TOP SECRET

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG
SEPTEMBER 1982

P.L. 86-36

DOCID: 4011953

CRYPTOLOG

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call[   ]3369s

To submit articles or *letters*
via PLATFORM mail, send to

cryptolg at barlc∅5
(bar-one-c-zero-five)
(note: no 'O' in 'log')

P.L. 86-36

Editorial

At the end of the first year as editor, I
ought to have some profound thoughts, but I
don't. The magazine is coming out more or
less regularly each month, and that was our
first goal. Some of the other goals have been
met, including the matching of the distribu-
tion against the locator file. Some goals
remain to be met.

The purpose of CRYPTOLOG is to help you to
do your tasks. Our emphasis is primarily
technical, but we don't always limit ourselves
to the purely technical. Helping you do you
job might be achieved by showing you how to do
something, or by letting you know that someone
else has worked on something similar. It may
also be done by making you more aware of what
is going on around you, both in space (at the
other end of the building) and in time (last
year on a related problem), because many of
the best technical people are basically curi-
ous people.

For some of you, CRYPTOLOG offers an oppor-
tunity to stretch yourselves by writing; you
might be surprised at how few readable writers
there are in certain fields, whose output is
intelligible to readers outside their own ter-
ritory. Developing a reputation as a writer
could give your career a boost. If you are
thinking about writing something and are wait-
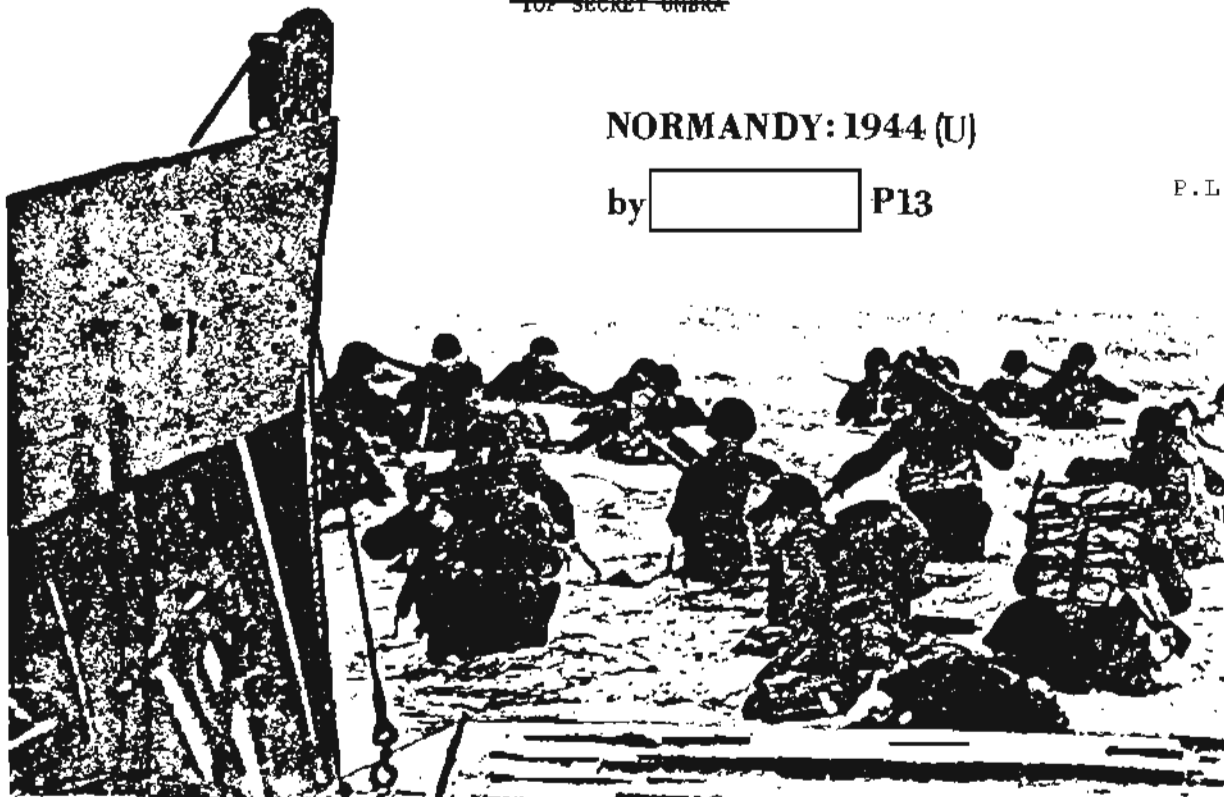ing to be asked, call me and I'll ask you.

In years past, CRYPTOLOG often skipped a
month in the summer. However, as an experi-
ment, we are offering instead an issue con-
taining three somewhat longer articles. Their
subjects, interestingly enough, are the past,
the present, and the future.

NORMANDY: 1944 (U)

by [ ] **P13**

REVIEW: Six Armies in Normandy, by John
Keegan, Viking, 1982, NY.

(U) American, English, Scottish, Polish, French, and German armies clashed in a decisive land battle in Normandy from June till September 1944, in one of the major campaigns of modern history. Half a million German troops were lost, most of them killed; their 50 infantry divisions and 12 panzer divisons had been reduced to 24 infantry divisions at quarter strength, and 11 panzer divisions had shrunk from 150 to 10 tanks each. Even the destruction of the Army Group Center in June and July 1944 by 140 Soviet rifle and tank divisions, which had cost 300,000 German soldiers, was a lesser defeat. The Western Allies had committed only 34 divisions to the battle against the 62 German divisions. When the Germans finally lost in Normandy, they lost all of France and fled in disorder to the Dutch frontier.

(U) John Keegan, a lecturer at Sandhurst whose previous book The Face of Battle became a minor classic, has written synoptic accounts of six different divisions in their most critical battles in Normandy, to illustrate not only the key events in the battle seen from battalion down to squad level, but also to illustrate something of the national character of the different armies. Where did the troops and weapons come from? Why did they fight? How did they fight? How did they react to the stress of 1944 warfare?

(S) The salient advantages the Western allies had in the land battle were seapower, airpower, plentiful supplies, and COMINT. As a result, the Germans had to defend everywhere, and this left them too weak at many points, and unable to move forces to the battlefield. When they did try to move, the radio communications were deciphered in time to paralyze the movements and prepare defenses. The cardinal contribution of COMINT was that it allowed the Allied armies to defeat the German Schwerpunkt tactics by giving prior knowledge of intentions. [6] In general, the Allied armies were no match, tank for tank or battalion for battalion, with the first-line German divisions. General Alan Brooke, British Chief of Staff, considered the Germans the best soldiers in the world and tried to keep the British forces away from them by a "peripheral" strategy, while the Americans sought a direct cross-Channel attack to destroy the German Armies in the field. Normandy was the result of this prolonged dissent on Allied strategy.

(U) The British had sound reasons for regarding the German Army with caution. In World War I the German Army was the only one in Europe that did not have mutinies. It marched out of the Rhineland in 1919 in perfect order, still willing to fight. In World War II the German soldiers fought until the last few days of the war and Germany had to be invaded and crushed; they would not surrender as long as they could still fight. At Dieppe in 1942 an invading force of 5000 Canadian
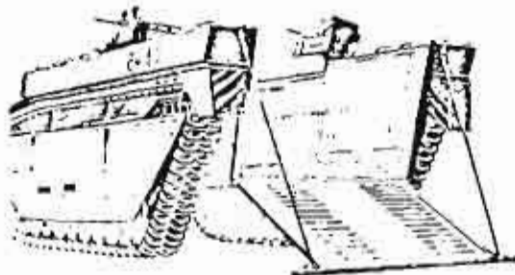
soldiers attacked a coastal town defended by a garrison of 400 German soldiers and nearly all were killed in spite of 12-to-1 odds. The German Soldiers in 1942 were in France training for or rehabilitating from the Russian campaign. In 1944 many of the defending divisions at Normandy were bodenstaendige divisions, equipped with captured foreign weapons or other inferior equipment, without transport, and the soldiers were old or unfit. Thanks to the excellent Allied intelligence, most of it from COMINT (although Keegan does not mention this), the initial landings were aimed at these relative weak spots.

(U) The German command system was able to react very quickly by converting spare personnel into infantry formations and putting weak units in front of SS regiments to stiffen their will to fight. German officers did not wait for orders from above, but put their forces into battle very skillfully in anticipation of orders from above. Orders gave objectives, rather than detailed directions, so that German reactions were tailored to the battle situation--rather than premeditated. The troops obeyed orders to the end because they had confidence in the Officers. [13] The German Army ended the war with only half its billetted officer strength because officer casualty rates were much higher than enlisted casualty rate, and the Germans would not commission unsuitable people because it would have destroyed confidence in the Officer Corps as a whole. [4]

(U) At the end of June, the Panzer divisions were committed to the battle and the 9th and 10th SS Panzers, who later destroyed the British and Polish parachutists at Arnhem [3], were taken from the Russian front and moved to Caen, where they smashed into the 2nd Argyll and Sutherland Highlanders in the "Scottish Corridor" west of Caen. An ULTRA decrypt revealed the assembly area of the German attacking force and naval gunnery destroyed the German armor before it could mount its attack in force. This COMINT assist was helpful, for the Scots had no tanks and only six-pounder guns and PIAT antitank weapons for their inexperienced infantry, in their first battle, to fight SS Panzer soldiers who began their war in Poland and had spent several years in armored warfare in Russia.

(U) Because the Germans had no navy left, except U-Boats, and no effective air force, they were unable to drive off the supporting task force, which fired on coastal targets for weeks with long-range indirect fire. These Allied assets were not always well used however, for the helpless city of Caen was reduced to rubble by naval gunfire and then further devastated by a massive strategic bombing operation because Montgomery did not want to expose his troops to heavy losses by the Germans. The Germans were not in Caen, so there was no military result. The French, trying to survive in cellars, were buried under more rubble. An insane asylum, used as a refuge and hospital in the outskirts of Caen, was devastated by Allied bombing. The Germans, however, had to keep huge formations tied up defending coasts from Norway to Italy because they could not match Allied mobility and force at sea or in the air. As soon as they tried to move forces, COMINT read their orders and the transportation facilities were wrecked. Hence Normandy was as much a war of interdiction as it was a war of attrition or maneuver.

(U) For a representative American division, Keegan chose the 101st Airborne Division, which landed by parachute and glider before the invasion to protect certain bridges so that the troops at Utah beach could get inland. The aircraft navigation and the formations were thrown off by clouds, so that the troops were scattered all over the Cotenin peninsula and some were dropped in the sea. With typical staff planning, the communication equipment--essential to coordinate and regroup the scattered airborne troops--was dropped separately from the troops, and virtually all lost. As a result, almost all the operations were impromptu little clashes by tiny packets of troops. Ad hoc formations and chains of command were set up, as circumstances

dictated, and sometimes several different ele-
ments attacked the same target at the same
time without knowing who the others were.
Runners were used to find higher and lower
units and deliver messages. Small groups. of
paratroops were adrift for weeks, out of touch
with everyone. Many units vanished, presum-
ably exterminated by the Germans. Virtually
no one spoke French, and the local population
was reluctant to get involved in the combat.
The resulting disorder apparently confused the
German command, who could not decide where the
point of the attack was. The results were
bloody but successful, with very few prison-
ers. Keegan compared the American airborne
troops to pioneers, ignorant of the language,
landmarks, or dangers around them, who simply
relied on their own weapons and skills. The
metaphor is apt, for the American troops fre-
quently outfought the German troops in the
light infantry battles and never waited for
orders or refined intelligence. General
Maxwell Taylor was cut off from his command
and from the invading force until after the
invasion forces had gotten inland, but the
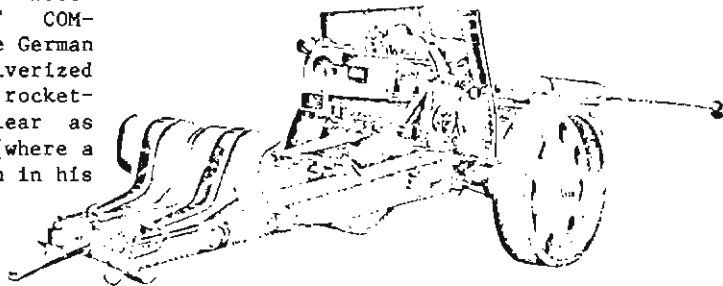lower level elements achieved their objectives
anyway.

(U) (It has since been said that Germans
could never understand why they lost a battle
to the Americans at any point in World War II,
because they tended to perceive American
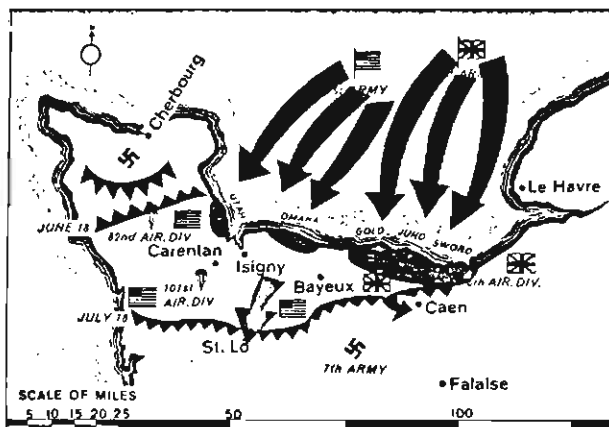attacks as disorganized and confused.)

(TSC) American military operations are men-
tioned elsewhere in the book, from the pre-
invasion buildup in England (where Keegan as
a schoolboy was impressed by the wonderful
"cornucopia" of vehicles and equipment the
"Yanks" brought with them), to the breakout at
Avranches and the sweep across France. The
Americans were much more willing to take
casualties than the British because they had
not felt the devastating effects of the trench
warfare of the First World War. By 10 July,
the Americans had suffered 40,000 casualties,
still short of St. Lo. Then they lost 11,000
men in 5 days taking St. Lo. On the third
try, carpet bombing was used to break the thin
crust of German defenses, infantry crashed
through the stunned defenders, and armor
poured south into Brittany. American foot-
ballers would call this a "power play." COM-
INT revealed the exact details of the German
response and the American defenses pulverized
the counterattack. Then masses of rocket-
firing P-51's kept Patton's flanks clear as
his armor swept eastward toward Metz (where a
tiny German defending force stopped him in his
tracks). [16, 18] The Americans also
did well on logistics. The British
favored complicated gadgets such as
the Mulberry harbors, two years in

construction, which were wrecked in one night
by a storm, after which the Americans unloaded
massive quantities directly onto the beaches
and did far better than the British achieved
with their rebuilt Mulberry harbor. [18]

(U) German defense was frequently very
tenacious. At Carpiquet on 4 July 1944, two
Canadian regiments fought all day to take an
airfield from 50 young soldiers of 12th SS
Division. In Operation Goodwood in mid-July,
a massed formation of British "Guards" armored
divisions attempted to break out from Caen,
following a raid by 1000 bombers. Battle
Group von Luck of the 21st Panzer division
threw the attack offstride by hitting its
flank, without any orders from above, and then
half a dozen Tiger tanks blocked the advance
of a Guards Armored Division. Soon the First
SS Panzer Division (Liebstandarte Adolf
Hitler), which had been in combat since
Poland, brought the British attack to a halt.
Montgomery was severely discredited by this
defeat. The British "Guards" divisions were
actually Horse Guard regiments from the
yeomanry and gentry of England, who reluc-
tantly gave up their horses and switched to
tanks as World War II become imminent. Brit-
ish tanks were unreliable and no match for the
1930's-era German tanks, but the British fit-
ted a new gun and turret to the American Sher-
man tank and the result was a fairly good
tank. However, it could not defeat the Tiger
tank, which the Germans used defensively in
Normandy. The Guards regiments had experience
in desert fighting, but in the terrain of Nor-
mandy, the German tactics of using 88-mm anti-
tank guns in conjunction with tanks that fired
from cover proved superior. At the same time,
the policy of fighting on a rigid line, as
ordered by Hitler (and required by the Allied
interdiction of the German rear area), left
the Germans vulnerable to the breakthrough and
encircling operation that occurred in late
July and August.

	German 88 mm L/70
Weight:	4 tons
Muzzle velocity:	3,700 fps
Length (calibres):	71
Weight of shot:	22·2 lbs

(U) Keegan chose the landing of the North Shore regiment of the Canadian 3rd Division at Juno Beach on D-Day and contrasted it with the slaughter of the Canadian 2nd Division two years earlier at Dieppe. The Canadians generally played an unsung part in the war. Their battle doctrine was British, but much of their equipment and logistics were American, particularly the indispensable tanks and trucks. Canadian regiments trained for four years before they fought in Normandy, and had to compete to be selected for overseas service. [12] Because of the long training and association in the same battalions and regiments, the Canadian forces were able to withstand the savage battles with the SS Panzer Divisions from Caen to the Rhine. (By contrast the U.S. stripped 60,000 cadets out of flight school in Summer 1944, and 75,000 from advanced training programs, and shipped them to France for immediate combat duty as infantrymen. [15]) Canadian losses were high; a single 2nd Division Regiment (the Algonquins) suffered 1300 casualties, about one third of its strength, from August 1944 to May 1945. [12] Similarly, the U.S. 35th Infantry Division lost 3000 men in a few days in the St. Lo breakout. [17]

(U) In an effort to trap the Germans in the Falaise pocket, the First Polish Armored Division got onto a hill near Chambois and fought off repeated German attacks, although it was itself cut off. At this point the Polish Home Army in Warsaw was facing annihilation by the Germans, while the Russian Army paused not far from the city. The Polish parachute bri-

gade went on a hunger strike because the Western Allies would do nothing to help the Home Army in Warsaw. The First Polish Armored Division had risen from the ashes of successive defeats. After the invasion of Poland in 1939, 100,000 refugees got to France, and an army in exile was formed in France. Only 17,000 got to England, with no equipment, after the fall of France in 1940. They recruited Poles from around the world and manipulated American Lend-Lease to equip and train an armored division. An Austro-Hungarian officer, Maczek, was put in command. This re-formed army kept the titles and colors of various Polish regiments, long since destroyed. It formed part of the Army of the Republic of Poland, rather than being merely a division in the British Army. The Poles were notoriously disdainful of danger and, when given an order to close the Falaise gap, set off without waiting for resupply of fuel and ammunition. They took the wrong road and wound up in an excellent military position on high ground, ready to block the German retreat, but cut off. Twenty German divisions were trying to break out past them. On the same night that the Home Army retreated through the sewers of Warsaw, the Germans began to fight for control of the hill at Chambois. The Poles' resupply was airdropped five miles away. They fought without supplies or support for three days against massed German infantry, tanks, and antitank guns. They also had to guard 800 German prisoners. Seventy percent of the survivors of the Westheer who had tried to escape at Falaise had been stopped by the Poles and taken out of the war. In Warsaw the survivors of the Home Army had to surrender to the Germans. After the war most of the surviving Poles from the First Armored Division stayed in England; their battle to free their homeland had been in vain.

(U) The French Army was commanded by General LeClerc, a nom de guerre for Vicomte Jacques-Phillipe de Hautecloque. LeClerc was actually much higher up in French society and military life than DeGaulle, his nominal superior. His 2nd Armored Division, which fought its way into Paris after the Normandy breakout, actually began its existence in Southern Chad in 1940. The cadre consisted of black Senegalese soldiers and outcast French officers from Fort Lamy. This swashbuckling crew of officers and bloodthirsty soldiers soon made a trek 1000 miles north across the Sahel to the Sahara, where they fell upon the Italians in Southern Libya. In 1942 they made further attacks, in collaboration with the British Long-Range Desert Group, and then left the base in Chad to move into Tunisia. They joined with some Foreign Legionnaires and Levantine soldiers serving under Koenig. They

filled out the cadres with Algerian and Moroccan mercenaries, and it was these Berber mountain troops who broke the defenses at Monte Cassino in Italy. The Moroccan troops, by some accounts, were paid three centimes for bringing back trophies cut from the enemy corpses. For political reasons it was important to recruit native Frenchmen to fight in the reconquest of France itself. The Americans promised equipment for a full armored division. Former Vichy troops and officers in Africa were permitted to join, on probation. The Senegalese were not regarded as suitable liberators of the white French nation, and were sent back to Chad over their protests. Christian Arabs from North Africa replaced some of the Senegalese. The officers were largely St. Cyr graduates, all known to each other. LeClerc himself, an aristocratic hereditary leader, indifferent to danger, was the central element in healing the divisions between the Vichy and anti-Vichy officers and men. French military pride had been deeply wounded by the ease with which the German Panzers brushed their armored units aside in 1940, so they worked diligently to be up to battle standard by D-Day. They went to France on 1 Aug 1944 under Patton's command.

(U) The battle for Paris was fought for domestic political reasons, rather than for military reasons. Eisenhower wanted to bypass the city, but the underground, Communist and maquis, was too strong politically, so it had to be liberated by the Free French in order to establish DeGaulle as a force in the French government. The German commander, Choltitz, had been ordered to destroy Paris and intended to give an episode of resistance in order to salvage German honor before surrendering the city. The French ran armored columns through the streets of Paris in three columns to reach certain politically important objectives. Their aim was to establish DeGaulle's appointees as the heads of key ministries by fait accompli. They did not want to destroy Paris and were criticized by the Americans for "advancing on a one-tank front." Within a day they achieved their purpose. The Parisians, expecting to be liberated by the Americans, were thrilled to see the insignia and pompoms of French regiments. A huge crowd turned out to rush along with them, just as they hit a German strong point. Battles raged around the Arc de Triomphe, Place de la Concorde, Hotel Meurice, and other parts of a battlefield deluxe. After the honor of the officers was satisfied, the troops were ordered to stop fighting. A European civil war has its protocol.

(U) In his epilogue, Keegan remarks that military analysts are now looking at the Ger-

man defense in Normandy as a model for how NATO might fight a conventional war where the rear area was disrupted, no territory could be given up, supplies were scarce, and air superiority was held by the enemy. He does not think much of the idea, for the Allies were able to use seapower to attack a coastal point without warning, while a Soviet advance would have to follow some obvious land route. However, there are several factors in the Normandy battle that are worth considering, even if the particular tactics are no longer pertinent. The Allies, with only 34 divisions, defeated some 62 German divisions, destroying half of them. By the book, it should have taken 180 Allied divisions to push the Germans out of France. Despite the inexperience of the Allied divisions and the great tactical ability and experience of the German divisons such as Panzerlehr, etc., the Allied casualties were comparatively low. Airpower was critical, especially in interdiction and in protecting the Allied logistic flow, but one key factor was the Allied ability to avoid slaughters.

(U) Keegan mentions COMINT, citing Bennett's book Ultra in the West, but his treatment is fairly sketchy. ULTRA COMINT was generally of only limited tactical use because it was either too late, or the Germans did not send detailed tactical orders over ENIGMA. There were some exceptions, especially when Hitler sent tactical plans directly, such as the counterattack at Mortain after the Avranches breakout. Many of the read ENIGMA messages were unusable because the British General Staff had thrown away the only copy of the French military map that the German Army was using, which gave the names of many little towns. [5] Reconnaissance, patrolling, prisoners, and captured documents gave most of the timely tactical intelligence. [14] The French, Poles, and Canadians were not direct ULTRA recipients.
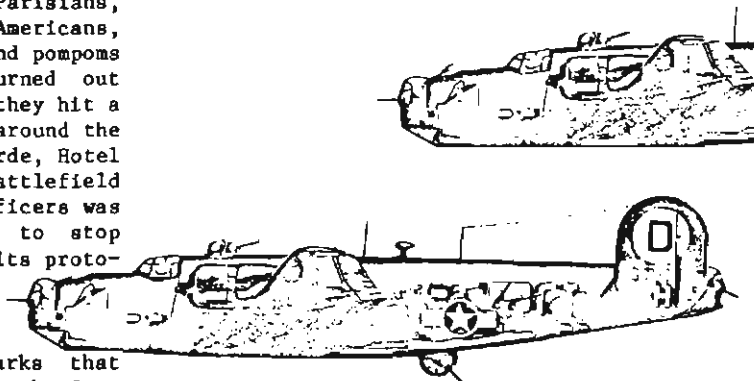
(TSC) ULTRA did not set the strategy. That resulted from a long conflict between the British and Americans over the "second front," described by Keegan in a chapter. The plan to fight the German Army after a cross-Channel invasion set the conditions for COMINT, which then had to work on the Army keys and other ciphers pertinent to the German defenses. [10] ULTRA from many sources gave an incomparable picture of the German dispositions, fortifications, and preparations for the invasion. It also showed in 1943 that the Foreign Armies West Intelligence was "channel blind" and thus vulnerable to the strategic deception that tied major forces in the Calais area. [8] COMINT on German SIGINT and Intelligence and Agent systems showed that strategic deception was working, and spared the Allies from a devastating surprise in the landing. [9] After that, COMINT continued for several months to give a lot of operational intelligence about major ground and air movements, and high-level reports, so that the Normandy breakout and the sweep across France could be pursued without fear of strategic surprise.

(TSC) Although strategic deception worked well, COMINT showed that tactical deception schemes were virtually always penetrated by the Germans. [5] Someone always gave the game away. Knowing that deception was NOT working was probably very valuable in holding down the "butcher's bill" in Allied attacks.

(TSC) Some of the main points of the COMINT effort are interesting. No German Army Enigma keys were read from mid-1940 until the spring of 1944. The solution of the cipher tele-printer TUNNY in May 1944 was the biggest success of the year in giving German strength, dispositions, plans, and appreciations in the West. Before D-Day, and for three months afterwards, COMINT was the primary or only source of a vast amount of information about German dispositions, preparations, etc. Almost all of this COMINT was obtained from German military traffic. COMINT gave routine intelligence about the German forces and actions up to the American breakout at St. Lo, after which it became spectacular. In the counterattack at Mortain, messages from the XLVII Panzer Corps and from C-in-C, West were read within hours, giving intentions which had been decided by Hitler. The messages were out of date before they could be acted on because of Allied actions. German intelligence on Allied intentions at Falaise was known from decrypts. German fears of encirclement and Hitler's refusal to permit a withdrawal were known from COMINT. German confusion was reflected in the decrypts, which were often translated and sent to the users within a few hours. When von Kluge vanished on the battle-field at Falaise, Hitler personally ordered a counterattack which was successful, but the message was not read for ten days. The order to withdraw behind the Orne River given on 16 August was read and forwarded in five hours. During the retreat after 18 Aug 1944, most of the decrypts were too late to keep up with the fluid battle situation. Decrypts showed a temporary lapse in German discipline and morale. [7] (Entire paragraph)

(TSC) Allied use of COMINT changed radically after the crossing of the Seine River, because only events in the North were covered by the arrangements between GC&CS (Govenment Code and Cipher School) and 21st Army Group. The American forces in France handled ULTRA COMINT differently from all other intelligence. Despite security rules, ULTRA was discussed at all time on the Signal Corps telephone circuits in France. [6] (Entire paragraph)

(TSC) Only a small fraction of the decrypts produced were used actively to conduct operations. Most COMINT was used passively to confirm other intelligence, or for information. COMINT was found of less use to the attacker, who had the initiative, than to the defender. One common active use of COMINT was to direct reconnaissance at specific targets. This confirmed and covered the COMINT. In general, active use of COMINT required much more than timely decrypts, but the results were significant. [6] (Entire paragraph)

(TSC) By September, as their Army was retreating, German COMINT became very good, while their COMSEC tightened and Allied COMINT quickly fell off [10]. German SIGINT gave 90 percent of their Intelligence about Allied O.B. [8] The Allied advance came to a halt at about the same rate that Allied COMINT dried up. After another six-month buildup and several major calamities, such as Arnhem and the Battle of the Bulge, the Allies were finally able to penetrate Germany and occupy it, but the Intelligence situation was generally very poor and COMINT had serious outages for months.[8] The German Army fell back onto landlines inside Germany, and the gradual spread of Reflector D on Luftwaffe Enigma circuits cut down on decrypts. [7] Three German Army keys were heavily read for the last three months of the war but Tunny was the main source, although it took longer to decrypt and therefore was not as timely. [7,10] At Remagen COMINT gave the German plan to bomb the bridge. [7] Allied aircraft bombed the German airfields, and COMINT also gave damage assessment from the raid.[7] This protected the bridgehead. After the Allied armies broke into Germany, knowledge of German Order of Battle and capabilities was critical to the speed at which the Allied forces moved East. [7] Revelations of German intentions were confused by the disparity between orders given and actions taken. [7]

(TSC) Although COMINT fell off after September 1944, because the Allies had extraordinarily good COMINT during the critical months before and after the invasion, they were able to apply their local superiority in airpower and seapower to hold down casualties and keep the German ground forces from splitting their armies apart or driving them back to the sea. COMINT gave an unparalleled insight, at the operational level, to what the Germans were doing, and even though the beachhead expanded much more slowly than the planning called for, the Allies avoided disaster until they were strong enough to achieve a breakout.

(U) Summing up, Six Armies in Normandy is a very readable and interesting review of a campaign that, in hindsight, can be seen as an outstanding military success for the side that had the best COMINT and COMSEC. German tactical effectiveness generally offset Allied material advantages. The small size of the Allied force, and the low casualties, compared to the German losses and collapse, suggests that COMINT and COMSEC combined had a much higher tactical value than is generally recognized.

References

[1] Keegan, John, Six Armies in Normandy, New York: Viking, 1982.

[2] Bennett, Ralph, Ultra in the West, New York: Scribners, 1980.

[3] Bauer, Cornelius, The Battle of Arnhem, Kensington, N.Y. 1979

[4] Gabriel, Richard and Savage, Paul, Crisis in Command, New York: Bill and Wang, 1978.

[5] G.C.&C.S. Army and Air Force Sigint, Vol. XIII, p.196, 228-30, 1952. (TSC)

[6] G.C.&C.S. Army and Air Force Sigint, Vol. XVIII, p.193. (TSC)

[7] G.C.&C.S. Air & Military History, Vol. VIII, Ch. 1,V, 1952 (TSC)

[8] G.C.&C.S. Air & Military History, Vol. XI, pp.220-5. (TSC)

[9] G.C.&C.S. Army and Air Force Sigint, Vol. XVIII, pp.125-7. (TSC)

[10] [   ] History Lesson, Cryptolog, May 1982.

[11] [   ] Der Fall Wicher, NSA Technical Journal, Vol XX, No. 2, Spring, 1975. (TSC)

[12] Cassidy, G.L., Warpath, Toronto: Ryerson, 1948.

[13] Shulman, Milton, Defeat in the West, Secker & Warburg, 1948.

[14] G.C.&C.S., Army and Air Force Sigint, Vol. XIII, pp. 14, 20. (TSC)

[15] U.S. Army in WW II, Army Ground Forces, Procurement and Training of Ground Combat Troops. GPO, 1948, pp 72-85.

[16] U.S. Army in WW II, Breakout and Pursuit, GPO, 1950, pp. 692ff.

[17] U.S. Army in WW II, Lorraine Campaign, GPO, 1950, p. 1.

[18] Mallory, K. and Ottar, A., The Architecture of War, Pantheon, 1973. p. 123, Ch. 10.

SECRET

TSS REVOLUTION (U)

by A33
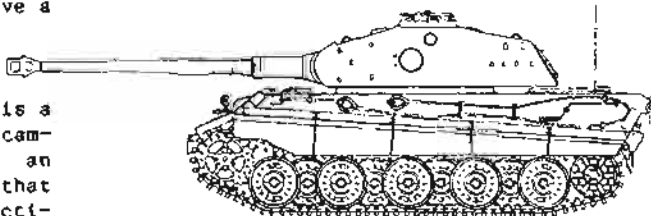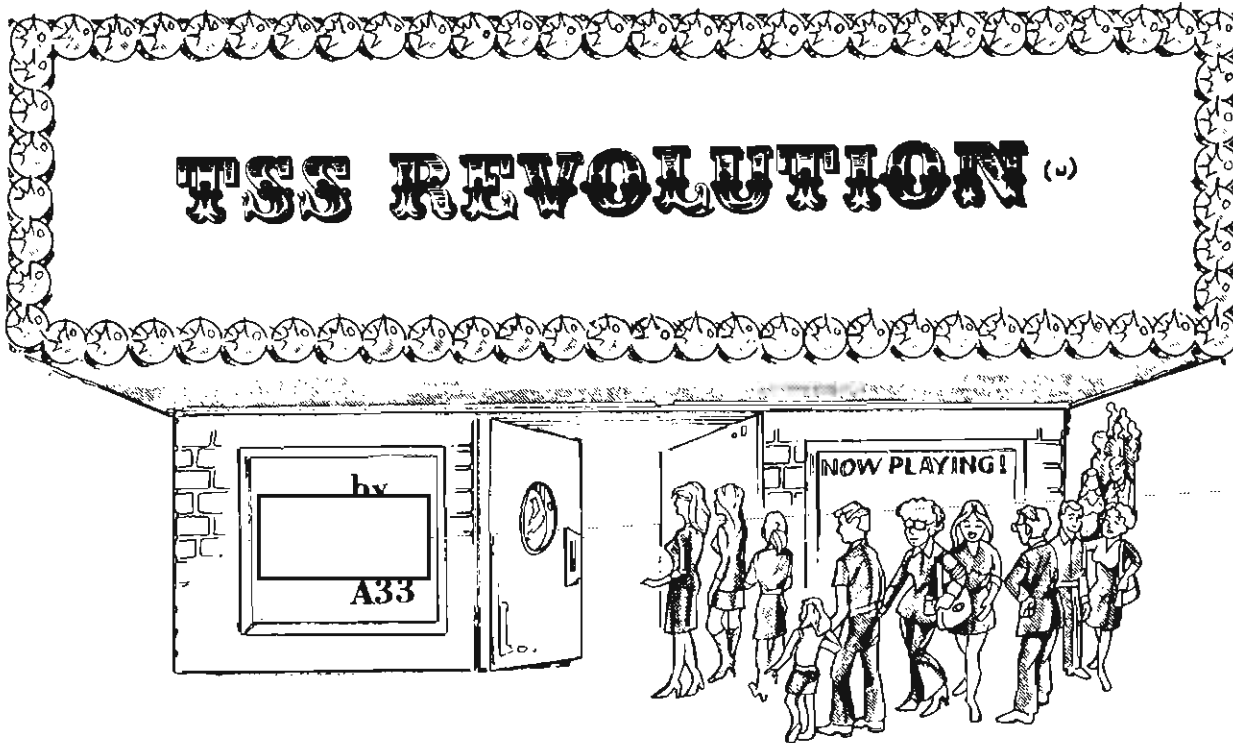
his paper will convey some of the lessons that have been learned about the effect that Terminal Sub Systems (TSSs) have had on NSA.

(U)

TSS REVOLUTION

(C) I can sum up the major effect that TSS has had on the Agency in one word: REVOLUTION (sudden, complete change). The technology is revolutionary because:

☐ it is a friendly (but not lovable) machine/human interface;

☐ the PLATFORM network provides access to remote data; and

☐ the software facilitates a flexible, adaptable system that can satisfy many active analytic requirements.

The TSSs have brought about cultural changes that are revolutionary for those analysts, software developers, and Agency managers who have access to or deal with the TSSs.

(C) Therefore, I will speak about the

This paper was presented at the CISI Conference, 25 May 1982.

technical cultural revolution that has been going on in the Agency for the last five or six years. I believe that we now stand on the brink of yet another revolution at this agency: that of the powerful personal computers, local area networks, and true distributed processing. Some of the lessons we learned during the TSS Revolution can give us insight into the next revolution that lies ahead.

TECHNICAL REVOLUTION

(C CCO) First, what's revolutionary about the TSS technology? The PDP11 and UNIX version 6 are mid-70s technology—certainly not state-of-the-art in 1982! But if you step back and consider what a TSS gives you, it might be viewed in a different light. It's a mini-computer that is not overly powerful in terms of performance, but quite powerful in terms of:

SECRET   HANDLE VIA COMINT CHANNELS ONLY

★ software;

★ the connection with PLATFORM that provides access to analytic systems and data all over the building and in spots around the world; and

★ the tempested smart terminal that can be loaded with several different software packages.

(U) What's so great, you ask, about the software? After all, it gives you the ability to sort, edit, compile and execute programs, and do the normal things that most systems do. Well, UNIX has some features that set it apart from traditional operating systems, especially in the interactive analytic environment.

SIGINT as an Art

(C-CCO) One point we must realize is that SIGINT analysis, like programming, is an art. Individual analysts perform similar jobs in different ways, reflecting their individual styles and approaches to problems. For example:

■ one analyst may have a collection of message traffic that he scans in several passes, first very quickly to get an idea of the content, then in several additional passes extracting relevant information from which he is generating his report;

■ The next analyst might make only one pass, extracting all the information needed by carefully going through each message only once;

■ The next person may extract data and reformat it with, say, a permuted index or a matrix to present the data in a form which he can analyze.

Each is doing the same job, but doing it in a different way. In this dynamic, multi-faceted Agency environment, a system that forces an analyst to conform to the way the system wants him to work and that does not adapt to individual analytic approaches will not achieve widescale acceptance.

Flexibility and Adaptability

(U) The key to the acceptance of UNIX by analysts has been its flexibility and adaptability. The I/O is set up so that, instead of writing a special program that does all the

functions you want, you have a large set of programs that perform specialized functions and chain them together in the sequence you need to do the work. The output of one program goes into the input of the next program, until the series of functions is complete. This gives a tremendous amount of flexibility in the sequencing of functions an analyst might need to perform a job.

(U) Add to this feature the ability to create INTELLIGENT command files--shells--and you have a powerful set of functions that can be configured easily into a tailored human interface that is analyst-friendly.

P.L. 86-36

(C) Add to this the ability to acquire data electronically from [   ], and other major and minor computer systems via PLATFORM, and you have an Analyst Support system that helps an analyst:

☐ get the data he needs;

☐ format it they way he wants it;

☐ manipulate it for various types of analysis;

☐ store and accumulate data to monitor trends;

☐ update data bases on major hosts, if appropriate;

☐ access word processing functions to generate reports;

☐ forward it electronically for release through [   ] (soon); and   P.L. 86-36

☐ interact with analysts on other systems using electronic mail and OPSCOMM-like functions.

(U) So, even though TSS technology is mid-70s, and not state-of-the-art, it does represent what I call a technical revolution at NSA.

CULTURAL REVOLUTION

(U) Now, what about the cultural revolution? I spoke earlier about the cultural effect that TSSs are having on analysts, software developers, and managers. I would like to briefly describe these effects.

SECRET

Software Developers

(U) The TSS revolution has had a significant effect on software development. We learned through experience which approach to software development seems best for this type of system.

Turn-Key Approach

(FOUO) The first applications project that we tried to develop was a TSS-based transcription system. Since this was a formal system acquisition, we did a lot of work on requirements analysis and came up with a design which was given a formal review. The review determined that the UNIX software which existed at the time would not produce the desired result, so a UNIX-based development was not started and an alternate approach was taken. This project is still in development and hasn't been operationally used by an analyst.

Evolutionary Approach

(U) In our next few projects, we felt that it was necessary to take a less formal approach to development, especially since we didn't really understand exactly what the analyst wanted and the analyst didn't really understand what the system could do. So we prototyped--we experimented. Our psychology changed from delivering a turn-key system to that of evolving into a system through iterations--build what we best understand is needed, try it out in an analytic environment, make changes, try it out, etc. THIS APPROACH WORKED!

(C) This brought about many cultural changes. Software developers actually talked with SIGINT analysts. They actually learned about some of the functions that SIGINT analysts performed. They built small systems (and some not so small) that allowed the analyst to do a job. This was a good motivator for the developers and the analysts. REAL users were using the software that was developed on real targets (some of them very high priority). This stimulated and challenged the software developers. Analysts were getting prompt attention to their needs (on a small scale) and getting a growing set of functions that helped them do their jobs. Also, their advice and guidance was being sought--they had great influence over the software functions that were developed.

P.L. 86-36

Analysts

(C) I think you can imagine the effect that TSS has had on the end-user from my previous description of how the system might be adapted to different analysts and analytic approaches. The flexibility that I described not only permits each analyst to do a specific job in his own way; it also provides a wide range of functions that allow each analyst to do many different types of jobs. UNIX supports a wide range of cryptologic functions: collection, CA, TA, linguistics, reporting, data processing, management, and others. It is thus a powerful tool.

(FOUO) Yet, there are frustrations. It has been estimated that less than five percent of the analysts in the Agency have access to TSSs. People in A3 are literally lining up to use the terminals. So, in a sense, we have not kept pace with the success of TSS in making the system available to analysts on a large scale. Also, the performance and reliability can be trying at times--hardware, software, and communications problems can interfere with the consistency of use that analysts should receive.

(FOUO) Some systems are overloaded to the point that performance has degraded to a serious degree. I believe [   ] T44, coined the term "Tyranny of Success" to describe a system that was so successful that it quickly bogged down because it was so popular. Tyranny of success is what we're experiencing on many of our TSS systems. These problems are being addressed, but they do have a cultural effect on end-users.

SECRET   HANDLE VIA COMINT CHANNELS ONLY

(U) The people developing the TSS utilities, like Data Base Management Systems, forms packages, intelligent terminal software, etc., had some feedback on how useful the tools they built were, and what other functions might be needed--and this was very important. It caused an impressive set of utility functions to be built and made available, based on feedback from REAL users and applications software developers.

Analytic Approach to Evaluation

~~(S-CCO)~~ The analysts we worked with had two basic approaches to deciding what they needed. One approach was to get onto a UNIX host, go through all the programs available, and try to do their job. If they ran into a situation where there wasn't an existing function to do what they needed, they would ask us to build one. A good example of this is the sort routine. It did most of what was required. The ASCII codes for characters didn't give the proper sort sequence, so P1 requested a version of 'sort' that could handle non-standard alphabets--and it was provided.
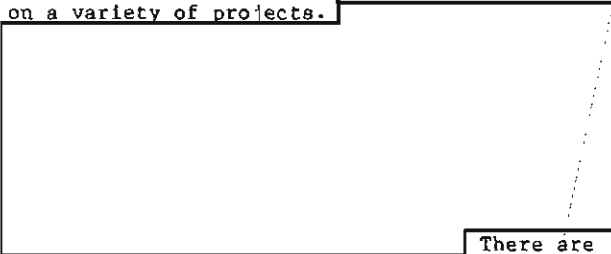
~~(C)~~ The other approach used by analysts to decide what they needed was to write a specification of some type--a concept of operations (CONOP), a requirements specification, or some similar document--and we would develop the capability in an iterative fashion. This approach worked well for the larger, more comprehensive projects like _____ This was different from the transcription system experience I mentioned earlier because we understood from the beginning that it would be an evolutionary development rather than turn-key. Users were generally pleased with this approach because they would get the opportunity to evaluate the development while it was going on and give feedback to the developers on changes they might need. In some senses, it was a rapid prototype environment.

(U) After this had gone on for a while, we looked around and discovered that a significant stockpile of basic software components existed for various types of analytic work. We basically had a box of analytic tools that had been developed and tested in operational areas on real problems.

Generalized Software

~~(S-CCO)~~ An important lesson that was learned during this development period was that the software could be generalized quite nicely in many cases, so that the same program, properly parameterized, could be used on various targets, by different organizations, on a variety of projects. There are many instances where this generalizing, if designed into the project from the beginning and developed iteratively, has worked better than we had thought possible.

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

Graphics Experience

~~(FOUO)~~ An important example of this is the work the Graphics Investigation Group (T4, T3, R53) did on computer graphics, which resulted in a highly generalized graphics capability available to any TSS. In 1980 and 1981, the GIG sampled analytic organizations to find out what the general requirement for graphics was at the Agency. We concluded that most of the organizations had similar graphics requirements: mostly overlays on geography and management displays (charts, graphs, etc.). The similarity of functions at the software level told us that we could satisfy a wide range of requirements with a comparatively small software effort, by means of generalized graphics software.
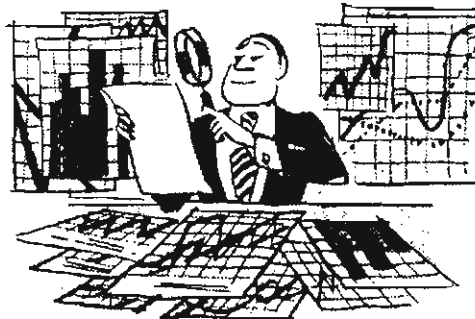
P.L. 86-36

(U) To make a long story short, a generalized graphics package was developed (partly commercial, partly in-house) and installed on a TSS. This gave us a powerful, adaptable graphics software capability that operated on a TSS and could interface with the existing "alphanumeric" graphics programs.

(S CCO) More and more TSS systems were deployed, and more and more people learned about the ability of TSSs to assist them with their work; we began to get a lot of requests for software systems.

The system required some sophisticated alphanumerics, graphics, and transaction processing that challenged us to deploy what is probably the most sophisticated software system I know of on a TSS today. The development effort was successful: the system is in operation today. I would like to acknowledge the substantial software effort put forth by R53 in developing nearly all of the graphics software for OMS.

Management

(FOUO) As you might suspect, with approximately 50 TSS systems in existence, the management problems in dealing with the many aspects of these systems are quite significant. This is an entire revolution in itself; we certainly don't have time here to even scratch the surface, but I do want to emphasize one point: there is a significant management problem throughout the Agency in dealing with this many systems.

(FOUO) The TSS Configuration Control Board was established last year to gain control over TSS management. They are currently dealing with many management issues that affect current operations and future architectures and policies. The need to provide more direct customer support for a large number of interactive users and software support organizations may require significant changes in DDT and DDO organizations.

(U) The lessons we have learned from the current TSS Revolution--mixing operational prototyping, experimental development, evolutionary development, generalized software, etc., may, and SHOULD, have an effect on the acquisition of interactive systems. We can't afford on a corporate basis to get too informal, yet the more formal route has been shown to be not very successful.

REQUIREMENTS

(FOUO) One final note. There is one substantial weakness in the software development process, whether on TSSs or other systems, that I feel is the cause of many failures and problems in system acquisition: REQUIREMENTS SPECIFICATION. Based on my experience, we don't do it well. It is a very difficult task. It's the most critical stage in the development of a project, yet it has the weakest set of tools of any phase of software development. I feel very strongly that if we had an automated method that would generate the requirements documents--or a functional prototype that both users and technical people could understand and work with--it would dramatically increase the Agency's ability to develop systems that really satisfy user requirements.

(U) I've tried to give you some of my thoughts and observations on what I call the TSS Revolution at NSA. Even though I've only touched on a small number of the issues involved with a technological and cultural revolution, we must remember that we are now on the verge of a new revolution. They are going to start coming more frequently now because of the rapid advances being made in technology. We have to learn how to deal with them with as little negative effect and as much positive effect on the Agency's mission as possible. We're learning!!
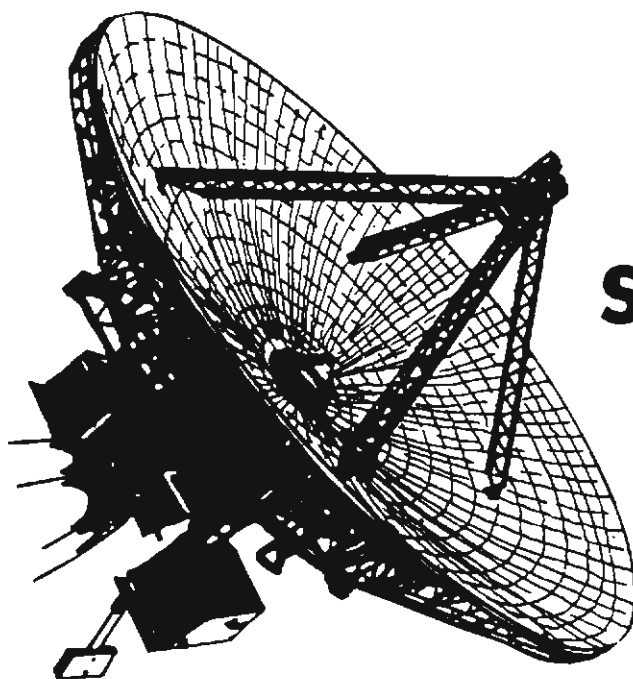
SIGINT: 1990 (U)

by Joseph Meyer, P13

Major developments in telecommunications technology and systems during the 1980's will have a profound effect on SIGINT by 1990. The main (U) 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.
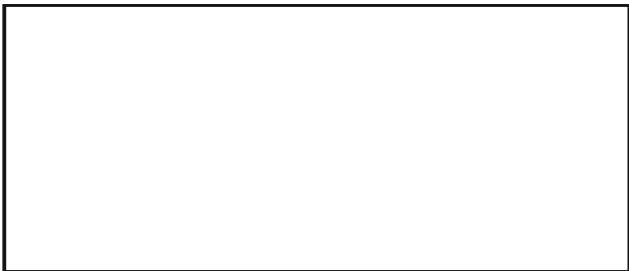
(U) There is little basis at present for optimism about the future if SIGINT continues to operate in its present framework, yet unoptimistic forecasts are rarely welcomed. As a

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.

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.

The Sequence of Inventions in Telecommunications, 1840-2000
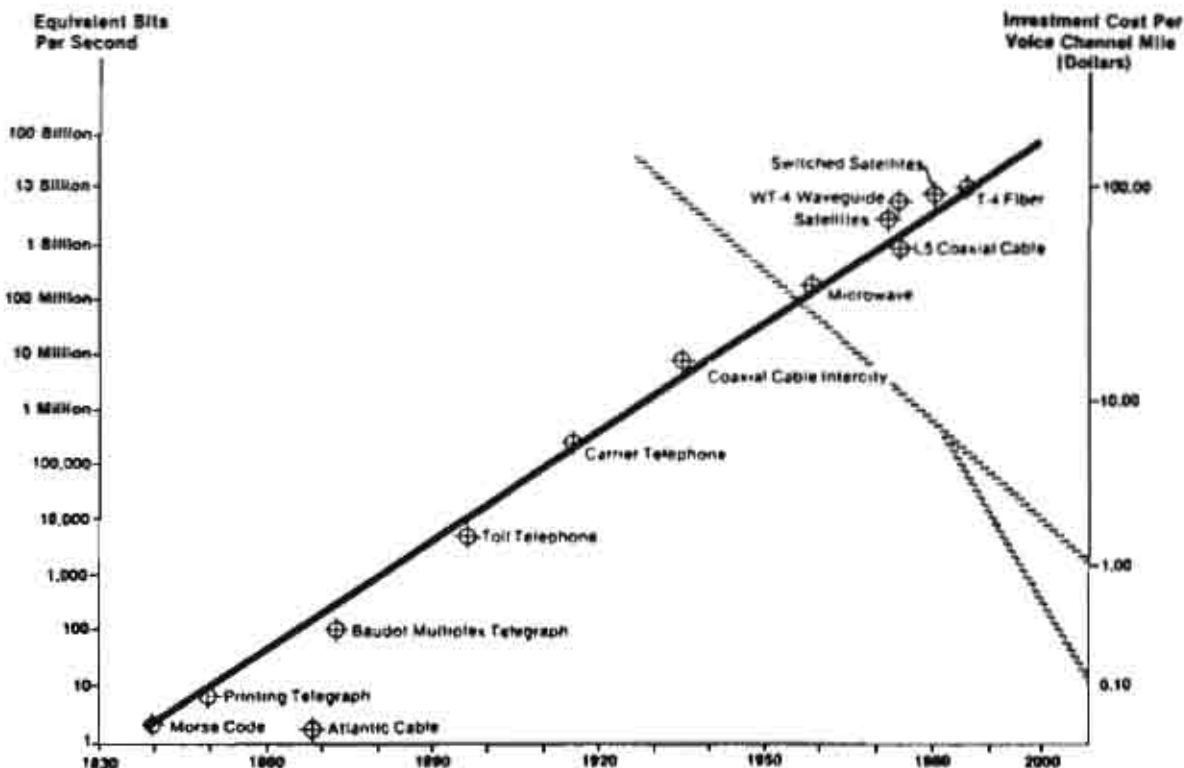
Source: Richard J. Solomon, Massachusetts Institute of Technology

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.

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.

DOCID: 4011953
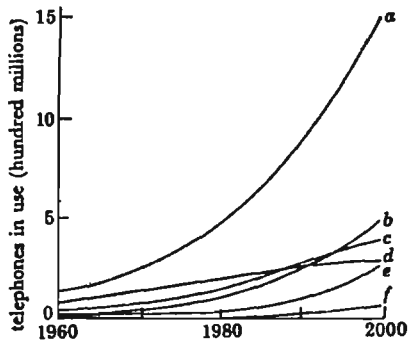
Forecast growth in the number of telephones in use: (a) the world; (b) Asia and Oceania; (c) Europe; (d) North America; (e) Central and South America; (f) Africa.

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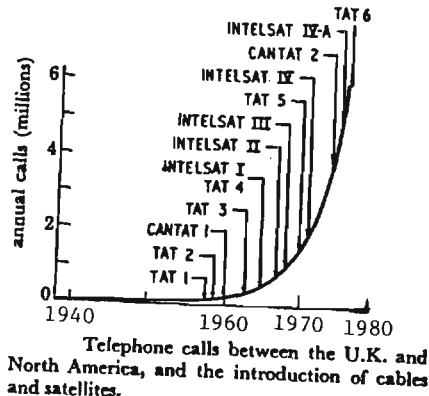
3. PHONE CALLS U.S./U.K.

(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 cir-
cuits. During the late 1980's this trans-
Atlantic capacity will be more than quadrupled
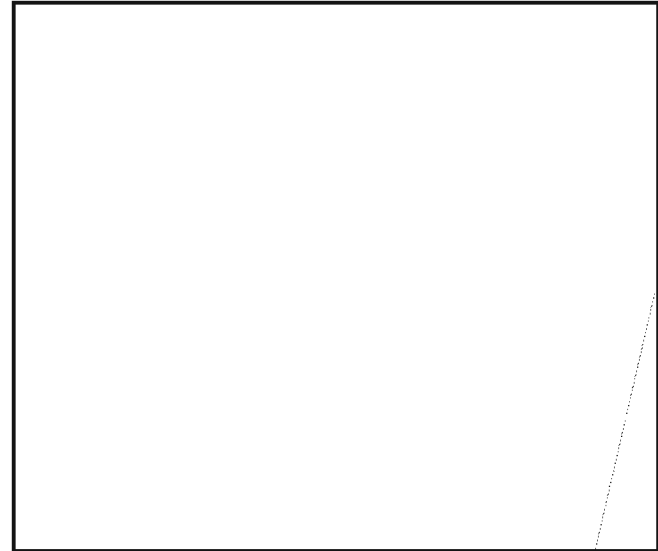(see undersea cables, discussed below).

(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 capa-
city to the 12,000 two-way channels now in
service.

voice.

Télécommunications, objectif 2000
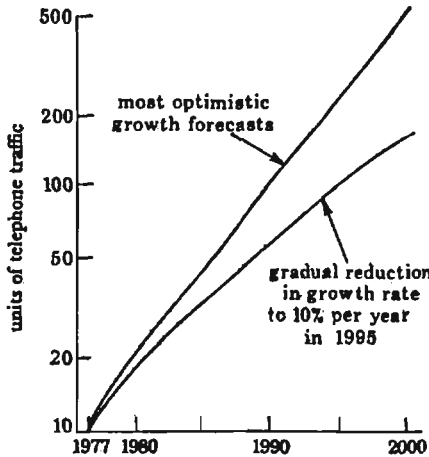
Intercontinental traffic forecasts: telephone calls from the U.K.

4. INTERCONTINENTAL TRAFFIC FORECASTS

Évolution du trafic téléphonique total

5. 6% to 12% INCREASING TRAFFIC GROWTH

(U) Various authorities, including Intel-
sat, 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 gen-
erally placed in a short time window when peo-
ple on both sides of an ocean are at their
desks. Thus, late afternoon in Europe con-
nects 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 inter-
national circuits, particularly digital fac-
simile, 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

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

(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.

will be almost no aspect of the economic, pol-
itical, 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

millers d'équipements / nombre de voies multiplexées (millions)

Équipements d'extrémité

millers de circuits

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 neigh-
bors. The hidden element is that the French,
as well as the other Europeans, intend to stay
away from satellite circuits in favor of opti-
cal 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.
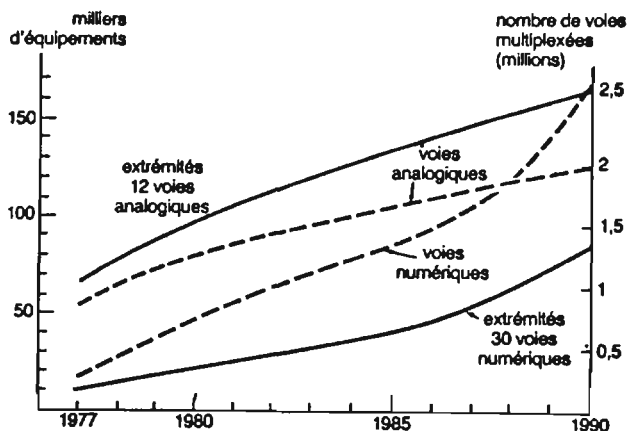
(TS CCO) The impact on SIGINT of the Euro-
pean preference for optical fiber cable over
satellite is that their international traffic
will be harder to intercept. If the relations
between the U.S. and Europe change during the
1990's (e.g., by the dissolution of NATO or by
a political shift toward the 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
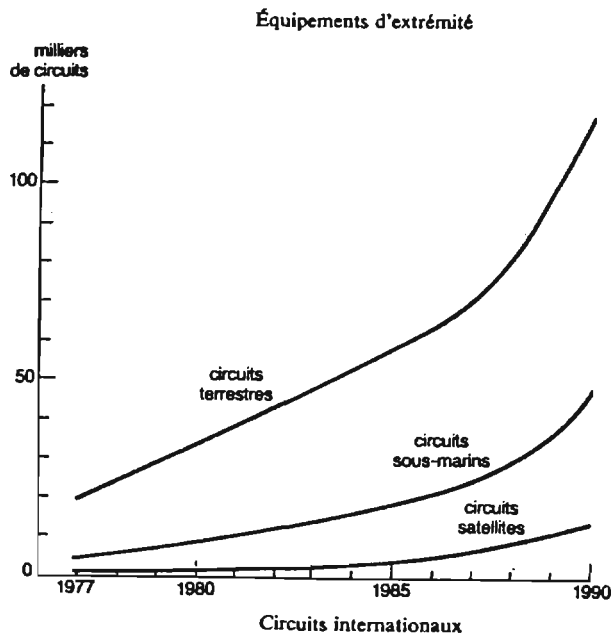
(U) The correlation between national wealth
and telephone density is well established (see
page opposite). The rich industrial countries
have a high telephone density, as many as 70
phones per capita, while poor nations such as
India have only about 3 telephones per 1000
inhabitants. In Africa the telephone 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 telecommunica-
tions 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 prac-
tically 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 tele-
phone service into the rural areas of the

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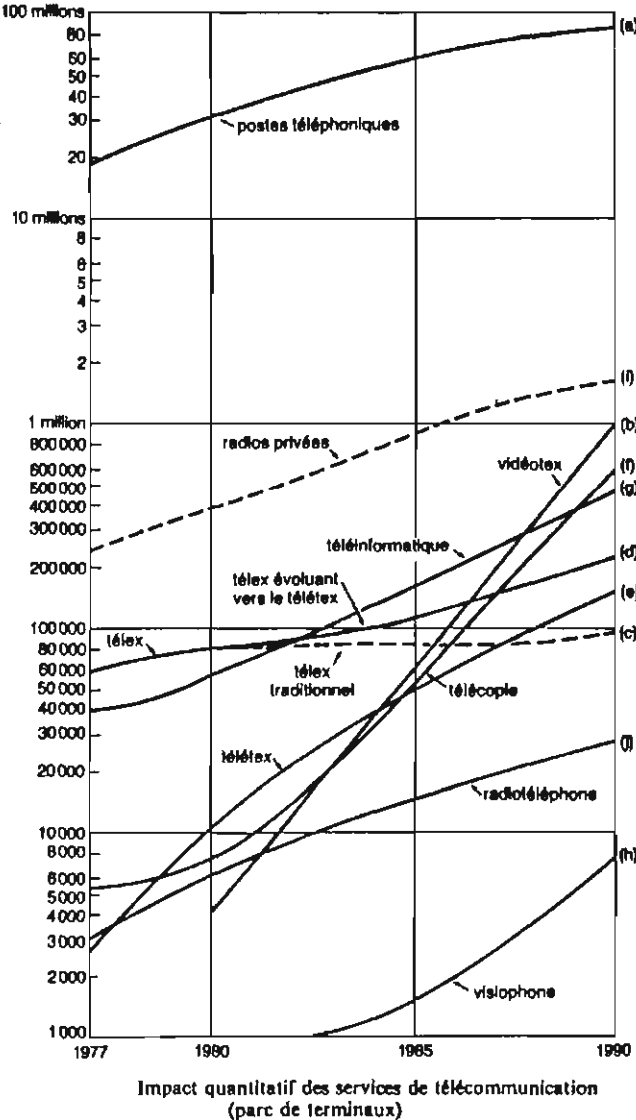GROSS DOMESTIC PRODUCT IN VARIOUS COUNTRIES
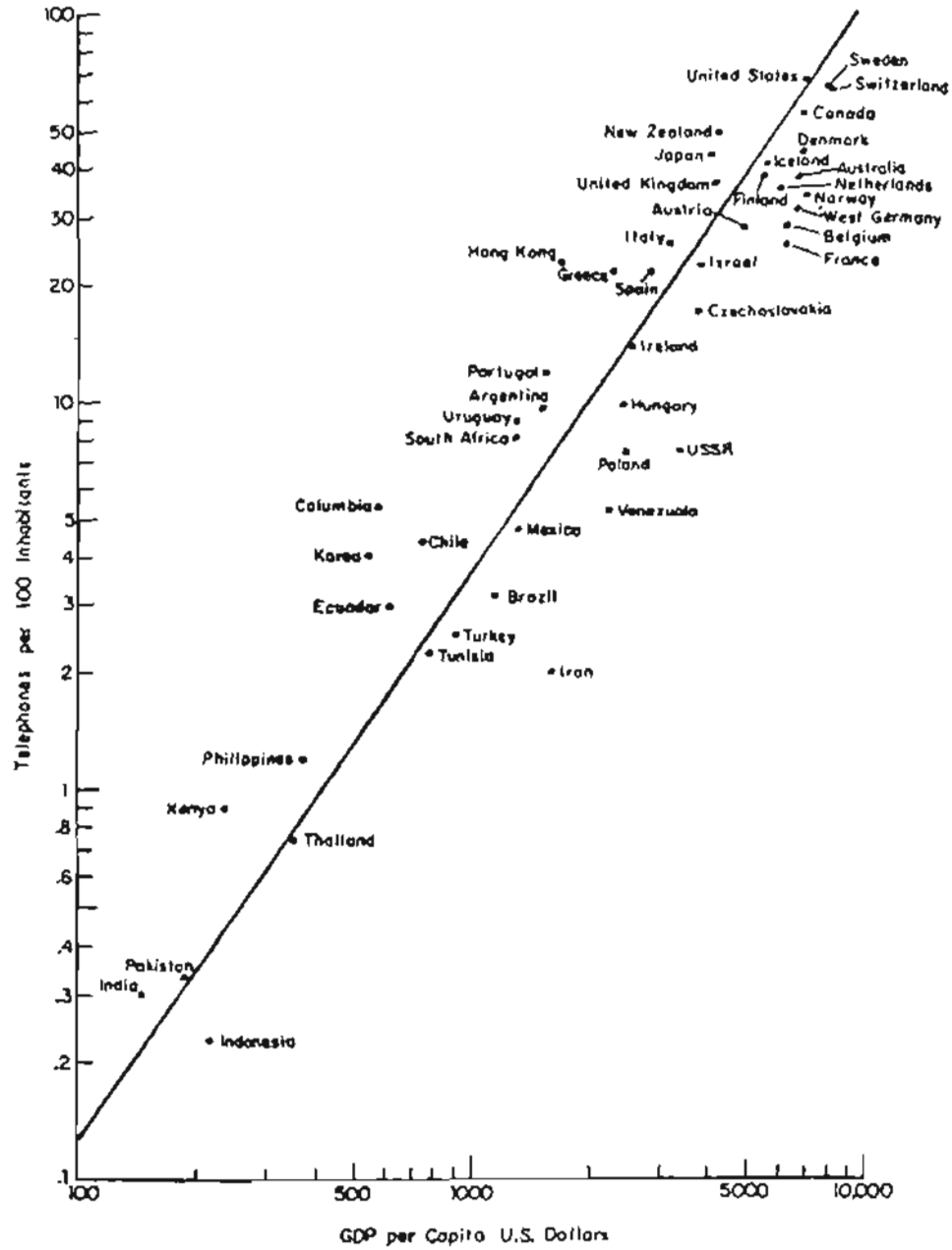
Source: INTELTRADE

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.

(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 ser-

Impact quantitatif des services de télécommunication
(parc de terminaux)

(I) En dehors du terminal annuaire.

8. CNET: QUANTITATIVE GROWTH OF VARIOUS TELECOMMUNICATION SERVICES

vices 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

Sep 82 * CRYPTOLOG * Page 20

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 domes-
tic 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 success-
ful computer services, even though its
microelectronics VLSI technology is as good
as that of the U.S. leader Intel Corp. (Busi-
ness 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 posi-
tion to challenge the U.S. seriously.
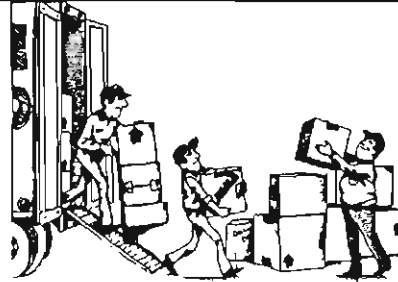
FACTORY SHIPMENTS OF ELECTRONICS

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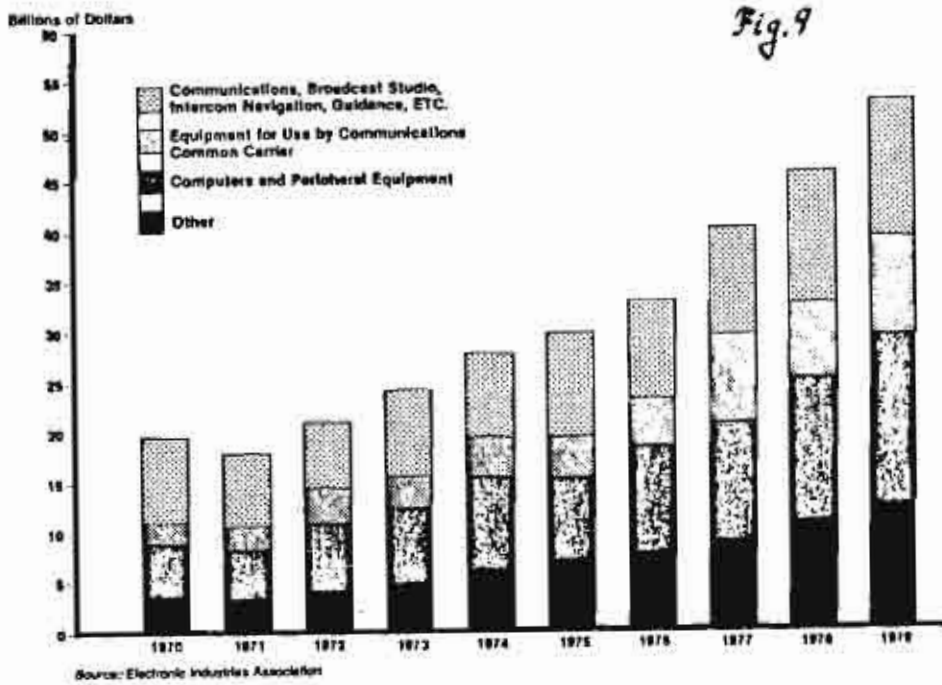more by future demands from "home information"
systems.

                        P.L. 86-36
                        EO 1.4. (c)
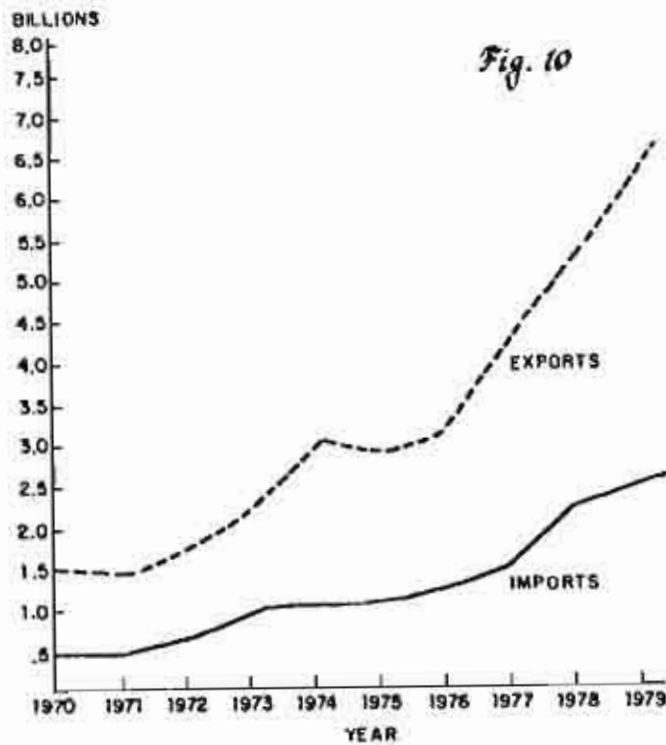
U.S. TRADE IN COMPUTERS

(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. telecommun-
ications industry is fragmented in the name of
competition, more foreign computers, communi-
cation equipment, and services will take over
parts of the U.S. market, e.g., for PBX's,
interconnections, satellite links, data termi-
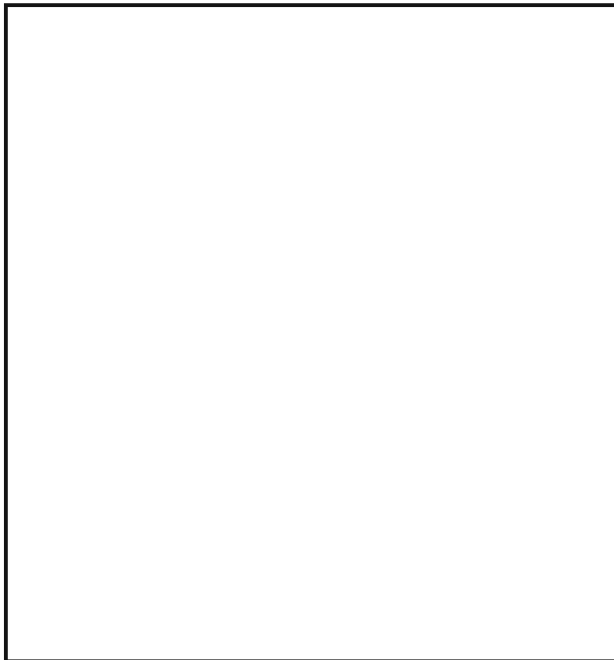nals, and even basic transmission and
switches.

                                       P.L. 86-36
                                       EO 1.4. (c)
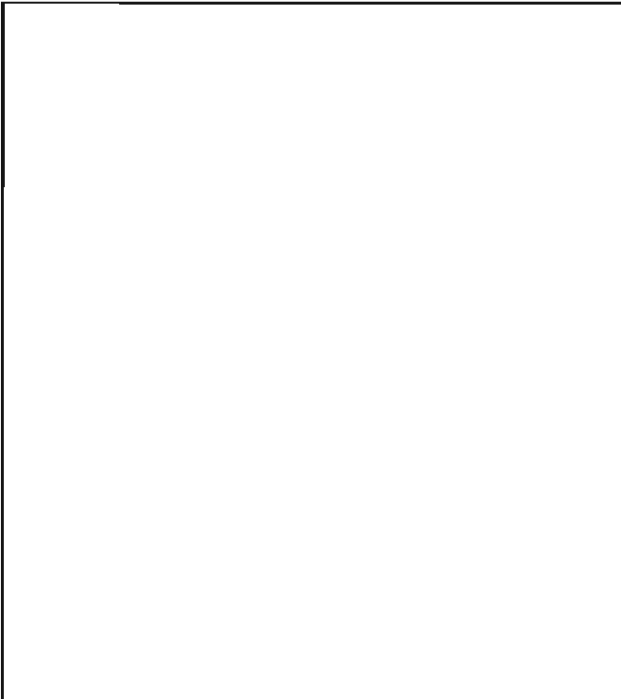
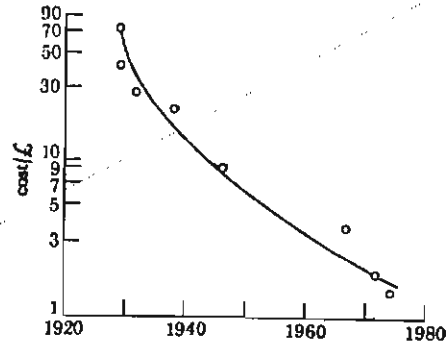## Annual Factory Shipments: Communications and Electronic Equipment by Type, U.S., 1970-1979

Fig. 9

Source: Electronic Industries Association

U.S. TRADE IN COMPUTERS AND RELATED EQUIPMENT

Fig. 10

Source: CBEMA

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 expan-
sion in capacity to the 12,000 two-way chan-
nels in service now.
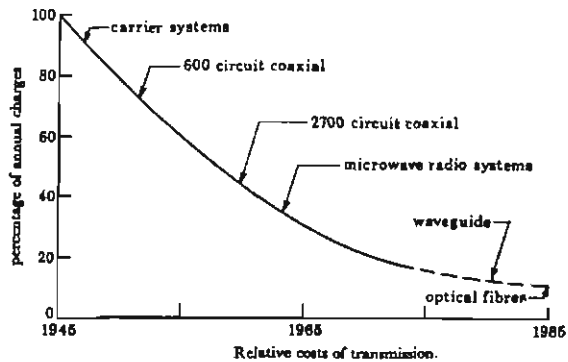
12. TRANSMISSION COSTS FOR DIFFERENT MEDIA

COSTS

(U) At the same time that the civil
telecommunications plant has greatly increased
in size and traffic capacity, the cost of ser-
vices 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 tech-
nology 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, surviva-
bility, etc., so that the unit cost of mili-
tary 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.

Satellite bandwidth cost trends.
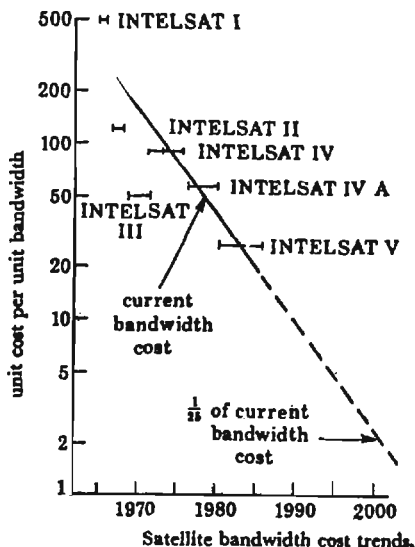
13. SATELLITE BANDWIDTH COST TRENDS

(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.
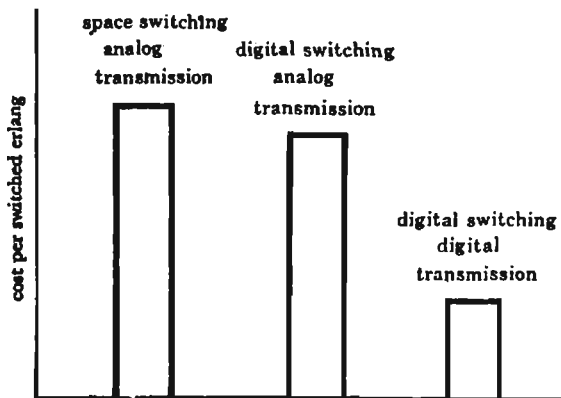
14. TELEPHONE SWITCHING COSTS

(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

Sep 82 * CRYPTOLOG * Page 24

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 SIG-INT 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.
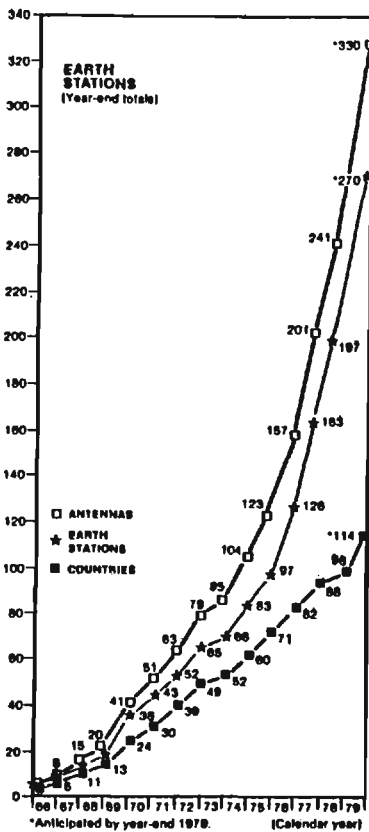
Source: INTELSAT Annual Report, 1979

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
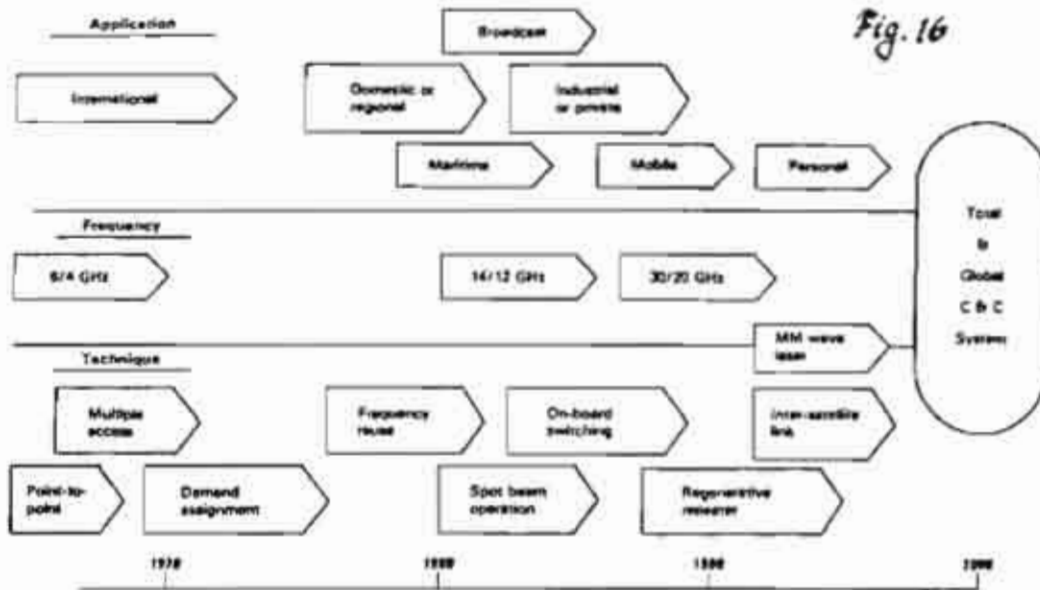
FUTURE OF SATELLITE COMMUNICATIONS

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
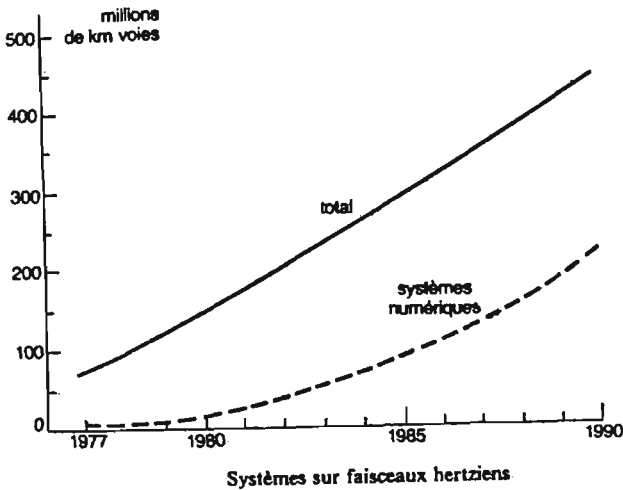
Mbps trunk encryption.

(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.
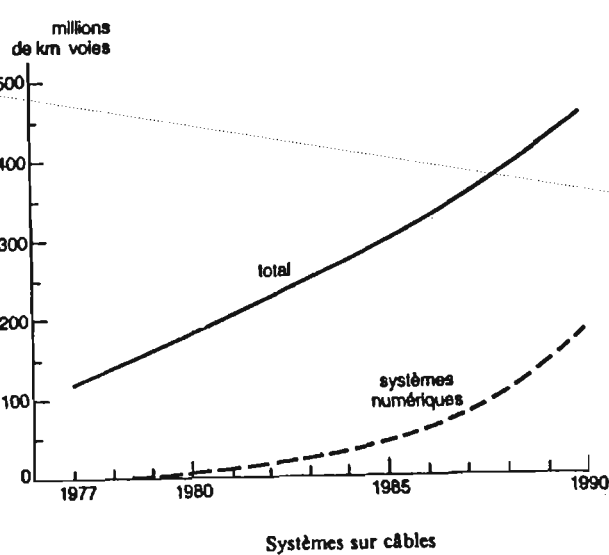
18. GROWTH IN FRENCH CABLE

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

(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.

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.


(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.

ADVANCED MOBILE PHONE SYSTEM (AMPS)
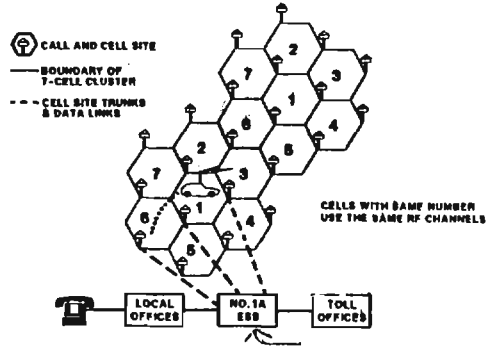
Switched Digital Capability

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
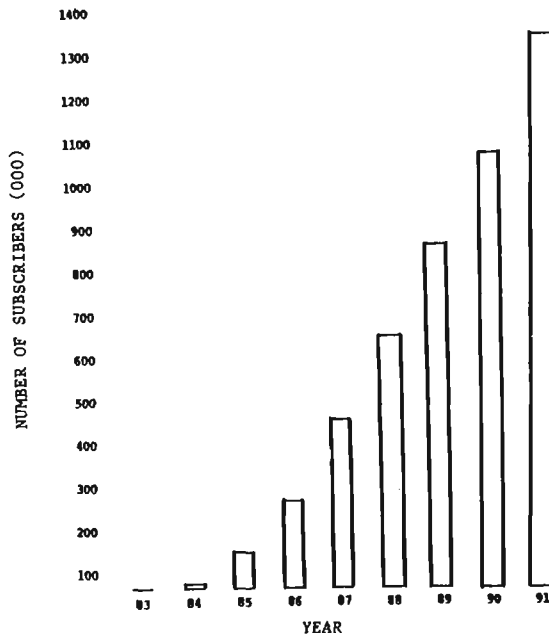
Source: Motorola

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

TOP SECRET

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 [   ] 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!

[   ]
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 [   ] in P14 on 3369s.

P.L. 86-36

SOLUTION TO NSA-Crostic No. 42

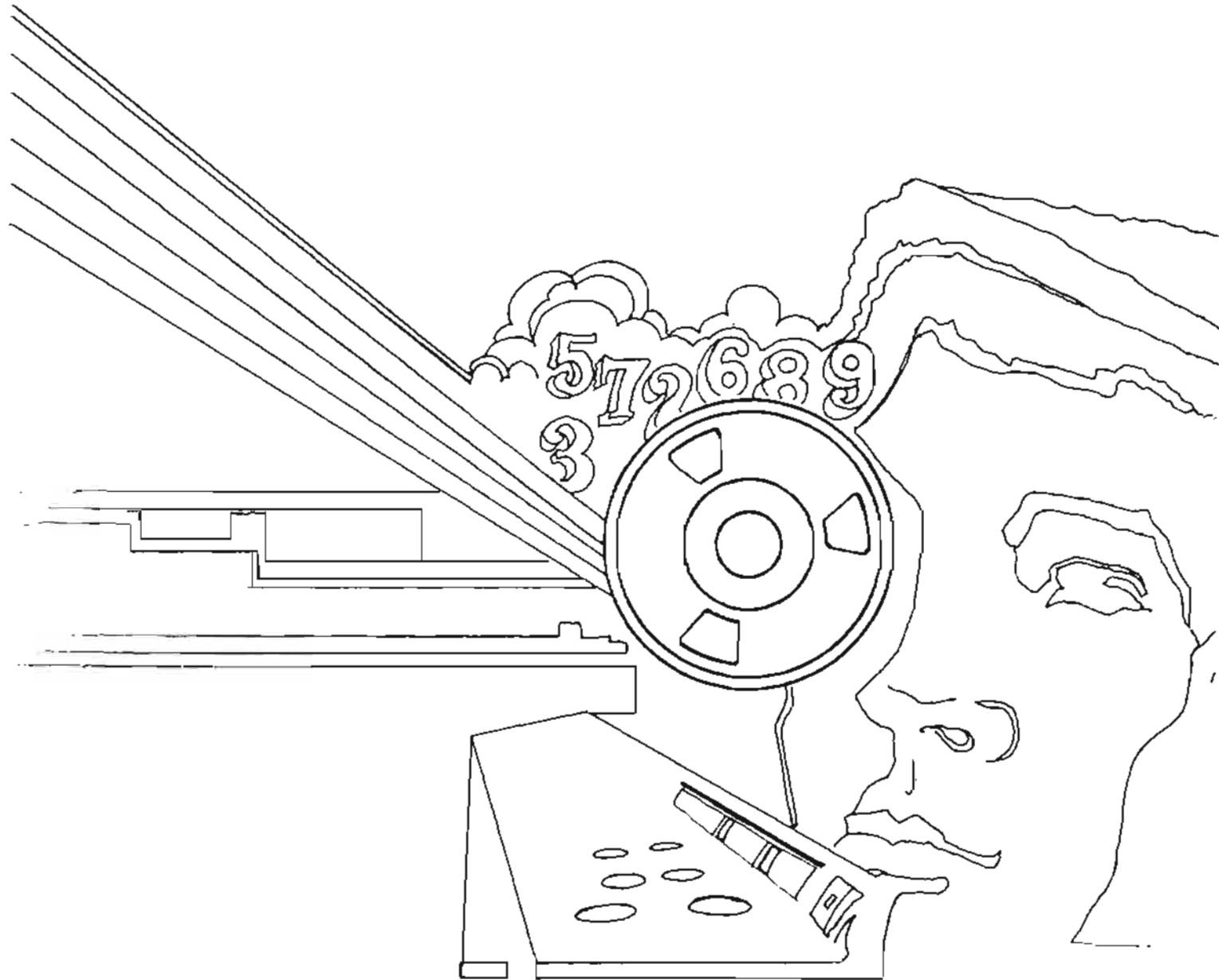[   ] "NSA Information Desk,"
CRYPTOLOG, May 1982

"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) [   ] 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) [   ] 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.

NOT RELEASABLE TO CONTRACTORS   TOP SECRET   HANDLE VIA COMINT CHANNELS ONLY

P1-Sep 82-S3-28567