~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

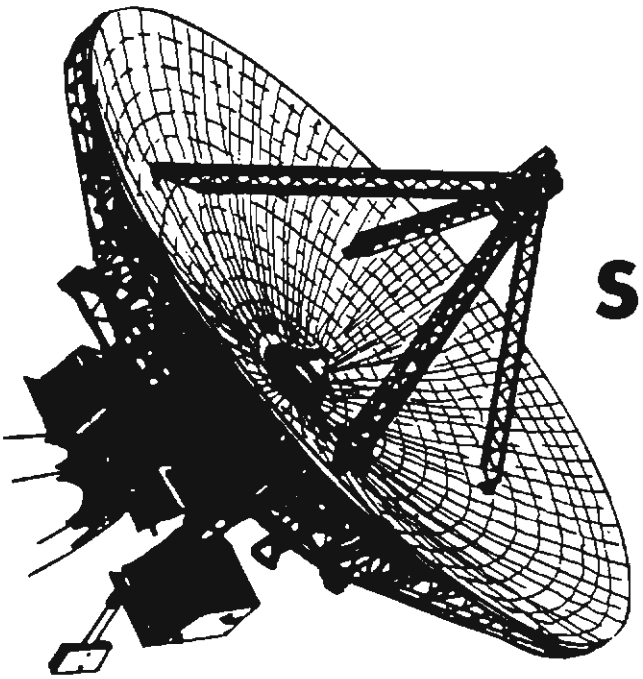
SEPTEMBER 1982

P.L. 86-36

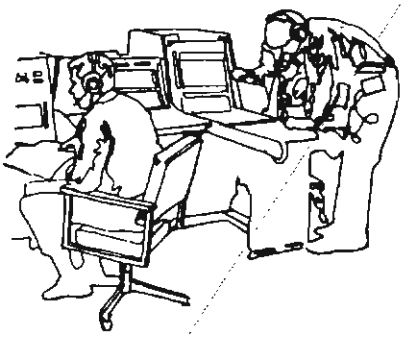
~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by NSA/CSSM 123-2
Declassify on: Originating Agency's Determination Required~~



SIGINT: 1990 (U)



by Joseph Meyer, P13

(U) Major developments in telecommunications technology and systems during the 1980's will have a profound effect on SIGINT by 1990. The main threads of this development are new satellite systems, optical fiber cable, electronic switching, the coalescence of computers and communication nets, and the increasing complexity of telecommunications.

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in several monthly installments, from his presentation at a January 1982 session of CA-305. The overall classification of the series will be TOP SECRET UMBRA.

(U) In order to see what the communications environment of 1990 will be like, and to analyze the impact on SIGINT, we will begin by looking at current trends in technology, networks and traffic growth, costs, and specific systems.

SIGINT 90: TRENDS, IMPACT, CHOICES

(U) In order to respond to the changes in the telecommunications environment, it is necessary to make some choices and to consider some specific actions, policies, and projects that will be needed. Most of these will be dealt with later in the paper; however, a fundamental choice is to begin with a suitable definition of SIGINT, viz.

SIGINT is the process of obtaining secret or unknown information from communication systems or signals.

(U) In this definition, it is the process, not the product, that is important. Also, the desired information, which may be intentionally kept secret or merely unknown to us, is to be obtained from "communications systems," not merely from "communications." The "system" includes all the traffic, but also includes things such as computer memories, circuits, switches, software, documents, etc. Any method of getting secret or unknown information from the "communication systems" or from "signals" falls under the authority of SIGINT.

(U) The importance of getting the definition of SIGINT right is that the classical "passive" model of SIGINT sitting back waiting for signals to reach it is no longer appropriate for the problems of 1990. The attacks against computer-communication nets, and against systems such as optical fiber, require operations based on physical and electronic penetration of the target links and nets, tightly coordinated with monitoring and analysis, to gauge how well the penetration is doing. This cannot be handled by multiple agencies trying to "coordinate" a mission; the authority and operations must be unified into SIGINT.

[redacted]

(U) There is little basis at present for optimism about the future if SIGINT continues to operate in its present framework, yet unoptimistic forecasts are rarely welcomed. As a paper "Why Pollyanas Prosper," at the January 1982 AAAS meeting noted, the meliorists discount the future at an extremely high rate in favor of confidence about the present. Thus, all the forecasts are rosy up to the very end.

THE TECHNOLOGY BASIS FOR TELECOMMUNICATIONS

(U) Many of the major advances in telecommunications have stemmed from advances in materials science.

MATERIALS SCIENCE IN TELECOMMUNICATIONS

Material	Application
Copper	Telegraph lines
Carbon Microphone	Telephony
Gutta Percha	Ocean Cables
Tungsten	Vacuum Tubes
Crystal Growing	Stable Frequencies
Semiconductors, Transistors	Computers
Magnetic Oxide	Core Memories, Disks, Tapes
Cryogenics	Space Communications
Solar Cells	Space Communications
Glass	Optical Fibers

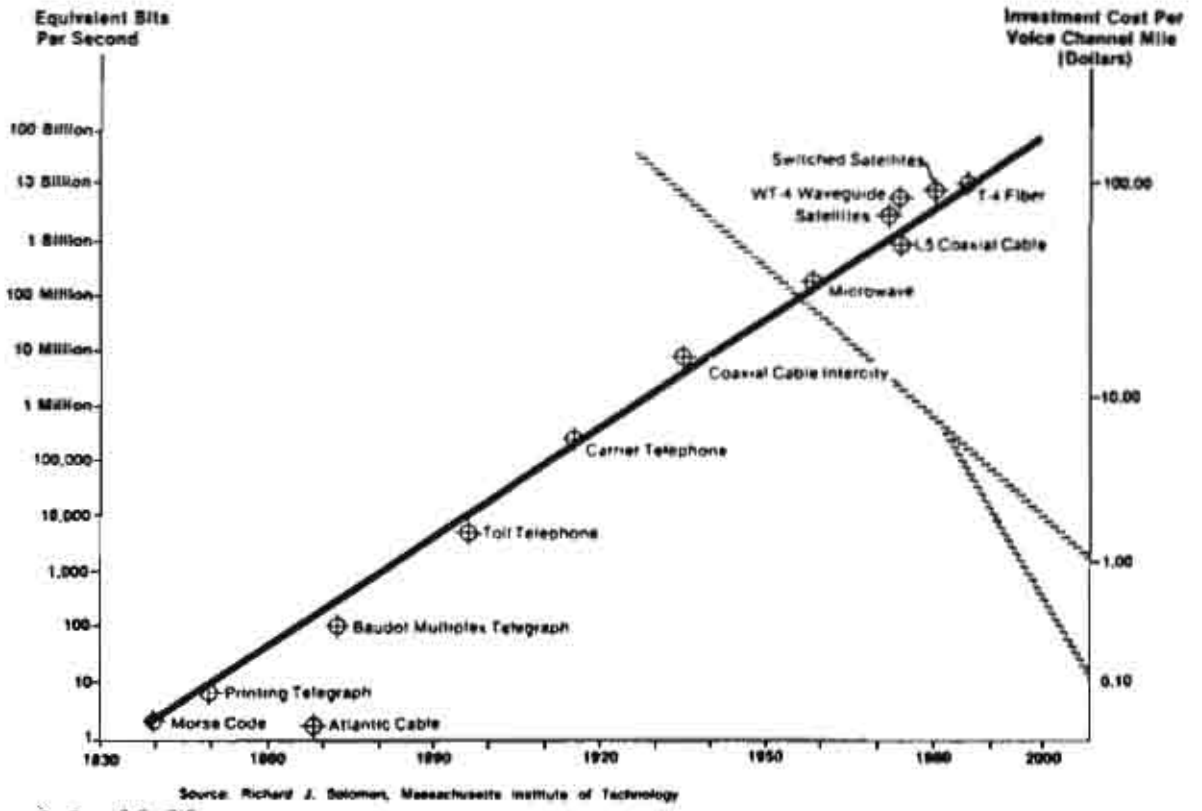
(U) The list above, although not exhaustive, indicates the importance of improvements in materials in the growth of telecommunications. The purification of copper was a fundamental step, for it made possible electrical engineering of all kinds, and electrochemistry has been a basic technique for purification of other materials. The advances in glass technology are currently bringing about a revolution in telecommunications by making landline cheaper than radio relay or satellites.

[redacted] P.L. 86-36 EO 1.4.(c)

(U) The effect of applying materials advances and various other inventions to telecommunications has been a steady improvement in technology, so that much more information can be sent at a much lower cost.

~~TOP SECRET~~

The Sequence of Inventions in Telecommunications, 1840-2000



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

1. SEQUENCE OF INVENTIONS IN TELECOMMUNICATIONS

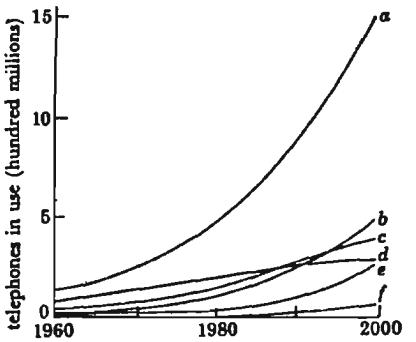
(U) From the primitive 10 words-per-minute (wpm) transmissions of landline Morse telegraph to the gigabaud satellites and optical fibers of the late 1980's, there has been a steady advance in transmission capacity amounting to a tenfold capacity increase every 20 years since the invention of the electric telegraph. At the same time the average capital cost of building these systems has dropped tenfold in the last 50 years.

[redacted]

[redacted]

VOLUME FORECASTS

(U) Both traffic and equipment have increased in volume, so that the 400-million telephone plant of 1977 is expected to grow to a 1500-million subscriber plant by 2000.



Forecast growth in the number of telephones in use: (*a*) the world; (*b*) Asia and Oceania; (*c*) Europe; (*d*) North America; (*e*) Central and South America; (*f*) Africa.

2. FORECAST OF NUMBER OF TELEPHONES

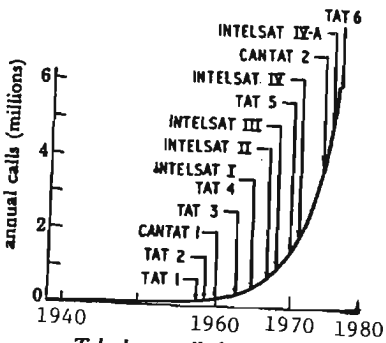
(U) The total "book value" of the world telephone plant at present is about $300 billion. An A.D. Little study predicts that $640 billion will be spent over the next 10 years for a new telecommunications plant, with expenditures rising to about $80 billion by 1990. This will be for a predominantly civil telecommunications plant.

(U) In the developed world the growth of telephone stations has slowed, as shown in curve (d) above, but in Europe and Asia the growth is faster, as high as 10-12%. In Africa the telephone density is not only low, but will remain low because of lack of money to install the plant.

(U) The cost of adding a telephone station to a network is about $2000, which covers the cost of the subscriber loop, local switch, and long-distance transmission facilities. Hence, the expected cost of telephone plants from 400 to 900 million phones by 1990 will require an outlay of about $1000 billion (reduced somewhat by more economical switching and transmission plants).

~~(S-CCO)~~ The impact of this growth in telecommunications plants, which will carry many services in addition to POTS (plain old telephone service) is that more and more of the political, economic, and military activities of the world will pass over telecommunications circuits and will be dependent upon those communications. This means that the potential returns from SIGINT will increase at least as rapidly as the telecommunications traffic, which is already growing at 20% annually. However, the vast physical plant, along with many of the technical improvements in switching, transmission, and security, will make it harder for SIGINT to find and exploit the specific traffic that is worth working on. To quantify this, the U.S., with about 40% of the world's telephones, generates about 170 billion calls per year, of which about 20 billion are toll calls. Non-U.S. toll traffic is about 20 billion calls, each about 10 minutes long. No agency can look at all of this traffic. The problem of selection is paramount and selection will become much harder.

~~(S-CCO)~~ A second impact of the growth of plants is that the turnover time for equipment will decrease. At present transmission systems have a cycle of about 15 years, after which it becomes economical to introduce new transmission technology, e.g., analog satellites of 1965 are being replaced by digital satellites of 1980. Switches have had 30 year cycles, even though old switches often are operated for 50 years. But these long service lives are no longer economical, and equipment will be replaced at a hastier rate by more capable equipment. This means that the lifespan of certain kinds of SIGINT systems and techniques will also be shortened, and new SIGINT plants and methods will be needed to keep up with the target changes.



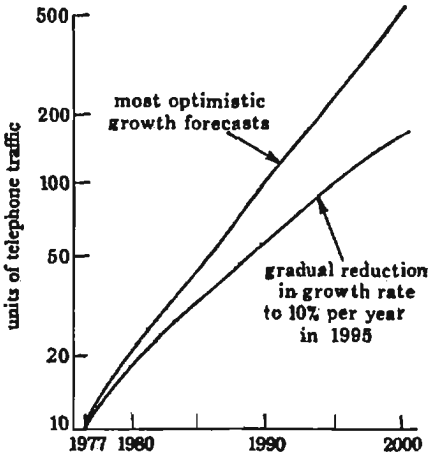
Telephone calls between the U.K. and North America, and the introduction of cables and satellites.

3. PHONE CALLS U.S./U.K.

(U) One of the most dramatic effects of telecommunications advances has been the increase in intercontinental traffic, as cheaper and better systems have allowed economic and governmental activities to operate on a global scale. In 1927 transoceanic telephony was initiated, with calls averaging 2000 per year. The first submarine telephone cable in 1956 brought about rapid growth in traffic, which continued to grow at 20% annually. The development of higher

capacity satellites and cables has given a transoceanic capacity of about 12,000 circuits. During the late 1980's this trans-Atlantic capacity will be more than quadrupled (see undersea cables, discussed below).

(U) In 1927, when there were only 2000 trans-Atlantic phone calls, each of those calls cost about $400, but today, with the increased volume and improved equipment, a trans-Atlantic call costs only a few dollars. The introduction of cable in 1956 improved call quality so much that it uncovered a demand which has justified expanding the capacity to the 12,000 two-way channels now in service.



Intercontinental traffic forecasts: telephone calls from the U.K.

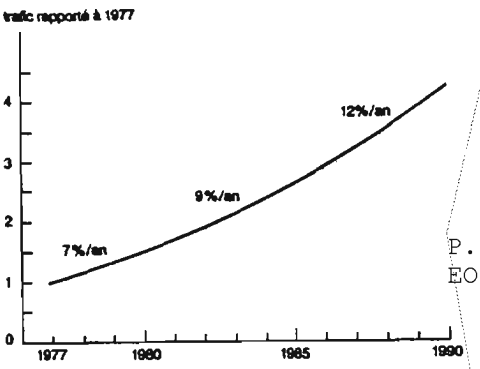
4. INTERCONTINENTAL TRAFFIC FORECASTS

(U) Various authorities, including Intelsat, have estimated intercontinental traffic growth at 22% annually, but more conservative estimates expect growth to taper down to 10% after 1990. The growth of telephony however does not express total traffic growth because, owing to time differences, the calls are generally placed in a short time window when people on both sides of an ocean are at their desks. Thus, late afternoon in Europe connects to early morning in the U.S.

(U) The transoceanic networks are designed to pass this peak load traffic, but so far have been comparatively idle during off hours, with traffic dropping to 20% of trunk capacity outside the peak four-hour period. The development of new kinds of traffic for international circuits, particularly digital facsimile, electronic mail, and computer data traffic, will tend to fill up the slack hours of the nets, so that total traffic flow will grow much faster than 20%. By 1990, the major telephone operating authorities expect digital facsimile to be the next major traffic after voice.

[redacted]

Télécommunications, objectif 2000



Évolution du trafic téléphonique total

5. 6% to 12% INCREASING TRAFFIC GROWTH

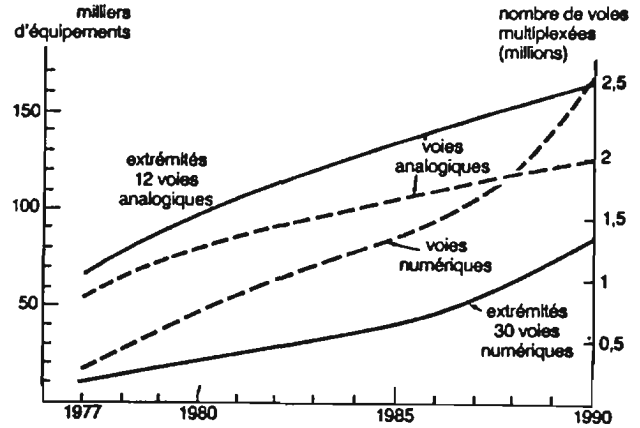
(U) CNET (Centre National d'Etudes des Telecommunications) has projected increasing growth rates for French traffic from 7% in 1977 to 12% in 1990. The projection is apparently due to expected improvements in speed, reliability, and cost of the services, as it becomes easier to use the network. Penetration of the telephone into new user areas is also a factor, for as more people are brought into the network, telephony replaces mail and travel.

[redacted]

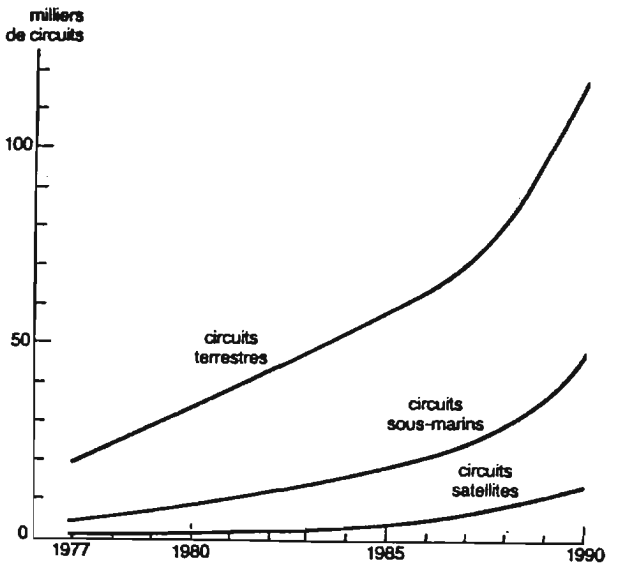
P.L. 86-36
EO 1.4.(c)

will be almost no aspect of the economic, political, social, or security activities in any country that does not use and depend upon the telecommunications systems. Hence SIGINT will have the highest potential growth rate of any intelligence service, and will be capable of the deepest and most extensive penetration into the activities of any target country--providing it can be done successfully and is adequately funded.

Télécommunications, objectif 2000



Équipements d'extrémité



Circuits internationaux

6. CNET: INTERNATIONAL CIRCUITS

(U) The French forecasts of international circuits up to 1990 show several interesting characteristics. Total circuit growth will be about sevenfold, but satellite circuits will only be a small part of the total, in spite of the fact that the French have been developing Telecom satellites. The main growth will be terrestial circuits, which is logical since France has substantial business with neighbors. The hidden element is that the French, as well as the other Europeans, intend to stay away from satellite circuits in favor of optical fiber interurban and international trunks. Satellites will be used for mobile services, and for backup and to establish new services temporarily until landline or optical cable can be installed.

~~(TS-CCO)~~ The impact on SIGINT of the European preference for optical fiber cable over satellite is that their international traffic will be harder to intercept. If the relations between the U.S. and Europe change during the 1990's (e.g., by the dissolution of NATO or by a political shift toward the Soviet Bloc or to Eurocommunism) those countries may become active targets, but access to their traffic will be harder. This access will be even harder if the U.S. presence is greatly reduced, e.g., by withdrawal of U.S. military and governmental organizations from Europe.

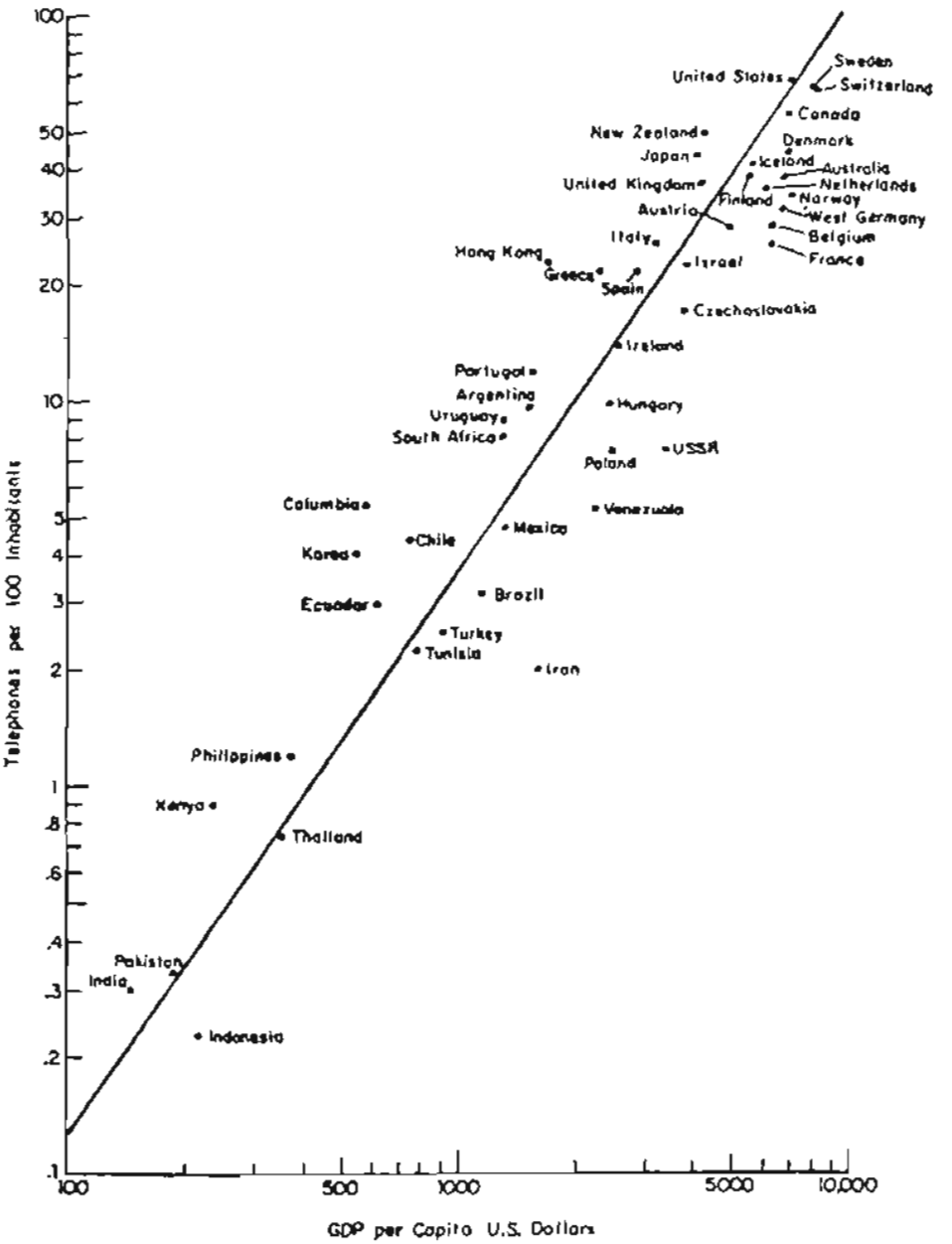
PHONE DENSITY/GNP RATIO

(U) The correlation between national wealth and telephone density is well established (see page opposite). The rich industrial countries have a high telephone density, as many as 70 phones per capita, while poor nations such as India have only about 3 telephones per 1000 inhabitants. In Africa the telephone plant is so undeveloped, that only Kenya appears on the graph at all.

(U) In spite of the lack of civil telephone facilities, the governmental telecommunications plants are often more advanced, with satellite and microwave and long-distance shortwave nets. The U.S.S.R. is a case of special interest because its telephone density is quite low, yet it has a highly developed governmental telecommunications network.

(U) One of the striking features of civil telecommunications in Africa and Asia and other low-income areas is that there are practically no rural telephone plants at all. At INTELCON 80, the Communications Minister of Nigeria asked his fellow Ministers of other African countries if any of them could name a single case of a rural telephone system, and there was no reply. The World Bank has been pursuing projects to introduce public telephone service into the rural areas of the

THE RELATIONSHIP OF NUMBER OF TELEPHONES TO
GROSS DOMESTIC PRODUCT IN VARIOUS COUNTRIES

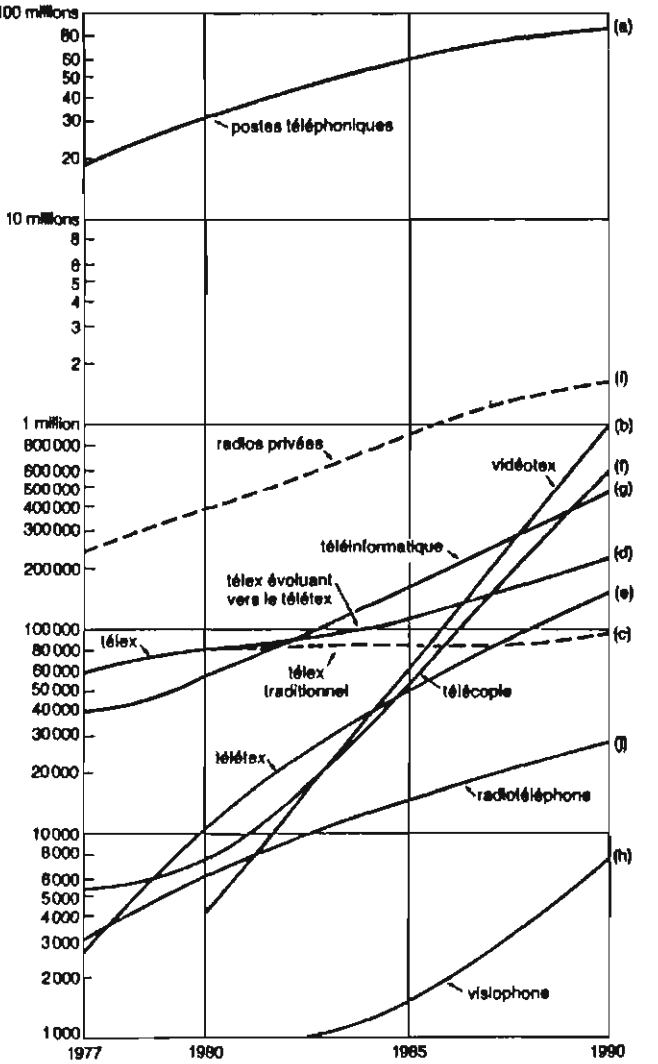


Source: INTELTRADE

Fig. 7

Third World, on the economic argument that the phone service will pay for itself, but progress is slow. The basic problem is cost, coupled with problems of equipment reliability. Satellite communications are not seen as an answer to Third World telecommunications in general, because the population is too sparse and the economic margins too slender to make two-way earth stations feasible even at the town level. Even when nations get some cash flow, e.g., from mineral exploitation, the money tends to stay in the cities where the rate of return is highest.

~~(S-CCO)~~ The impact of this telephone/GNP correlation on SIGINT is that for the rest of the century the spread of telecommunications services and the flow of traffic in the undeveloped countries will be tied to the cities and to economic and governmental activities, with the exception of broadcasting. The demand of the Third World countries for robust long distance communications created a problem at WARC 79 over HF allocations and assignments. The Third World nations will probably crowd into the HF spectrum as fast as they can buy equipment, but there is not nearly enough HF spectrum to accommodate them. The best alternative communications for remote area communications will be low-cost over-the-horizon systems such as meteor burst (cited below), thin route tropospheric scatter, and low bandwidth mobile satellite services, using high-powered satellites with big antennas. At the same time, the main telecommunications trunks serving cities and the industrialized countries will carry traffic that penetrates to every business, household, and government function. In brief, economic status will be the primary selector of telecommunications plant and traffic. The higher the relative cost of a message (or an enciphered message) in a country, the greater its expected information value.



Impact quantitatif des services de télécommunication (parc de terminaux)

(1) En dehors du terminal annuaire.

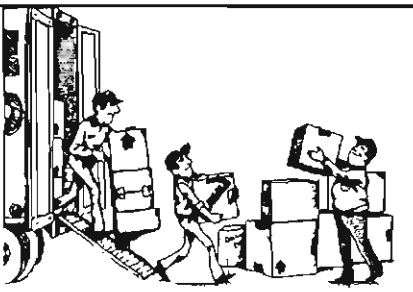
8. CNET: QUANTITATIVE GROWTH OF VARIOUS TELECOMMUNICATION SERVICES

~~(S-CCO)~~ The SIGINT systems will cover increasing masses of traffic in which the expected value of any message continually decreases, even though the total value of the information in the networks will continue to grow at least as fast as the GNP. One of the most interesting SIGINT factors is that the third world nations, being poor, are still largely open markets for well designed, heavily subsidized basic telecommunications plants which could, with enough ingenuity, create interesting SIGINT opportunities.

(U) While overall growth of POTS (plain old telephone service) will increase at about 6% annually, a number of specialized and new services will grow at higher or lower rates. The CNET graph above shows projections till 1990 for French services. Traditional Telex, which is already a saturated market, will grow very slowly, while new services such as private radio, videotex, teletex, and telecopier will grow at much higher rates. Private radio has been resisted by European PTT's, but CNET shows an expected fivefold growth over the next ten years. Teletex, at 2400 bps, is expected to have fifteenfold growth from 1980 to 1990, and more significantly is expected to become the "lingua franca" between various

information systems such as telex, videotex, computer data, etc.

(U) The growth potential of new specialized services is sometimes misleading, as the case of SBS (Satellite Business Systems) shows. Originally developed to sell high-speed data services to the top Fortune 100 companies, it has only managed to attract about 25 major companies, and they want POTS, viz. corporate voice traffic services. Long-term growth potential of network computing services is expected to be good, but over the short term the system and software costs may eliminate all but the richest companies. L.M. Ericsson has bought up Datasaab, to position itself in computer networks, AT&T is trying to develop a computer net service, and IBM is looking to extend its computing capabilities to overseas markets by international operation of a domestic satellite SBS system. Other domestic satellite (Domsat) operators are also looking for overseas outlets for their services. Even the German telecommunications giant Siemens is struggling to develop and incorporate successful computer services, even though its microelectronics VLSI technology is as good as that of the U.S. leader Intel Corp. (Business Week, 1 Feb 82, p. 87). The French government has undertaken a high technology program in telecommunications, aimed at export markets, and French industry is in a leading position in electronic switches and terminal equipment. For the modern telecommunication services, software development is a critical element, and only the Japanese are in a position to challenge the U.S. seriously.



FACTORY SHIPMENTS OF ELECTRONICS

(U) The steady growth of electronic sales (see figure 9) in all categories shows a tripling in dollar value. Electronics for information processing is the largest segment of the electronics industry, but the demand for communications common carriers has been growing the fastest in the last half-decade. Common carrier growth may be accelerated even more by future demands from "home information" systems.

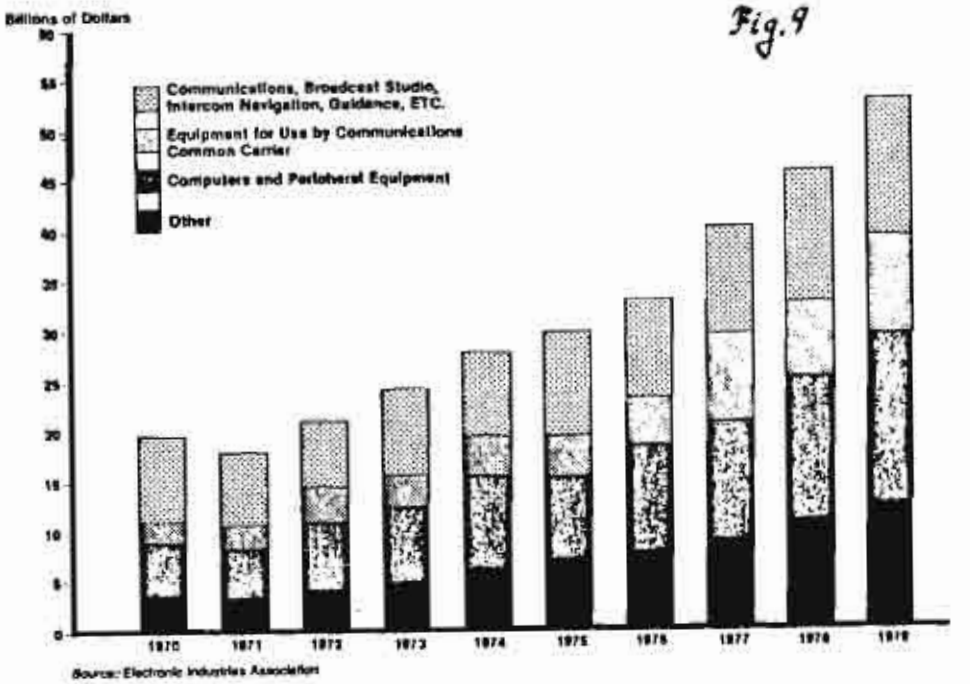
P.L. 86-36
EO 1.4.(c)

U.S. TRADE IN COMPUTERS

(U) The continuing growth in computer sales, and particularly the growth in imports, is a manifestation of the spread of computer manufacturing technology. The coalescence of computers and communications, examined below, will make this computer base a major factor in telecommunications. The strength of the foreign technology, especially the Japanese, is manifested in the imports. Another factor of some importance is that the U.S. market for telecommunications equipment is now virtually unrestrained for foreign competitors, who can subsidize sales to the U.S. to force an entry into the U.S. market. As the U.S. telecommunications industry is fragmented in the name of competition, more foreign computers, communication equipment, and services will take over parts of the U.S. market, e.g., for PBX's, interconnections, satellite links, data terminals, and even basic transmission and switches.

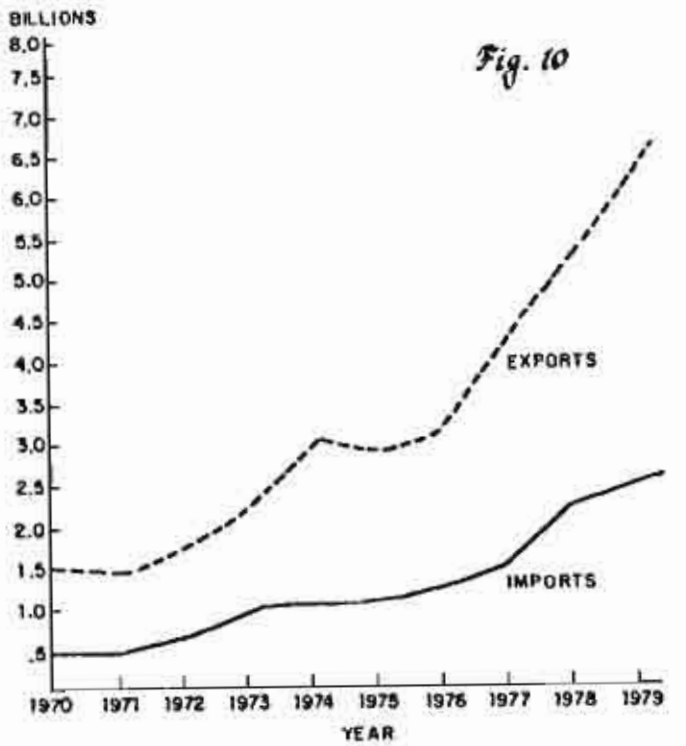
Annual Factory Shipments: Communications and Electronic Equipment by Type, U.S., 1970-1979

Fig. 9



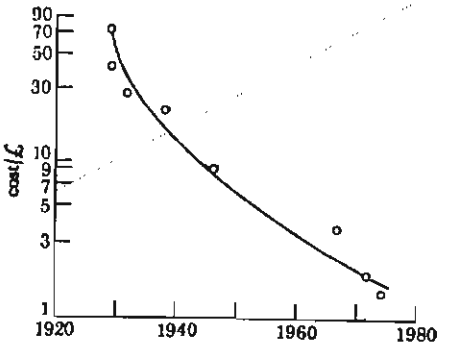
U.S. TRADE IN COMPUTERS AND RELATED EQUIPMENT

Fig. 10



Source: CBEMA

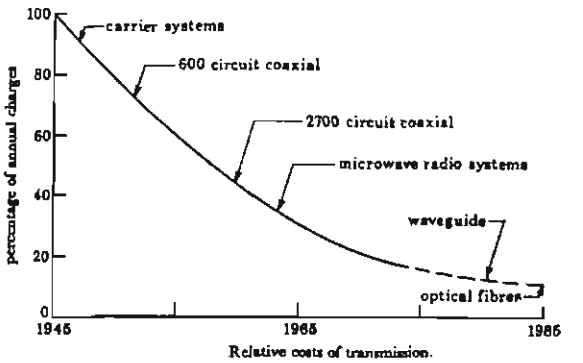
P.L. 86-36
EO 1.4.(c)



11. NY-LONDON PHONE CALL

(U) In 1927, when there were only 2000 calls per year, each of those calls cost about $400, but today such calls cost only a few dollars. The introduction of cable in 1956 improved call quality so much that it uncovered a demand which has justified expansion in capacity to the 12,000 two-way channels in service now.

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



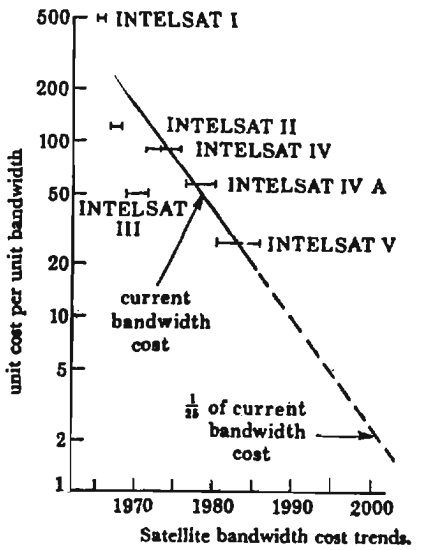
12. TRANSMISSION COSTS FOR DIFFERENT MEDIA

COSTS

(U) At the same time that the civil telecommunications plant has greatly increased in size and traffic capacity, the cost of services and equipment has gone down drastically. This has encouraged greater usage by a wider public, giving a larger revenue base which in turn leads to faster expansion and greater cost reductions.

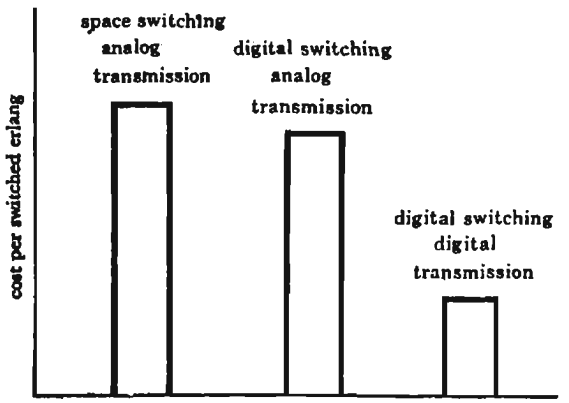
(U) To some extent the economies in technology in the civil nets have been applied to governmental and military dedicated nets, but at the same time the military nets have been given more difficult requirements, e.g., anti-jam, security, transportability, survivability, etc., so that the unit cost of military communications has not fallen much, and the demand for much greater capability and higher information rates has made military telecommunications more expensive for the same mission.

(U) Technological advances in transmission have greatly reduced the costs of moving traffic. For many years microwave radio relay was unsurpassed as the cheapest medium for trunk traffic. Efforts to develop radio waveguide transmission were unpromising, but optical fiber waveguide has developed so rapidly in the past ten years that even the major manufacturing companies have been surprised. Over the next ten years optical fiber will be substituted for existing or new cable and radio relay on many thousands of kilometers of trunk routes, particularly where traffic is heaviest.



13. SATELLITE BANDWIDTH COST TRENDS

(U) Reductions in satellite costs have been even more rapid than in terrestrial systems. The development of stabilized satellites which could keep solar panels and directional antennas pointed at sun and earth has given much increased power efficiency. A combination of improvements in space and earth systems has produced more than twentyfold reductions in channel cost in little more than a decade.



14. TELEPHONE SWITCHING COSTS

(U) Capital cost of switches used to be 50 percent of the total cost of the telephone plant. This was one of the reasons that switches were designed for 30-year financial lifetimes, viz., the cost of the switches was amortized over 30 years in calculating the rate base for subscriber costs. This led to a great deal of conservatism in telecommunications planning and a resistance to innovation. By contrast, computers and the associated operating systems and manufacturing plants have usually been written off after 7 or 8 years, because of the rapid changes in technology. Now, as digital switching is introduced into telecommunications networks, the capital cost of the switches is dropping to about 15 percent of the total network, so that much less money is tied up in the switches. At the same time the switches are more capable. The No. 4 ESS of AT&T has undergone a complete replacement in hardware technology, while keeping the software and functions the same, and this has reduced frame cost, space, and power requirements by 60 percent.

~~(S-CCO)~~ A major implication of the reductions in switch cost, which is further affected by the deregulation of telecommunications in the U.S. and the opening of the U.S. market to foreign switch manufacturers, is that the financial and functional lifetime for switches may be reduced from 30 years to less than 10 years over the next decade. It will not be worthwhile to keep an old switch in service when a cheaper and better switch can do more and provide entirely new services. This has an important implication for "SIGINT cultivation" discussed below.

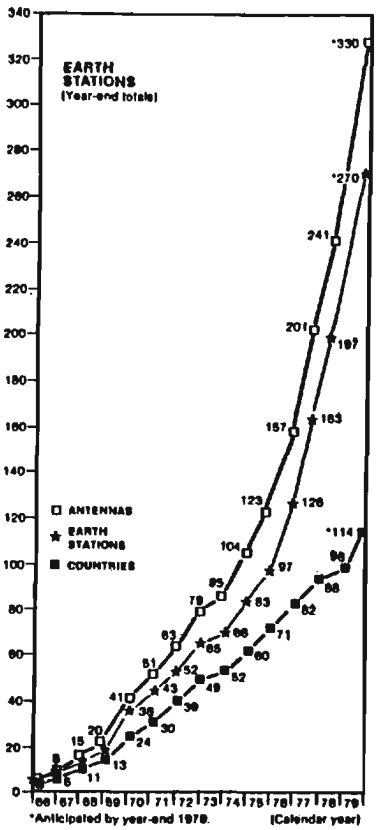
~~(S-CCO)~~ The major impact on SIGINT of all these cost reductions in telecommunications systems is that the target costs to install and operate nets are going down, while the costs of SIGINT are not going down. SIGINT is inherently labor intensive, and because it must extract unknowns from the target nets and traffic, it can never match the level of automation and efficiency of ordinary telecommunication nets. By analogy, a computer can search text for words, or do lengthy calculations far better than a human, but a person is far better at writing an essay or deciding how to attack and solve a mathematical problem. Most telecommunications is routine, while the most critical parts of SIGINT are very non-routine. Even the routine parts of SIGINT are subject to continuous change, so that economies of repeated large-scale operations are seldom realizable. When SIGINT is highly efficient, it is a result of chaining information in a highly non-routine way. Inevitably, the cost reductions in telecommunications will result in more and more plant and traffic, which will be more and more overwhelming to a fixed level of SIGINT effort.

~~(S-CCO)~~ One of the keys to reducing costs is to standardize the traffic, so that all

kinds of traffic (voice, facsimile, telex, data, etc.) can flow through the nets easily. Another key is to concentrate traffic so that efficient wideband transmission can be used. The immediate effect of these measures on SIGINT is that larger volumes of data have to be collected and scanned, with less easily identified characteristics, which means that the SIGINT costs per extracted message go up as the costs of transmitted messages come down. This is an ineluctable consequence of technologic advance, as long as SIGINT depends on a modus operandi and a physical plant which creates this cost exchange.

RADIO COMMUNICATIONS

~~(C CCO)~~ Because modern SIGINT has been predominantly based on radio interception, it is worth looking at some of the main trends in future radio systems, to see what effect these will have on targeting and collection, and on the subsequent analysis of radio traffic.



Source: INTELSAT Annual Report, 1979

15. INTELSAT GROWTH TO 1980

(U) The principal international satellite system, INTELSAT, began in the mid-1960's with one trans-Atlantic satellite and a few big earth stations, and by 1980 had over 400 antennas at about 270 earth stations.

FUTURE OF SATELLITE COMMUNICATIONS

(U) Saturation of the radio bandwidth has been a mounting problem in satellite communications (figure 16). This is particularly crucial for orbital slots used for transoceanic communications. At WARC 79 arrangements were made to increase satellite bandwidth allocation to nearly twice the pre-WARC amount. During the 1980's the major satellite developments will be in the 12-14 GHz frequency range, but by 1990 current projects show that demand for satellites will outrun the availability of those frequencies, and various countries are now developing technology for the 20-30 GHz range for the 1990-2000 era. For special purposes, millimeter wave and laser beams will be used for up-down and for intersatellite links.

(U) The initial applications of satellites were to international circuits, through the INTELSAT organization. Now the area of rapid growth appears to be in domestic and regional satellites that operate outside the INTELSAT framework. During the next decade NASA will launch over 100 payloads, most of which will be communication satellites. During the same period ARIANNE will launch about 50 payloads, also mostly communication satellites. Market estimates expect a demand for 1000 transponders for the Western Hemisphere, and about the same number for the rest of the world, added to existing satellite systems. Broadcast satellites for direct-to-home, or for broadcast distribution to fairly small antennas, will also grow. These broadcast satellites will also be capable of one-way message services. Mobile communication satellite services, particularly for shipping, are already in operation, and will extend their services to isolated fixed and mobile users.

(U) These new satellites will be capable of significant traffic volumes because they will be able to reuse frequencies. A typical transponder has a nominal bandwidth of 40 MHz and will carry about 40 Mbps. If 1000 foreign transponders are in service, this corresponds to a traffic capacity of about 40 gigabits. In addition to the foreign and international satellites, there is a proposal to allow domestic U.S. satellites to crossnet into foreign networks, because many of the multina-

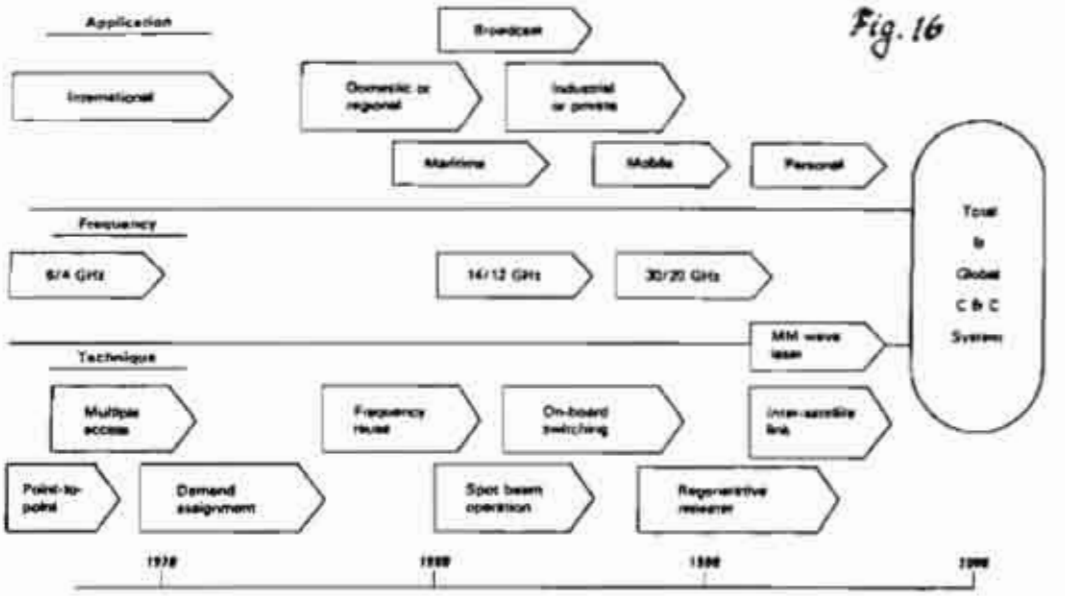


Fig. 16

FUTURE OF SATELLITE COMMUNICATIONS

tional customers have foreign facilities and they want their dedicated corporate satellite nets to reach directly to the foreign sites. The power of these companies is so great that they may cause the foreign PTT's to yield to their needs.

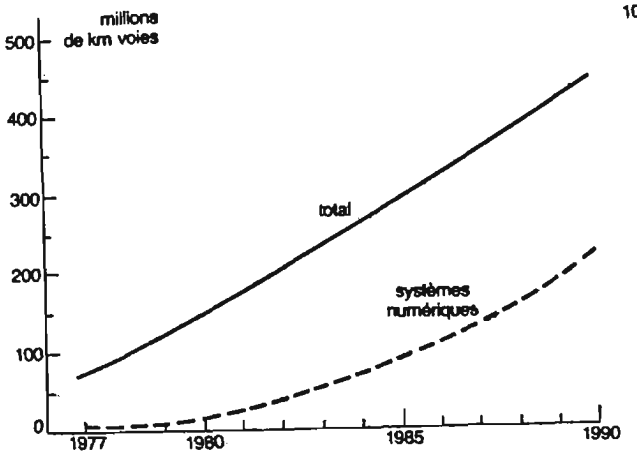
(U) Various new techniques will be used to increase the efficiency of satellite communications, principally spot beam operation, on-board switching, and regenerators on the satellites. By 1990 the transmission techniques will have advanced to the point where it will be necessary to measure the position of the satellite within a few millimeters, and to transmit a timing signal accurate to a picosecond around the U.S. to allow the high bit rate (10 gigabits/sec) operation, and on-board switching. The spot beams will switch from ground point to ground point to direct satellite energy to time-switched users.

(U) An example of the new trend in satellite communications is the French TELECOM I, which combines the features of MARISAT and SBS and provides a low-speed wide-area service and spot beam high-speed data relaying, with 25 Mbps trunk encryption.

~~(TS-CCO)~~ The impact on SIGINT of this expansion of satellites and traffic, and the introduction of new technology, is that, first, the data volumes will be overwhelming. Second, the spot beam operations will require intercept earth stations to operate within the "footprint" of each targeted satellite; and, third, the collection technology will have to be at least as sophisticated as the target satellite. The fourth problem, implied by the change to spot beams, is that intercepted traffic must be relayed from outside the U.S. in great quantities.

[redacted]

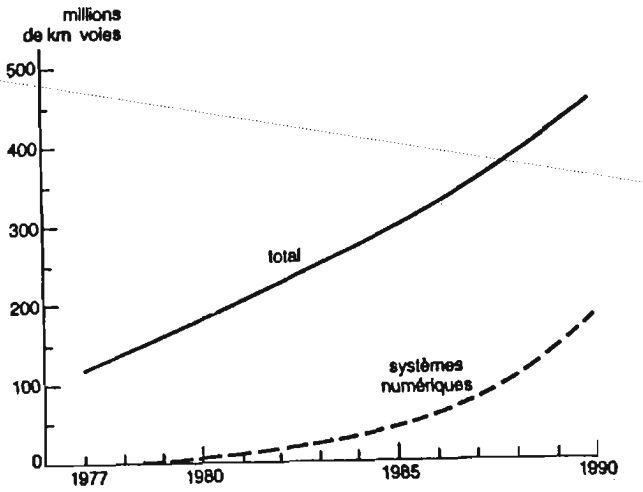
~~(TS-CCO)~~ Obviously, it would be better to select desired traffic before relaying the data, but improvements in switching, especially Common Channel Signaling and bulk encryption of satellite channels, will defeat the existing systems of preselection and targeting.



Systèmes sur faisceaux hertziens

17. GROWTH IN FRENCH RADIO RELAY

(U) The advances in satellite systems has by no means canceled the growth of terrestial radio relay. The French CNET studies show a fivefold increase in their radio relay over the next decade, with digital transmission accounting for half the growth. The digital microwave systems, pioneered by the Japanese, have shown robust performance in the presence of urban noise. In addition, they lend themselves to data communications and to bulk encryption.



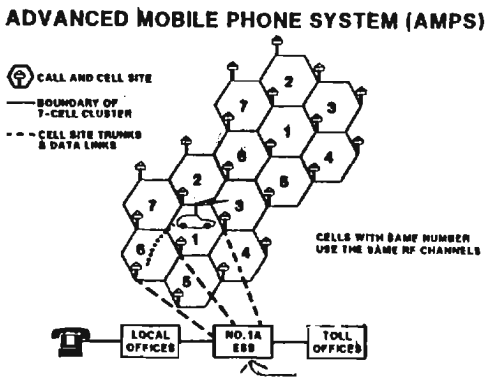
Systèmes sur câbles

18. GROWTH IN FRENCH CABLE

(U) The French, who had concentrated on cable, have not abandoned this medium, and CNET studies show a fourfold increase in cable capacity over the next decade. Digital cable transmission is also a fast-growing subset of this new plant.

~~(C-CCO)~~ The impact of these French developments on SIGINT derives from the fact that the French have an aggressive export policy in the area of telecommunications technology. Only a small part of the $60-billion world market is actually accessible to competitive marketing, but the French have studied this problem and have established a program to make equipment developed for the French PTT particularly suitable for the export market. The French banks and government collaborate in getting the overseas contracts, despite keen competition from the Japanese and other European manufacturers. As a result, technology developed for the French market, including switches and terminal equipment, will be sold on favorable terms in the Third World market to get the French manufacturers in on the ground floor. The French are even selling new switches and terminal equipment in the lucrative U.S. market. The result will be a steady flow into Third World countries of modern digital telecommunication equipment, accompanied by the adroit national presence of the various supplier countries.

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



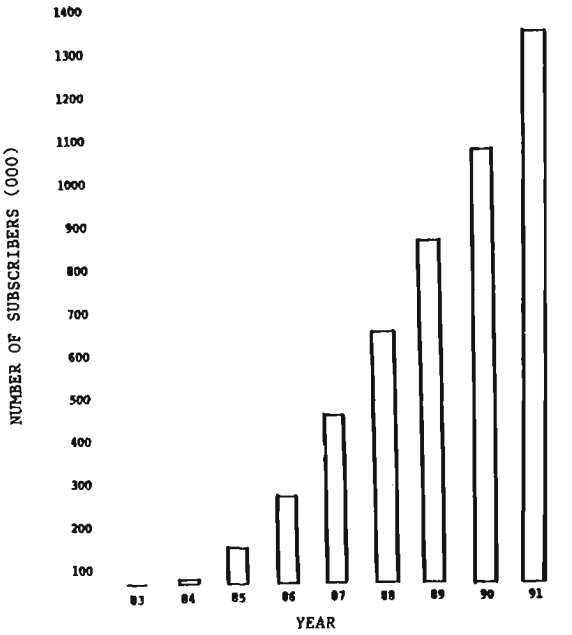
Switched Digital Capability

19. CELLULAR RADIO

(U) One of the large growth areas expected in new telecommunications equipment and services is mobile telephone, which can connect directly into the civil telephone nets. The current scheme for such mobile phone systems is to have a large number of frequency channels, and many transmitters in an area, e.g., a city. The radio system will track each user vehicle and switch the call to a radio channel that can be heard by the mobile station. The mobile receiver is switched at the same time. For ordinary FM radio links, the user is unaware of the switching. As the vehicle moves, it is assigned new frequency channels. As a result, the circuit for a single conversation may change frequencies many times as the vehicle moves. A large electronic switch (No. 1A ESS) is used by the Bell System for their mobile telephone system. Other proposed schemes would use spread-spectrum transmission so that many competing services could operate competitively in the same geographical area. With the interest in privacy and security for voice, digital mobile services are being studied, but the synchronization and switching are much more difficult.

~~(C-CCO)~~ The interception threat is not trivial, for a BEARCAT 300 scanner can monitor current mobile telephone channels easily. However, the problems of intercepting the switching circuits at 800 MHz is beyond a simple device such as a BEARCAT scanner.

PROJECTED GROWTH IN CELLULAR RADIO



Source: Motorola

20. GROWTH IN CELLULAR RADIO

(U) Motorola has projected rapid growth in U.S. mobile radio equipment over ther next decade, from less than 100,000 to over 1.4 million sets. Since Motorola is the dominant company in U.S. mobile radio, they are in a position to make the forecast materialize. The technology will will be copied abroad in the countries with high telephone density.

~~(TS-CCO)~~ The impact on SIGINT of the growth of these switched public telephone mobile services is that very interesting information may become available in the UHF spectrum in major cities, but it will present a complicated interception problem. Usually a set of frequencies is assigned to each transmitter and in the Bell scheme a seven-cell cluster is used to provide geographic separation for frequency reuse. SIGINT collection can thus be locked to the frequency plan, as the radio switching signals are also transmitted. However, analog encryption will probably come into vogue since most conversations will probably occur in a single cell. The mobile telephones are expensive, so that the traffic will have a higher expected value than ordinary telephony. This, combined with the large market, may encourage improved encryption systems that can operate over the switched radio links without loss of synchronization.

~~(S-CCO)~~ The cellular scheme contains an

indirect hint to SIGINT about how to do certain kinds of collection of mobile terrestial targets, for the propagation and noise studies and the tracking systems could be adapted to SIGINT.

(U) In addition to the high-growth radio systems cited above, there are a number of radio systems of special interest which will be mentioned later in the paper.

From: lrm at geishg04
Subject: Kudos
To: cryptolg at barlc05
cc: lrm

(U) Orchids again to [redacted] whose particular interests and insights never cease to interest and enlighten me. As a frequent writer of documentation for several volunteer groups (none of which have anything to do with computers) and an NSA manager, I found her June-July review to have almost universal applicability. I spend a lot of time off the job documenting procedures ranging from the mechanics of writing a business letter to the sweeping problem of handling customers' complaints. Mary's review has sent me scurrying to find a copy of the original article to see what other valid points the author might have on any area of instruction. Most of the highlighted points are equally applicable to any personnel manager who is either training an employee or assigning tasks, whether they be computer related or not. How true the quote: "If you tell a user to do something he does not know how to do...." Substitute person for user and you've got a great management guide!

Keep 'em coming!

[redacted]
G71 4007s
lrm@geishg04

MORE FREE GOODIES....

~~(C-CCO)~~ Delayed somewhat by a war, the third P14 "How to" working aid detailing UNIX/PINSETTER techniques for the traffic analyst is in final draft and should be in distribution shortly. This working aid, titled "How to Search", details the mechanics of using the search keys and the "binsrch," "grep," and "precog" commands.

(U) Organizations and individuals already on the distribution list for these working aids should receive copies by mid-August. If you or your organization is now or will be using TSS and UNIX/PINSETTER and would like to receive additional copies or be added to distribution, please contact [redacted] in P14 on 3369s. P.L. 86-36

SOLUTION TO NSA-Crostic No. 42

[redacted] "NSA Information Desk," CRYPTOLOG, May 1982

"Many times, NSA employees have [brought] to our [knowledge] the fact that NSA has been mentioned on the news or that they have read an article where the Agency has been mentioned. We appreciate this ...because it enables our office to keep the senior-level people better advised."

P.L. 86-36

~~(C-CCO)~~ [redacted] will be the speaker at the Autumn meeting of the KRYPTOS Society on 14 September 1982, at 0930 in the Friedman Auditorium. His talk, entitled "Twice Told Tale," pertains to a description of the "solution" of a cryptosystem which had been solved before, including analysis of indicators, cipher text, and cipher alphabets, as well as depth reading, programming, and historical research. The talk is classified TOP SECRET CODEWORD.

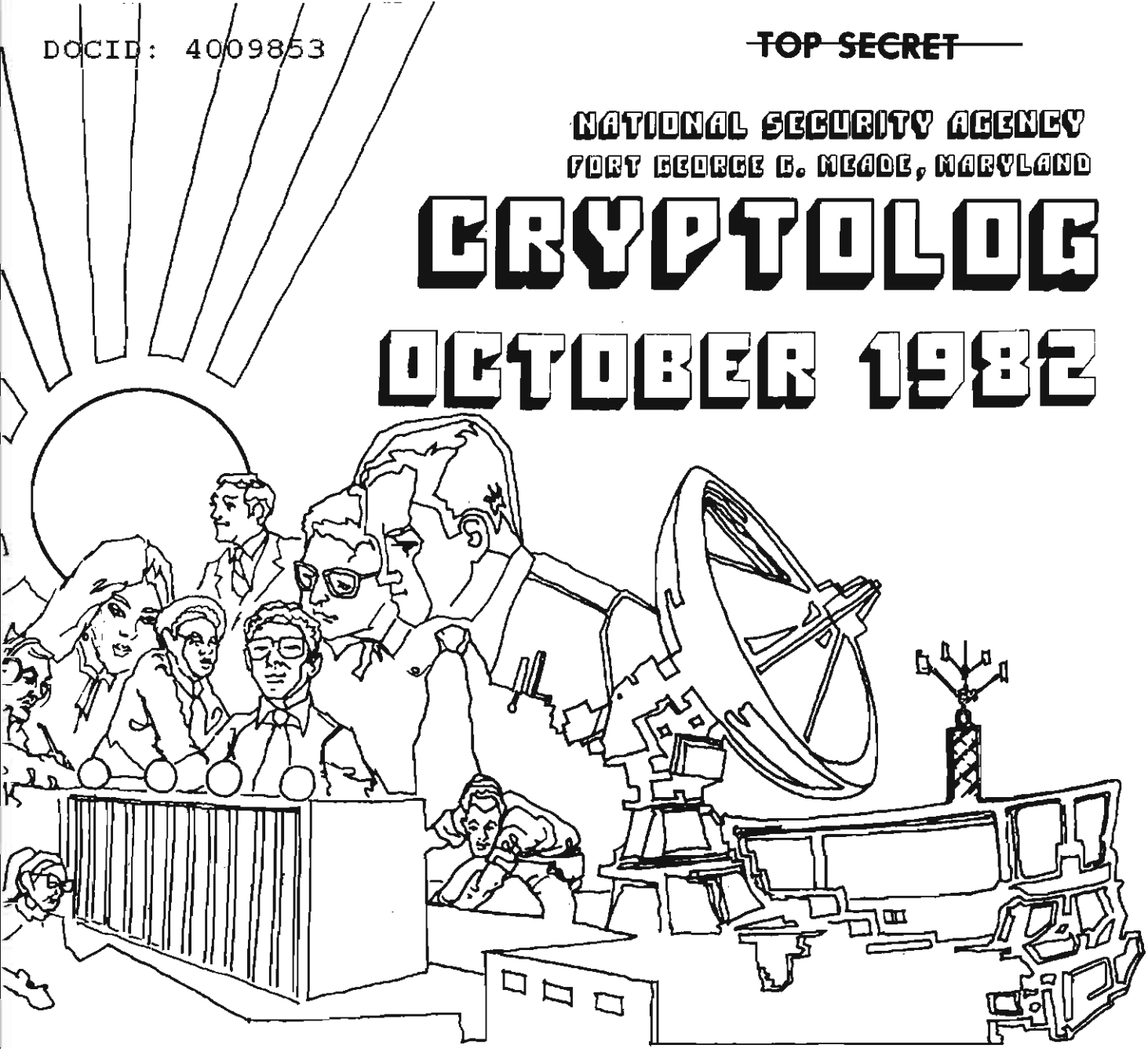
(U) [redacted] came to the Agency as a French linguist in 1952. The bulk of his career has been spent as a cryptanalyst in G Group. He spent several years as an instructor in the NCSch, and is currently a member of the Cryptographic Skills Enhancement Program in P15.

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1982



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

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

SIGINT: 1990 (U)

P.L. 86-36

Part 2

by [redacted] P13

OPTICAL FIBER

[redacted]

OPTICAL FIBER COMMUNICATIONS (NEC)

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in the second of several monthly installments, from his presentation at a January 1982 session of CA-305.

(U) Initial applications of optical fiber were for specialized applications, such as the communications circuits (see figure 21) that were installed with buried power cables. The fibers were unaffected by the powerful electrical fields, and gave reliable wideband circuits. Other specialized applications used the resistance to electrical noise and interference for shipboard and military applications, despite the fact that neither the glass nor the electro-optical components were very good.

(U) Rapid advances in glass technology and in laser and LED (light-emitting diode) and detector technology have occurred during the past ten years. These improvements have made short-distance circuits, e.g., within computer nets, economically feasible, and the telecommunication operators are beginning to install short-distance and medium-distance (up to a few kilometers). circuits in parts of the existing networks.

(U) By 1990 better glass and more reliable electro-optical components will make long distance trunks economical, and by the mid 1990's optical fiber loops will be introduced from the local switches to subscribers' premises. By 1982 the various Bell System companies had already installed over 25,000 miles of optical fiber trunk. A typical application will be the Northeast Corridor, a 400-mile trunk from Washington to Boston, using 3C digital transmission at 90 Mbps/fiber. Some fiber systems will use three separate light wavelengths at once, to give 270 Mbps/fiber. Typically an installed fiber system will have 12 fibers, with repeater spacing at 35 kilometers. Since coaxial cable repeater spacing is

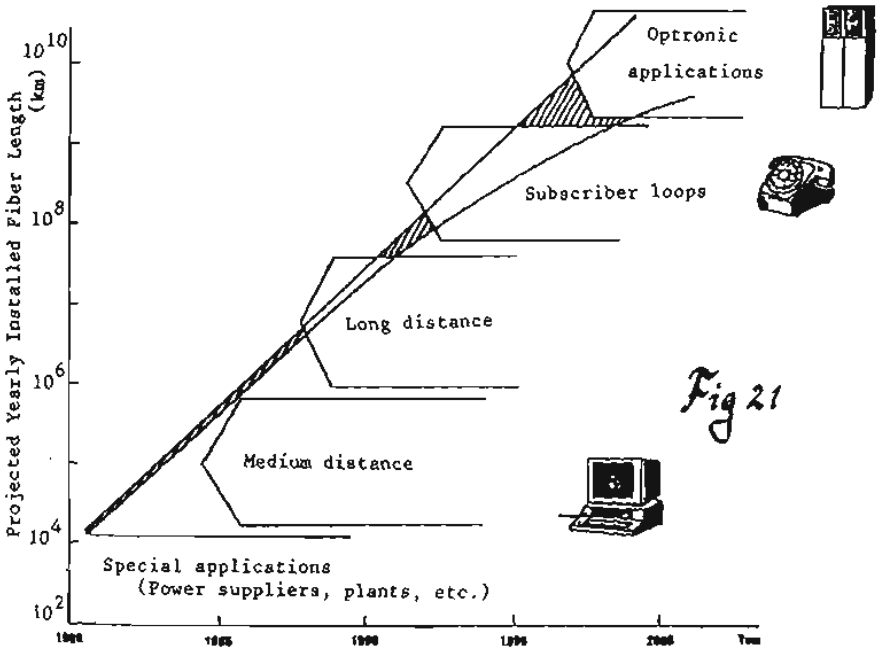
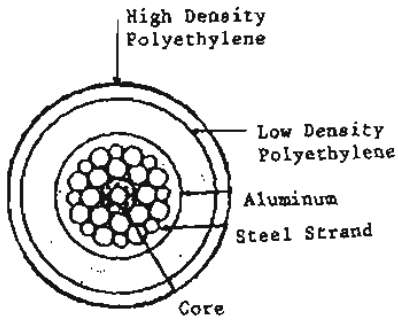
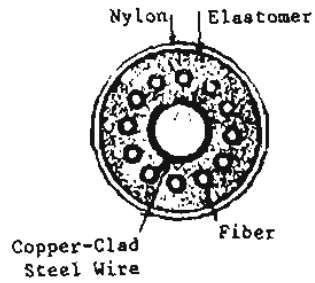


Fig 21

OPTICAL FIBER COMMUNICATIONS



CABLE



CORE DETAIL

Fig 22 UNDERSEA FIBERGUIDE CABLE

about 4 km, the optical fiber offers big improvements in system design, maintenance, and cost.

(U) NEC predicts a million kilometers of installed fiber by 1985 and 100 million kilometers by 1990. Since the Japanese are among the world leaders in both the technology and the marketing, they are in a position to make this prophecy materialize.

UNDERSEA OPTICAL FIBER CABLE

(U) One of the most dramatic illustrations of the advances in optical fiber is the development of a transatlantic optical fiber cable (fig 22), to be operational by 1988, which will carry 72,000 two way voice channels between the U.S. and three foreign countries over a 6500-km undersea cable. Transmission bit rate will be 375 Mbps per fiber, and a TASI (Time-Available Speech Interpolation) will be used to triple the traffic capacity.

(U) Power will be supplied over a copper-clad central steel cable, and a dozen single-mode fibers will surround the core. SG cable repeaters will be used, with a regenerator for each fiber, spaced at 35 km. The system is expected to have a 25-year life. The first cable will probably be the start of a revolution in transoceanic communications, just as the first transoceanic coaxial cable began the explosion of transatlantic telephony.

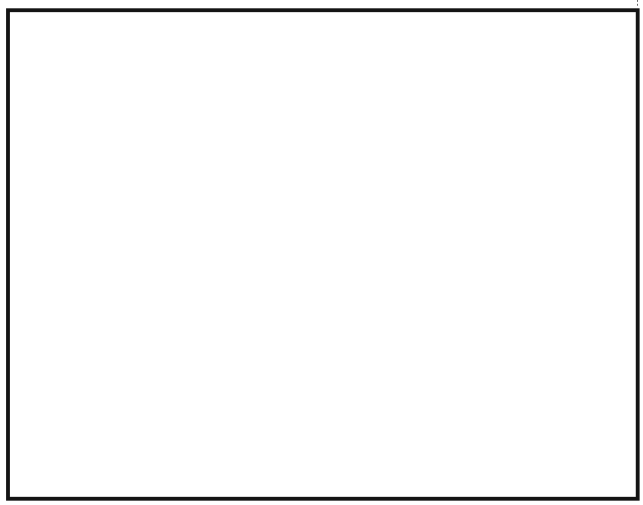
(U) While the AT&T undersea fiber trunk will use digital regenerators, the Japanese are now proposing a 5000-km undersea optical fiber cable with no regenerators, which will use linear optical amplifiers along the fiber. This will allow changes to the digital technology at the cable ends as technology improves. Experiments have already shown that power can be sent along light fibers to operate remote devices, so a completely optical system, with no electrical power or copper wire, should be feasible.

COST COMPARISON FOR UNDERSEA SYSTEMS

(U) Analysis by BTL has shown that, compared to the older 30MHz coaxial cable systems, the 274 Mbps optical fiber cable will give a 5-to-1 improvement in circuit costs. The very high bit rate will make special services such as video, video conferences, and data services feasible.

(U) While satellite technology will improve over the same time period, satellites are a stable technology, while optical fiber is still going through explosive growth in performance. The critical choke point in satellite communications is at the midocean points, where demand for spectrum and services is growing, while orbital and spectrum resources are fixed. The development of intersatellite links will relieve this problem to some extent, but in the long term the transoceanic capacity of optical fiber submarine cable--and its resistance to antisatellite weapons and electronic warfare--will make fiber the primary transoceanic medium. P.L. 86-36 EO 1.4.(c)

~~(S)~~ The impact on SIGINT of the development of transoceanic and overland optical fiber trunks is that traffic which now must go primarily by satellite will disappear onto fiber. The extreme publicity given to SIGINT over the past eight years by the revelations of World War II COMINT and by the excoriations of U.S. and British SIGINT agencies by governmental bodies, by journalists, by former employees, and by COMSEC and "communication protection" advocates, has made the telecommunication authorities highly conscious of satellite interception and microwave interception. Optical fiber will be a preferred transmission medium because it is so difficult to intercept.

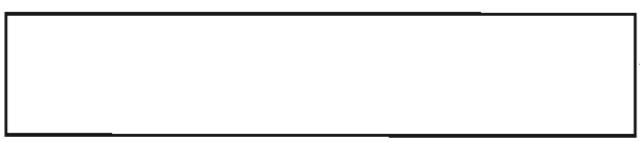


BIGFON: OPTICAL FIBER LOCAL LOOP

(U) A number of European countries are now experimenting with applications of optical fiber to the local network. The BIGFON network (see figure 23) will be tested in several German towns over the next few years, to determine how various subscriber services are used. An optical fiber pair with a capacity of hundreds of millions of bits will run from the local switch to the subscriber premises, and will carry various two-way services, including telephony, television, facsimile, data communication, telex/teletex, and stereo reception. At the local switch, selected channels of video, stereo, etc., will be connected to the individual loop. Current estimates are that a fiber pair can carry three TV signals and a variety of other services.

(U) Glass quality and cost are important considerations, since the total amount of glass fiber will be large, replacing the copper wire loops of current local nets. Optical fiber glass is made primarily by two processes, viz: the crucible method which gives a cheap and stable method of producing low-quality glass (10 dB attenuation/km), and the MCVD (multiple chemical vapor deposit) method which gives a very flexible technique for producing high quality but expensive glass (0.2 dB/km loss). Expert opinion (Midwinter) expects industrial techniques to produce a stable low-cost glass at about 1 dB/km which will allow fairly long local loops. The better glass would also allow economical higher bit rates.

~~(C)~~ The effect of low-cost optical fiber local networks would be twofold, viz., a much wider range of services, including videophone and conference nets with high grade voice security at 64 Kbps, would be available in the local nets, and the plant would be cheaper and more reliable than the conventional copper wire networks, leading to expansion of local (urban) telecommunications services in less affluent countries.



(U) One of the main attractions of optical fiber local nets from the point of view of the PTT's is that over the air broadcasting could be almost eliminated, and this would put all information flow completely under the control of the PTT's.

GLASS PURITY

(U) The driving factor in the development of optical fiber communications has been the improvements in glass purity. In 1966 the first article proposing monomode waveguide operation of glass fiber was published, but the glasses available at that time made the proposal appear absurd because the attenuation was too high for any useful system. However blocks of pure silica were found commercially available with losses as low as 10 dB/km, and this spurred enormous progress in glass chemistry.

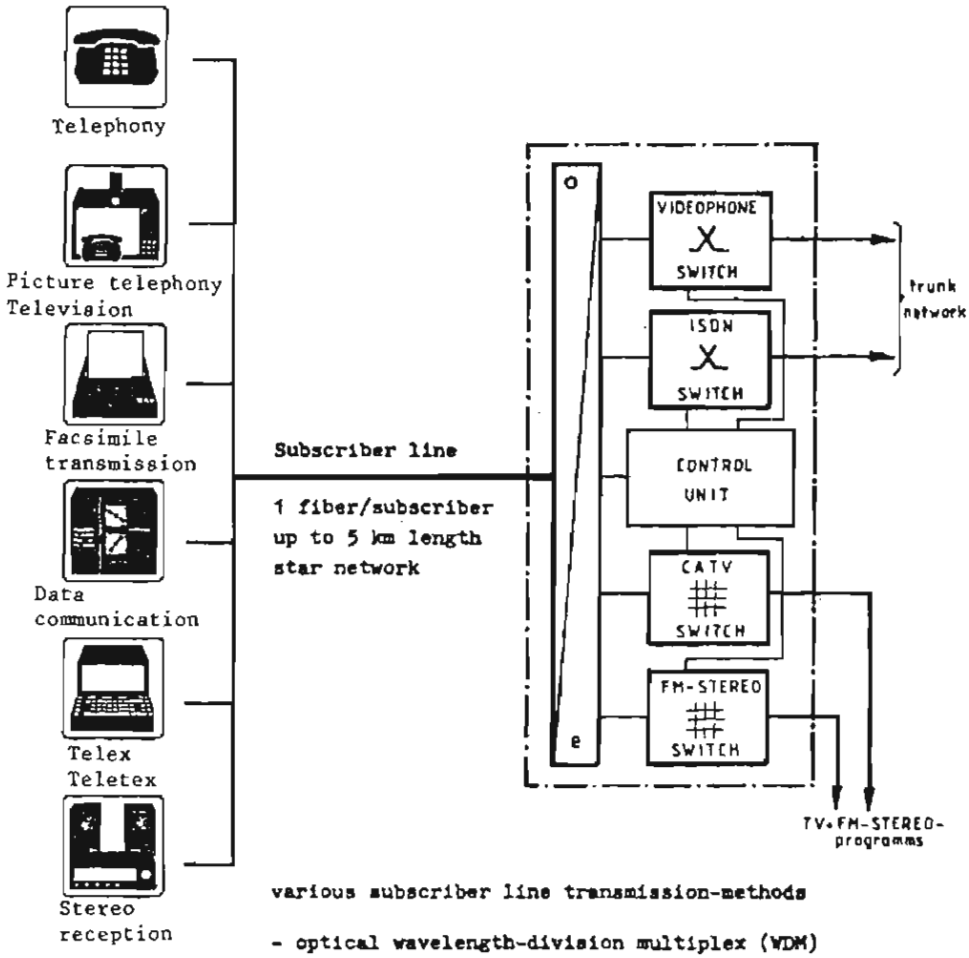
(U) The crude glasses of Egyptian times (3000 B.C.) had attenuation losses of 10 million dB/km, and over more than four millenia glass purity was gradually improved to the quality of Venetian glass of 1500 A.D. with losses of 10,000 dB. This represented a significant decline. Over the next 450 years, through the development of modern chemistry and industrial quality control, a further improvement was made to give the optical top quality glasses of 1970 with losses of 1000 dB per km. Then suddenly, in a decade of explosive development, completely new methods of purifying glass and drawing it into fibers were invented, with the result that a 10,000-dB improvement in glass attenuation was made in only ten years.

(U) The ratio of 10,000 dB corresponds to the number 10 raised to the power 1000, or a 1 followed by 1000 zeros, a truly phenomenal improvement.

(U) To visualize the effect of this improvement on optical communications, if all the power generating stations in the world converted all their power into light with perfect efficiency, and these many gigawatts of light were transmitted into a glass fiber with 1000 dB/km attenuation, then an observer one kilometer away would have to wait over a trillion years for the first photon to emerge. The glass fiber of course would be vaporized in an instant by the light absorption. By contrast, modern glass, at 0.2 dB/km loss, can transmit a few milliwatts of light 100 km without a repeater, at high bit rates over 100 Mbps.

BIGFON

broadband integrated optical fibre local telecommunications network



various subscriber line transmission-methods

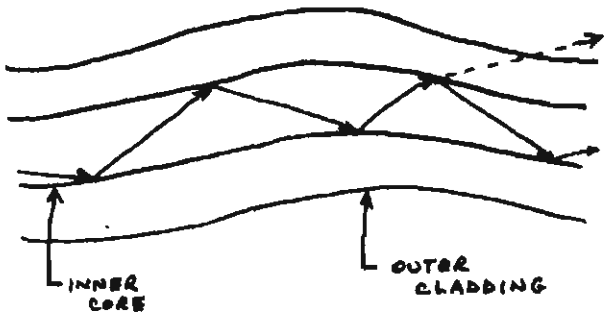
- optical wavelength-division multiplex (WDM)
- time-division multiplex (TDM)
- frequency-division multiplex (FDM)
- space-division multiplex (SDM)

Fig 23

ISS' 81 CIC Montréal 21-25 sept. 1981

(U) At the same time that the glass has been improved, the light transmitters and detectors have also been improved, especially in matters of lifetime and reliability. A few years ago the lasers and light emitting diodes had lifetimes measured in a few hours, but this has been improved to 100,000 hours, with further improvements to more than a million hours expected. Efficiency has also been improved so that very low power consumption will keep a long series of repeaters operating. This is important to submarine cables, where the repeaters are inaccessible.

(U) A comment about fiber manufacturing is in order because it implies certain limitations on SIGINT operations against different fibers. The manufacture of high-quality optical fiber is done primarily by two processes, viz., Modified Chemical Vapor Deposition (MCVD) and Vapor-phase Axial Deposition (VAD). Both MCVD and VAD produce a large glass rod that is subsequently drawn into very long fibers in a high-temperature furnace. A subtle chemical process known as thermopheresis is used to allow various chemical gases to penetrate into the hot glass while it is a tubular form turning on the lathe, and this process captures unwanted molecules and also deposits desired chemicals in a systematic way. The glass tube is then collapsed into a rod and drawn into a fiber. The lower-quality optical fiber is produced by a "double crucible" process in which a mixture of chemicals is put into two crucibles and melted, giving two kinds of glass of uniform composition but not as pure as MCVD yields. Glass from one crucible is allowed to gravity-feed into a thin fiber, and this is drawn through a gravity-formed tube of an outer glass, still in molten condition, to form coaxial fiber. The light travels in the inner fiber, and is reflected by the outer cladding.



24. MICROBENDING

(U) Because of the very high purity of the best glasses, the losses of light energy in propagation have been greatly reduced, but some losses still occur from a phenomenon known as "microbending," in which the light rays hit the interface between the inner and outer glass at a high enough angle so that some energy is transmitted into the outer cladding and escapes. The fibers are currently stored inside small-diameter plastic tubes so that they are not bent too sharply as the cables are laid around curves. The critical angle seems to be about six degrees. At higher angles of incidence microbending losses occur. In the design of the transmission systems, an allowance for such microbending losses is provided. The geometry of light propagation down a coaxial fiber is very complicated because of coupling between different propagation modes, so that the exact light path is unknown. In the graded-index fibers produced by the MCVD process, an axial focusing and defocusing of light takes place, but even that propagation is very difficult to describe. The result is that, in general, light energy is launched into one end of a lightguide and some of it emerges at the other, with random losses due to absorption, escape, etc.

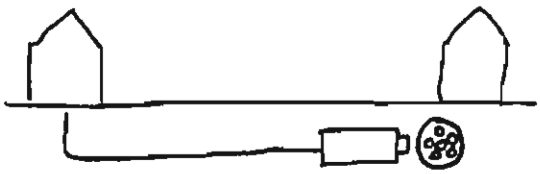
P.L. 86-36
EO 1.4.(c)

[redacted]

[redacted]

~~(S)~~ The central aim of optical-fiber SIGINT would be the concept of "proven reserves," derived from the petroleum and mining industries, rather than the current journalistic concept of hand to mouth immediate exploitation of whatever is easiest to get or fits current consumer requirements.

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



25. MOLE

[redacted]

[redacted]

[redacted]

systems, this after the fact access is not a workable scheme. If it took several years to get access to several fiber cables in an urban area, a crisis could come and go before any traffic could be collected.

~~(S)~~ The "proven reserve" concept does not only apply to interception, but to analytic and exploitation capabilities as well, so that the resources to attack and exploit systems should be developed and proved before there is a desperate need. Arguments that this is unaffordable should be evaluated by looking at the enormous success and wealth of the oil and mining companies, who do find this system affordable.

affects the entire SIGINT activity, rather than just hardening one problem at a time.

~~(S-CCO)~~ There is a historical precedent for this, in the World War II context, where the German traffic security, which at first thwarted Allied efforts at efficient collection, was solved for most of the war, and then at the end of 1944 became so secure that high-level cryptanalysis on the ENIGMA problem almost came to a halt because the traffic networks could no longer be identified or analyzed.

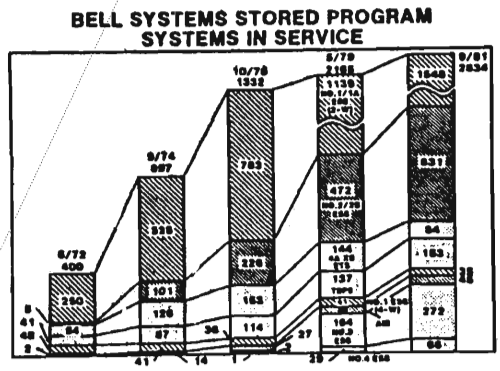
P.L. 86-36
EO 1.4.(c)

EVOLUTION OF EUROPEAN SWITCHING

(U) In the keynote papers at the International Switching Symposium in Montreal in 1981 (ISS 81), the rapid shift of the telecommunications plants of the Western nations from hard wired electromechanical switches to digital electronic switches was described. Although the old fashioned switches had been designed for a 30- to 50-year amortization, there is a growing trend to earlier replacement because the new switches are cheaper to operate and make more efficient use of the network. As a result, some 35 percent of subscriber loops will be connected to digital electronic switches by 1990, and 65 percent will be tied into the digital electronic switches by 2000.

~~(S)~~ As the new switches replace the old, the impact on SIGINT will be that the networks will become more flexible and efficient, and less rigid in the way traffic flows and in the services they provide. Some of the digital services, including those that use end-to-end encryption, will also have an impact on SIGINT.

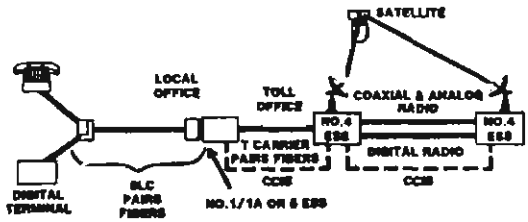
SWITCHING



26. BELL STORED PROGRAM CONTROL (SPC) SYSTEMS IN SERVICE

(U) In the U.S., the Bell System has also been very active in building and installing computer-controlled switches. Currently 47 percent of the local subscriber lines are covered by SPC switches, and the coverage in the Bell System by the early 1990's is expected to be 100 percent. There are now 2800 SPC systems in service.

(U) The SPC switches allow the network to provide new services, and also allow more efficient flow of traffic between switches.



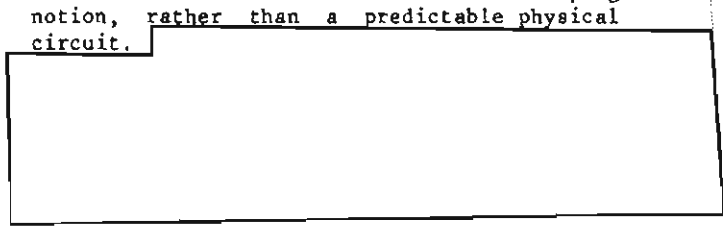
27. SWITCHED DIGITAL CAPABILITY

~~(S)~~ One of the significant changes in local services which the new switches will provide is high bit rate traffic over the subscriber loops. These high bit rates are made possible by the improvements in channel equalization and by sophisticated modems that can be implemented cheaply with the high density microelectronics. Some of the European nets are experimenting with 80 Kbps and 140 Kbps links, and the Bell System will offer 56,000 and 64,000 bps between the subscriber station and the local switch. Encrypted voice as well as facsimile and other data services will be available throughout the network where 1A ESS or No. 5 ESS switches are used. The Switched Digital Capability (SDC) will be introduced in 1984. For some subscribers, optical fiber will be used in the local loop. The 56,000 bps service will be end-to-end and will obviously provide high quality encrypted voice without the distortions that speech coders generate. This should lead to a rapid growth in encrypted voice for business traffic, with DES and Public Key interconnection between subscribers.

(U) Between the local switch and the toll switch, wireline or optical fibers will be used, under control of Common Channel Interoffice Signalling (CCIS). Coaxial cable, analog radio, digital radio, and satellite links will be used at the toll switches (No. 4 ESS), and CCIS signaling will be used where it is available. The CCIS information may flow over coaxial cable where the traffic itself flows over analog radio, digital radio, or satellite circuits.

~~(S)~~ The new Switched Digital Capability is an example of the new kinds of services which the digital electronic SPC switches will provide. In addition to the encrypted voice, encrypted high-speed (facsimile and electronic) mail and encrypted data services will flourish. Because the CCIS or other Common Channel Signalling will separate traffic addresses and routing from the traffic itself, the wideband transmission systems can be efficiently filled to capacity with a continuous stream of bits, or (in the case of analog radio links) successive talkspurts, without any indication of who the sender or recipient are. The toll switches are also capable of instantaneous automatic rerouting of traffic without any break in service, so that a given message or session may flow over various different channels. The effect is that the switches tend to act as transposition scramblers on relatively featureless and unidentifiable analog and digital traffic. The "dedicated" or leased channel will be a bookkeeping notion, rather than a predictable physical circuit.

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



Digital Switching
No.4 ESS

INTRODUCTION 1/16/76
• 67 offices now in service

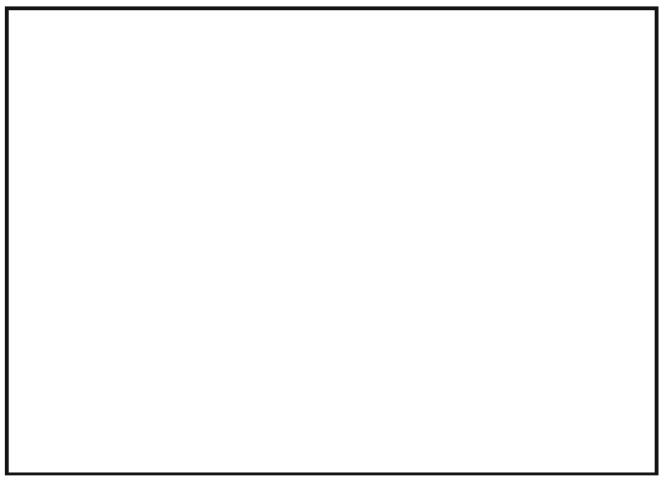
- **Characteristics**
  - **Time division switching network**
  - **Powerful central processor**
  - **New technology**
  - **Full duplication**
  - **Disciplined software methodology**
- **Features**
  - **Large capacity**
  - **Wide range of SPC network features**
  - **Extensive O.A. & M. features**

28. No. 4 ESS TECHNOLOGY

(U) At ISS 72, the No. 4 ESS created a sensation as a novel and ambitious functional and technological development. It was introduced into service in 1976 and 67 offices are now operating. However, the hardware technology of the switch has been completely replaced because of the technical superiority of newer microcircuits. No. 4 ESS uses time-division

switching in its internal logic, to give it very high resistance to "blocking" i.e., refusing a connection where a path actually exists in the switch.

(U) After the first shocking experience with switch software in the No. 1 ESS, the Bell System turned to disciplined software methodology, and now they can produce software which does not cause frequent switch outages. In spite of this, a new switch software product must "run in" for several hundred switch years before all the bugs are removed.



(U) The No. 5 ESS is a new local switch, designed to handle up to 100,000 lines, and designed to be used in rural areas. This switch applies time division switching to local nets. In contrast to the No. 4 ESS which is based on a powerful central processor, the No. 5 ESS architecture is based on distributed control. Powerful microprocessors are used in all of the peripheral modules, while the central processor performs more global control functions as well as overall administration and maintenance of the system.

(U) No. 5 uses modern software concepts, and all elements common to 512 lines are duplicated for reliability. An evolutionary plan has been set to provide a size range from very small to large offices of at least 100,000 lines with a large complement of customer, network, and administrative and maintenance features.

(U) The flexibility of the No. 5 ESS, and its production in various size ranges, is typical of the new developments in switching. The main producers of electronic switches are the French, Japanese, and L.M. Ericsson. The Swedish company produced a modularized AXE switch in the early 1970's, which in its original form routed signals in analog form, but was converted block by block to all digital operation. The first AXE switch was installed in Sweden in 1978, but has sold well abroad. Outside America there are only about 100 PTT customers for switches. The attraction of the AXE was that an analog network could be gradually converted to digital, and this technical lead enabled L.M. Ericsson to win the biggest telecom contract ever awarded, for a $5-billion Saudi telephone system. The conversion of existing analog networks over to digital operation, which involves the integrating of new switches into mixed analog and digital networks, is one of the most demanding problems in switch and network design.

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

ADVANCES IN TECHNOLOGY FOR ESS

- ■ VLSI
  - [] Microprocessors
  - [] Memory
  - [] Custom logic
- ■ Other Hardware
  - [] Optical fibers
  - [] High-voltage semiconductors
  - [] Display technology
- ■ Software
  - [] Architecture
  - [] Operating systems
  - [] High-level language
- ■ Development methodology
  - [] CAD
  - [] Program development support
  - [] Automated testing

(U) The switch designers have found it necessary to move into the forefront in development, manufacture, and application of the most modern hardware, design, and software technology. The network functions call for very complex logic, represented in VLSI hardware and software. Now the switch designers are converting software functions into "firmware" where the critical algorithms are designed in silicon from the start.

(U) Because of the high speed of modern

computers, various real-time telecommunications functions can be codified in higher level languages. Software has become a major part of switch and telecom plant production. At Bell Telephone Laboratories in 1950 no software was produced. Now half the staff works at software production. The advanced programming techniques enable software production at 100 times the rate of 15 years ago. The testing and debugging, and particularly the reliability of modern telecom software is a major technical factor. The other side of this coin is that once the software is designed and tested, it is very hard to change, because hundreds or even thousands of switches and transmission systems are made interdependent and interconnected by the software. Hence, even if the hardware is replaced, and parts of the software are codified into "firmware," the basic software system will probably have a long operational life. The software programs are often very large, running into hundreds of thousands of lines of code, and the developers are frequently protective of their "source level" program scripts.

[redacted]

[redacted]

[redacted]

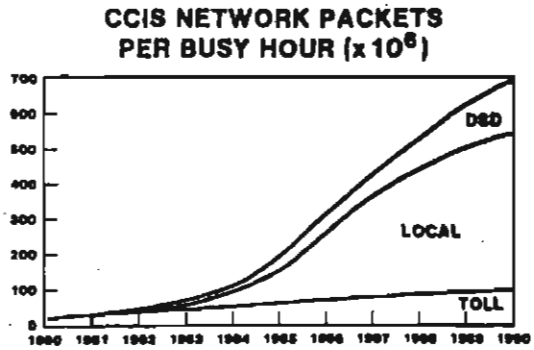
COMMON CHANNEL SIGNALLING

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

(U) In Common Channel Signalling the addressing information used to specify the call and the routing is not sent as a prefix on an idle channel. Instead, a separate dedicated channel is used to carry all the addressing and routing and signaling data. The result is that the transmission facilities are used more efficiently because idle channels do not have to be held open for some minutes while successive channels are found, and then until a called party finally picks up the telephone. On long distance calls, signaling and call setup used to take about half the channel time. The application of common channel signaling allows network efficiency to be practically doubled without building new plant.

(U) Three major systems are No. 6 CCITT, No. 7 CCITT and the Bell System CCIS Common Channel Interoffice Signalling.

[redacted]

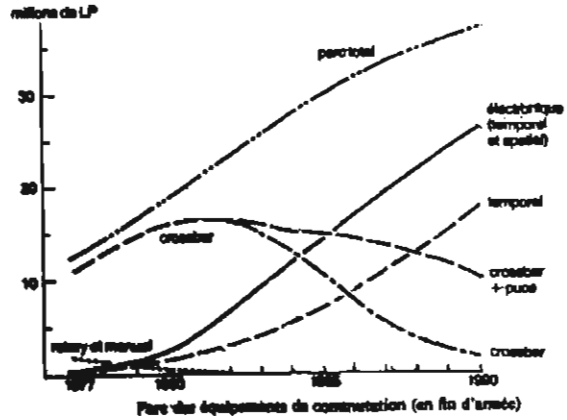


30. CCIS NETWORK PACKET TRAFFIC FORECAST

(U) In the Bell System, Common Channel Signalling is already in use between some switches and a packet network is employed to transmit the switching data. Currently some 20 million packets are sent during a peak hour. By 1990 the packet traffic rate for CCIS will rise to 700 million packets per hour. The dedicated CCIS packet network operates to set up the circuits switched network that will actually carry the traffic.

(U) While the new digital switches can be designed to implement common channel signaling, the older electromechanical switches, e.g., crossbar, are designed around a control system that uses in-channel prefix signaling. The French have developed an innovation for this problem called PUCE, which will retrofit an SPC computer into existing crossbar switches so that the crossbars can be controlled by common channel signaling. This will enable the entire French switched network to be operated by common channel signaling. The PUCE retrofit will allow the existing switches and transmission facilities to be operated more efficiently, without the expense of replacing the existing large investment in electromechanical equipment. This will also prolong the life of the crossbar plant. A plan published by CNET shows the effect of PUCE in extending the life of crossbar switches.

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



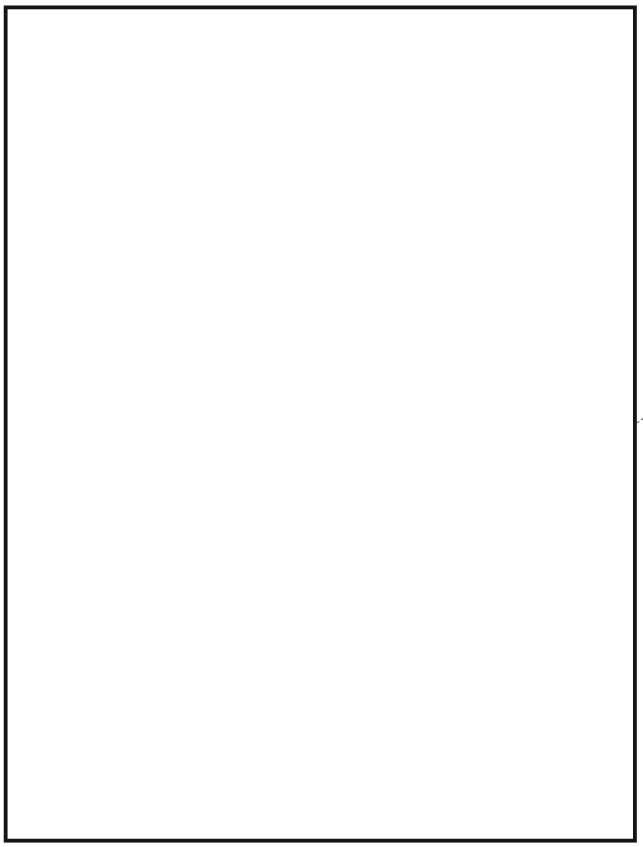
31. FRENCH SWITCHING EQUIPMENT ASSETS

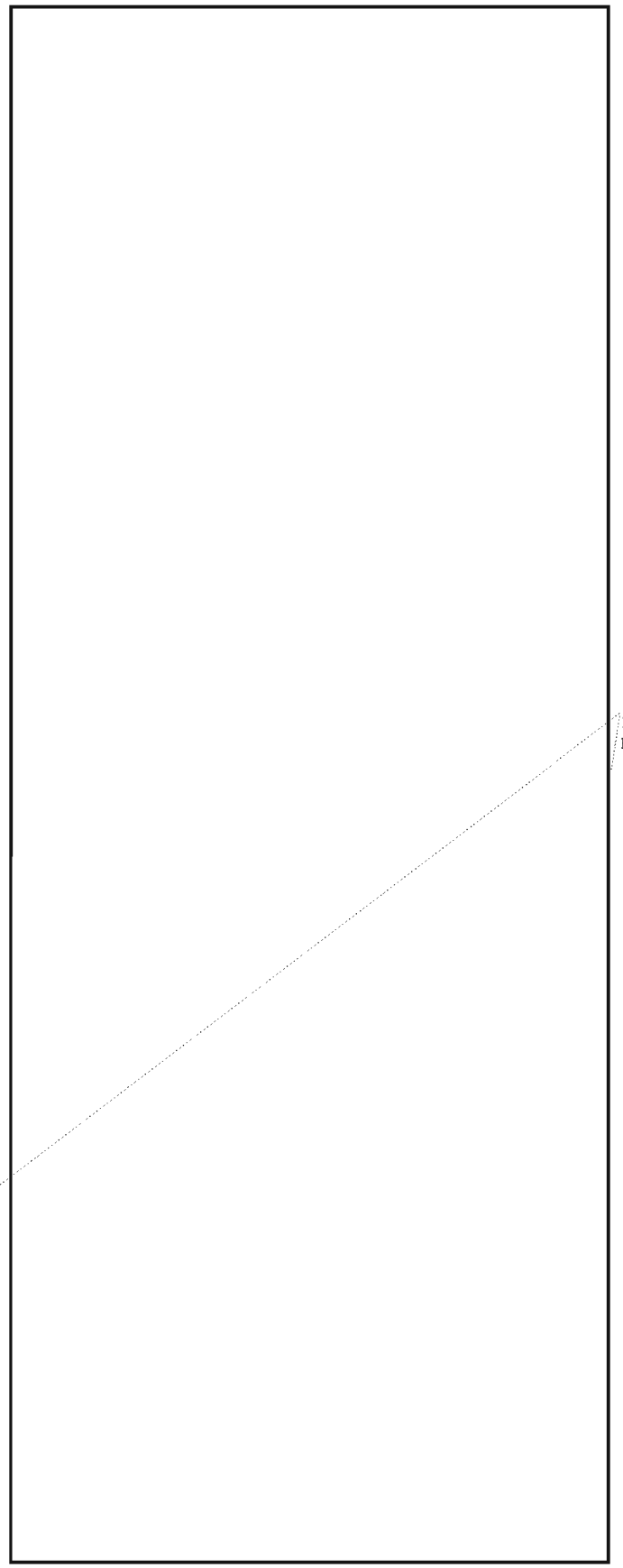
(U) The major growth will be in time-division electronic switches (temporel), with rotary and manual phaseout by 1983, and ordinary crossbar dwindling after 1984. The crossbar with the PUCE retrofit will remain at a fairly steady level up to 1990, presumably as a result of converting the ordinary crossbars.

(U) Summing up the switching trends, time-division has the greatest growth potential, and the wide use of time-division digital switches will reduce switching from 50 percent to 20 percent of total plant value, but many

years will pass before most countries can afford this. On the other hand, the low cost and high reliability of microprocessors and computers will make it increasingly attractive for PTT's to seek cheap retrofits and hybrid systems which will give more efficient operation and more or newer services, without the expense of replacing still serviceable equipment.

(U) In most poor countries, the problems of maintaining outside plant will be as significant a factor as shortage of money in retarding the successful introduction of digital electronic switches; defects and noise in the outside plant (subscriber loops and trunk transmission) cause errors that can disable the more critical digital technology. Another key factor in the introduction of digital switches in any country is the distribution of timing standards, because close synchronization through the networks is needed. This is already a problem in the U.S. where different suppliers provide equipment to hundreds of "independent" operating companies. Once a small country starts to introduce digital switches, the difficulties of time distribution and digital interface will cause special problems for any rival manufacturer who wants to sell in that market.





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

~~SECRET SPOKE~~

ANSWER: An Old Problem (U)
(CRYPTOLOG, August 1982)

When you finish, send up a flare!

Not
Secret
Anymore

P.L. 86-36

(U) May I add a few words to [redacted] reminiscences in the August 1982 Cryptolog, especially to his comments about the initials NSA standing for "Not Secret Anymore"? Like Brother [redacted] I recall those days of "M&M" (as we lovingly called Martin & Mitchell) and I also remember figuring out that expansion for myself, but I doubt if I was the only employee to come up with the clever meaning for "NSA."

(U) I remember including a cartoon in my book NonseNSA, showing President Eisenhower denying everything that M&M had said, ending up with, "and there is no such agency as NSA at Fort Meade, Maryland. In fact, there is no such place as Fort Meade, Maryland!" and scribbling on the bottom of the page "NSA now stands for 'Not Secret Anymore!'" Unfortunately, I loaned NonseNSA to [redacted] who used 2 or 3 cartoons from it in early issues of Cryptologic Spectrum and then retired without returning it to me, so I don't know if the book is still in existence.

(U) But at least I'm glad to see that somebody else used "Not Secret Anymore" since my other great discovery about what an agency's initials meant seems to have been restricted to me alone. When President Reagan appointed William J. Casey to be the head of CIA and then got our Admiral Inman to be his deputy, I remarked on several occasions that the CIA was "the Casey-Inman Agency" (which I thought was pretty clever--in fact, I was tempted to send it in to "The Ear" at The Washington Star--but to date I've never heard or seen it used by anyone but little ol' me...and now that Admiral Inman has left, I doubt if I ever will).

[redacted] P16

P.L. 86-36

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

~~SECRET SPOKE~~

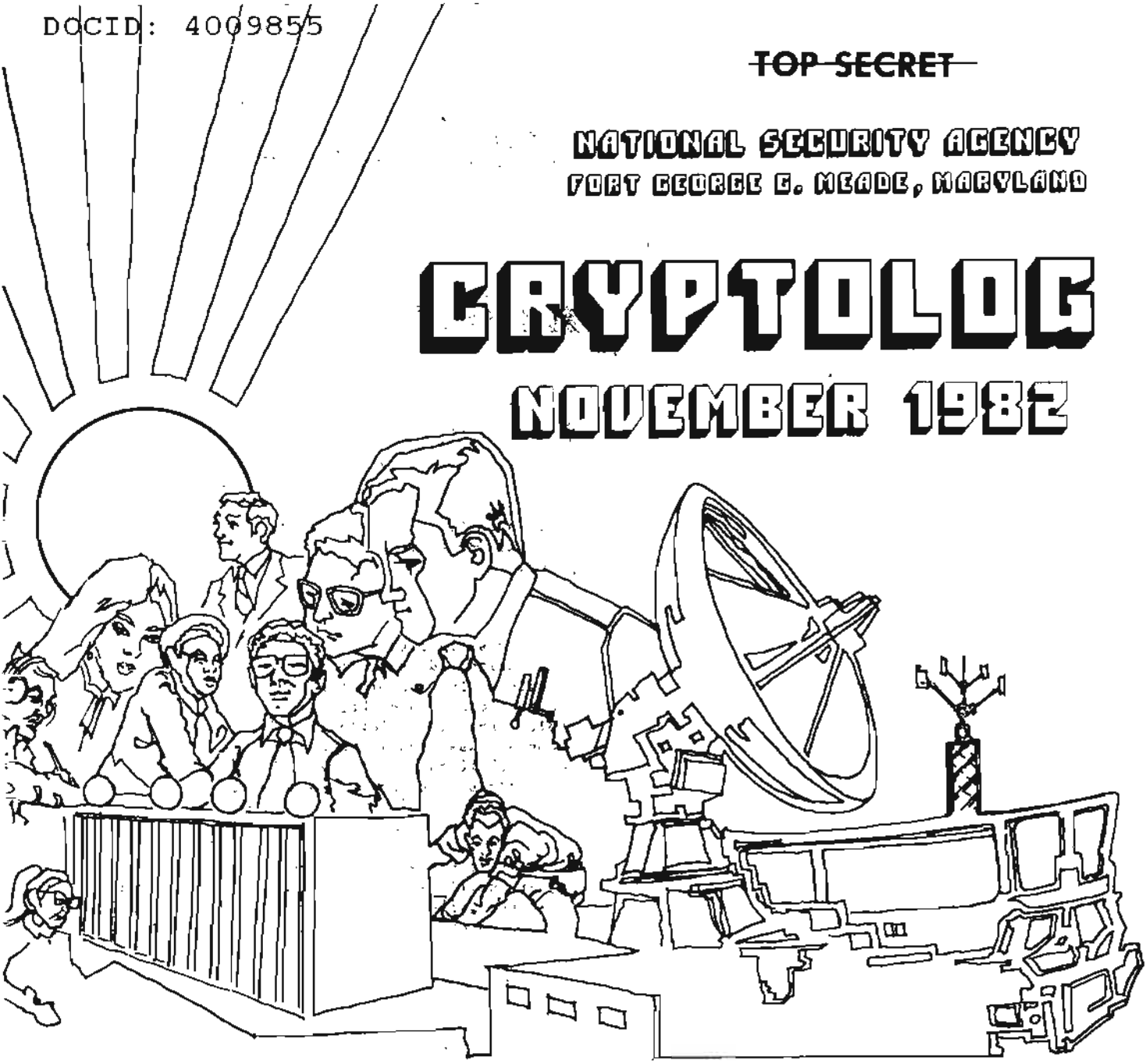
P1-Oct 82-SJ-21537

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1982



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Not Releasable to Contractors~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

SIGINT: 1990 (U)
PART 3

by [redacted] P13

P.L. 86-36

COMPUTER COMMUNICATIONS SYSTEMS

~~(S-CCO)~~ As computers become more tightly integrated into telecom nets, the central problems facing SIGINT will become what to target and how. The most useful data, from an intelligence or a SIGINT viewpoint, may be resident in the system in a computer memory, rather than passing over a communication channel. SIGINT, instead of waiting for data to be transmitted and then passively collecting and exploiting them, will have to penetrate into the nets, find what is there, and extract it.

~~(S-CCO)~~ Several points, which are obvious truisms, must be borne in mind. It is fairly easy and cheap nowadays to make a link secure. This is the COMSEC function, now virtually solved. On the other hand, it is very hard to secure a whole network against every possible attack. This is the NETSEC problem, and part of the NETSEC, viz., computer security, is actually operating as a separate organization inside NSA because it is a different problem.

~~(S-CCO)~~ Although the security role of NSA is extending from protecting channels to protecting nets, the analytic role still seems trapped in the passive posture of intercepting links rather than penetrating nets. By 1990 this will not be a viable SIGINT position.

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in the third of several monthly installments, from his presentation at a January 1982 session of CA-305.

This is one of the choices that must be faced and acted on.

[redacted]

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

~~(S-CCO)~~ The two major effects of having computers integrated into the telecom nets are logic and storage. The computers can provide services which are logically complicated, compared with old-fashioned manned message centers which were fully burdened just to receive and pass on messages. The modern storage systems can provide economical central repositories of data. Because of economics it is still not feasible to provide immense storage capacity at the subscriber outstation, because big memories cost far more than telephones. The effect of centralizing on-line memories around computer systems leads to a lot of man-machine and machine-machine data transfers. The total amount of storage capacity that is coming into the networks as on-line memory is quite significant, and currently sums to about 1 quadrillion bytes of data which can be automatically accessed by remote requests. By 1990 over 100 quadrillion bytes of online storage are expected worldwide, under various access controls. The SIGINT task is to penetrate into this on-line storage, find out what is accessible, and extract the useful data.

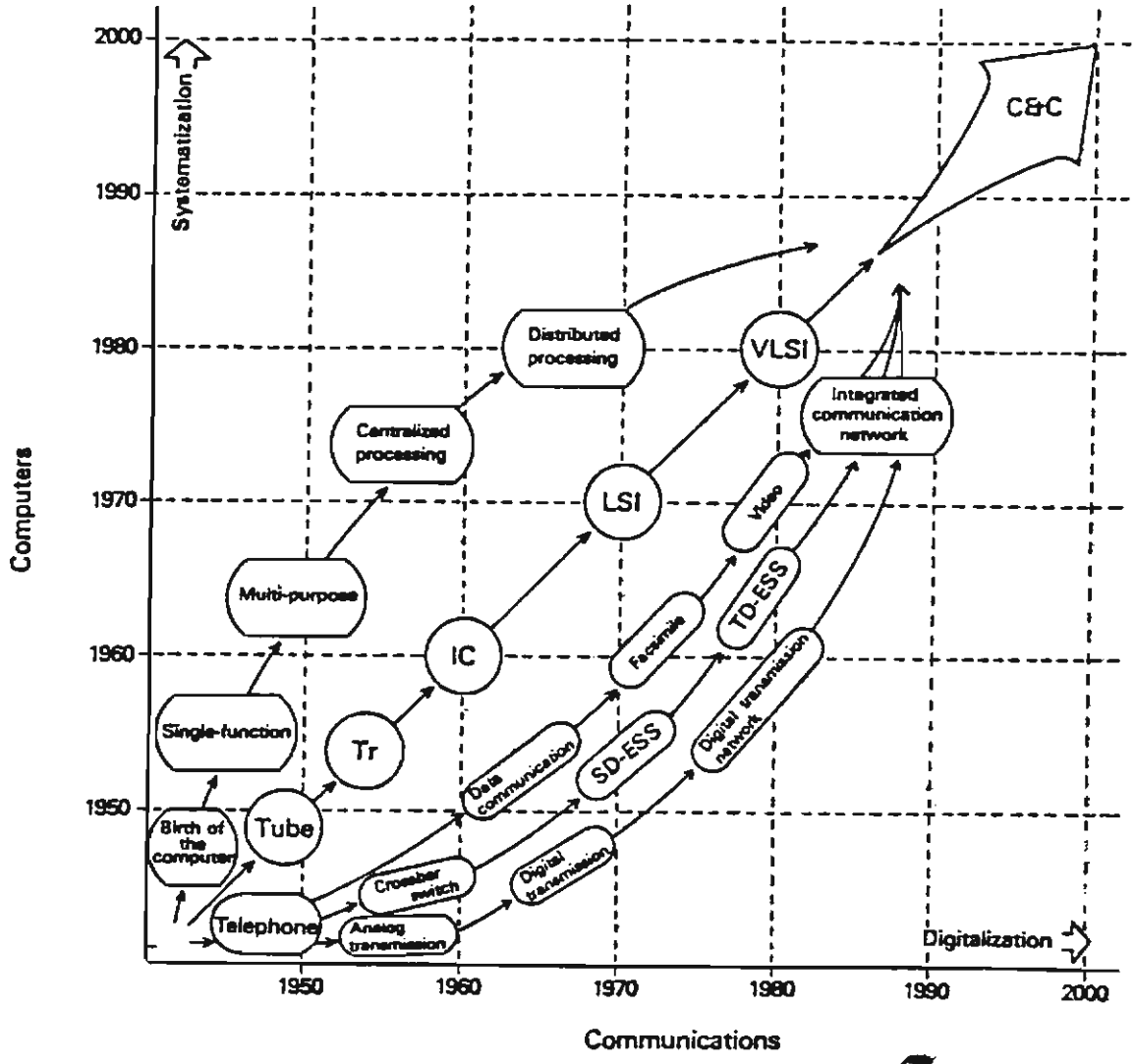
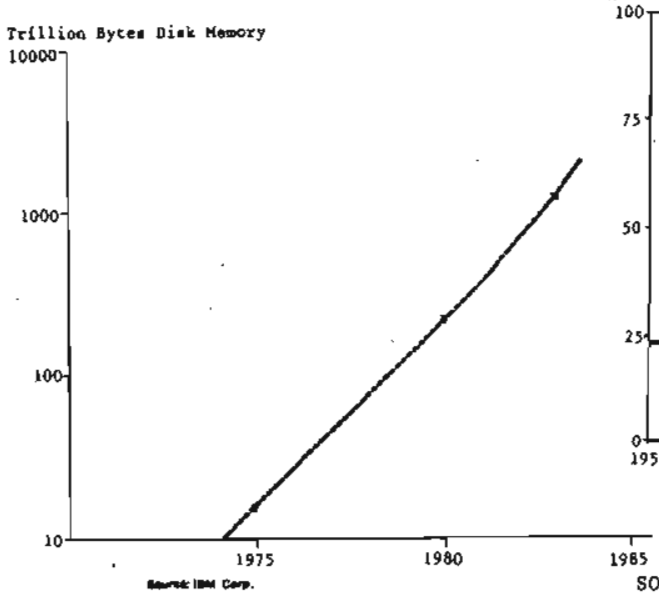


Fig. 32

PERSPECTIVE OF "C & C"



WORLDWIDE GROWTH OF
ONLINE COMPUTER STORAGE (Fig 33)

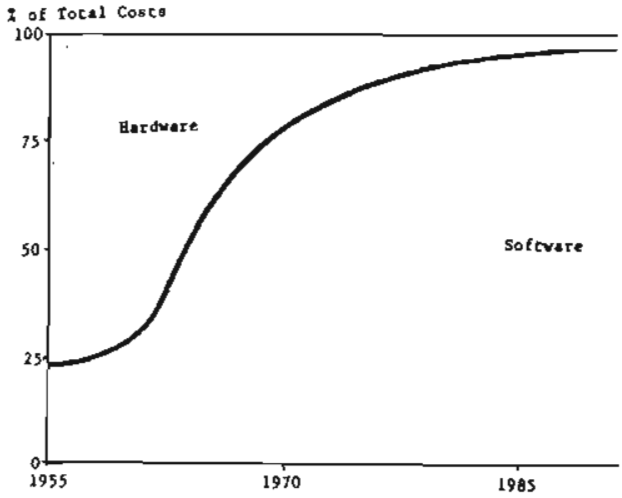
(U) Two unavoidable consequences of all this storage capacity are that:

[] first, information flow (not mere traffic flow) through the networks becomes very complicated, because data files may be located at dozens of different points as identical or slightly altered sets, and

[] second, the users are forced to think about and rely on the storage and the stored data.

(U) While a user can interact with a memoryless telecom system, e.g., a telephone net, through a mechanical terminal (telephone, teletype, facsimile), once the network has memory, especially on-line storage, the user needs elaborate protocols, embodied in software or firmware, to interpret what he wants to do into command sequences that the network can execute.

(U) The result is that in a C&C net the bulk of the investment shifts from the central switch and outside plant, which connects $10 telephones, to a huge investment in software and "intelligent" terminals which perform many different functions for the network users. Typically, 90 percent of the customer's investment is in the terminal, and the aggregate cost of producing software or firmware that the customers will purchase becomes the dominant factor in system cost and success.



SOFTWARE COSTS FOR SYSTEM DEVELOPERS (Fig 34)

(U) The performance requirements for the terminal software are not all trivial, because banking and financial services will be supplied more and more through terminals which not only give access to cash, but to many other banking services, from private or public locations. The software, firmware, and cryptography needed to assure reliable functioning will be critical.

(U) As an example, the major U.S. banks will soon be offering interstate banking services via terminals, and extension to international services is only a matter of time. Hence, critical economic information, generated by network terminals, will flow through public C&C networks, replacing much of the mail and conventional financial, shopping, and business activities.

~~(S-CCO)~~ As circuit technology has improved, software development has become the dominant factor in system cost and delivery (and performance). This software development burden will have the effect of "freezing" the network services to a considerable degree, even if the hardware is easily replaced, because of the "learning cost" that the users have to pay to get access to the system. At the same time, the burden of producing software will tend to freeze SIGINT methods, for the same reasons.

[redacted]

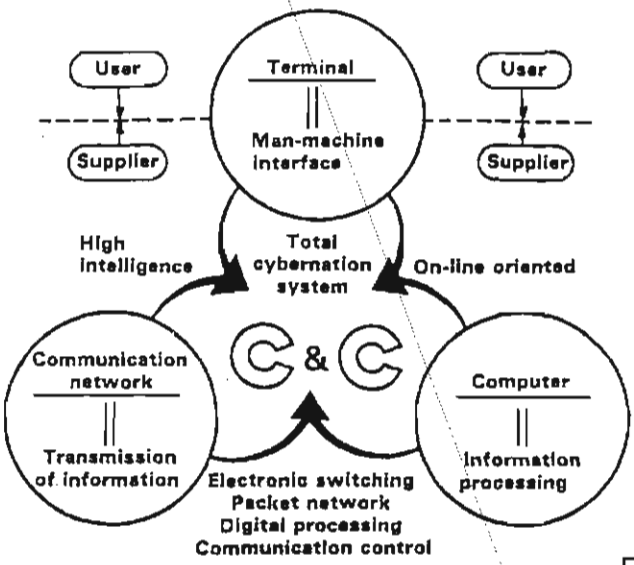


IMAGE OF C&C INTERACTION (Fig 35)

(U) A C&C network consists of a number of components, viz., computers, on-line storage, telecom circuits, switching, software, data bases, terminals, users, and projects or activities that use the C&C net.

(U) Over the next ten years the main effort in the industrial nations will be to establish the IDN (integrated digital network) as an operating entity. The object of IDN is digitalization of the local network and terminals in the form of a 4-wire digital circuit. When this is achieved, many new services can be provided, leading to the ISDN (Integrated Services Digital Network) based on 64-Kbps circuits all through the network. This will allow the C&C terminals to provide point-to-point switched encrypted voice, data, and facsimile with many data base services, and interface into other message services, such as Telex, Teletex, etc.

~~(TS-CCO)~~ The deliberate deregulation of the U.S. telecom market and the increasing role of computers and software and microprocessor terminals will tend to force experimentation and innovation onto the PTT's in both industrial and Third World countries, as powerful customers demand the procurement and introduction of useful and sophisticated new services, such as domsats, POS terminals, E-Mail, electronic banking, etc. A major advantage that U.S. suppliers have in C&C competition is the highly knowledgeable customer base that demands everything the technology can supply. The increasing internationalization of U.S. business will inevitably hurry the spread and export of the advanced C&C services and technology into all areas of the world where those companies operate. Many sophisticated foreign business C&C nets will be SIGINT targets, wherever they extend, and therefore the current backward state of a poor country's telecom plant is not a guarantee that they will not superimpose the most advanced C&C nets on top of the local plant, in the same way that inefficient subsidized jet airlines are superimposed as status symbols over oxcart economies.

COMPLEXITY OF TELECOMMUNICATIONS

(U) A century ago telecommunications consisted of Morse telegraphy. In the latter part of the 19th century telephony was added, after some initial resistance by the Post and Telegraph authorities. At the turn of the century coastal radio telegraphy was introduced and gradually brought into the network of services, although for some years the British Post Office, for example, would not allow the Marconi stations to have telephone or telegraph lines, since radio threatened their monopoly.

(U) Gradually new services were added, many based on radio, to take care of special needs such as safety services, mobile radio, marine and aircraft traffic, air traffic control, amateur, radar, broadcasting, TV transmission, facsimile, and so on.

(U) Now the capabilities of digital networks, with computers to carry out the details of providing user interface and networks access, have encouraged many new notions about what telecommunications are, and what role they should play in a modern nation.

(U) The French CNET study for the year 2000 has formulated a large number of new services which can be integrated into the future networks. A table of 64 new services has been published in the study.

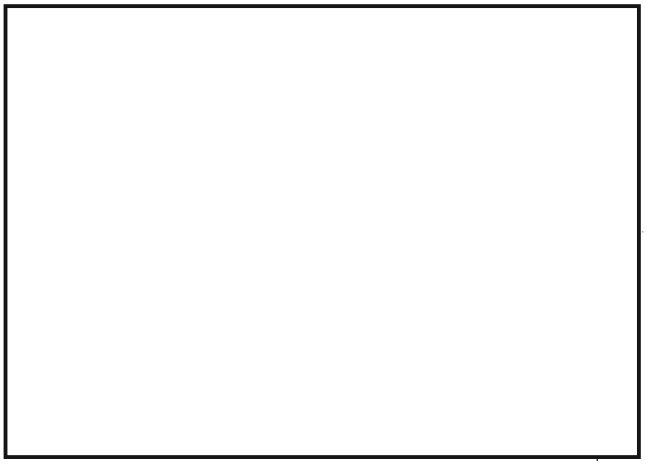
Telecommunications by 2000 — Some services for the year 2000

Fig. 36 - 64 additional new services

TELE-ENERGY Monitoring & control of energy consumption	EUROPHONE Handset H/T on a Europe-wide level	UNIVERSAL IDENT BADGE An electronic passkey (also see below)	TELEFINGERPRINT Enter without knocking, thanks to voice recognition	TELEWORK Shiftwork in your home (Cf. HOUSEWORK)	TELELIBRARY Look at books, documents, newspapers, etc.	TELECONFERENCE Color, hi-fi, graphics, on a Europewide level	TELEMAIL Telecopying of the future
2-1/2D IMAGES For those who want to change their point of view	TELEHELP Pinpointing of dangerous situations	TELECONTROL Location of individuals	TELEDESIGN The Office of R&D in era of TV automation	"SLY BISON" Videotex version that can be used in a car	WEATHERCULTURE Weather forecasting in the service of agriculture	TELEFILING To save paper ...& space. (Cf. TELELIBRARY)	TELECHECKING Electronic pay cards
TELEANALYSIS Detection of pollution & toxic products	VOICE PLACEMENT OF ORDERS No more dialing; forget the keyboard!	TELEDIAGNOSTIC In case the electronic housekeeper breaks down	TELESIMULTANEOUS TRANSLATION For better understanding between people	HOUSEWORK With videomatic assistance (Cf. TELEWORK)	TELEHEALTH Computerized preventive medicine	TELESURVEILLANCE Videosurveillance for various purposes: family, social, business ...	TELEWARNING National net for detecting & warning about disasters
3D TELEMOLDING 3-dimensional facsimile	TELEANIMATION A companion, a babysitter, the life of the party	QUICK CALLS A guarantee of short duration	TELECOMPUTERS All the computers in the world want to lend you a hand	TELEVILLAGE A real estate office	IGB or IMB Individual Genetic (or Medical) Badge	TELEINFORMATION TELEADVICE Starting with data banks or a group of experts	TELETEACHING Education marches on
TELECLEANING Automatic housecleaning w/centralized supervision	TELESEARCH For doing research & paging people	TELEJUKEBOX Songs & music on the phone, w/a TELE/HI-FI version	TELESCRIPTING For the handicapped, converts the written word to Braille	TELETAXI Automated location of vehicles	TELEWEATHER A real-time service	AUTOMATIC RECALL There's this phone number that you've called (over & over)	AUTOMATIC FILTERING Freedom from the telephone
TELEDECORATING A new kinetic & musical art in your home	TELEMAINTENANCE Remote repairs. System connected to TELEDIAGNOSTIC	TELEVOTING Electronic democracy	TELEAVAILABILITY To be called or recalled when wanted	TELESTOCKMARKET Automated trading & data (Cf. TELEWANT ADS & TELESWAP)	TELEPROGRAMS Bidding on TV programs	TELEWANT ADS Videotex want ads (Cf. TELESTOCKMARKET & TELESWAP)	TELERESERVATION For shows, hotels, travel, w/automatic payment
TELECOUPLE Marriage by TV technology. A form of Computer-Assisted Design	TELEOPTIMIZING It will solve all your problems	TELEPOLLING See the box above	TELESOFTWARE To plug your pocket calculator into the network	TELEPRICE LIST for HCRPS Wholesalers National Computerized Retail Price Service	TELEFORUM Meetings & debates over the phone	TELESWAP A second-hand store in connection with TELEWANT ADS	TEACHING TERMINAL You'll learn how to use all the other terminals
TELEGAMES Interactive video games for one or more persons	TELECOMMAND A generalization of the automatic wake-up call	INTERNETWORK Don't send anything but flowers...	TELEFLEA MARKET A teleautomated second-hand shop, employment agency, etc.	TOM-TOM Your dialing time shortened, using a card	AUTOMATIC PCV Just what its name says (PCV = Reverse the charges)	TELESHOPPING Videodiscatalogue & automatic shopping by phone	TELEAUTOMAT Away from all those fareway counters

CNET: NEW TELECOMMUNICATIONS SERVICES IN 2000 (Fig 36)

(U) This tabulation expresses the significant increase in the complexity of future telecommunications. Even marriage by telecommunications (see TELECOUPLE) is included in the plan. There is so far no mention of telenuptials. The different services interact to some extent. Some teleservices will be forced onto the user, e.g., by the banks eliminating paper checks, or by the existing French plan to eliminate the telephone books throughout France in favor of small text terminals which a telephone subscriber will use to request directory service. As the teleservices extend farther through the society and economy, the PTT's will have a much greater policy role in determining what transactions will occur in a nation. The recent telephone cutoff in Poland and in the USSR, to enforce government control, illustrates the importance attached to controlling teleservices.



~~(C-CCO)~~ SIGINT is familiar with the conventional point-to-point communications and with point-to-mass (broadcast) nets, but computers now make mass-to-point nets feasible, which collect data or serve a star net of subscribers.

(U) Different parts of the networks will grow at different rates; e.g., in Japan computer production has grown at 20 percent, while video tape recorder and robot production have grown at almost 50 percent. Facsimile, word processing and other office information equipment have grown at 40 percent.

(U) Both government and business, through teleservices, will be able to reach out through the telecom nets and extend an interactive environment over time and distance. The teleservices may extend from the exercise of police or taxing power to the marketing of luxuries. Ownership of the teleservices will be important, just as ownership of the telecom plant also confers power. As competitive nets, offering similar teleservices, extend further, there will be greater emphasis on controlling the flow of information within and between nets. Encryption will be only one of the means used to control or regulate access and flow.

(U) Although the French model projects the future in terms of different services, a rather different view of current telecommunications and media was presented in recent Congressional hearings about competition in the communications industry.

THE MEDIA BUSINESS, 1981 (Fig 37)

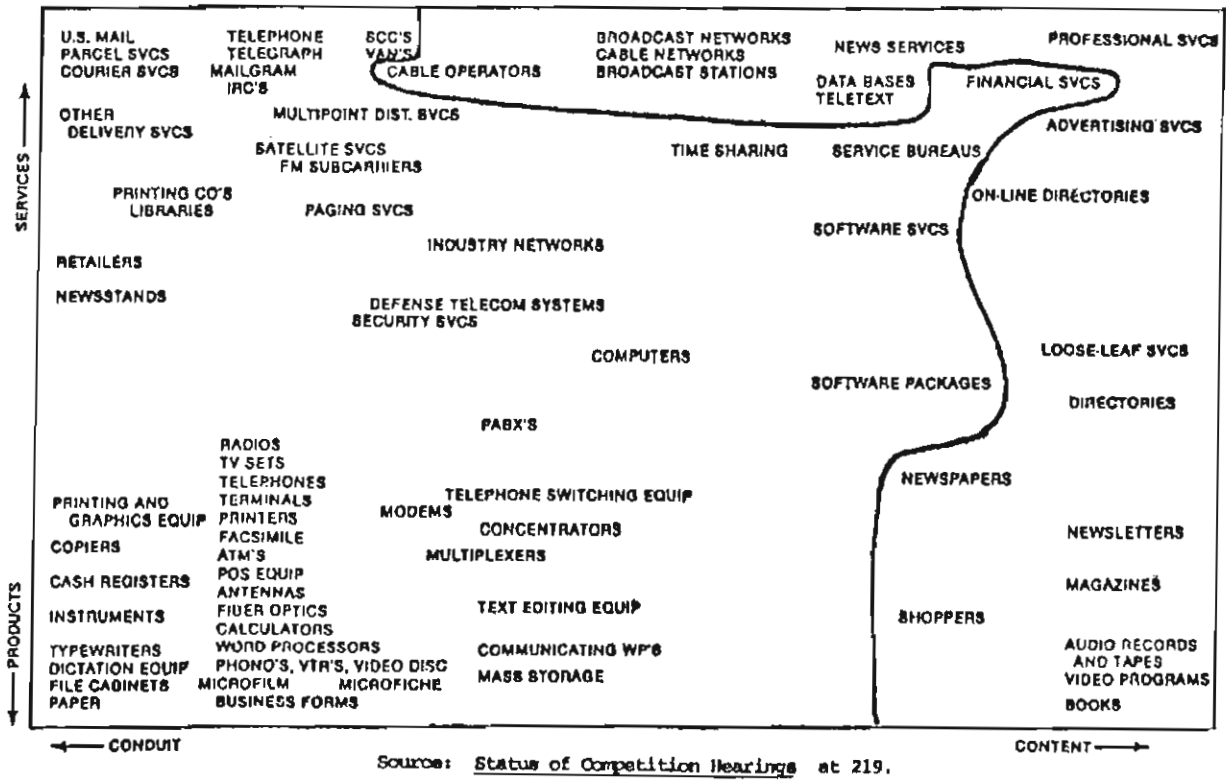
(U) The tabulation in the hearing record, which was adapted from a Harvard study, roughly segregated the broadcast services from the various means of delivering information. The resulting somewhat crowded and inscrutable chart is a testament to the difficulty of describing the conglomerate of products, services, channels and content that constitute modern communications.

~~(S-CCO)~~ This variety and complexity would not matter directly to SIGINT were it not for the fact that as the new networks become more efficient, it will become a matter of economic necessity to supply the products and services by electronic means. The development of E-Mail, to compensate for the cost and delay of postal services, and the corresponding development of robots to answer phone calls, place calls, and telemeter building conditions--because of high labor costs, lack of servants, and a consumer market for such "personal" services--is a further illustration of the increasing use of electronics and telecoms to perform social and economic functions.

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

~~(S-CCO)~~ The "mining" of some of the teleservice transactions would be comparable to the vast diamond recovery operations off the coast of South Africa, where a bulldozers continuously work to push a sand dike farther out to sea, while huge machines dig up the exposed seafloor and screen alluvial diamonds.

THE MEDIA BUSINESSES, 1981 Fig. 37



Source: Status of Competition Hearings at 219.

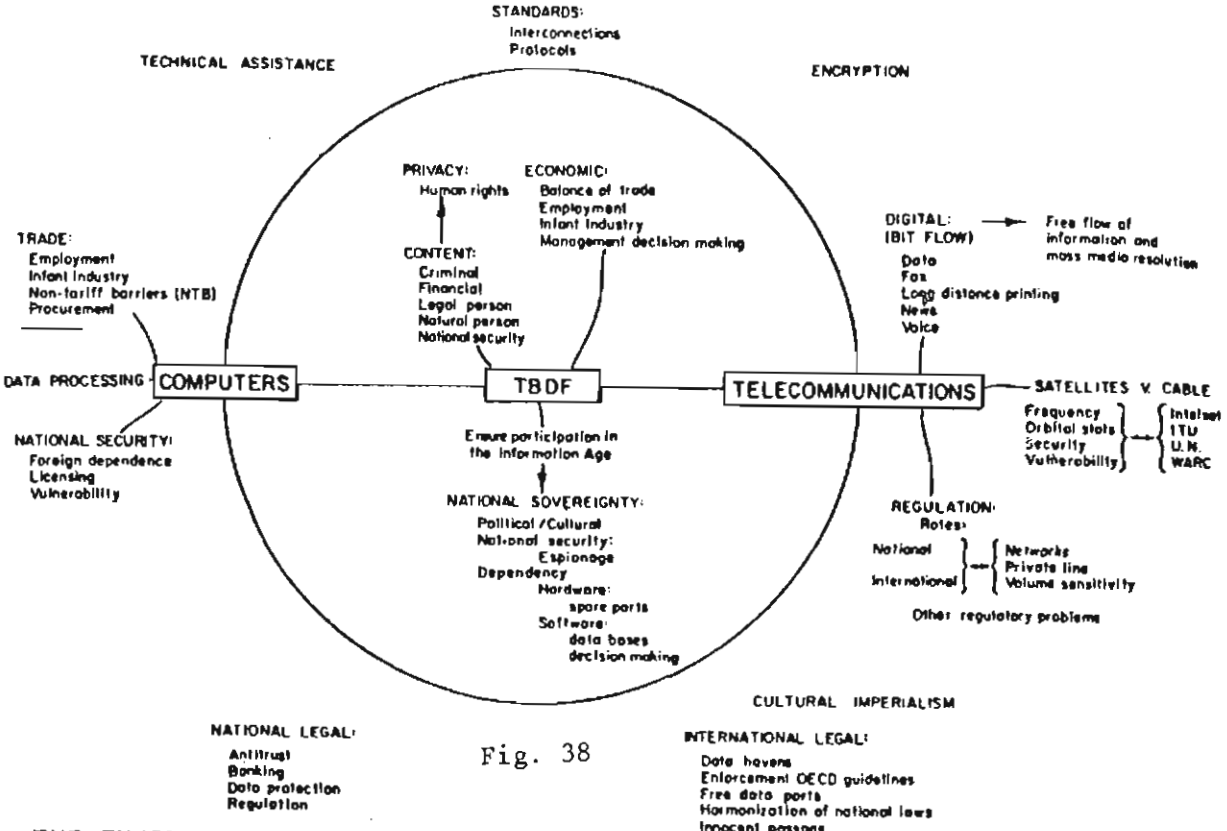


Fig. 38

THE ENVIRONMENT OF TRANSBORDER DATA FLOW

The ratio of sand moved to diamonds extracted is about 130 million to one. While some SIGINT will continue to operate against high grade teleservices such as dedicated military and diplomatic cipher links, other SIGINT will have to work the huge mass of low grade transactions, which may be coded or encrypted in a way that conceals their lack of value.

~~(C)~~ Put in different words, the teleservices will represent the actual policies of a nation, just as transactions and teleservices within a small computer net embody the net policies. In the course of analyzing the complex networks and teleservice repertoires, SIGINT will inevitably discover just what the social, economic and, in many cases, security policies of the target nation are. As policies change, teleservices will change with them, just as the U.S. imposed peacetime censorship on international radio and cable services in 1914, and many countries impose such censorship on various internal and transborder telecom services and transactions during wars and crises nowadays.

~~(C)~~ One elementary example of the significance of teleservices and transactions in defining policy and status is the power currently possessed by computer network managers to access and change passwords, access and rename and move files, change access codes, and monitor or alter the actual usage of network facilities, and even to take the network down or change the operating systems gradually or totally without much reference to the users or even to the owners of the nets. Their "privileged" terminals, plus far-reaching power to change and tamper and inspect, and to deny access or shut down, shows how teleservices define policy and power. In future, the power of the network managers will be a key index of where actual power in a target system is concentrated--always an interesting fact.

~~(S-CCO)~~ In capsule form, teleservices are the image of policy. Teletraffic is the image of operations defined by policy. SIGINT is the insight channel.

~~(S-CCO)~~ One of the most vivid illustrations of the complex intertwining of telecommunications and social policy is the issue of transborder data flow.

ENVIRONMENT OF TRANSBORDER DATA FLOW (Fig 38)

~~(S-CCO)~~ A Harvard study represented the TBDF (transborder data flow) problem in a semi-inscrutable diagram, with "encryption" apparently floating freely as an environmental factor. In fact, encryption will be one of the major issues in TBDF.

~~(S-CCO)~~ TBDF began as an endeavor in Europe to protect certain personal data which in several countries is protected by law from exploitation in bordering nations. This privacy interest gave it political power, and the discussion soon turned to the more interesting matter of controlling the power of foreign e.g., U.S., corporations by limiting the kinds of files and data they could send across borders by telecommunications. In France a small tax is levied on many kinds of data exports, not for revenue purposes, but to keep records on what is passing. The principal method for moving sensitive business files across borders has long been to fly them by courier as magnetic tape files, because this is much cheaper and more accurate for subsequent processing on U.S.-based computers. However, the European nations have begun to draft regional legislation to control all kinds of files to establish non-tariff trade barriers and other limitations on foreign companies. The Canadians have also taken a view that TBDF represents a loss of jobs in Canada.

~~(S-CCO)~~ U.S. business interests not only want "free flow of information," but also claim a "right" to operate cryptographic devices over transborder data channels. Most transborder telephone lines to and from the U.S. are leased and are used by corporations for their internal communications.

~~(S-CCO)~~ For the foreign governments to impose their TBDF policies, they must have access to the contents of the traffic passing over their borders. Under international law (The International Telecommunications Convention) they have the legal power to examine any non-government traffic that terminates in their territory. Encryption would thwart the power of the state. Therefore, encryption will be a central issue in TBDF.

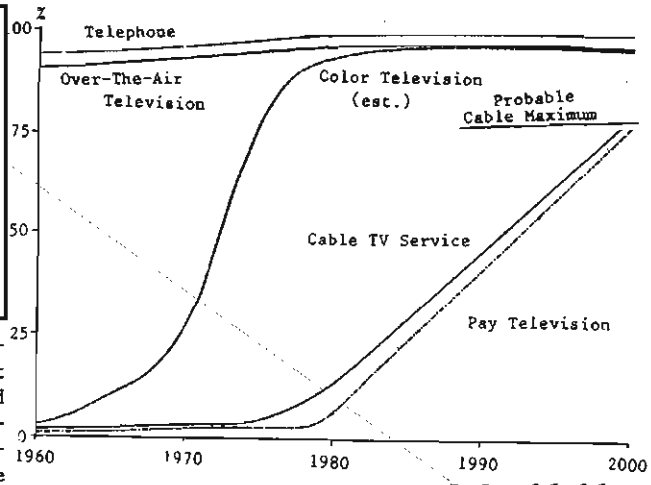
~~(C)~~ Because there are many subtle ways to send traffic across borders (e.g., indirect transmission to an undeclared recipient, etc.), the PTT's and security services will have to use their own SIGINT and intelligence services to verify that the actual TBDF corresponds to their laws and policies. The U.S. is one of the most important players in the TBDF controversy, because quite a lot of technology transfer occurs from U.S. data bases to foreign subscribers, and U.S.

transnational corporations are major users of advanced data services.

[redacted]

(U) One of the driving factors in telecommunications and teleservices which is not under the control of the telecom planners and managers, is the market penetration of consumer communications devices, such as telephones, TV sets, radios, stereos, mobile radios, home computers, etc.

Percent Penetration in U.S. Homes



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

(U) As the public acquires these communication devices, the PTT's and manufacturers and network designers have to develop supporting services to correspond to the consumer needs. Thus, for example, microwave radio relay stations and trunk routes spread throughout the U.S., Europe, and the rest of the world at a very high rate after World War II to provide a cheap wideband channel for distribution of TV programs. The programs were expensive to produce, compared to radio programs, and, before video tapes existed, had to be distributed from central studios. There was no security problem, so radio relay was acceptable. After the microwave trunks were installed and functioning, additional equipment was developed to carry telephone traffic. The driving factor was the success of the TV receiver in the market, which created a demand for the wideband network.

(U) Even consumer communications reflect commercial or governmental policies. In Israel only black and white programs are broadcast, to thwart sales of imported color TV sets, because the Israeli economy cannot stand the outflow of hard currency. At the same time, TV sets in Israel are only allowed to receive UHF so that the powerful Arab VHF programs cannot be heard. In the U.S. the broadcasters with good VHF frequencies have been influential in retarding the use of UHF and cable as a competing medium.

MARKET PENETRATION OF CONSUMER ELECTRONICS (Fig 39)

[redacted]

(U) A very different implication comes from the growth of pay-TV. This has been shown to be a profitable way of selling certain kinds of entertainment because the revenues are directly connected to market success of specific entertainment products. In order to keep non-paying viewers out, TV encryption systems have come into use. At present most of them are very weak and can be circumvented, but much better systems are under development. In the U.S. the pay-TV distribution consists of two parts, viz., the distribution of program material from a central point to local CATV companies, and the further distribution by local broadcasting. There is also a background of TVRO small earth stations which intercept both pay-TV and ordinary TV satellite relay transmissions.

(U) As pay-TV gains in success and is able to sell better programs, the economic value of TV encryption will increase. On the satellite links it is worth while to provide fairly secure encryption, but the emphasis is on program quality after decoding. In general the voice channel will be secured by something equivalent to DES. At the local level, quality is less important to the supplier than being able to defeat piracy and assuring that all customers pay their bills. The emphasis in encryption is on the command channel that shuts sets off if they are stolen or delinquent in payment.

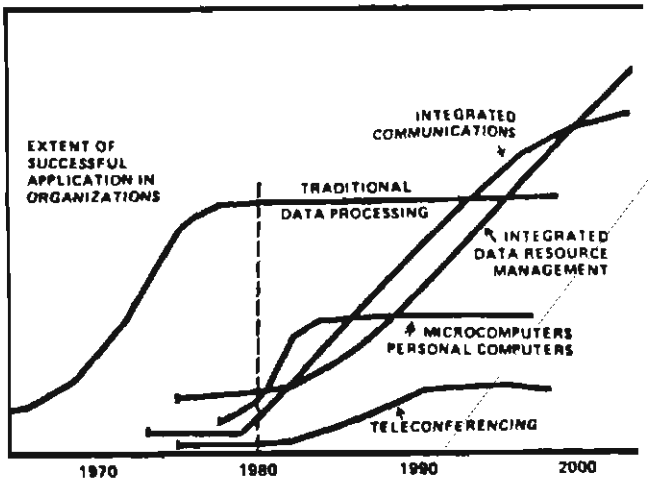
(U) The growth of many specialized TV services, including pay-TV, has made U.S. domsats (domestic satellites) a profitable industry over the past two years, and three quarters of the domsat transponders are used for TV relay.

~~(C)~~ As these new TV services, especially pay-TV, spread to foreign countries as ways of making money or raising PTT revenues, the encryption schemes will spread with them. The result will be that most of the foreign domsats will be carrying encrypted wideband traffic. The U.S. market study shows pay-TV at a 40-percent penetration level by 1990. The penetration will probably lag in most foreign countries, but the use of wideband encryption on TV satellite relays may spread faster than local TV encryption to thwart interception or copying of national programs.

~~(S-CCO)~~

(U) All of this will add to the burden on SIGINT to know what is passing through the networks, and what services are being offered, on channels which in the past have been of no interest at all.

(U) An additional implication is that the development and deployment of wideband encrypted broadcast trunks, in the U.S. or elsewhere, will have a significant strategic impact because of the difficulty of knowing the true purpose of the broadcast facilities. At the very least, it will create more international tension and suspicion unless special arrangements are made for exchange of keys on benign entertainment links. But any such exchange of keys would defeat the marketability of conference services, so that commercial interests may be directly contrary to strategic interests.



Concurrent learning curves for new technologies.

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

LEARNING CURVES FOR USERS (Fig 40)

(U) When a new technology or service is introduced, it does not usually reach its full development at that point. There is an S-shaped learning curve, and at the beginning progress may be quite slow. At some point the utility levels off.

(U) In service industries there are usually diseconomies of scale because internal coordination and administration increase faster than the size of the organization. One of the schemes for reducing these inefficiencies is for the high-level people, both technical and managerial, to use automatic systems, viz., terminal systems, to get their work done, without having to expend energy in human coordination and administration. Even this kind of scheme implies a long learning time, for individuals or organizations.

~~(C-CCO)~~ The implication to SIGINT is twofold. In the first place, no matter how quickly new technologies and services are introduced into target networks, it will take the target users some time to learn how to use them efficiently, or even to use them at all. Security or political limitations may slow down this learning even more. This creates a theoretical opportunity for SIGINT to pick up the target usage at an early stage, and follow

it as the users become more proficient and extend the usage. However, this creates a requirement for continuity and for slack capacity within the SIGINT system so that some response to new events is possible without tearing up all the existing operations.

[redacted]

~~(C-CCO)~~ In any service activity, the diseconomies of scale are always a peril to competitive survival. SIGINT faces the special hazards that the target telecom nets are expanding inexorably in a way that will defeat any small analytic and processing effort, while at the same time the combination of secret and unknown information, and technical complexity, will force more and more internal coordination--through the "unified integrated" centralized analytic centers. With this combination of an increasing volume of data and greater coordination and decision cost per datum, any mathematical model of the process would explode.

MAIL BOX

From: rcg at BROWN2
Subject: shell game
To: cryptolg at barlc05

Hi,

~~(C)~~ We just received a copy of the August 1982 CRYPTOLOG here at Menwith Hill Station (association with NSA is CONFIDENTIAL). I read with interest the SHELL GAME article. By the way, I think it is a good idea to maintain this kind of interchange.

P.L. 86-36

(U) I have some comments on the shell written by [redacted] to transfer files using cftp. I believe it a good idea to begin using programs which request the user account name and password when connecting to other systems. We all have too many shell files which place the login line complete with password right in the file. The newer version of UNIX (PWB), in addition to including the 'gather' program, provides some new features which may accomplish the same purpose. Specifically, the shell process now allows one to easily read input direct from the terminal. The 'pump' command, implemented within the shell, allows the user to place input parameters into command lines of a called process (like cftp), where normal shell arguments ($1,...) do not work.

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

(U) Also I might note the writer's problem with the line 'stty -echo > /dev/ttyX'. On any Agency UNIX system, the generic device name '/dev/tty' may always be used to specify the current terminal which is being used. Thus there is no need to worry about finding one's terminal ID to put into a shell.

[redacted]

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 43

"[The] Uses of Elegant English," [redacted] CRYPTOLOG, November, 1976.

"It was Engelbert Humperdinck, I think, who sang a song recently, whose lyrics are the epitome of originality and poetic imagery of which today's songwriters can be so proud. 'I'm yours,' sang Mr. Humperdinck, 'till the stars fall from the sky, for you and I.'"