System costs include selective level meter with single sideband (SSB) detector.



NOTE: Dashed lines denote optional automatic control functions

FIGURE 18
EQUIPMENT CONFIGURATION FOR ACQUISITION OF SATELLITE SYSTEMS SIGNALS

acceptable. An equipment configuration suitable for employing a subscriber earth station for unauthorized reception of satellite system signals is shown in Figure 19. As with other intercept systems considered previously, a selective level meter is employed to select and demodulate the single FDM telephone channel of interest.

Although, strictly speaking, all equipment configurations considered in this section apply only to the acquisition of the INTELSAT IV satellite system signals, the parameters of this satellite system are sufficiently typical of all presently proposed or existing systems that these equipment complements themselves, may be considered typical. As with the INTELSAT earth stations, subscriber-owned earth stations for receiving signals from domestic satellites (e.g., WESTAR) could be easily modified and adapted for the unauthorized reception of other subscribers' traffic over the same satellite or over other satellites such as COMSTAR.

8.2.1.2.2 Citizens Band, Mobile Telephone and Public Service Radio

Reception of citizens band (CB), mobile telephone and public service radio communications is readily accomplished with equipment legally sold over-the-counter. A wide variety of receiving equipment is available. Some equipments are designed for the reception of particular types of broadcast only (e.g., CB, police band, marine band, radio telephone). Other available receiving equipment combines into one receiver combinations of these bands. Since these equipments are designed for use by the general public they require no or very little knowledge to install and are simple to operate. Costs are low (ranging from about \$15 to \$400) and are available in sizes ranging from about 20 to 550 cubic inches. Weight varies from less than one pound to more than 30 pounds.

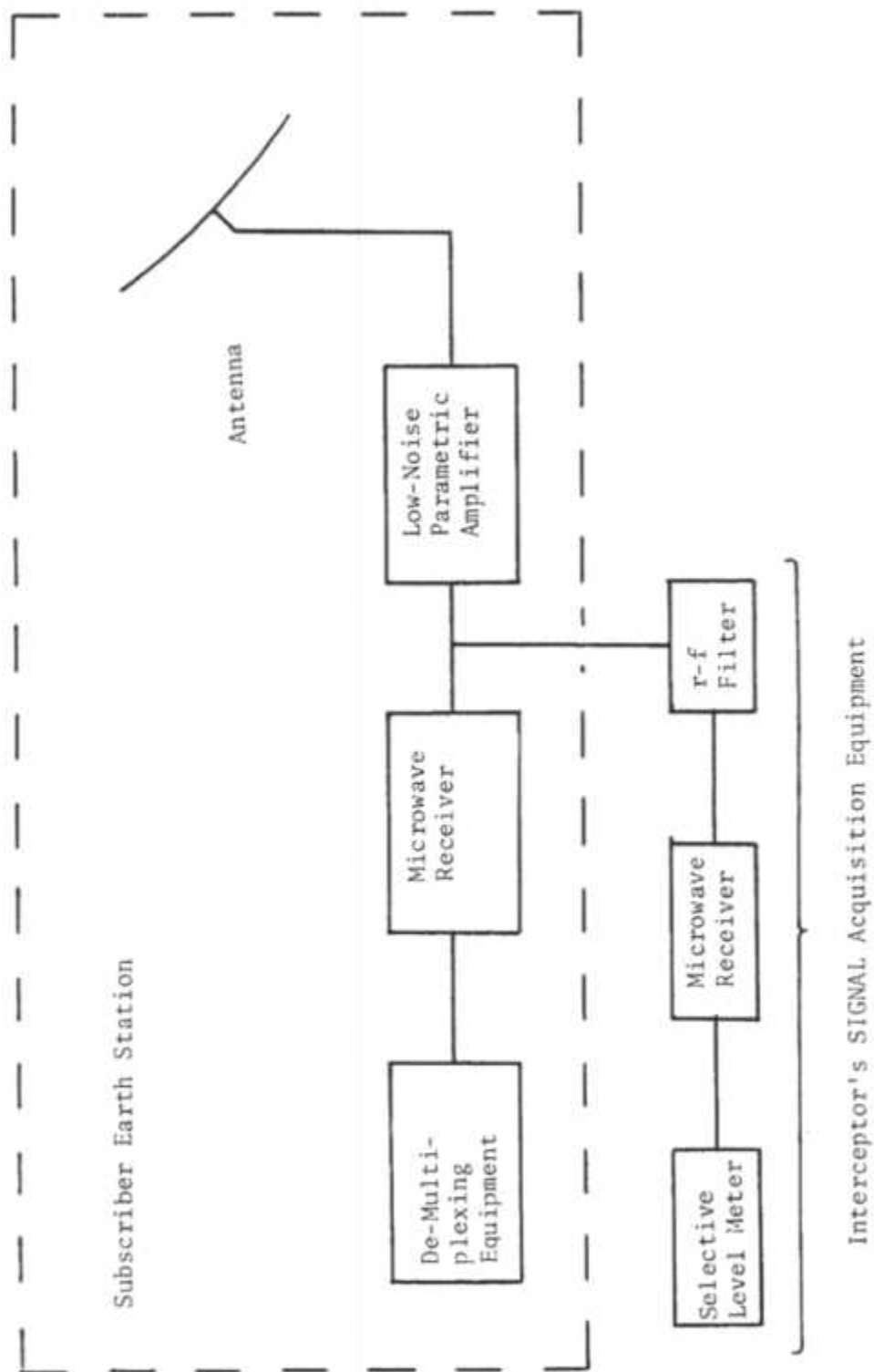


FIGURE 19
USE OF SUBSCRIBER EARTH STATION FOR THE UNAUTHORIZED TELEPHONY SIGNAL ACQUISITION

Targeting of specific individuals using CB radios is difficult because the targeted individual may use any of the channels assigned to this band (40 channels as of 1 January 1977), many other people use the same channels, and the interceptor must be within reception range of these low power units. Targeting certain classes of individuals (e.g., truck drivers) or types of communication (e.g., distress calls) can be more easily accomplished since certain prearranged channels are more likely to be used for these communications.

Targeting of specific mobile telephone subscribers is somewhat easier (although the interceptor must be within the range of the low power mobile transmission unit) because individual mobile telephone transceivers are usually equipped with a very few channels.

Organizations (such as police, fire, ambulance) using public service radio are readily targeted because they use relatively few fixed frequencies each of which is usually assigned for a specific use.

8.2.1.3 Summary Comparison of Transmission Media

Table IV presents a summary of the transmission media in terms of their interceptability characteristics independent of the nature of the network form using the media. The ratings listed are ordered from very low to very high, reflecting increasing adverse effect on interception. In order to eliminate variations due to the type of traffic, this table is based on voice traffic. Other types of traffic are treated in the following section. "Difficulty of physical penetration or radio reception" refers to how difficult it is to acquire the primary electronic signal (e.g., electrical voice frequency waveform in the case of open wire and the radio frequency radiation in the case of the microwave medium). "Difficulty of signal acquisition" is defined as how difficult it is to obtain the signal in an individual

TABLE IV
A SUMMARY COMPARISON OF TRANSMISSION MEDIA IN TERMS OF THEIR
INTERCEPTABILITY CHARACTERISTICS

TRANSMISSION MEDIUM	DIFFICULTY OF PHYSICAL PENETRATION OR SIGNAL RECEPTION	DIFFICULTY OF SIGNAL ACQUISITION	DIFFICULTY OF TARGETING	INTERCEPTABILITY OF INTERCEPTOR				INTERCEPTOR IMPLEMENTATION COMPLEXITY	SIGNAL ACQUISITION EQUIPMENT COST
				VISUAL DETECTION	SYSTEM ALARMS	DELIBERATE TESTING	SYSTEM DEGRADATION		
<u>Wire & Cable</u>			(1)			(1)	(1)	(1)	(1)
Local Loop									
Low Density									
Open Wire	Very low	Very low	Very low	Medium	None	Low	Low	Very low	Low
VC/Pair ²	Very low	Very low	Low	Medium	None	Low	Low	Low	Low
MX/Pair ³	Low	Medium	Low	Medium	Low	Low	Low-Medium	Low-Medium	Low
High Density									
MX/Open Wire Pair	Very low	Low-Medium	Low-Medium	Medium	Low	Low	Low-Medium	Low-Medium	Low
VC/Pair	Low-Medium	Low-Medium	Low-Medium	Medium	Low	Low	Low-Medium	Low-Medium	Low
MX/Pair	Low-Medium	Medium	Low-Medium	Medium	Low	Low	Low-Medium	Low-Medium	Low
<u>Trunks</u>									
(6 pairs or greater)									
Open Wire	Very Low	Low	Medium	Medium	None	Low	Low	Low-Medium	Low
Open Wire Carrier	Low	Low-Medium	Medium	Medium	Low	Low	Low-Medium	Low-Medium	Low
Multi-Pair Cable	Medium	Low	Medium	Medium	Low-Med	Low	Low	Low-Medium	Low
Pressurized	Low	Low	Medium	Medium	Low-Med	Low	Low	Low-Medium	Low
Non-Pressurized									
Multi-Pair Cable	Medium	Low-Medium	Medium	Medium	Low-Med	Low	Low-Medium	Low-Medium	Low
Carrier	Low-Medium	Low-Medium	Medium	Medium	Med-Hi	Low	Low-Medium	Low-Medium	Low
Cable	Low-Medium	Low-Medium	Medium	Medium	Med-Hi	Low	Low-Medium	Low-Medium	Low
Repeater	High	Medium-High	Medium-High	Medium-High	High	Medium-High	Medium	Medium-High	Medium-High
Coaxial Cable Carrier	Medium	Medium	Medium-High	Medium-High	High	Low-Medium	Low	Medium-High	Medium-High
Cable									
Repeater									
<u>Microwave</u>									
Terrestrial	Low	Low	Medium-High	Low	None	None	None	High	High
Satellite	Low	Low-Medium	Medium-High	Low	None	None	None	Very high	Very high

¹This table is based on voice message traffic; these columns will rate higher if the channel is carrying data traffic

²VC/Pair: Voice channel per pair of wires

³MX/Pair: Several multiplexed voice channels on a single pair of wires

channel after the medium has been penetrated (e.g., the demultiplex operations required when intercepting signals carried on a coaxial cable). "Difficulty of targeting" reflects the difficulty presented by the medium to the interceptor in targeting a particular individual or channel (e.g., targeting communications employing multiplex systems would become increasingly more difficult as the number of channels multiplexed together increases). "Detectability of the interceptor" refers to the likelihood that the intercept will be detected (assuming he has the required equipment and knows how to use it properly). "Interceptor implementation complexity" is a measure of the complexity of the interceptor's job. "Signal acquisition equipment cost" includes only that equipment necessary to physically penetrate the medium and acquire the signal of interest. It does not include the equipment necessary to extract the information or to help him identify a particular targeted individual or channel.

8.2.2 Effects of Multiplexing and Signaling on Communications Interceptability

Multiplexing systems and signaling systems are two features of common carrier transmission systems that can have a major impact on an interceptor's ability to monitor communications. Some consideration of multiplexing was covered previously in the discussion of "carrier" systems that use multiplexing techniques to carry two or more conversations simultaneously over a single transmission medium. Signaling information carried by the transmission media may be of use to an interceptor in that it may reduce the amount of time and effort required by the interceptor to monitor specific communications and target specific individuals or organizations. Each of these features is discussed below.

8.2.2.1 Multiplex Systems

Wire and cable carrier, coaxial-carrier and radio-carrier transmission systems utilize a process called "multiplexing" to combine

two or more voice, teletype, data or video circuits for simultaneous transmission over a common medium. The selection of multiplexing technique and transmission medium to be used is generally a function of the amount of traffic between two points. Where the required capacity is 60 channels or less, the channels will probably be multiplexed on wire or cable pairs. On routes where the capacity is to be 60 channels or more (up to hundreds of thousands), coaxial cable or microwave radio will probably be installed. However, microwave radio systems may be found carrying anywhere from a few voice channels to more than thirty thousand. Rough or impassable terrain may preclude the laying of any type of cable, leaving microwave radio as the only practical way of providing even a few channels.

Carrier transmission systems make use of frequency division multiplexing (FDM) and time division multiplexing (TDM). Each of these multiplexing techniques is discussed in the following sections. Table V lists some of the characteristics of major Bell System long-haul and short-haul wire and cable multiplex systems. The tables indicate the types of multiplex equipment used with various transmission media. The FDM and TDM systems are described further below.

8.2.2.1.1 Frequency Division Multiplex (FDM) Systems

Virtually all FDM carrier systems in use today have their designs based on the requirement to multiplex the so-called "standard" voice channel, which is defined as the frequency band lying approximately between 300 Hz and 3400 Hz. When a number of voice channels are to be combined for transmission over a single medium, the FDM system shifts each basic 300 - 3400 Hz channel to a different frequency band and "stacks" the signals for simultaneous transmission.

To allow for adequate spacing between voice bandwidths and ensure against one channel interfering with another, 4 kHz is allotted to each

TABLE V

MAJOR BELL SYSTEM CARRIER SYSTEMS
SHORT HAUL

	<u>N1</u>	<u>N2</u>	<u>O</u>	<u>ON1</u>	<u>ON2</u>	<u>T1</u>	<u>N3</u>	<u>T2</u>
Line Facility	Cable	Cable	Open Wire	Cable	Cable	Cable	Cable	Cable
Channels on Cable Pair	12	12	16	20	24	24	24	26
or Coaxial Tube								
Multiplex Type	FDM	FDM	FDM	FDM	FDM	TDM	FDM	TDM
Frequency Allocations								
Lowest Trans.Freq.(KHz)	36	36	2	40	36	(1)	36	(2)
Highest Trans.Freq.(KHz)	268	268	156	264	268	(1)	268	(2)
System Length (Miles)								
Minimum	15	15	15	15	15	10	35	--
Maximum	200	200	150	200	200	50	200	500
Approx. Repeater Spacing	5	5	50	5	5	6000 Ft.	5	205
(Miles)								

NOTES:

- (1) Line signal consists of bipolar pulses at rate of 1.544×10^6 bits/sec which occupies band between DC and 1.544 MHz.
- (2) Line signal consists of bipolar pulses at rate of 6.32×10^6 bits/sec which occupies band between DC and 6.312 MHz.

TABLE V (Continued)

MAJOR BELL SYSTEM CARRIER SYSTEMS
LONG HAUL

Line Facility Channels on Cable Pair or Coaxial Tube	C5	J2	K2	L1	L3	L4	L5
Multiplex Type	Open Wire	Open Wire	Cable	Coax	Coax	Coax	Coax
Frequency Allocations							
Lowest Trans. Freq. (kHz)	3	12	12	600(1)	1860(2)	3600	10,800
Highest Trans. Freq. (kHz)	FDM	FDM	FDM	FDM	FDM	FDM	FDM
System Length (Miles)							
Maximum	60	125	75	75	75	75	75
Minimum	1000	4000	4000	4000	4000	4000	4000
Approx. Repeater Spacing	150	30	17	8	4	2	1

100

NOTES:

- (1) Or two one-way TV Channels
 (2) Or 660 Telephone Channels and two one-way TV Channels

channel in most modern multiplex systems. For example, on one open wire carrier system, 12 voice channels are simultaneously carried on a single pair using a 108 kHz bandwidth. Two mutually exclusive frequency ranges are used on the same wire pair to effect two-way transmission. In one direction, 12 voice conversations are inserted between 40 kHz and 88 kHz, and in the opposite direction, the band between 100 kHz and 148 kHz carries 12 voice bandwidths.

Many cable carrier systems are similar but usually operate in different frequency ranges. For example, Bell's N-carrier system transmits 8 KHz channels (double sideband channels) for each voice channel and places 12 such double-sidebands between 36 kHz and 140 kHz in one cable section, and 164 kHz and 268 in the next. A separate pair is used for each direction of transmission.

A standard plan for high capacity multiplex systems, which ride either radio or coaxial cable media, assembles 12 voice channels into a basic "group" having a frequency range of 60 kHz to 108 kHz. Five groups are then combined to form a basic 60-channel "supergroup" in the range 312 kHz to 552 kHz. Ten supergroups are combined to form a basic 600-channel "mastergroup" lying between 564 kHz and 3084 kHz. Six mastergroups are combined to form a basic 3600-channel "jumbogroup" lying between 564 kHz and 17.548 MHz.

A class of low-capacity multiplex systems permits the superposition of more than one channel on one or two pairs between a group of telephone instruments and an exchange office. Such multiplex systems are referred to as "station carrier" or "subscriber carrier" systems. Station-carrier systems have a number of different channel capacities and modulation plans. A typical 6-channel system uses an 8 - 56 kHz band for transmission in one direction and 72 - 140 kHz for the other direction over a single pair.

In today's telecommunications systems, the 300 - 3400 Hz voice channels carry not only voice conversations but also digital data signals. Voice channels can also be subdivided into low-speed data or teletype channels by means of filtering techniques. For example, a bandwidth of 120 Hz can carry a 75 bps teletype channel so that up to 25 such channels (each modulating its own subcarrier) can be made to share a single voice channel.

In most high-capacity frequency division multiplexed carrier systems, pilot signals are transmitted along with the voice channels to aid in monitoring a system's performance and to provide alarm capabilities in the event of system degradation or failure. Pilots are often surveyed during routine maintenance and trouble-shooting as an indication of trouble location and general system performance.

8.2.2.1.2 Time Division Multiplex (TDM) Systems

A TDM system permits the simultaneous transmission of a number of individual digital signals over a single path by synchronously sequencing pulses taken alternately from each separate signal into a single bit stream. TDM equipments exist which can handle low-speed data (teletype), voice-band data (1200 - 9600 bits per second), or wideband data (above 9600 bits per second).

TDM systems have found their most widespread usage in Bell's T1 cable-carrier and similar systems. In the T1 cable-carrier system, voice signals are sampled 8000 times per second. Each sample is encoded into an eight-bit binary number. This process is referred to as "Pulse Code Modulation (PCM)". The T1-carrier system has a capacity of 24 channels producing an $8 \times 24 = 192$ -bit frame. One synchronization bit is added at the end of each frame, making a 193-bit total frame length. Since 8000 samples are made on each

channel in each second, there are 8000 frames transmitted each second. Consequently, a pulse rate of $8000 \times 193 = 1,544,000$ bps is sent into the line.

8.2.2.1.3 Impact of Multiplex on Interceptability

There are several ways in which the use of multiplex over communications media impacts the interceptability problem. The principal effect of multiplex is to make interception equipment and systems more complex, voluminous, power consuming and, of course, more costly. With the large variety of multiplex systems used on wire and cable, additional effort is required on the part of the interceptor to determine the type of multiplex used in order to have the proper match for demultiplexing. The interceptor has some flexibility as to where in the interception process the demultiplexing must be performed; that is, he may record the signal and demultiplex it at a later time in another location.

The sensitivity of the wideband multiplexed signals carried by cable has a significant impact on an interceptor's ability to penetrate and tap such systems. As indicated previously, the transmissions are easily perturbed by improperly designed tapping devices. These perturbations cause frequency-dependent variations in the signal levels received at the terminal central office. In addition, the wideband multiplexed signals also have "pilot" signals riding along with the information signals. In many cases the pilot signals will trigger an alarm in the central office if their levels are significantly affected by inexpert interception.

The sensitivity of the wideband multiplexed signal may mean that an interceptor must employ more costly, carefully designed equipment and must have a higher degree of expertise than that required for simple wire tapping or radio interception activities.

8.2.2.2 Signaling Systems

There are two basic categories of signaling systems used in the telephone industry: Voice Channel Signaling and Common Channel Inter-office Signaling. Each of these is discussed below and the impact on interceptability is assessed.

8.2.2.2.1 Voice Channel Signaling

Communications networks, large or small, require a means for the various nodes of the network to tell each other what interconnections are desired and to respond to such requests with appropriate information regarding their operating status on a real-time basis. Examples of responses commonly encountered by telephone subscribers are: A dial-tone that tells a subscriber that a dial switch is ready to accept his dialing the number representing the destination of his call; a busy-tone that is received when the number dialed is already connected to the network; and a trunk-busy-tone signifying that all network paths between the caller and his destination are unavailable. In addition to these well-known information signals, there are other information paths between nodes of which the subscriber is normally unaware. These make requests, pass information, and respond appropriately to operate the network in the proper fashion.

The jargon used in the communications industry developed progressively as the systems themselves evolved. The following paragraphs define some of the terminology used in the communications industry.

Definitions of Signaling Terminology

In order for one end of a communications circuit to call the other (establish a call), the calling end of the circuit must notify the called end that a communication is desired. This

notification is accomplished by means of "signaling". A completed call (or connection) may consist of several communications circuits in tandem, each of which has been selected from a number of alternative paths. In this case the connection is said to be a "switched" call regardless of whether a human operator or a device performs the interconnection, and signaling always participates in some way or other in establishing the connection.

It is obvious then, that in telecommunications jargon the noun "signaling" and the verb "to signal" have meanings that are quite distinct from the everyday uses of the words. The following examples demonstrate the meanings of the word "signaling" as used in the telephone industry:

(1) When one end of a circuit informs the other end, by whatever means, that a communication is desired, the calling end is said to "signal" the called end. Sometimes the motive for this act is to have the signaled end add another circuit in tandem with the first to reach a more distant point. When this occurs, the call is not "completed" until the most distant point is added to the connection.

(2) When a switched call is being set up, one end of a circuit transmits information to the other regarding the destination, routing, and nature of a call.

(3) When a switched call is being set up, some point along the connection tells the calling end what is happening to the call or why it cannot be completed.

"Signaling" is an ambiguous term. It can be used as the verb as defined above, or it can denote the entire assemblage of equipment and facilities required for one end of a circuit to signal the

other. For example, out-of-band signaling systems, the single frequency (SF) signaling system, and the common channel interoffice signaling system (CCIS) are all used to transmit "supervision" and dial pulse signals from one switch to another in the public dial network.

Types of Signals

The three meanings given above for the verb "to signal" can be aligned with the three signal categories commonly employed on telephone circuits. They are:

(1) Supervisory signals - These signals originate from telephone sets or PBX's at subscriber locations. An "off-hook" signal is produced when a telephone set is taken off-hook (i.e., receiver is removed from the cradle), and an "on-hook" signal when a telephone set is put on-hook (hung up). The off-hook signal tells a central office that a subscriber wants to make a call (or remain connected) and the on-hook signal indicates that the subscriber is finished with the connection. On trunk circuits, supervision is used by one dial switching machine to tell another that an attempt will be made to establish a call, and, at the end of the call, that a connection will be relinquished. By analogy, machine-to-machine signals are also referred to as "off-hook" and "on-hook" signals.

(2) Dial Pulse Signals - Whether rotary dial signals or Touch-tone signals are generated by a telephone, the dial-pulsing tells the dial switching machine at the local central office the number the subscriber wants to call. Similarly, on trunk circuits, whether direct current (DC) dial pulsing or Multi-Frequency (MF) pulsing is employed, the dial-pulsing from the calling machine tells the called machine the destination of the call being established. Touch-tone and MF signaling both represent each dialed digit by a combination of two frequencies passed over the voice channel. Touch-tone is used on subscriber lines and is a different set of frequencies from the MF used on trunks. Both the rotary dial at the customer

locations and the pulsing from some dial machines make use of DC dial-pulses to transmit dialed digits. The digits are transmitted by starting from the off-hook state and sending forth a series of on-hook pulses for each dialed digit. Touch-tone is becoming more common in telephone sets and the majority of trunks transmit pulses using MF.

(3) Information Signals - These are usually complex audible tones or announcements that give the caller information about the state of the call being established; e.g., dial tone, busy tone, trunk busy tone, audible ringing tone, and recorded announcements. These signals are usually not part of specific signaling systems on trunk circuits. They generally originate from dial machines or PBX's and are sent over the local loop to the caller.

Trunk and Intertoll Signaling Systems

Private line circuits and public switched network trunks, although designed and used for different purposes, often employ the same type of signaling systems over the facilities between the local central offices which serve all subscribers. Therefore the description of a relatively few signaling systems will suffice to cover the operation of signaling systems for most existing trunk and private line circuits.

(1) The Single Frequency (SF) Signaling System

SF signaling systems are intended to pass supervision and dial pulses over voice frequency channels. This is done by using the DC supervisory conditions or dial pulses to control the presence of a 2600 Hz tone on the voice channel. Thus an on-hook condition is indicated by the presence of the 2600 Hz SF tone on the voice channel and an off-hook by the absence of SF tone. The SF signals are carried over the same four-wire voice channel that is used for conversation. Normally, the SF tone does not remain on the line during conversation.

The present standard SF inband signaling system employs 2600 Hz in each direction on four-wire circuits, and both 2600 and 2400 on the same voice path on two-wire circuits. The SF signaling system can be used on a variety of wire and radio systems.

(2) Out-of-Band Signaling Systems

The Bell N1, N2, 0 and ON-carrier systems employ "out-of-band" signaling systems using 3700 Hz as the signaling frequency. The term "out-of-band" refers to the fact that the signal is outside of the 300 - 3300 Hz bandwidth allocated for the voice signal. An off-hook on the near end cuts off the transmitted 3700 Hz, and when the distant receive end detects the loss of 3700 Hz, it outputs an off-hook along with the voice signal for transmission on the line. Lenkurt has an out-of-band signaling system that uses a 3825 Hz tone.

(3) TDM Signaling Systems

The Bell T1-carrier and the Lenkurt 9002A-Carrier systems have TDM digital signaling systems built into the digital transmission system. In a digital channel bank the voice channel and signaling inputs are sampled separately for conversion to a digital pulse train. Each signaling pulse train is time division multiplexed with the digitized voice for transmission over the digital line. As with voice communications, each signal amplitude is also encoded into a binary number. The binary signaling information is transmitted as the least significant bit of the eight-bit voice amplitude number once every sixth frame.

It is quite often the case that the built-in signaling of PCM/TDM systems is not used at all, and an SF signaling system is superimposed on the voice path. The SF signal is then subjected to PCM/TDM processes identical to normal voice conversation information.

8.2.2.2.2 Common Channel Interoffice Signaling (CCIS)

In an effort to modernize their inter-switch signaling, Bell has introduced the CCIS. Bell is not the first nor the only organization to utilize forms of common channel signaling. Individual telephone organizations outside of and within the Bell System have used channels of voice frequency carrier telegraph (VFCT) systems to extend DC signaling leads between switches for years. Such telegraph circuits used for signaling purposes are called "signal paths". Lenkurt has recently developed the 11A Common Channel Signal System which time division multiplexes the signaling systems for 24 voice circuits onto a single common voice channel.

The Bell CCIS design differs from its forerunners in that it transfers not only normal supervision and dial pulsing from one switch to another, but also passes network management and maintenance information. The CCIS will transmit signaling/network management/maintenance information for a large number of trunks over, at least, a single high speed data link, and, at most, a large multipath packet switching network of high speed data links.

When the CCIS is applied to a trunk group, all SF or built-in signaling systems must be removed from the trunks and disconnected from the switches. The signaling information for the trunk group is passed over a CCIS signaling link or network inserted directly between the switching machine processors. The CCIS terminal interconnects the switch processor to a modem which, in the simplest case, will communicate with a like modem at the distant switch. The CCIS modems presently operate at 2400 bits per second, but this may eventually be increased to 4800 bits per second.

Processor signaling information is transmitted as a parallel 28-bit word to the data modem via the signaling terminal. Twenty bits are useful data, and 8 bits are for error checking.

When more complex CCIS's are deployed, certain switches known as signal transfer points (STP's) will act as nodes for passing the information packets originating on one signaling link over to the next signaling link in the network. The CCIS will be implemented by dividing the country into geographic "signaling regions", each containing two STP's. Each toll office in a signaling region will be interconnected to both STP's to provide signal routing diversity. The two STP's in one region will be interconnected with each other and fully interconnected with the STP's in another region in such a way that each STP has links to every other STP.

When the CCIS is fully implemented, it appears that the information regarding signaling on specific trunks will often be routed through multiplex systems that will take completely different routes than the voice conversations. On some occasions it appears that CCIS information routing may change from call to call.

8.2.2.2.3 Impact of Signaling Systems on Interceptability

This section addresses the impact of the two types of signaling on communications interceptability.

Impact of Voice Channel Signaling Systems on Interceptability

An interceptor can take advantage of signaling system information to reduce the amount of time and effort required to target the communications of specific individuals or organizations. Special signal decoding equipment could be developed for use in tapping a local loop. The signal decoder could recognize both on-hook and off-hook conditions and the dialing of telephone numbers of interest.

Decoding equipment could be used in the intercepting of trunk circuit communications to sort through the telephone numbers being forwarded between switches and to find particular numbers. The decoding equipment could be used to turn recording equipment on and off, making unattended operation of the intercept equipment possible.

The most common voice channel signaling system used on trunk circuits in this country is the 2600 Hz in-band SF signaling system. The SF signaling system is used mainly for supervision on long-haul trunk circuits; dial pulses are passed mainly by means of multi-frequency (MF) pulses. The interceptor's equipment must be able to detect both SF supervision and MF dial pulses. The important simplification which arises from the use of in-band SF signaling is the common sharing of the voice trunk circuit by the signaling tones.

Interceptor uses of the 3700 Hz out-of-band signaling system benefits and constraints are almost identical to those of the SF signaling system. The only difference between the two systems is that the out-of-band signaling system lies outside (beyond the upper edge) of the voice band used by the subscriber. The dial numbers are still mainly transmitted using MF pulses, but DC dial pulsing is employed to a somewhat greater extent.

The TDM signaling system of the T1-Carrier PCM system requires a digital decoder which most logically would be made an integral part of the TDM/PCM voice demodulator used to separate the multiplexed channels on such a system. However, even in this case the supervision and signaling will generally remain associated with the voice trunk sought by the interceptor.

Impact of Common Channel Interoffice Signaling (CCIS) on Interceptability

Common channel interoffice signaling (CCIS) systems entail both some benefits and serious drawbacks for the interceptor. On the plus side there are strong indications that not only will the dialed number (destination) be transmitted from the originating switch but the calling number will also be transmitted. This would permit the interceptor to pin down calls that should be intercepted much more closely than he can by using only the destination number. The cross-section of calls to be monitored is markedly decreased. In fact, the interceptor could select calls on the basis of calling numbers only. This would not be possible without the CCIS.

On the negative side, the CCIS information packets must be decoded and will, in all cases, ride a totally different voice channel than the sought-after conversation. In fact, when CCIS is more fully implemented, it is probable that the signaling information will occupy a different route than the sought-after conversation. Due to the switched packet nature of the CCIS with multiple redundant paths, the signaling packets may travel different routes from time to time. The following variations may be encountered by the would-be interceptor in the event CCIS is fully deployed:

- (1) The voice conversation to be intercepted rides one channel of a multiplex system on a route, and the CCIS signaling packet rides another channel on the same route;

- (2) The voice conversation to be intercepted rides one route, and the CCIS signaling packet rides a different route;

- (3) The voice conversation to be intercepted rides one kind of medium, and the CCIS signaling packet rides a different medium and different route (for example, the voice conversation is on microwave and the CCIS is on a coaxial cable);

(4) The voice conversation to be intercepted rides one route and the CCIS signaling packet is switched between two routes which are different from that of the voice channel.

Thus, it appears that there are both targeting advantages and disadvantages to be derived from the CCIS.

8.2.3 Vulnerability of Communication Systems as a Function of the Network Type

This section addresses the vulnerability of communications systems to electronic interception from the viewpoint of the type of network that has been formed using combinations of the switching systems and transmission media. Factors considered in this analysis include:

- (1) whether the network provides switched or dedicated service,
- (2) the type of traffic carried by the network (e.g., voice, data, teletype)
- (3) the point on the network chosen for making the interception, and
- (4) the targeting requirements of the subscriber.

This section is divided into four subsections in order to minimize repetition and reduce the discussion to a manageable size while covering the full range of variables. The first subsection discusses the vulnerability of voice traffic on the public telephone switched (Direct Distance Dialing) network. The second and third subsections consider the vulnerability of message traffic on the switched teletype networks and of voice traffic on dedicated networks, respectively, as variations from the discussion in the first subsection. The fourth subsection discusses the variations due to data traffic carried by the networks from the considerations in the first three subsections.

Although this study has assumed that the interceptor does not have access to the premises of the targeted subscriber or the offices of the common carrier, it is necessary to consider the types of equipments used by the subscriber within his premises. Therefore, the first subsection has been further subdivided into sections covering various situations. The first is the situation where the communication of interest occurs between subscribers having only one telephone on each of their premises (e.g., private residences, small business, etc.). Subsequent sections cover the variations in vulnerability due to a PBX or a Centrex located on the subscriber's premises, a Centrex located at a telephone company central office and the special case of a subscriber to Wide Area Telephone Service (WATS).

Each situation is further subdivided into specific cases, each of which considers the vulnerability of a portion of the network (e.g., drop wire and distribution cable, main and branch feeder cables, etc.). Each case is discussed in terms of the communication plant characteristics, intercept equipment required, strategies the interceptor might use, how the interceptor might be detected and constraints on the interceptor.

The vulnerability of a particular network is also dependent on those objectives of the interceptor which determine what or who will be the target of his intercept activities. The communications of interest may concern only one targeted individual, communications between two specific individuals, the communications of a particular office or department (e.g., the purchasing department) of a business, a certain type of information (e.g., grain futures) or any of a number of other possibilities. Consideration of all the possible targeting variations is beyond the scope of this report. However an indication of the consequences of the range of targeting possibilities

can be obtained by considering two extremes for each specific case: Random snooping (no specific target) and the targeting of specific individuals.

8.2.3.1 Public Direct Distance Dialing Network (Voice Traffic)

8.2.3.1.1 Single Telephone to Single Telephone

A simplified block diagram of the public direct distance dialing network is shown in Figure 20.

Case 1: Drop wire intercept (Intercept of communications between A and B, A and C, or A and D)

Random Snooping:

Communication plant characteristics:

One wire-pair for 2-way communication at voice-band frequencies

Intercept Equipment:

Required equipment: A high impedance wire-tap and headphones (No external power source necessary)

Optional equipment: Low power audio amplifier, tape recorder, signaling decoder (could be battery powered)

Strategy for Interceptor:

Point of intercept could be at entrance to building, at connection to the distribution cable or along the drop wire. The monitoring station could be located at a point removed from the location of the tap.

The impedance of the wire tap can be increased (decreasing the probability of detection by telephone company personnel if they test the subscriber loop) by placing a low power audio amplifier near the tap point. The audio amplifier is required if the monitoring station is located more than a few yards from the tap point.

The party being called by the subscriber could be identified by using a signaling decoder to obtain the telephone number of the called party.

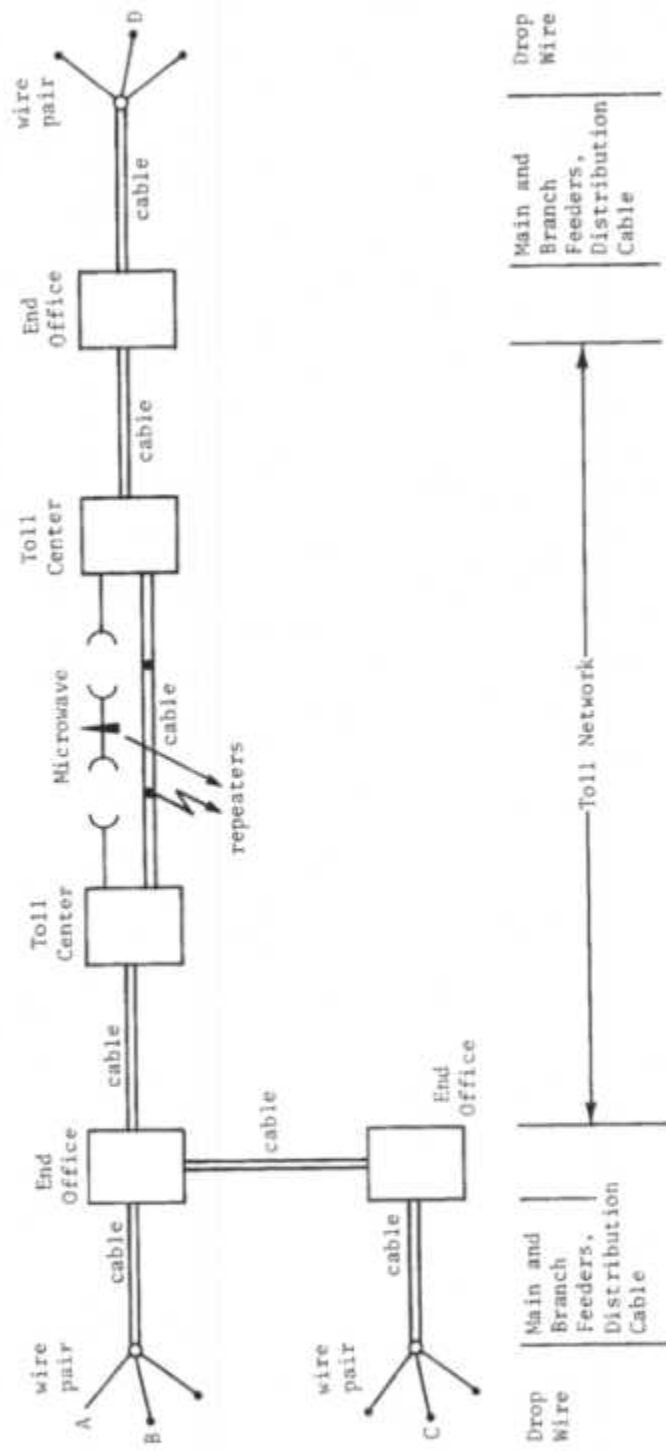


FIGURE 20
DIRECT DISTANCE DIALING NETWORK

The tape recorder could be used to refresh the interceptor's memory at a later time or allow the monitoring station to be unattended for extended periods of time. The signaling decoder could be used to turn the tape recorder on only when an "off-hook" condition is detected, thus decreasing the amount of tape required.

Detection of Interceptor:

Observation of tap or monitoring station either by local citizens, telephone company employees or police. The tap might be detected by telephone company employees at the central office testing the subscriber loop if the impedance of the wire tap is too low.

Constraints on Interceptor:

Interceptor would be rather conspicuous, particularly if seen digging up buried drop wire, climbing pole or penetrating a terminal housing.

Targeting Specific Individuals

(Only the differences due to targeting specific individuals will be listed.)

Communication plant characteristics:

Numerous drop wires in most areas. Communications between A and B will appear only on the drop wire, distribution cable, branch feeder cable or main feeder cable. The same situation exists if A and B are connected to different exchanges but the exchanges are collocated.

Intercept equipment:

Optional equipment: A ring generator and microphone (could be battery powered).

Strategy for Interceptor:

Locate structure housing the targeted telephone. If the targeted telephone is the only one in the structure, physically trace (if overhead) or look for nearest "appearance" (if buried). If the targeted telephone is one among many in the structure (e.g., apartment building), look for telephone terminal housing. Determine correct circuit by listening to each line until correct circuit is found. A ring generator and microphone could be used to ring the telephone on each circuit and talk to individual who answers until correct line is found.

- Case 2: Main feeder cable, branch feeder cable, or distribution cable (Intercept of communications between A and B, A and C, or A and D)

Random Snooping

Communication plant characteristics:

- Case 2.a. Multiple open wires or multi-pair cable for 2-way communication over individual pairs at voice frequencies
- Case 2.b. Open wire or multi-pair cable using a carrier multiplex system (FDM or TDM) (Main or branch feeder cable only)

Intercept equipment:

- Case 2.a. Required equipment: Tools for penetrating cable (if used), a high impedance wire tap and headphones (No external power source necessary)
- Optional equipment: Low power audio amplifier, tape recorder, signaling decoder (could be battery powered).
- Case 2.b. Required equipment: Tools for penetrating cable (if used), one or two high impedance wire tap(s), one demultiplexer with two outputs or two demultiplexers, a mixer (could be battery powered)
- Optional equipment: Tape recorder, signaling decoder (could be battery powered)

Strategy for Interceptor:

- Case 2.a. Point of intercept could be at "appearances" or along main or branch feeder cable. The monitoring station could be located elsewhere by running own wires or by making use of telephone company wires.
- Case 2.b. Point of intercept could be at "appearances" or along main or branch feeder cable. Determine type of multiplex used. The monitoring stations could be located elsewhere, but some equipment would have to be located near point of intercept.

Detection of Interceptor:

Observation of tap point or monitoring station by telephone company employees or police.

Constraints on Interceptors:

Risk of inadvertently setting off central office alarm is increased, particularly if tap is made into multiplex system.

Targeting Specific Individuals

Communication plant characteristics

Communication between A and B will appear only at the distribution, branch and main feeder cables or the dropwire. The same situation exists if A and B are connected to different exchanges but the exchanges are collocated.

Intercept equipment:

Optional equipment: A ring generator and microphone (could be battery powered).

Strategy for Interceptor:

Case 2.a. Determine correct circuit by listening to each line until correct circuit is found. A ring generator and microphone could be used to ring the telephone on each circuit and talk to individual who answers until correct line is found. Search time could be significantly reduced by physically tracing a subscriber line through cable appearances if the interceptor is familiar with the "home count" pattern used by the local telephone company.

Case 2.b. Determine correct circuit by listening to each multiplex channel until correct circuit is found.

Case 3: Intercept point on trunks between end office and other end office, tandem office or toll center (Intercept communications between A and C or A and D)

Random Snooping

Communication plant characteristics:

Case 3.a. Multiple open wires or multi-pair cable for 2-way communication over individual pairs at voice frequencies

Case 3.b. Multi-pair cable using 2 pairs for 2-way communication at voice frequencies

Case 3.c. Open wire or multi-pair cable using a carrier multiplex system (FDM or TDM)

Case 3.d. Coaxial cable

Intercept equipment:

Case 3.a. Required equipment: Tools for penetrating cable (if used), a high impedance wire tap and headphones (no external power necessary)

Optional equipment: Low power audio amplifier, tape recorder, signaling decoder (could be battery powered)

Case 3.b. Required equipment: Tools for penetrating cable, two high impedance wire taps, a mixer and headphones (no external power required)

Optional equipment: Two low power amplifiers, tape recorder, signaling decoder (could be battery powered)

Case 3.c. Required equipment: Tools for penetrating cable (if used), one or two high impedance wire tap(s), one demultiplexer with two outputs or two demultiplexers with two outputs, a mixer and headphones (could be battery powered).

Optional equipment: Tape recorder, signaling decoder (could be battery powered)

Case 3.d. Required equipment: Tools for penetrating cable, coaxial probe, two demultiplexers, a mixer and headphones (could be battery powered)

Optional equipment: Tape recorder, signaling decoder (could be battery powered).

Strategy for Interceptor:

Cases 3.a. and b. Locate physical route. Point of intercept could be at repeaters (if any) or along wire or cable. The monitoring station could be located elsewhere by running own wire or bridging to a nearby local loop (if any).

Cases 3.c. and d. Locate physical route. Point of intercept could be repeaters (if any) or along wire or cable route. Determine type of multiplex used. Monitoring station could be located

elsewhere but some equipment would have to be located near point of intercept.

Detection of Interceptor:

Observation of tap point or monitoring station by telephone company employees or police.

Constraints on Interception

Risk of inadvertently setting off alarms at telephone company switching centers. Digging up buried or underground cable is a rather conspicuous activity but interceptor may have no choice if there are no repeaters on the circuits and the entire route is either buried or underground. Repeater enclosures are likely to be locked and some may be alarmed. Multipair and coaxial cables may be pressurized and alarmed.

Targeting Specific Individuals

Communication plant characteristics:

The two switching machines are connected together by trunks. The collection of all trunks connecting the two machines form a trunk group. The two end offices serving the targeted individuals may be connected via alternate trunk groups. For example, A and C might be connected thru a high usage trunk group between their respective end offices, but an alternate path would also be available through trunk groups connecting the end offices to a toll center or tandem office. A high percentage of the traffic between the two end offices would be handled by one preferred trunk group. Trunk group sizes vary from relatively few to over a hundred trunks. Many other trunks and/or feeder cables may also occupy the same physical route. Most switching machines will select trunks within the trunk group in a specific order. (Although some new machines use a random selection process.)

Intercept Equipment

Optional equipment: Multiple-input signaling decoder, signal generator with acoustic coupler, signal detector, microprocessor (could be battery powered)

Strategy for Interceptor:

Location of the particular physical route of the preferred trunk group and the specific trunks that make up the preferred trunk group by physical survey to determine location of possible routes and testing trunks in each (starting with likeliest route). Search can be considerably

simplified by a priori knowledge such as the type of route (overhead, buried or underground, open wire, 2-wire multi-pair cable, 4-wire multi-pair cable or coaxial cable), type of multiplex (if any) used, type of signaling used, etc. Testing of trunks might consist of simply listening to conversations on individual trunks. Considerable time might be saved by employing two confederates at telephones in each exchange area to make calls to each other. A distinctive signal would then be acoustically coupled via the telephone hand set for transmission over the circuit and detected by the monitor. The distinctive signal could be as simple as an agreed-on phrase(s) spoken by either (or both) confederate(s) or an electronic signal generator which could be automatically detected by means of an electronic detector.

After locating the trunks in the preferred trunk group, the interceptor might simply tape record all trunks and sort out the communications of interest later by listening to each channel, one at a time. Considerable effort might be saved for cases 3.a. and 3.b. if the interceptor employed a multiple-input signaling decoder (one input for each trunk) which could detect when either of the targeted telephones was being called. A microprocessor could be used to advantage in cases 3.c. and 3.d. to control the demultiplexers, signaling decoder, signal detector and tape recorder.

Constraints on Interceptor:

Interceptor will not be able to intercept conversations between A and B nor monitor all conversations of a particular single target. The interceptor must either accept the probability that some communications of interest will not appear on the preferred route or also monitor additional routes.

Case 4: Intertoll Routes (Intercept of communications between A and D)

Random Snooping

Communication plant characteristics:

- Case 4.a. Multi-pair cable using 2 pairs for 2-way communication at voice frequencies
- Case 4.b. Multi-pair cable using a multiplex system
- Case 4.c. Coaxial cable routes
- Case 4.d. Terrestrial microwave routes
- Case 4.e. Satellite microwave routes

Intercept equipment:

Case 4.a. Required equipment: Tools for penetrating cable, pressure sealant or bypass, two high impedance wire taps, a mixer and headphones (no external power required)

Optional equipment: tape recorder, signaling decoder (could be battery powered)

Case 4.b. Required equipment: Tools for penetrating cable, pressure sealant or bypass, two high impedance wire taps, two demultiplexers, a mixer and headphones (could be battery powered)

Optional equipment: Tape recorder, signaling decoder (could be battery powered)

Case 4.c. Required equipment: Tools for penetrating cable, pressure sealant or bypass, two coaxial probes, two demultiplexers, a mixer and headphones (could be battery powered)

Optional equipment: Tape recorder, signaling decoder (could be battery powered)

Case 4.d. and e. Required equipment: one or two antennas, two RF receivers, two demultiplexers, a mixer and headphones (need motor-generator set or access to AC power)

Optional equipment: Tape recorder, signaling decoder (use same power source as above), Van, or fixed structure for housing equipment.

Strategy for Interceptor:

Case 4.a. Locate physical route. Point of intercept could be at repeaters or along cable route. Monitoring station can be located elsewhere by running own wire or bridging to a nearby local loop (if any).

Case 4.b. and c. Locate physical route. Point of intercept could be at repeaters or along cable route. Determine type of multiplex used. Monitoring station could be located elsewhere but some equipment would have to be located near point of intercept.

Case 4.d. Locate physical route. Point of intercept could be near microwave tower with small antenna or up to several miles to either side of line between towers with larger antennas. Determine type of multiplex used.

Case 4.e. Point of intercept can be anyplace within the coverage area of the downlink beam (nearly an entire hemisphere of the earth for the INTELSAT "Global" beam, the entire U.S. for domestic satellites, and several thousands of square miles for spot beams). Both sides of the communication will be available to the interceptor unless two spot beams covering different areas are used. One antenna is required in the former case, two antennas in the latter case, one of which picks up uplink transmission from the earth station. Also need to determine the type of multiplex used. Intercept equipment (particularly the large antenna) could be hidden in a large barn. Another possibility would be to subvert a legitimately installed antenna such as subscriber-owned earth stations or astronomical observatories, or to set up an intercept station which has the outward appearance of such legitimate enterprises.

Detection of Interceptor:

Case 4.a., b., and c. Observation of tap point or monitoring station by telephone company employees or police.

Case 4.d. If van with small antenna is used: Observation of van which stays near tower for extended period of time by telephone company employees, police or other officers in the area (e.g., forest rangers, game wardens, etc.). If intercept equipment in open or van with 3-foot or larger externally mounted antenna, observation of antenna by telephone company employees, police or other officers in the area. If housed within a building or other structure probability of detection is quite small.

Case 4.e. Observation of large antenna (15 feet or larger) by police or other officers unless in large structure such as a barn.

Constraints on Interceptor:

Case 4.a., b., and c. Risk of inadvertently setting off alarms at telephone company switching centers. Digging up buried or underground cable is a rather conspicuous activity while repeater

enclosures are likely to be alarmed. Most cables are likely to be pressurized.

Case 4.d., and e. Radio reception equipment is likely to be quite costly, particularly for satellite intercept and require very knowledgeable person to assemble and operate. Risk of being observed unless in area not frequented by others or equipment can be completely housed within a normal structure (shed, house, barn, apartment, etc.)

Targeting Specific Individuals

Communication plant characteristics:

Trunks in a particular trunk group normally will be divided between more than one physical route (usually two or three). If the intertoll route is a long haul route, several different types of route sections (multi-pair cable, coaxial cable or radio) and multiplex systems may be used in tandem. Physical routes which might be carrying the trunks of interest may be separated by hundreds of miles at some points. The number of trunks in a trunk group vary from relatively few to many tens of trunks while the total number of trunks which must be searched to find the trunks of interest could number several tens of thousands. Additional switching centers may intervene between the two toll centers serving the end offices of interest.

Intercept equipment (additional)

Optional equipment: Multi-input signaling decoder, signal generator with acoustic couplers, signal detector, microprocessor or mini-computer (may need source of AC power)

Strategy for interceptor:

Location of the particular physical routes of the preferred trunk groups and the specific trunks making up the preferred trunk group by physical survey to determine location of possible routes and testing trunks on each route (starting with the likeliest route). The search can be simplified by locating the point on each

physical route having the least number of trunks. A priori knowledge such as type of route sections, multiplex systems, type of signaling etc. used could also reduce the search effort considerably. Testing of trunks might consist of simply listening to conversations on individual trunks if the total numbers of trunks to be tested is not too great. Considerable time might be saved by employing two confederates as in Case 3 above.

After locating the trunks in the preferred trunk group, the same strategies could be used as in Case 3 above.

Constraints on Interceptor:

The separation of possible physical routes could require considerable time to physically locate all routes and find the point on each route having the smallest number of trunks. The amount of time required to find the trunks in the trunk group of interest could be prohibitively large without some a priori knowledge.

8.2.3.1.2 Between a PBX and Other Telephone Terminations

The simplified switched network diagram shown in Section 8.2.3.1.1 above must be modified to include the PBX as shown in Figure 21.

The number of subscriber loops connecting a PBX to the end office varies from a few to hundreds, depending on the size of the PBX and the needs of the subscriber. If the interceptor is external to the subscriber's premises, he does not have access to A's individual telephone wire, and may find the communication of interest on any of the "outside lines" connecting the PBX to the end office. PBXs always have an operator to handle inward dialed calls. Some PBXs require the PBX operator to dial all inward and outward calls but other PBXs permit outward calls to be made directly without going through the manual switchboard. In either case, the dial information available to the interceptor is the same. (i.e., the called telephone is identified verbally for inward calls and by dial pulses (or Touch-tone pulses) for outward calls).

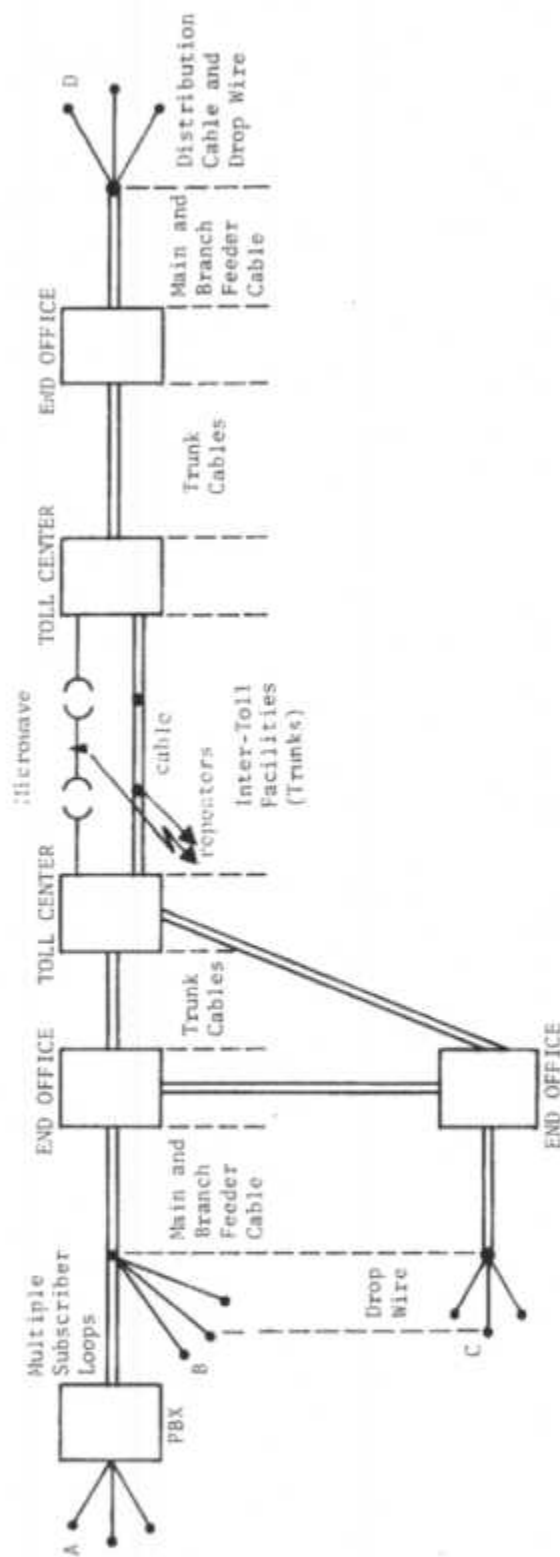


FIGURE 21
PUBLIC DIRECT DISTANCE DIALING NETWORK WITH PBX ADDED

Therefore, the only significant difference from the cases considered for the single-telephone-to-single-telephone-situation are "Case 1: Drop wire or distribution cable intercept" and "Case 2: Main and Branch feeder cables."

Case 1: Dropwire or distribution cable intercept (Intercept of communications between A and B, A and C or A and D)

Random Snooping

Communication plant characteristics:

Multiple pairs of drop wire for small PBXs and multi-pair distribution cable for larger PBXs.

Intercept equipment:

No change

Strategy for interceptor:

No change

Detection of interceptor:

Add: Observation of tap or monitoring station by plant security personnel

Constraint on interceptor:

No change

Targeting Specific Individuals

Communication plant characteristics:

Communication of interest could appear on any of the wire pairs terminating at the PBX.

Intercept equipment:

Optional: change "signaling decoder" to "multiple-input signaling decoder"

Strategy for interceptor:

Locate structure housing the PBX.

If the PBX services all telephones in the structure, physically trace (if overhead) or look for nearest "appearance" (if buried).

If the PBX does not service all telephones in the structure, look for terminal housing. Locate subscriber loops terminating in the PBX by listening to each subscriber loop until all circuits terminating in the PBX are identified. A ring generator and microphone could be used to ring subscribers (PBX operator and others) and talk to individual who answers until correct circuits are found.

After the correct circuits have been identified, all circuits could be tape recorded for listening to each circuit at a later time.

At the risk of losing some of the communications of interest, the interceptor could simply listen-in on a circuit for a short time to determine if the communication is of interest, etc. until he finds the circuit being used by the target.

Recording and/or listening time could be significantly reduced by a multiple-input signaling decoder which indicated when each circuit is in use.

If only conversations between A and B, A and C or A and D are of interest, a multiple-input signaling decoder which has the additional capability to decode outgoing telephone dial pulses could be used to reduce the amount of recording and/or listening time required on outgoing calls (but the interceptor would still have to monitor or record all incoming calls).

Detection of Interceptor:

No change.

Constraints on interceptor:

Must trade-off assurance of intercepting the communication of interest against additional equipment.

Case 2: Main or branch feeder cable (Intercept of communications between A and B, A and C or A and D)

Random Snooping

No change

Targeting Specific Individuals

No change except those noted in Case 1 above relating to the need to monitor all subscriber loops terminating in the PBX.

8.2.3.1.3 Between a Centrex on the Customers Premises and Other Telephone Terminations

The simplified switched network diagram is the same as in Section 8.2.3.1.2 (Figure 21) above except the box labeled "PBX" is labeled "Centrex."

The difference between a PBX and a Centrex is the added capability for direct inward dialing. There is no essential difference for the "random snooping" case.

For the "Targeting Specific Individuals" case, the interceptor has the same options as he has for interception of PBX traffic except that a multiple-input signaling decoder capable of decoding dial pulses can be used to determine when the targeted telephone is being called.

8.2.3.1.4 Between a Centrex Located at an End Office and Other Telephone Terminations

The simplified switched network diagram is the same as in Section 8.2.3.1.1. (Figure 20) above except the box labeled "END OFFICE" is labeled "END OFFICE and CENTREX."

The intercept problem is the same as in section 8.2.3.1.1 above for the case where many telephones are located in the same structure. The interceptor does have one additional opportunity. He can target the internal communications of the subscriber.

8.2.3.1.5 Wide Area Telephone Service

Wide Area Telephone Service (WATS) is a public switched network service whereby one or more access lines are provided the subscriber from his location to a toll center near him. Beyond this toll center, the regular switched distance dialing network is used. A subscriber to this service can be reasonably expected to use WATS for most of his

long distance calls. The various options open to the interceptor are those considered in sections 8.2.3.1.1. thru 8.2.3.1.5 above except that once he has located the access lines (either subscriber loops or dedicated trunks between the subscriber's central office and the toll center), most of the intertoll traffic originated by the targeted subscriber will be available to the interceptor.

8.2.3.2 Teletype Switched Networks

There are two teletype switched networks, TWX and TELEX, both operated by Western Union. Both networks are real time dial-up services. The two networks are interconnected via a message-switching store-and-forward computer system that accepts and records messages, releases the caller from the line, then forwards the message to its destination on an immediate or selectively deferred basis.

8.2.3.2.1 TWX Switched Network

Approximately 5% of the trunks between TWX switches operate via the Direct Distance Dialing public telephone system. Interception of this traffic presents essentially the same problems as that discussed above for the intertoll portion of the Direct Distance Dialing network except the extraction of information requires the additional capability to decode the TWX signal as discussed below.

A simplified TWX switched network diagram is shown in Figure 22.

Case 1: Dedicated Customer Loops - (Intercept of communications between A and B, A and C or A and D)

Communication plant characteristics:

Customer loops usually consist of telephone company drop wire, distribution cable, branch feeder cable, main branch feeder cable and nonswitched circuits between telephone company offices. All but the drop wire will normally share cables with regular voice circuits. It

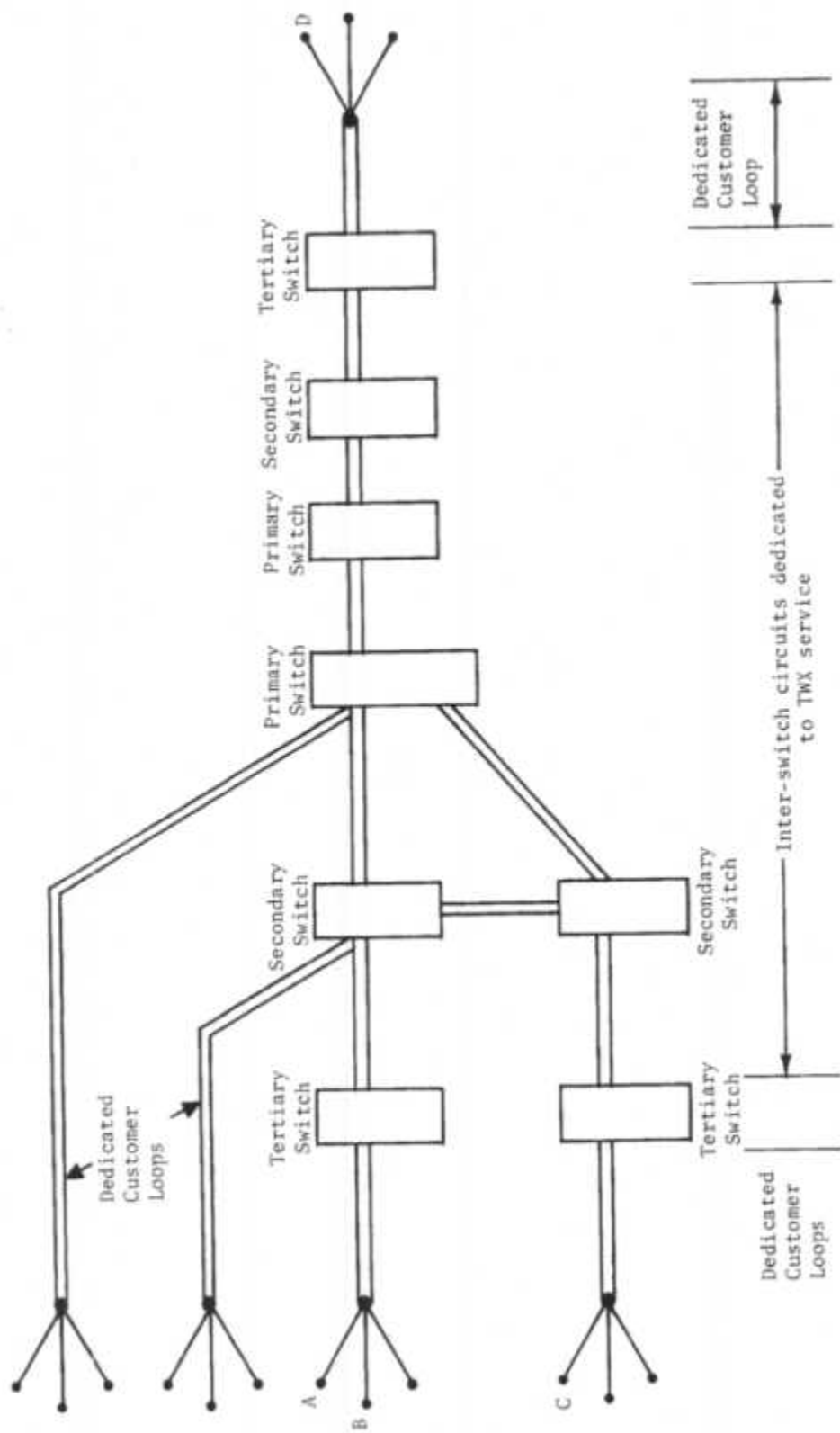


FIGURE 22
TWX TELETYPE SWITCHED NETWORK

is noted that the physical location of customer loops normally will be included with the switched trunks considered in Cases 3 and 4 in Section 8.2.3.1.1 above as well as the non-switched wires and cables considered in Cases 1 and 2. With a few exceptions, a customer loop will be voice grade circuit carrying one teletype circuit. The circuit may be half duplex (a single pair of wires carrying traffic in both directions, but not at the same time) or full duplex (two pairs of wires, one carrying inward traffic and the other carrying outward traffic).

The signal will normally be an electrical current which can take on two different (binary) values. The binary code used in nearly all cases is the American Standard Code for Information Interchange (ASCII) and is transmitted at 110 bits per second (bps). (Some TWX machines operate at 45 bps and use the Baudot code).

Intercept equipment:

The same equipment is required as that for the corresponding cases considered in Section 8.2.3.1.1 above (Direct Distance Dialing network, single telephone to single telephone) except the optional ring generator and microphone and signal generator and signal detector is not needed, but a receive-only teletype machine or equivalent is required. The teletype machine will require a source of AC power.

Strategy for interceptor:

Headphones could be used to identify the circuits carrying the distinctive teletype signal. Otherwise, the strategy would be the same as the strategies considered in Section 8.2.3.1.1 above except in those cases involving trunk groups. In the latter case, only the circuit carrying the teletype signal of interest need be monitored.

A tape recorder could be used to eliminate the necessity of having a teletype machine at the monitoring site.

Detection of Interceptor:

Same as Section 8.2.3.1.1 above plus the possibility of the teletype machine being heard.

Constraints on Interceptor:

Same as Section 8.2.3.1.1

Case 2: Intercept Point on Inter-switch Circuits (Intercept of communications between A and C or A and D)

Communication plant characteristics:

Inter-switch circuit groups may use any of the facilities listed for cases 3 and 4 in Section 8.2.3.1.1 above for the Direct Distance Dialing network. However, wherever possible, Western Union will use its own facilities (mostly Western Union terrestrial and satellite microwave routes).

Many teletype circuits may be multiplexed into one voice circuit. Nearly all such circuits will use frequency shift keyed (FSK) modulation and frequency division multiplex (FDM) techniques.

Interceptor equipment:

In addition to the equipment indicated for Case 1 of this section, the interceptor will require one or two FDM demultiplexers and FSK demodulators. (Could be battery powered).

Strategies for Interceptor:

Headphones could be used to identify the circuits carrying the distinctive teletype signal. The strategies outlined in section 8.2.3.1.1, Cases 3 and 4 can be generally adapted to this case except those involving the ring generator and microphone or the signal generator and signal detector. A tape recorder could be used to eliminate the necessity of having a teletype machine at the intercept site.

Detection of Interceptor:

Same as 8.2.3.1.1, Case 3 and 4 above plus the possibility of the teletype machine being heard.

Constraints on Interceptor:

Same as 8.2.3.1.1, Case 3 and 4 above.

8.2.3.2.2 TELEX Switched Network

A simplified TELEX switched network diagram is shown in Figure 23.

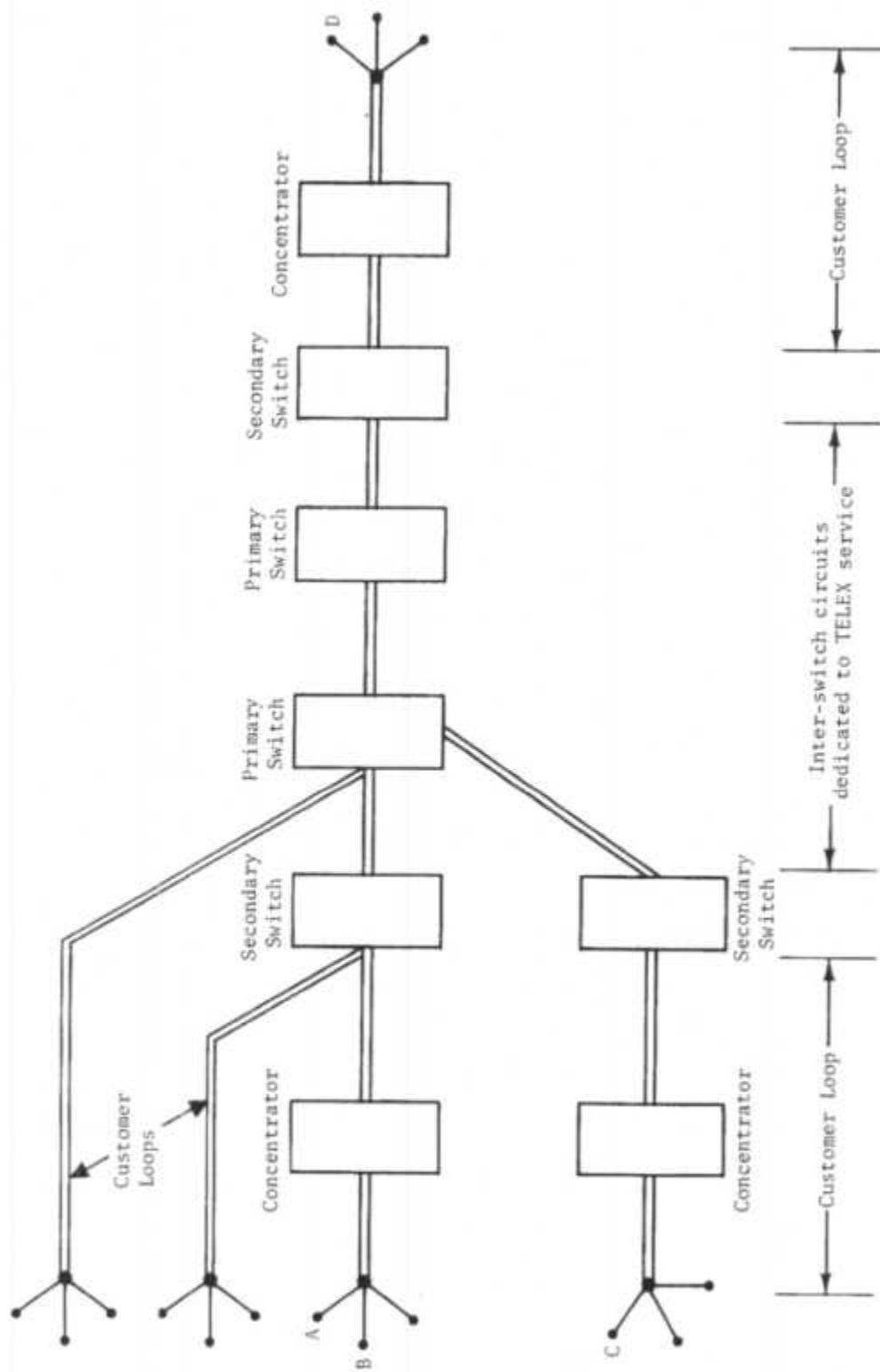


FIGURE 23
TELEX SWITCHED NETWORK

The TELEX communication plant characteristics are essentially the same as the TWX communication plant characteristics with the following exceptions:

- More of the plant is owned by Western Union (e.g., all TELEX switches are on Western Union premises).
- Tertiary switches are sometimes replaced by concentrators (multiplexers).
- TELEX messages are transmitted using the 5-level Baudot code at a binary rate of 50 bps.

The required and optional intercept equipment, strategies for the interceptor, detection of the interceptor and constraints on the interceptor is the same as for the TWX switched network discussed in Section 8.2.3.2.1 (with allowance made for the exceptions noted above.)

8.2.3.3 Dedicated Networks (Voice Traffic)

8.2.3.3.1 Public Telephone Switched Network Carrier Facilities

Communication plant characteristics:

The public telephone switched network carriers provide dedicated (private) circuits and networks for the part-time use of subscribers. Private circuits are hard wired through the same telephone company offices which house the switches used in the Direct Distant Dialing network. The rest of the telephone company plant is shared by the Direct Distance Dialing network and the private line circuits. However, signaling may be provided by the telephone company so that the subscriber can perform his own internal switching (e.g., on-hook, off-hook and dial information between subscriber PBXs). Individual circuits (including circuits tied together to form networks) tend to remain in place for long periods of time (six months to several years). All communications over some private networks are available to the interceptor at all points on the network.

Intercept equipment

Required and optional equipment is the same as that discussed in Section 8.2.3.1, "Public Direct Distance Dialing Network (Voice Traffic)" except the signal

generator and signal detector and the microprocessor (or minicomputer) are not useful. Signaling decoders need have only one or two inputs.

Strategy for interceptor:

Strategies for the interceptor are the same as those discussed in Section 8.2.3.1, except:

- The use of a ring generator and microphone or a signaling decoder capable of decoding dial information would be of no use where no dial signaling is provided by the telephone company.
- The strategy of employing two confederates at telephones in each exchange area to make calls to each other is not applicable (under the assumption that the subscribers internal communications at any one location is not available to the interceptor).
- Multiple (more than two) taps or probes or multiple-input signaling decoders or recorders would not be useful unless more than one private circuit between the same two points is provided to the subscriber.

Detection of interceptor:

Same as those discussed in Section 8.2.3.1.

Constraints on interceptor:

Same as those discussed in Section 8.2.3.1 plus the identification of the parties using a particular private line circuit will be more difficult.

8.2.3.3.2 Specialized Common Carrier Networks

Except for those specialized carriers which propose to provide direct access to their satellites by earth station located on the subscriber's premises, specialized common carriers use the private line services provided by the public telephone switched network common carriers to connect their subscribers into their facilities. The facilities owned and operated by the specialized carriers are far less extensive than the public telephone switched network and consist of microwave terrestrial routes and/or satellite relays as well as the

appropriate multiplex, modulation, transmission and control equipment. Two types of networks are considered: Those designed for digital signal transmission and those designed for analog signal transmission.

(1) Analog Signal Transmission Networks

Except as noted above the communication plant characteristics are the same as the dedicated network portion of the public switched network.

Intercept equipment

The same required and optional intercept equipment as the dedicated network portion of the public telephone switched network (both the portion provided by the public telephone switched network and the portion provided by the specialized carrier).

Strategy for the interceptor

The location of the specialized carrier's route is greatly simplified because the route will be a terrestrial microwave route or a satellite relay with at most one alternate route. (In nearly all cases, there is no alternate route to consider.) Otherwise, the strategy is the same as that which would be used against the dedicated network portion of the public telephone switched network. This strategy applies to both the portion provided by the public telephone switched network and the portion provided by the specialized carrier.

Detection of interceptor:

The same as that discussed in Section 8.2.3.1 above.

Constraints on interceptor:

The same as that discussed in Section 8.2.3.1 above.

(2) Digital Signal Transmission Network

Only one specialized carrier has proposed to provide a capability for voice transmission over a system designed for digital signal transmission. The proposed system will utilize a satellite to relay both voice and data traffic between earth stations located on various properties owned by the subscribers. The earth stations will be owned, maintained and operated by the carrier.

Communication plant characteristics:

Voice waveforms are analog-to-digital converted, compressed and time division multiplexed with other voice and data inputs. The resulting bit stream is scrambled (but may be encrypted) before being transmitted together with control information in bursts at a data rate of between 40 and 50 Mbps using a phased-shift-keyed (PSK) modulation technique. The burst transmission is timed to arrive at the satellite such that it will fit into the particular time slot assigned to the earth station. The downlink transmission will appear as a time division multiplex of the bit streams from all users of the system. The downlink transmission is available anywhere within the limits of the continental U.S.

Intercept equipment:

Required equipment: Antenna and PSK receiver sufficiently powerful to receive the downlink signal if both sides of a communication are to be intercepted. Also required is signal processing equipment to descramble (or decrypt) the burst, decode the control signal to find the particular time location of the voice signal(s), acquire the digital bits of the voice signal(s), expand the compressed voice signal(s) and digital-to-analog convert the result. (A motor-generator set or access to AC power is required).

Optional equipment:

Tape recorder (could be battery powered)

Strategy for interceptor:

Install the monitoring equipment any place within the continental U.S. which minimizes the possibility of being detected. Time slot assignment could be obtained by measuring the time of burst transmission from all earth stations which may be transmitting the communications of interest and calculating the time of arrival of the burst at the intercept site.

Detection of interceptor:

Observation of the intercept equipment (particularly the antenna) by employees of the targeted subscriber (if monitoring site is near the subscriber's premises), police, forest rangers, game wardens, etc.

Constraints on interceptor:

It will be extremely difficult to obtain the required signal processing equipment without detailed inside information or acquiring an actual signal processing station. In addition, the interceptor must know how the signal processors located at the earth stations of interest are programmed (programs will vary from earth station to earth station and will change over time as the subscriber changes the services he wants). If the targeted subscriber elects to use an encryption device the difficulty of breaking encryption code increases with increasing sophistication of the encryption device.

8.2.3.3.3 Private Commercial Microwave Systems

Communication plant characteristics:

A wide variety of standard and special design microwave systems are available to meet the specific requirements of a particular private commercial microwave system.

Equipment requirements:

Specific equipment requirements can only be determined after the interceptor obtains a knowledge of the particular system being used by the commercial target. However, once this knowledge is obtained, the components to build an intercept system will nearly always be readily available through suppliers of microwave equipment. (Most private commercial microwave systems use standard components or modest modifications of standard components.)

Strategy for interceptor:

Discreet inquiry of knowledgeable employees of the commercial enterprise should provide the interceptor with some, if not all the knowledge necessary to determine his equipment requirements. Otherwise, physical observation of the installation, radiation measurements and analysis of the signals being transmitted should provide the interceptor with sufficient information to deduce what his equipment requirements are and what strategy he should employ.

Detection of interceptor:

Employees may become suspicious of inquiries about the installation. The interceptor may be observed while making his own physical observations and measurements or while monitoring the communications of interest.

Constraints on interceptor:

The interceptor (or a confederate) must have a sound knowledge of microwave systems and how to make the appropriate measurements and analyze the transmitted signals.

8.2.3.4 Digital Data Service

Digital data may be communicated using any of the network's discussed above; teletype channels, single voice channels, channels which occupy a number of voice channels and networks specifically designed for digital data transmission. Network and channel characteristics previously discussed will not be reiterated in this section unless needed for clarity of presentation.

8.2.3.4.1 Teletype Channels

Communication plant characteristics:

Technically, all teletype service could be regarded as a digital data service. The Western Union TWX and TELEX services could be regarded as (and used for) switched data service. Dedicated teletype services may be provided by the dedicated portions of facilities shared with the public telephone switched network as well as by the specialized carriers. Teletype machines are frequently used for remote input and output to digital computers. In addition, modems which provide output signals in teletype format have been developed for the transmission of low speed (up to 150 bps) data.

Interceptor equipment:

In addition to the equipment previously listed for intercept of teletype traffic, a printer and modem which is designed to decode the appropriate teletype signal

and drive the printer are optional equipment if the digital code is the same as one of the standard teletype codes. Otherwise they are required equipment. Note:

In the latter case "printer" should be taken to mean any device for the appropriate display of the information (e.g., a graphic display).

Strategy for interceptor:

In addition to the strategies previously listed, the interceptor must obtain knowledge of the particular code being used either by a priori knowledge or by analysis of the observed signal.

Detection of interceptor:

Same as that previously listed for teletype traffic.

Constraints on interceptor:

In addition to constraints previously listed for teletype traffic, the interceptor may have some difficulty determining the code being used (particularly if the code is non-standard).

8.2.3.4.2 Single or Multiple Voice Channels

Communication plant characteristics:

Standard data rates for transmission over single voice channels are 300, 600, 1200, 3600, 4800 and 9600 bps. Standard data rates for transmission over channels which occupy multiple voice channels are 56 and 1344 kbps. Other data rates are available but are not used extensively. Modems (sometimes called data sets) are used to convert the digital data bit stream into analog waveforms suitable for transmission over channels designed for voice traffic. Many different modem designs are in use and new designs are constantly being added to the inventory. The analog waveforms for transmission of data at rates of 1200 bps or lower are not complex. As the data rates increase above 1200 bps, the analog waveforms become increasingly complex. Modems operating at the higher data rates (2400 bps and above) are designed to compensate for the adverse effects of voice channels. In addition, scramblers are employed at these higher rates in order to minimize interference with other voice channels.

The subscriber may have multiplexed several lower-speed digital bit streams into one bit stream for transmission.

Interceptor equipment:

In addition to equipment listed previously for the appropriate networks, the interceptor will need a modem matching the characteristics of the modem used in the system, either by obtaining an identical modem or by designing one which has the same characteristics (normally requires a motor generator set or a source of AC power). A printer or other suitable output device will be required to recover the information. (Requires a motor-generator set or a source of AC power).

Strategy for interceptor:

In addition to the applicable strategies previously discussed for the appropriate voice channel, the interceptor must find out which type of modem is being used by the subscriber whose communications he will be intercepting or deduce the type being used from monitoring the subscriber's communications.

Detection of interceptor:

The same possibilities exist for detection as those previously discussed for the appropriate network.

Constraints on interceptor:

In addition to the constraints discussed previously for the appropriate network, it would probably be impractical for the interceptor to have a stock of all the possible modems that might be used. Inquiries about the modem being used might alert the target. The interceptor will need a considerable knowledge of modem characteristics in order to deduce the type of modem required.

8.2.3.4.3 Networks Designed for Digital Data Transmission

Three types of networks designed for digital data transmission were studied. The first (known as the Digital Data System (DDS)) provides dedicated digital service and shares transmission facilities with the public telephone switched network. The second is the terrestrial microwave backbone networks of a specialized carrier. The network makes extensive use of dedicated transmission facilities leased from

the public telephone switched network common carriers. The third network uses a microwave satellite relay for data transmission between earth stations located on various properties owned by the subscribers.

(1) Digital Data System (DDS) Network

Communication plant characteristics:

Local and short haul circuits utilize the same plant as described in Section 8.2.3.4.1 and 8.2.3.4.2 above. Long haul circuits are provided by microwave radio facilities known as Data Under Voice (DUV). Digital data from a number of subscribers are time division multiplexed to form a 1.544 Mbps bit stream for transmission over DUV facilities. A modem is used to convert the multiplexed digital bit stream into an analog waveform suitable for transmission over the AT&T FM microwave radio system, using the lower 500 kHz of the baseband. The particular modulation technique used is known as a four-logic-level/seven-power-level partial response system. The digital bit stream is converted to Gray code and scrambled prior to transmission.

Interceptor equipment:

The equipment requirements for intercept of individual subscriber loops is the same as indicated in Sections 8.2.3.4.1 and 8.2.3.4.2 above. Once the subscriber's data is multiplexed with data originated by other subscribers, a demultiplexer will be needed for intercept. (Could be battery powered). If the intercept is to occur on the DUV radio route, one or two antennas, two FM receivers (discriminators), two low pass filters (with cut-off frequency of 500 kHz), two four-logic-level/seven-power-level partial response demodulators (with Gray code converter and descrambler), two TDM demultiplexers and two printers or other suitable output devices will be required to obtain two-way transmission. (Only one of each of these equipments are required if only one-way transmissions are to be intercepted.) (A motor-generator set or source of AC power is required).

Strategy for interceptor:

Same as Sections 8.2.3.4.1 and 8.2.3.4.2 above for interception prior to TDM by the carrier. The same as for dedicated voice service over terrestrial microwave given in Section 8.2.3.3.1 above.

Detection of interceptor:

Same as Sections 8.2.3.4.1 and 8.2.3.4.2 above for interception prior to TDM by the carrier. The same as for dedicated voice service over terrestrial microwave given in Section 8.2.3.3.1 above.

Constraints on Interceptor:

Same as Sections 8.2.3.4.1 and 8.2.3.4.2 above for interception prior to TDM by the carrier. The same as for dedicated voice service over terrestrial microwave given in Section 8.2.3.3.1 above.

(2) Specialized Carrier Terrestrial Microwave Network

Communication plant characteristics:

The terrestrial microwave specialized carrier provided both switched and dedicated service. Only one switch was in service (although others were planned). The subscriber was provided with a unit which interfaced the subscriber's digital input to the carrier's TDM multiplex units via leased voice frequency circuits (data rates of 2400, 4800 or 9600 bps were available). The interface units contained modems which scrambled the data and generated an analog waveform suitable for transmission over voice frequency circuits. Multiplex units were located in each city served by the carrier. If the city was located at an entry point on the microwave route, data would be fed directly to the microwave route. Otherwise, data would be forwarded to the microwave route or other multiplex units via circuits leased from the telephone company. At entry points on the microwave route, several sources of traffic were multiplexed together to form the high speed (44.66 Mbps) bit stream for transmission using a PSK modem (which contained two scramblers and two binary-to-Gray code converters, each operating on one half the bit stream).

Intercept equipment:

Intercept at points other than the specialized carrier's microwave route requires the same types of equipment indicated in subsection "1" above for the DDS. Equipment required for intercept along the microwave route requires: One or two antennas, two RF receivers, two PSK modems having the same characteristics as the carrier's modem (each including two Gray-to-binary code converters and two descramblers), two TDM demultiplexers, two digital decoders which match the subscriber's coders (including multiplexers, if any) to obtain both sides of a two-way communication. (Only one of each of the above equipment is needed if a one-way intercept is to be made.) (A motor generator set or access to AC power is required.)

Strategy for the interceptor:

Intercept at points other than the specialized carrier's microwave route requires the same strategy as that indicated in subsection (1). The interceptor may locate his monitoring site any place along the route between the entry and exit points for the communication of interest which will minimize the risk of being detected. Since only the route is involved, its location should be relatively easy.

The most difficult problem for the interceptor is the acquisition of the required intercept equipment. The radio (receiver and PSK modem) equipment is not as readily available as the more commonly used FDM/FM equipment. He might try to buy the identical radio equipment from the original manufacturer or design and build his own equipment either from a priori knowledge, by measurements and analysis of the observed radio signal or a combination of both. Once the interceptor has the capability of recovering the two bit streams making up the 44.66 Mbps bit stream, he must determine how to demultiplex the bit stream to obtain the bit stream of the target. A priori knowledge of the carrier's time division multiplex format or analysis of one or both bit streams will be necessary for the interceptor to make or buy the proper demultiplex equipment.

The interceptor must also obtain a decoder matched to the coder used by the target or build his own based on analysis of the coded signal.

Detection of interceptor:

Same as that discussed in 8.2.3.1 for the corresponding transmission media.

Constraints on interceptor:

In addition to the constraints discussed in Section 8.2.3.1 for the corresponding transmission media, the interceptor may be severely handicapped by lack of knowledge about the equipment used by the carrier or the subscriber's equipment or both. Further, he may not be able to purchase the equipment necessary to demodulate and demultiplex the high-speed bit

stream transmitted by the carrier because the carrier's equipment was designed and manufactured specifically for the carrier. If the interceptor must deduce the signal characteristics and build his own intercept system, he must be thoroughly conversant with the requisite technology. However, given that the interceptor has such knowledge, it would not be particularly difficult for him to assemble an appropriate intercept system.

(3) Satellite Microwave Relay Network

Communication plant characteristics:

This is the same plant as that considered in Section 8.2.3.3.2, Subsection (2), a dedicated service digital signal transmission network using satellite relay. Subscriber digital data enters the earth station signal processor via data ports, is compressed, coded to provide forward error correction and time division multiplexed with other data and voice inputs. The rest of the plant is the same as that described in Section 8.2.3.3.2, Subsection (2).

Intercept equipment:

The intercept equipment is the same as that listed in Section 8.2.3.3.2, Subsection (2), except that digital decoders are substituted for the digital-to-analog converters.

Strategy for interceptor:

Same as the discussion of these items in Section 8.2.3.3.2, Subsection (2).

Detection of interceptor:

Same as the discussion of these items in Section 8.2.3.3.2, Subsection (2).

Constraints on interceptor:

Same as the discussion of these items in Section 8.2.3.3.2, Subsection (2).

8.2.4 Information Extraction

This section presents a generalized functional diagram of the steps and types of equipments required for intercepting all forms of traffic from all modes of electronic communication used by the electronic common carriers. The functional block diagram of Figure 24 is intended to illustrate the relative complexity of equipment needed

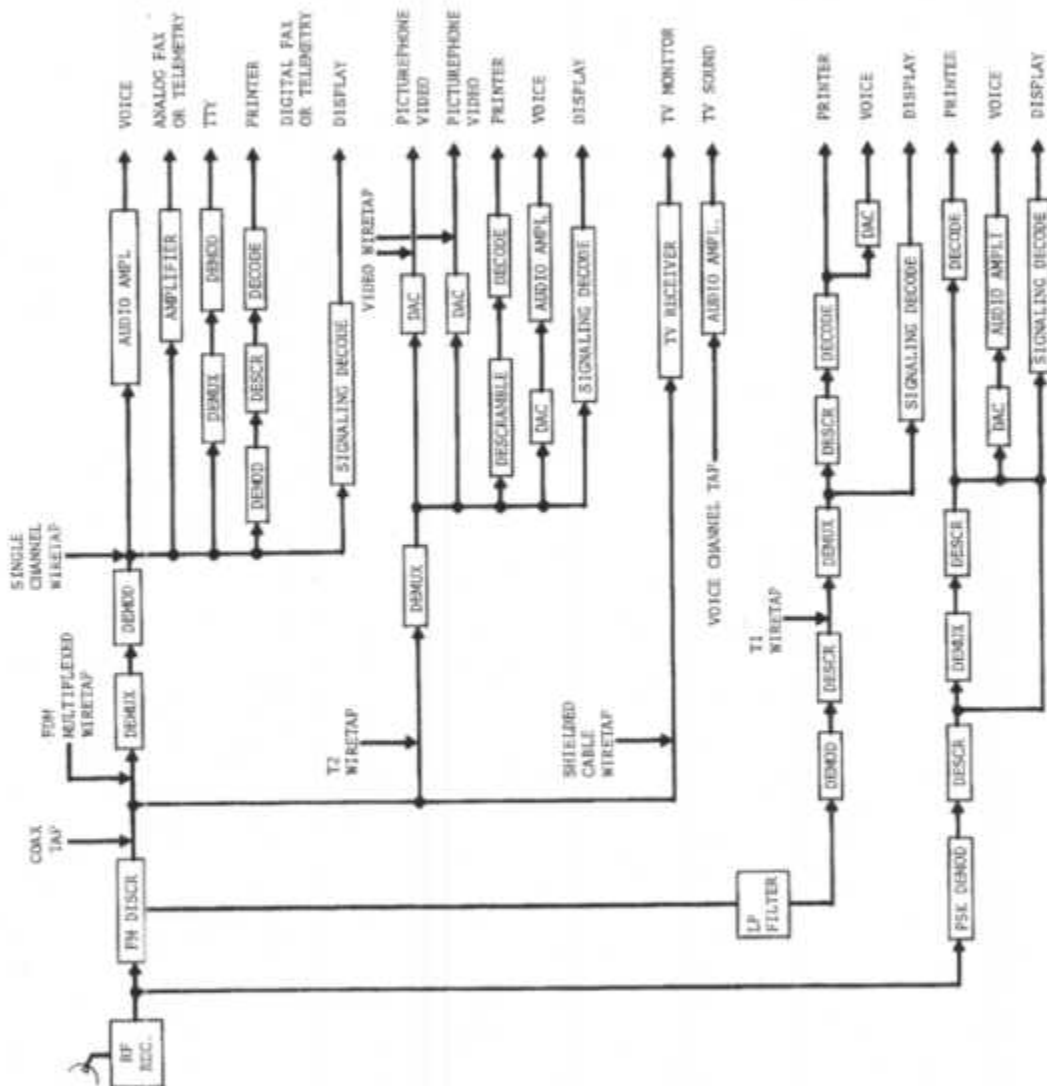


FIGURE 24
COMPOSITE INFORMATION EXTRACTION FUNCTIONAL
BLOCK DIAGRAM

depending on the type of information being intercepted and the point in the common carrier's communication system being accessed. It should be interpreted neither as a complete list of equipment needed nor as a minimum set of equipment. It is intended to summarize the variety of options open to an interceptor. For example, if the interceptor is interested in intercepting both sides of a conversation, he will need two audio amplifiers (or one audio amplifier and a mixer) for tapping into a 4-wire system. If he taps into a coaxial cable, he will need two DEMUX (demultiplex) units in addition to the audio amplifier since the two sides of a conversation will usually be on separate coaxial cables. The DEMUX itself need not be a true demultiplexer; the same result might be achieved by using a bandpass filter or selective level meter. If the interceptor is only interested in conversations and can otherwise determine the particular pair of wires needed, he may have no use for a signaling decoder.

All the equipment depicted need not be located at the signal acquisition site since magnetic tape recorders could be used on site and the rest of the processing performed at another location. On the other hand, additional equipment might be of considerable use to the interceptor. For example, special purpose equipment might be used to aid in the search for the proper channel and to switch in the appropriate monitoring equipment. A mini-computer or microprocessor could be used either to automate a number of functions which might otherwise be too time consuming or to simulate operation of other devices.

The tap of a wire-pair requires the least amount of equipment. In most cases, a wire-pair will be carrying a single analog voice channel. However, some wire-pairs will carry an FDM carrier system having between 4 and 24 voice channels. In the latter case, a demultiplexer and a demodulator will be necessary. The types of traffic

carried over the analog channel may be voice, facsimile, digital or analog telemetry, teletype messages or data. Simple amplifiers are sufficient to obtain the voice and analog facsimile and telemetry signals. Conversion of these signals to useful form will require headphones or speakers for voice, a compatible facsimile machine for facsimile and a suitable paper recorder for analog telemetry.

Teletype traffic will require a demodulator and a teletype machine which operates at the baud rate being transmitted or a signal converter and printer if only one teletype signal is being transmitted over the channel. A demultiplex unit (which might be a simple bandpass filter) will be needed if more than one TTY signal is being transmitted over the channel.

Digital data and telemetry traffic will have to be demodulated to obtain the transmitted bit stream which, if scrambled, will have to be descrambled and decoded using the same (or equivalent) type of descrambler and decoder as that used by the targeted subscriber. The demodulator must also be of the same type as that used by the targeted subscriber or have an equivalent capability, (same bit rate, line compensation, etc.). A minicomputer or microprocessor could be used as a versatile tool to perform these functions for a wide range of descramble and decode operations and as a controller for a general purpose demodulator. The information may be recovered using a printer.

A signaling decoder may be useful by itself if the interceptor is interested in the analysis of calling patterns or it may be used to assist in the job of locating which voice channel to tap or when to tap a particular channel.

Two other wiretaps are shown (labeled T1 for 1.544 Mbps and T2 for 6.3 Mbps digital transmission) for acquiring digital signals.

T1 is the most extensively used at this time. T2 is included since it will be used for picturephone service. The T1 digital signal may be carrying either voice or data. The 1.544 Mbps signal must be demultiplexed (time division) into individual channels (64 kbps) and the individual channels decoded. If the individual channel is carrying voice traffic a digital-to-analog converter (DAC) is required to recover the analog voice waveform. If the individual channel is carrying data traffic, it will have to be further demultiplexed if data rates of individual subscribers are less than 64 kbps (e.g., 2400, 4800, 9600 bps). After the individual subscriber's bit stream is obtained, it must be decoded to obtain the information being communicated. A descrambler may also be required. In any case, the decoder and/or descrambler must be of the same type (or equivalent) as that used by the targeted subscriber. Since signaling is included in the bit stream, a digital signaling decoder might be employed.

The T2 wiretap will require a more complex demultiplexer (time division) than the T1, but requires the same equipment types if voice or data traffic is being intercepted. If picturephone traffic is being intercepted, video must be separated from the audio and both digital-to-analog converted. If only the audio is to be intercepted, a simple audio amplifier with headphones may be the only additional equipment needed. On the other hand, if the video is to be intercepted as well, a picturephone receiver (or equivalent) will be required. Note that the audio and video may be obtained directly if the interceptor taps into the local subscriber loops.

Coaxial cable is used mainly for analog message traffic, although some closed circuit television and some very high data rate TDM traffic may be transmitted via coaxial cable. If high bit rate TDM traffic is intercepted on coaxial cable, the same functional blocks as for intercept of T2 wiretap is required. Of course the demultiplex equipment will be much more complex. If TV traffic is intercepted only the video is likely to be present, but shifted upward in frequency. The TV receiver will have to shift the frequency down to the normal video region before it is placed on a monitor. The sound portion of the TV may be carried along with the video, in which case the TV receiver must be able to separate the sound from the video. However, at the present time, the sound is usually carried over a separate voice channel. Most intra-exchange TV traffic is carried over shielded cable and can be treated the same as any hard wire tap. Analog message traffic will require an FDM demultiplex and amplitude demodulation, after which it could be treated in the same manner as the analog channel wiretap.

Interception of FM radio traffic requires an FM discriminator to recover the baseband signal. The baseband signal may be entirely FDM message traffic and can be treated in a manner similar to a coaxial cable tap. However, the lower 500 kHz may consist of the data under-voice (DUV) signal. The rest of the bandwidth can be treated the same as a coaxial cable tap. The DUV signal can be obtained by use of a low pass filter with a cut-off frequency of about 500 kHz. The DUV signal must be demodulated from the 7-level partial response waveform used for transmission of the bit stream. Since the DUV bit stream is scrambled, a descrambler is required. The resulting bit stream can be treated as discussed above for the T1 wiretap.

Interception of PSK radio traffic requires a PSK demodulator followed by a descrambler to obtain the original multiplexed digital bit stream. Since individual data channels may be scrambled also,

a descrambler may be required to derive the data bit stream. The data bit stream may contain either digital data or digitized voice or both. If it contains digital data only, the bit stream must be decoded in order to recover the data being communicated. If it contains digitized voice, a DAC is required to obtain the voice signal. In some cases, the subscriber may have multiplexed several data and/or voice bit streams before transmission off premises, thus requiring another level of demultiplexing before the decoder and/or DAC. Signaling information of interest may be present (in digital form) after either or both of the descramblers.

In summary, the equipment and knowledge required by the interceptor depends strongly on what kind of telecommunications traffic (voice, data, etc.), what kind of multiplex systems he will be intercepting and where in the telecommunications system (analog channel wiretap, radio intercept, etc.) he is to make the intercept.

9.0 SUMMARY OF INTERCEPTOR EQUIPMENT CHARACTERISTICS

Table VI presents a summary of the characteristics of the equipment that can be employed for the interception of electronic communications. The nature of the equipment required varies considerably depending on the type of signals to be acquired and the type of traffic to be intercepted. The table indicates the relative availability and costs of the equipment and gives estimates of complexity of installation and operation. The table also gives estimates of the effectiveness of using the equipment to intercept communications and of the relative detectability of intercept operations employing the equipment.

The table is arranged in three parts. The first part is a listing of the equipment needed to acquire the signal of interest from the transmission media. The second part is a listing of the required and optional equipment needed to extract the information being communicated. The third part lists the equipment (taken from the first two parts) which would be needed for a complete intercept system for some selected intercept strategies.

Most equipment was selected on the basis of least cost. Two antennas are listed in Part I (Terrestrial Microwave, FDM/FM). These antennas would also be used for the TDM/PSK signal acquisition system listed on the following page. The horn is included to illustrate the type of antenna that could be used for a close-in reception and the parabolic dish is included to illustrate the type of antenna needed for adequate reception at distances up to approximately 20 km from a terrestrial microwave route. The 12-meter and 5-meter antennas listed in Part I (Satellite Microwave, FDM/FM) are associated with the helium-standard global and spot downlink beams, respectively. The same range of antenna sizes should be adequate for reception of the downlink of domestic satellites. The nitrogen-cooled parametric amplifier could be used for reception of the downlink of some domestic satellites.

The equipment necessary to extract information coded in digital format (listed in Part 2 of the table) must match the characteristics of the subscriber's equipment. For this reason, two representative digital-to-analog converters and three modems are listed. The cost of these devices will vary over a wide range depending on the accuracy and/or sophistication required to successfully extract the information of interest. The cost of tape recorders is a function of the strategy to be employed by the interceptor. This may range from the need for an expensive cassette recorder to an expensive multi-channel high fidelity recorder.

Part 3 of the table was included to illustrate how the equipments listed in Parts 1 and 2 could be assembled to form complete intercept systems. Three straightforward cases have been assumed:

(1) Wire-tap on a non-carrier subscriber's loop at an aerial cable appearance such as a terminal housing. It is assumed that the wire pairs of interest have already been identified.

(2) Interception of voice communications between two targeted subscribers on a wire carrier trunk circuit. The multi-pair cable is assumed to be non-pressurized and buried. It is further assumed that the interceptor has identified which channels of the multiplexed signal belong to the trunk group which will carry the communication of interest; that the interceptor has the tools necessary to dig up and penetrate the cable; and that the interception is performed in an isolated area.

(3) Interception of voice communications between two targeted subscribers on a terrestrial microwave FM/FDM radio route. It is assumed that the interceptor houses his equipment in a van which is successfully hidden and that the interceptor has identified which channels of the multiplexed signal belong to the trunk group that will carry the communication of interest.

Parts 4 and 5 of the table identify the citizens band and public service bands radio receiving equipment. This equipment is inexpensive, easy to use and readily available at retail outlets.

TABLE VI

INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 1: EQUIPMENT REQUIRED TO ACQUIRE A SPECIFIC CHANNEL OR SIGNAL
(TERRESTRIAL MICROWAVE, FDM/FM)

Interception Equipment	A V A I L A B I L I T Y					C O M P L E X I T Y		Effectiveness	Detectability
	Commercial	Other	Cost	Size	Weight	Installation	Operation		
<u>ANTENNAS</u>									
Horn	X		\$500	80 in. ³	2 lb.	Low to Moderate	Low to Moderate	Moderate to High	(Physical Surveillance) Low to Moderate
Parabolic Dish	X		\$2000 and up	50 cm to 1 meter	50 lb. and up.	Low to Moderate	Low to Moderate	Moderate to High	(Physical Surveillance) Moderate to High
RF Receiver with FM Demodulators	X		\$6000	4000 in. ³	50 lb.	Moderate	Moderate	High	(Physical Surveillance) Low
Baseband Demultiplexer (Selective Level Meter)	X		\$6000	2000 in. ³	45 lb.	Moderate	Moderate	Limited to High	(Physical Surveillance) Low

TABLE VI (Continued)
INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 1: EQUIPMENT REQUIRED TO ACQUIRE A SPECIFIC CHANNEL OR SIGNAL
(TERRESTRIAL MICROWAVE, TDN/PSK)

Interception Equipment	A V A I L A B I L I T Y					C O M P L E X I T Y			Effectiveness	Detectability
	Commercial	Other	Cost	Size	Weight	Installation	Operation			
PSK Digital Radio Receiver	X		Approx. \$10,000	7"x19"x15"	Approx. 30 lb	Moderate	Moderate	High	(Physical Surveillance) Low	
Scanning Control Processor	X		\$10,000	Approx. 12"x19"x30"	Approx. 65 lb	High	High	Moderate to High	(Physical Surveillance) Low	
Digitally Tuned Oscillator	X		Approx. \$4,000	Approx. 12"x19"x30"	Approx. 65 lb	Moderate	Moderate	Moderate to High	(Physical Surveillance) Low	

TABLE VI (Continued)
INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 1: EQUIPMENT REQUIRED TO ACQUIRE A SPECIFIC CHANNEL OR SIGNAL
(SATELLITE MICROWAVE, FM/FM)

Interception Equipment	A V A I L A B I L I T Y					C O M P L E X I T Y			Effectiveness	Detectability
	Commercial	Other	Cost	Size	Weight	Installation	Operation			
<u>Antennas</u>										
5M Steerable Dish	X		\$20,000	195"x103" x73"	3000 lbs.	Moderate	Moderate	Moderate	Moderate	Moderate
12M Steerable Dish	X		\$600,000	-	-	Moderate	Moderate	Moderate to High	Moderate	Moderate
<u>Low Noise Amplifiers</u>										
He-Cooled Paramp	X		\$70,000	8,000 in ³	-	Moderate	Moderate	Moderate	Moderate to High	Moderate
N-Cooled Paramp	X		\$20,000	8,000 in ³	-	Moderate	Moderate	Moderate to High	Moderate	Moderate
FM Radio Receiver	X		\$12,000	4,000 in ³	-	Moderate	Moderate	Moderate to High	Moderate	Moderate
Selective Level Meter	X		\$6,000	2,000 in ³	-	Moderate	Moderate	Moderate to High	Moderate	Moderate

TABLE VI (Continued)
INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 2: EQUIPMENT REQUIRED TO EXTRACT THE INFORMATION BEING COMMUNICATED

Interception Equipment	A V A I L A B I L I T Y					C O M P L E X I T Y			Effectiveness	Responsibility
	Commercial	Other	Cost	Size	Weight	Installation	Operation			
<u>Voice Traffic</u>										
Inductive Tap		Retail	At Most \$40	Negligible	Negligible	Low	Low	Moderate to High	Low	None
Headphones		Retail	At Most \$60	Negligible	Negligible	Very Low	Very Low	High	None	None
Audio Amplifier		Retail	At Most \$60	Negligible	Negligible	Very Low	Very Low	High	None	None
Audio Mixer		Locally Fabricated	At Most \$25	Negligible	Negligible	Low	Very Low	High	None	None
D/A Converter (Simple)	X		\$25 to \$75	19"x24"x20"	Up to 10 lb	Low	Very Low	High	None	None
(Delta 400)	X		\$1000 to 2000	19"x24"x20"	Up to 30 lb	Low	Very Low	High	None	None
<u>Teletype Traffic</u>										
Receive-only Teletypewriter	X		\$1000 to \$1500	19"x24"x30"	50 to 100 lb	Moderate to High	Low to Moderate	Moderate to High	Moderate	
FSK Demodulator	X		Less than \$500	19"x6" x12"	Less than 40 lb	Moderate	Low to Moderate	Moderate to High	Low	
<u>Data Traffic</u>										
Modem (Low speed)	X		Less than \$500	1500 to 2800 in ³	Apx 10 lb.	Moderate	Low to Moderate	Moderate to High	Low	
Modem (600-1200 bps)	X		Less than \$500	1500 to 2800 in ³	Apx 10 lb.	Moderate	Low to Moderate	Moderate to High	Low	
Modem (2400-9600 bps)	X		\$500 to \$8500	1500 to 2800 in ³	30 lb. to 60 lb.	Moderate	Low to Moderate	Moderate to High	Low	
Decoder	(EITHER X OR LOCALLY FABRICATED)		DEPENDS ON DIGITAL CODE AND OUTPUT FORMAT			Low to High	Low to High	Low to High	Low	
Printer	X		\$1000-\$15000	19"x24"x20"	30 to 100 lb	Moderate to High	Low to Moderate	Moderate to High	Moderate	
<u>Optional</u>										
Signaling Decoder		Locally Fabricated	Upper \$1000	24"x19"x10"	Less than 20 lb	Moderate	Low to Moderate	Moderate	Low	
Tape Recorder	X	Retail	\$50-\$5000	12"x19"x20"	5 lb to 30 lb	Low	Low to Moderate	High	Low	
Ring Generator w/ Testset	X	Locally Fabricated	\$600-\$1000	8"x19"x8"	10 lb to 30 lb	Moderate	Moderate	Moderate	Low	
Signal Generator w/ Detector	X		At most \$10	6"x8"x8"	Negligible	Moderate	Moderate	Moderate	Low	

TABLE VI. (Continued)
INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 3: EXAMPLES OF COMPLETE INTERCEPT ARRANGEMENTS

Interception Equipment	AVAILABILITY				COMPLEXITY			Effectiveness	Responsibility
	Commercial	Other	Cost	Size	Weight	Installation	Operation		
Simple Tools Inductive Tap Audio Amplifier Headset	WIRE TAP ON SUBSCRIBER LOOP (AERIAL CABLE AT AN APPEARANCE)								None
		Retail	Negligible	Negligible	Negligible	---	---	Very High	
			\$60						
			\$60						
		TOTAL	\$180	Negligible	Negligible	Very Low	Very Low	Very High	(Physical Surveillance) - Moderate
Penetration Tools Hard Tap 2 Baseband Demultiplexers Mixer Headset Signaling Decoding Device (Simple)	WIRE CARRIER TRUNK CIRCUIT (BURIED CABLE - NON-PRESSURIZED)								(Physical Surveillance) - Moderate
		Retail	\$50						

			\$12,000						
			\$25						
			\$60						
			\$1,000						
		TOTAL	\$13,085	6000 in ³	110 lbs.	Moderate	Moderate	Moderate	

TABLE VI (Concluded)
INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 3: EXAMPLES OF COMPLETE INTERCEPT APPEARANCES

Interception Equipment	AVAILABILITY				COMPLEXITY			Effectiveness	Responsibility
	Commercial	Other	Cost	Size	Weight	Installation	Operation		
		TERRESTRIAL		MICROWAVE	P/M/F/D/M	TRUNK CIRCUIT			
Shelter (Van)			\$7000						
2 Parabolic Dishes			\$4000						
2 RF Receivers with FM De-modulators			\$12,000						
2 Baseband Demultiplexers			\$12,000						
Scanning Control Processor			\$10,000						
2 Digitally Tuned Oscillators			\$8,000						
2 Signaling Decoders			\$2,000						
Mixer			\$25						
Headset			\$60						
TOTAL			\$55,085	27,000 in ³	455 lbs.	Complex	Complex	Low	(Physical Surveillance) - Low to Moderate

TABLE VI (Continued)
INTERCEPTION EQUIPMENT CHARACTERISTICS
PART 4: Citizens Band Radio (27 MHz Band)

Interception Equipment	A V A I L A B I L I T Y			C O M P L E X I T Y			Effectiveness	Detectability
	Commercial	Other	Cost	Size	Weight	Installation	Operation	
CB Transceiver		Retail Outlets	\$100 to \$400	69 in ³ to 300 m	3 3/4 lb. to 35 lb.	None	Simple	Very effective Within range Physical Surveillance Easily Hidden

