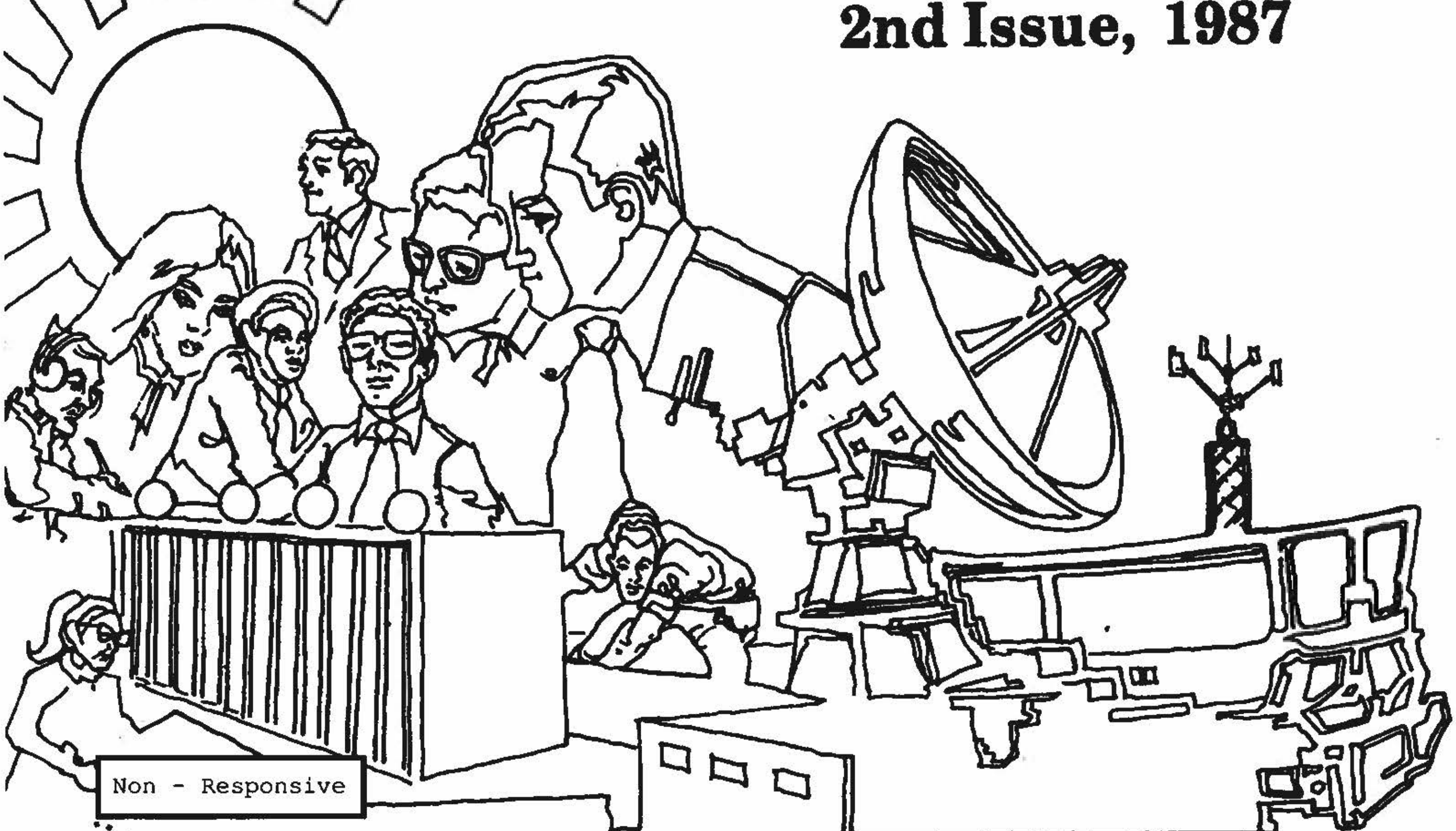
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue, 1987



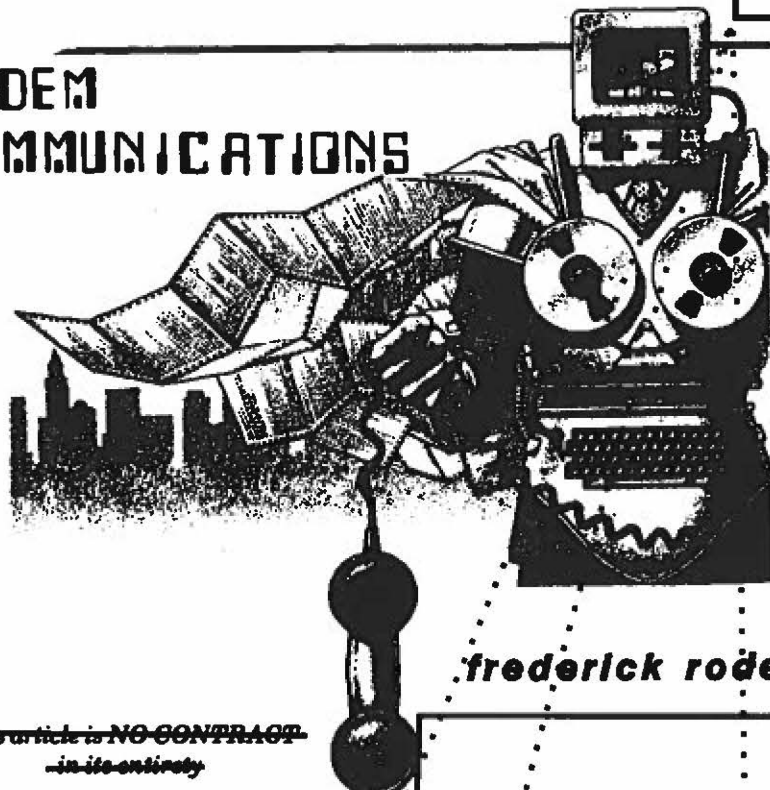
Non - Responsive

~~NOT RELEASABLE TO CONTRACTORS~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~

MODEM COMMUNICATIONS (U)



frederick rodean, g85

~~This article is NO CONTRACT in its entirety~~

~~(S-CCO)~~ Telecommunications are in transition from analog waveforms to digital ones-and-zeros. An early manifestation has been the use of modem devices that enable communicators to continue to employ existing analog transmission systems for passing information that is in digital form. This transition is already having an effect on the SIGINT community's ability to [redacted] We are taking actions to cope with this, but must also look ahead to the digital communications systems that are bound to be seen in the future.

THE IMPACT ON COLLECTION

[redacted]

• ~~(S-CCO)~~ *Higher transmission rates.* The basic conceptual design for most of today's [redacted] By the early 1980s, modem communications had become commonplace. The most common used for international communications was a V.26 device which operates at 2400 bits per second; today, the most common is the V.29, operating at 9600 bits/second, and already devices opera-ting at data rates of 19.2 kilobits/second in a voice-grade channel are being marketed. (Fig. 1.)

• ~~(S-CCO)~~ *Technical sophistication of modem devices.* The unending quest to obtain higher data transmission rates coupled with the need to maintain satisfactory bit error rates has lead to the development of extremely complex signaling devices. Among those that operate in standard 4kHz voice-grade channel is the now-common sixteen-state Quadrature Amplitude Modulation (16QAM); newer devices also employ complex coding schemes (e.g., Trellis coding) to achieve maximum data rates with satisfactory bit error rates. [redacted]

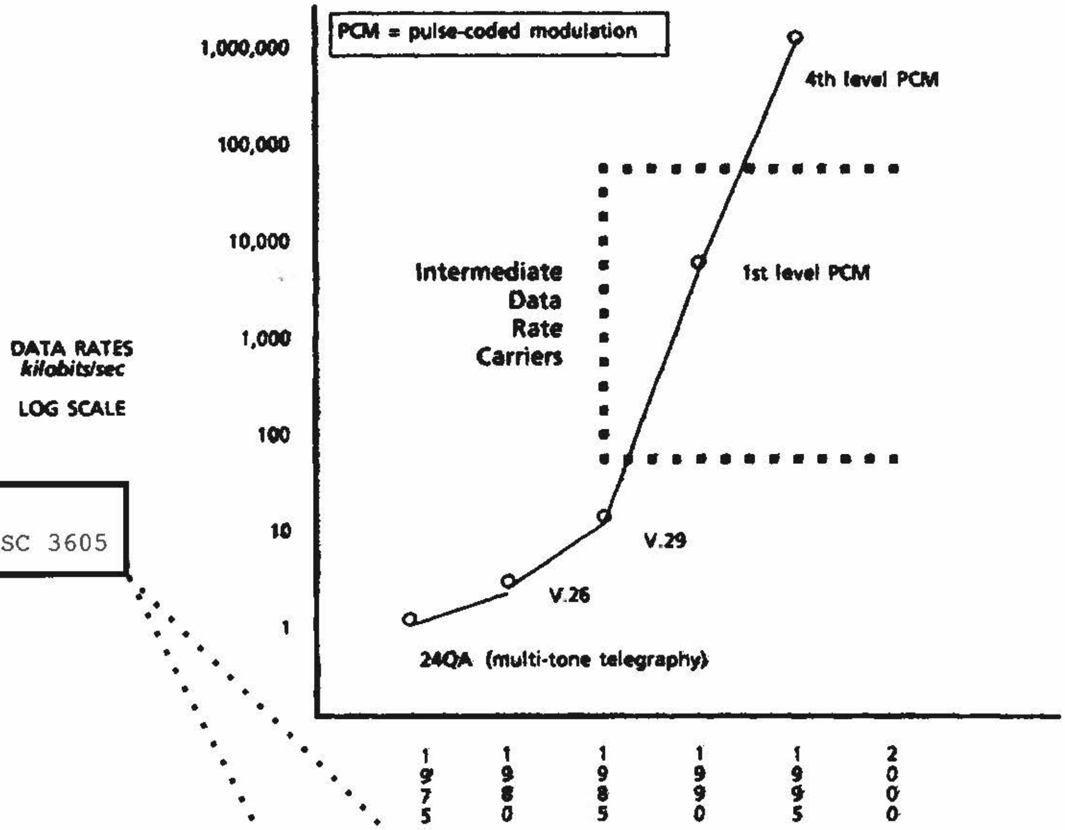


Fig. 1. DATA RATES COMMONLY USED IN INTERNATIONAL COMMUNICATIONS

EO 3.3b(3)
PL 86-36/50 USC 3605

[redacted]

[redacted]

THE IMPACT ON PROCESSING

~~(S-CCO)~~ [redacted] Although modem communications do carry this same type of traffic, they also are used to pass other types of communications, such as computer-to-computer file transfers, host-computer-to-terminal communications, electronic mail, etc. To further compound the problem, packet-switching is rapidly replacing circuit switching as the preferred means for digital communications. In a packet-switched communications network, the messages are broken into discrete data packets according to some rigid protocol. Each packet contains addressing and other communications overhead information and is handled as an independent entity thoughout the transmission path. When packets reach their destination, they are reassembled with other packets to reconstruct the orginal communication.

(U) In addition to the functions involved in the processing of normal message traffic, processes to handle modem communications must also address the following:

- (U) *Interpretation of protocol layers.* Characteristic of modem transmissions is the incorporation into the data stream of control information required by the communications system. This consists of bits which are added to the data stream and referred to as protocol layers. Each layer represents information required to carry out a specific communications function. (Figure 2.) The resultant bit stream is an amalgamation of the traffic being transmitted and all the protocol information. To correctly interpret a modem's output, these protocol bits must be identified and either removed or acted upon. Unlike noise in the analog world, these protocol bits serve a function. A major task of any modem processing system must be to identify, interpret, and act upon this "noise." Just as there are many different types of modem devices, there are many different protocols which must be addressed by any modem processing system.

- ~~(C-CCO)~~ *Handling heterogeneous data streams.* Traditional teletype traffic streams have homogeneous traffic types and employ homogeneous transmission codes, while data streams carried by modem signals are often hetrogeneous. An example of the latter is packet-switched communications. Because these systems may serve a wide variety of users and because the nature of the data to be passed is determined by each individual user [redacted]

- ~~(C)~~ *Man-machine interactive communications.* A significant percentage of modem communications involve interactions between a human and a computer. These interactions often take the form of a query by the human in the form of a command and the computer's response. [redacted]

- ~~(C-CCO)~~ *Non-message form of modem traffic.* [redacted]

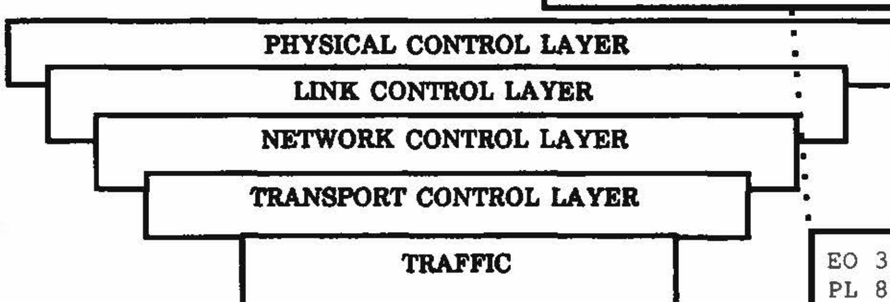


FIG. 2. TYPICAL LAYERS OF DIGITAL COMMUNICATIONS PROTOCOL

[redacted] One need only witness the chaos in an analytic organization when separation criteria for its traffic is incorrect to appreciate the importance of this function in our overall [redacted]

• ~~(C-CCO)~~ *Display of intercepted communications.* [redacted] requires that the information be presented to a target analyst in a form that he can readily comprehend. The recognition that computer-to-computer communications are a potential source of intelligence has added a new dimension to the interpretation and display of intercepted communications. Now they may be in the form of computer terminal displays, graphic presentations, data files, etc.

• ~~(C-CCO)~~ *Selection of desired traffic.* Perhaps the most important function in the [redacted] is extracting desired traffic from the vast volume of data that is collected. [redacted] The traditional method is to use selection equations and keyword dictionaries. [redacted] New methodologies will have to be developed.

COLORCAST

~~(C-CCO)~~ [redacted]

[redacted]

~~(S-CCO)~~ [redacted] Additional software can be loaded on the ASTW to provide pageprint of "printable" data streams and thus produce a level of quality control at the point of collection.

~~(S-CCO)~~ [redacted]

~~(C-CCO)~~ Once modem communications have been collected, the task of interpreting the resulting bit streams requires a detailed understanding of the various layers of

EO 3.3b(3)
PL 86-36/50 USC 3605

EO 3.3b(3)
PL 86-36/50 USC 3605

communications protocol that have been superimposed upon the information being sent. The complexity of these protocol layers varies greatly from one circuit to another, ranging from the fairly straightforward control information that is required on a dedicated circuit between a computer and a single printer to the extremely intricate mechanisms employed when packet-switched communications are passed from one network to another en route to their destination.

(U) COLORCAST has approached the task of correlating modem bit streams with established protocols in the following manner:

- ~~(C-CCO)~~ [redacted]

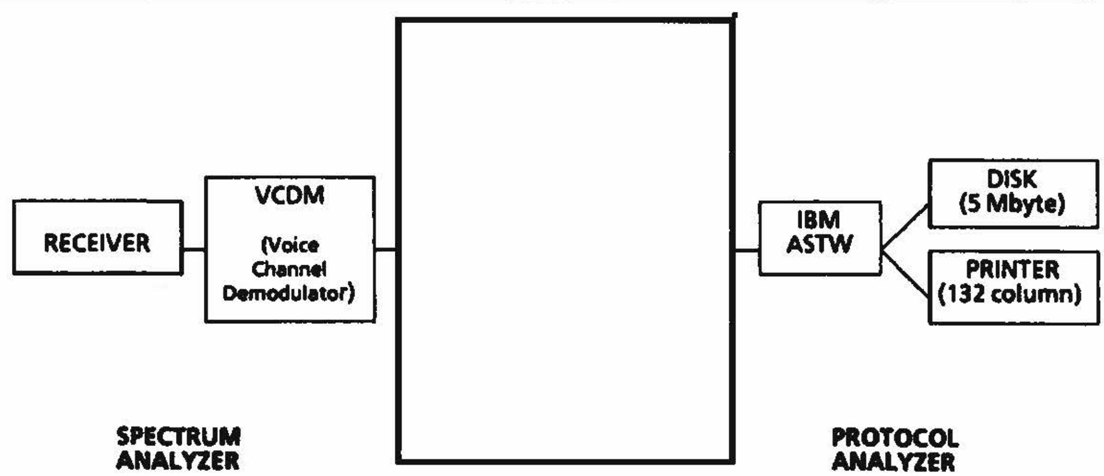
- ~~(C-CCO)~~ *Correlating intercepted bit streams with the models.* [redacted]

[redacted]

- ~~(C-CCO)~~ *Developing prototype software.* During the correlation process, we have to develop prototype software to interpret protocol bits and to convert the transmitted traffic into a readable form. While this software is not intended to function as a production process, it does provide a capability to produce sample output that can be used in cataloging modems in use.

- ~~(C-CCO)~~ *Evaluating commercial hardware.* COLORCAST is conducting a continuing evaluation of commercial hardware marketed to "process" digital communications., ranging from evaluations of various general-purpose protocol recognizers to testing special communications circuit cards for small computers. This effort is directed at identifing new hardware that may be applicable to our collection or processing efforts.

- ~~(C-CCO)~~; *Transferring experimental processes to production systems.* During the sampling and cataloging of the environment, specific signals with a high intelligence potential are encountered. When it is



Block Diagram of COLORCAST MODEM sampler

EO 3.3b(3)
PL 86-36/50 USC 3605

determined that further, sustained collection of such communications is required, a QRC collection package, optimized for the collection of that specific signal, is assembled and the processing algorithms necessary to handle its protocols are implemented on an appropriate processor, either in the field or at NSA. Such QRC actions enable us to provide a sustained collection/processing capability of high-priority communications long before we will be able to field a general-purpose modem collection/processing system.

[redacted]

~~(C-CCO)~~ *A priori* information concerning a network's structure and its operating characteristics can greatly facilitate a collection effort mounted against it. Such information is critical when dealing with the very complex and potentially dynamic routing of packet-switched networks.

[redacted]

FUTURE INTERNATIONAL COMMUNICATIONS

(U) The world-wide change from analog to digital communications is occurring at an increasing rate; some forecasts have predicted that by the end of this century, which is only 13 years away, over 90% of all free world communications will be passed by high data rate digital carriers. The rapid introduction of channel-level modems during the past several years is but the first step in this change. Already, "group band" modems, INTELSAT's intermediate data rate carriers (IDR), and digital radios with data rates in excess of 140 megabits per second are in operation.

(U) The next decade will see the SIGINT system continually confronted with the introduction of new technologies which will create problems in at least four areas:

[redacted]

EO 3.3b(3)
PL 86-36/50 USC 3605

[redacted]

(U) The trend appears to be towards to the establishment of integrated services digital networks (ISDNs). These networks will carry voice, data, and video information within multiplexed data streams by means of digital microwave, cable, fiber optic, and satellite transmissions. The structure of many of today's packet-switched networks has been designed specifically to facilitate the incorporation of ISDN technology. An ISDN is an end-to-end digital network that uses uniform transmission, signaling, and operating procedures. Access to the network and its associated services will be through a standard, physical interface using existing telephone systems.

(U) The key to ISDN is standards. A committee of telecommunications organizations in Western Europe began work in 1979 to develop standards for ISDNs. Today, ISDN standards are being further defined by the Consultative Committee on International Telephony and Telegraphy (CCITT), an international standards organization with a mandate to establish recommendations for end-to-end performance, interconnection, and maintenance of world networks of telephony, telegraphy and data communications. This group has already identified a number of fundamental standards of ISDN. Interestingly, though, planning for ISDNs has been progressing for at least seven years, it has only been within the past three years that the performance requirements for satellite networks have begun to take shape.

(U) The basic building block for voice, video and data communication in ISDN is a 64-kilobit per second channel, called a B channel. This same building block is used in existing digital telephony networks to transport pulse-code modulated voice-band signals. To achieve higher transmission rates, several B channels can be concatenated to form a channel with a bandwidth in excess of 64Kbps. The resulting channel is called an H channel.

(U) In existing telephony networks, signaling data for a communications channel is encoded within the channel, while in ISDN, it is carried in a separate, associated channel called a D channel. A single D channel can carry the signaling information for many B channels. This technique of separating the signaling channel from the data transmission channels is called common channel signaling and is fundamental to ISDN.

(U) A basic ISDN standard is the basic access interface. This 144-Kbps interface consists of two 64 Kbps B channels for voice, video and data transmission and one (16 Kbps) D channel for signaling. An alternate access interface for large organizations is the primary access interface. For North America and Japan, this is a 1.544-Mbps interface consisting of 23 (64-Kbps) B channels for voice, video, and data transmission and one (64-Kbps) D channel for signaling. In Europe and most of the rest of the world, the interface is a 2.048-Mbps interface consisting of 30 (64-Kbps) B channels for voice, video, and data, and one (64-Kbps) D channel for signaling.

(U) ISDN provides the flexibility of submultiplexing channels for applications that do not require the full 64-Kbps circuit capacity. It also supports packet switching, as well as the circuit switching found in existing networks. These capabilities provide great opportunity to maximize circuit capacity.

CONCLUSION

~~(C-CCO)~~ While the transition from analog to digital communications presents us with a set of difficult technical problems that must be solved if the SIGINT system is to continue to

EO 3.3b(3)
PL 86-36/50 USC 3605

Non - Responsive

function effectively, none is insurmountable.

[redacted]

[redacted]