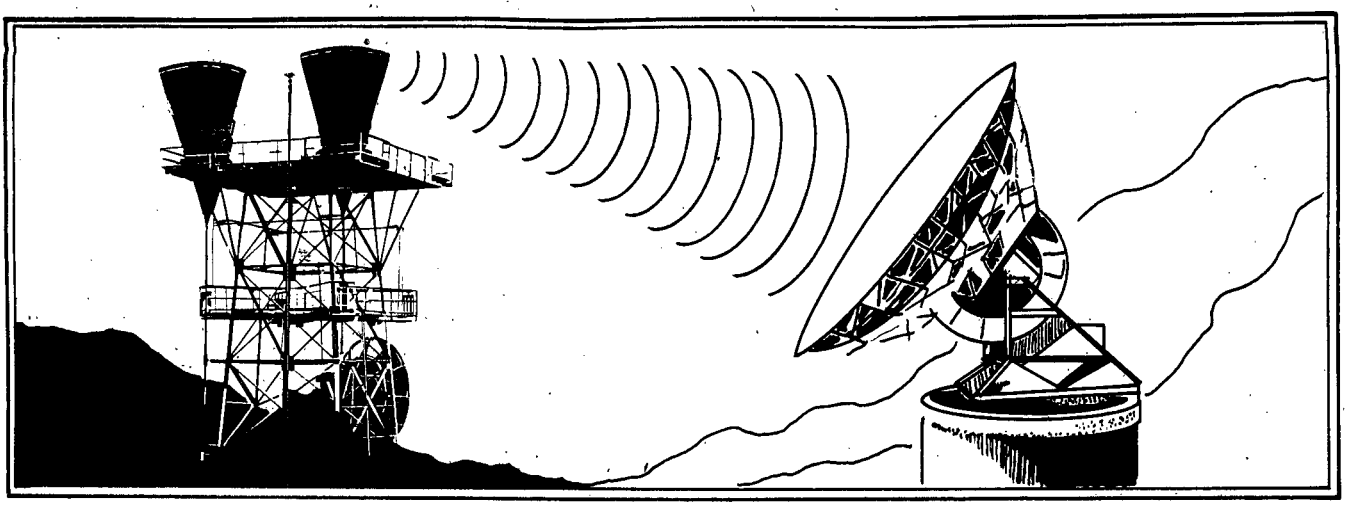


CRYPTOLOGY GOES PUBLIC

David Kahn

As the public demands more security for computerized records, the government weighs its need to protect state secrets.

In November of 1978, a remarkable conference took place in Germany. It brought together for the first time the Allies' backroom boys of World War II and those whom they had outwitted for nearly six years—the cryptographers of the Third Reich. Together with historians, they discussed what had been the most secret part of the intelligence war. This was the Allied solution of the principal German ciphers and consequent ability to read large segments of high-level military traffic, including the very messages of Adolf Hitler to his generals.

An Admiral of the Royal Navy described how his knowledge of U-boat orders enabled him to steer convoys around the wolf packs to help win the Battle of the Atlantic. An American intelligence officer told how foreknowledge of a German attack enabled the Seventh Army to repel it with minimal losses. The Royal Air Force's former scientific intelligence chief recounted how Ultra—as the Allied solutions of German messages were called—gave him the first clues to German V-weapons and enabled the Allies to bomb the research center at Peenemunde and later the launching sites in France. A historian discussed how the American solution of the Japanese diplomatic cipher machine revealed with the Japanese Ambassador in Berlin was reporting to Tokyo about his conversations with Hitler—intercepts that became, Chief of Staff George C. Marshall said, "our chief basis of information regarding Hitler's intentions in Europe."

All of this proved too much for one of the Germans. During the war he had repeatedly assured the Head of the Kriegsmarine, Grand Admiral Karl Dönitz, that the naval Enigma cipher machine was not being solved by the Allies—when, in fact, they were doing so almost solidly and often instantaneously. "If the Allies could read it all," he asked with some asperity, "why didn't they win the war sooner?" An American historian answered, "They did."

It was typical of the traditions of cryptology that the Ultra secret was withheld, from the Germans as well as from the public, for nearly 30 years after World War II ended. Governments maintain this sort of discretion for a number of practical reasons. To reveal how a cryptogram was solved would enable other countries to strengthen their cryptosystems to prevent such solutions. Even to reveal *that* a cryptogram had been solved

The author is with *Newsday*, Garden City, NY 11747.

Condensed and reprinted, with permission, from *Foreign Affairs*, Fall 1979.

0163-6804/80/0300-0019 $00.75 © 1980 IEEE

might awaken other nations' cryptographers to the possibility that their ciphers, too, might be broken and so might impel them to change them. Disclosing the details of one's own cipher systems would obviously nullify their ability to keep communications confidential.

Finally, to admit prying into other nations' messages would embarrass a country and so burden its international relations. In only one case, apparently, did a statesman refuse to read other countries' messages. In 1929, when Henry L. Stimson became Secretary of State, he ordered the closing of the combined State Department-War Department Cipher Bureau on the ground that "Gentlemen do not read each other's mail" and in the belief that mutual trust was the best road to world comity. But the times made it impossible. When he became Secretary of War in World War II, he was one of the grateful readers of intercepted Japanese diplomatic messages—provided by the War and Navy Departments, which had kept their codebreaking groups alive in 1929.

Thus, secrecy about cryptology has been the rule at least since the science became a permanent function of state through the establishment of letter-opening black chambers in the Renaissance. The Venetian Republic's Council of Ten ordained that any cryptologist who betrayed secrets could be put to death. In 1723, Britain's House of Lords asserted in a trial for treason that "it is not consistent with the public Safety, to ask the Decypherers any Questions, which may tend to discover the Art or Mystery of Decyphering." Governments still adhere to this principle as much as they can. In 1933 and again in 1950, the United States enacted laws that impose fines and jail terms for anyone revealing official cryptologic secrets. The National Security Agency (NSA), responsible for U.S. cryptology, operates under the tightest possible security. The same is true of its foreign counterparts.

Secrecy about cryptology has been the rule since the Renaissance.

Secrecy has been relatively easy to maintain because cryptology has been largely a monopoly of governments. Though businessmen have sometimes used codes or ciphers to conceal their messages, they seem almost never to have intercepted and solved competitors' cryptograms.

But it is becoming increasingly difficult to keep the official lid on. With the expansion of radio communications and advances in intercept technology, cryptology has become so extensive an activity of intelligence and security that political and military events will from time to time impinge upon it and expose portions of it. The 1964 clash of the U.S.S. *Maddox* with North Vietnamese patrol boats in the Gulf of Tonkin, the attack upon the U.S.S. *Liberty* during the Six-Day War in 1967, and the capture of the U.S.S. *Pueblo* by North Korea in 1968 revealed some details about American intercept operations. Previously, in 1960, two NSA employees, William H. Martin and Bernon F. Mitchell, defected to the Soviet Union and gave a press conference in Moscow about American code-breaking activities. And the 1974-1975 congressional investigations into the American intelligence community revealed a good deal about the vast scope of NSA's intercept operations.

More recently, cryptology has, perhaps for the first time, become the subject of formal intergovernmental agreement. In the final stages of the negotiations of the SALT II agreements now before the Senate, the American side insisted that the treaty bar "the encryption or encoding of crucial missile test information," as President Carter said in his June 1979 televised address to the Congress on the treaty. Concealing information on missile tests by encryption would make it harder for the United States to ascertain Soviet missile capabilities—and for the Russians to ascertain American.

To prevent this, the treaty provides that "neither party shall engage in deliberate denial of telemetric information, such as through the use of telemetry encryption, whenever such denial impedes verification of compliance with the provisions of the Treaty." But since the treaty does allow encryption when it does not interfere with verification, the question of when encryption interferes and when it does not is being carefully scrutinized in the Senate's deliberations.

But the SALT case is relatively limited and still mainly a government problem. What is today far more interesting and significant is the degree to which new factors are causing cryptology to spill over from the governmental domain into public awareness. Major governments today are not limiting their intercept activities to official communications; they seek to draw intelligence from the communications of tens of thousands of private firms and citizens of all nationalities. The protective countermeasures of target nations necessarily include the private sector. At the same time, concerns about foreign and domestic invasions of privacy have led private firms and individuals to demand security for their stored computerized files and their electronically transmitted messages. To meet the demand, private researchers have invaded the highly technical realms of cryptology that have long been a government monopoly.

In short, what has happened to other technologies, such as atomic energy, is happening to cryptology. It is becoming a public matter, raising a whole new set of public issues.

If one nation is intercepting communications on the territory of another, what is the proper diplomatic response to this? Should a government advise its nationals on protecting their communications from foreign exploitation when such advice might enable other nations

MICROWAVE EAVESDROPPING

In order to develop my subject, let me direct your attention to the scenario of a battlefield in this newest kind of electronic warfare.

You have before you the roadmap of a typical electronic battlefield (see map, below). This is the battle of Washington, D.C. The war is quietly being fought as we now sit in this chamber.

The terminals indicated by the crosses are AT&T microwave long lines towers. The circles are those of the Chesapeake and Potomac Telephone Company, a subsidiary of AT&T. The hexagons belong to the Western Union Company.

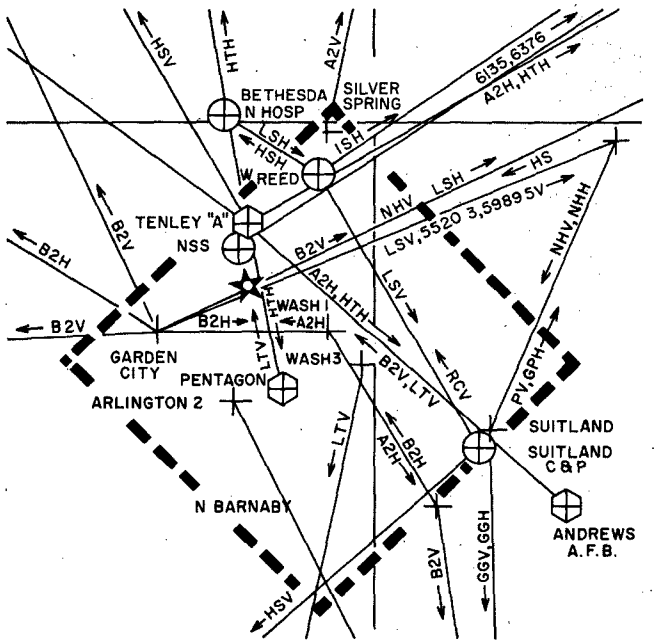
Most long distance telephone calls travel across the country through a vast lattice of thousands of such microwave links.

The great advantage of microwave transmission is its unusually broad bandwidth permitting large numbers of simultaneous talking circuits to exist on a single beam.

The advantage of microwave communication becomes its weakness. By tapping into the microwave beam, the space-age eavesdropper immediately has access to thousands of conversations, data transmissions, and telegraphic messages. A typical microwave link will have a multiple of 1800 voice channels in each direction.

Esoteric electronic snooping into microwave circuits may be achieved at almost any geographical point within the beam paths.

Movement of the Russian embassy to its new Washington, DC, location on Wisconsin Avenue at Calvert Street will place the Soviets in an ideal geographical position for the interception of critical microwave telecommunications circuit paths used by the Pentagon and other facilities carrying national security information.



This new vantage point, indicated by the star in the center of the microwave circuit map, will fix the extraterritorial eavesdropping facilities of the Russians directly astride two microwave beams each terminating in the "Garden City," Arlington, Virginia, telephone tandem switching station. The opposite ends of these links each respectively terminate in Beltsville and in Gambrills, Maryland. One of these circuits is a primary North-South trunk line for the eastern seaboard and interconnects the Langley, Virginia, facilities of the Central Intelligence Agency with Baltimore, Philadelphia, New York, and Europe. The other circuit carries much of NASA's missile and satellite tracking and data information.

Plans are now underway to neutralize this vulnerability by scrambling messages, by reducing electronic accessibility, and by reducing physical accessibility through direct burial of coaxial cable.

Enough is said here about the activity of foreign agents intercepting domestic telecommunications. Perhaps it is expedient that the discussion turn toward the main subject of this presentation, namely the interception of the communications of American citizens by the American intelligence establishment without benefit of court order under the criminal standard or under the noncriminal standard as proposed in several versions of S. 1566.

I ask you to look again at the diagram of the battle scenario. The microwave stations designated by circles all belong to the Chesapeake and Potomac Telephone Company. Each station is on a military facility. Among these are the National Security Agency at Fort Meade, the Naval Intelligence Support Center in Suitland, Maryland, and the Army Facility at Ft. Belvoir, Virginia. It may be seen also that there is an interconnection between this system and the local C&P Telephone Company circuits, and that there is an interconnection with the nationwide microwave domestic telephone system owned by AT&T.

The foregoing has little real significance taken by itself. The military require special high-volume circuitry, and at times it must interconnect with the national domestic system for service. The military must talk back and forth among its elements, both here and abroad.

The significance of the system shown interconnecting our domestic telephone system and the several secret military facilities is that a greater portion of these circuits are one way, receive only beams!

It is understandable that radio and television, weather, and press wire communication services would require only one-way circuits. It is not understandable that the National Security Agency would require thousands of times the circuit capacity of the world's press services combined, AP, UPI, Reuters, etc., except that these one-way circuits are thousands of remote wiretaps!

The above is adapted from the testimony of David L. Watters given during hearings before the Subcommittee on Intelligence and the Rights of Americans of the Select Committee on Intelligence of the United States Senate, Ninety-Fifth Congress, Second Session on S. 1566, Foreign Intelligence Surveillance Act of 1978.

to better protect their own communications and so deny the parent government valuable communications intelligence? May private individuals develop and publish cryptographic techniques that, because of their advanced nature, could also deprive a parent government of communications intelligence? Do First Amendment rights take precedence over the needs of national security?

We are only beginning to see the shape and scope of these and other issues raised by cryptology as it goes public. This article seeks to explore some of them.

Is There an Unbreakable Code?

A few words about terminology may help. "Cryptology" encompasses signal security and signal intelligence. The former includes all ways of keeping secret both human messages, such as telegrams and telephone conversations, and electronic messages, such as computer-to-computer data exchanges. Signal intelligence comprises all methods of extracting information from transmissions. These methods can include identifying radars or translating telemetered data of intercontinental ballistic missiles in flight. Other methods deal largely with human communications. Among these are interception of messages in plain language; traffic analysis, which matches radio call signs to particular military or other headquarters and draws inferences from the volume of traffic on various radio circuits; and cryptanalysis, which breaks the codes or ciphers that armor messages. These three are generally grouped together as communications intelligence, or COMINT.

Nonspecialists frequently ask two questions about cryptology. Is there an unbreakable cipher? There is indeed one that is absolutely unbreakable. This is the one-time pad. It cannot be used in every situation because it requires as many random letters for its key as in all messages that will ever be sent, and this presents an insuperable distribution problem. It can serve in restricted situations, however, as in spy messages and on the Moscow-Washington hot line. There are also many ciphers that, properly used, are unbreakable in practice, since the cryptanalyst cannot assemble enough text to analyze their complexities. Because they do not have the disadvantage of the one-time pad, such systems serve in most military and diplomatic networks today.

The other question is: Have computers not made it possible to solve all ciphers? They have not. Modern cipher machines are in effect special-purpose computers themselves. Since doubling the encryption capacity appears to square the number of trials the cryptanalyst has to make, the codemaker can always stay ahead of the codebreakers.

Telephone "Bugs"

In 1975, the Rockefeller Commission on Central Intelligence Agency activities revealed that the communist countries "can monitor and record thousands of private telephone conversations." News stories later said that the Russians not only could but did monitor "millions" of domestic American telephone calls—100 000 a year in the Washington area alone. Then President Carter, at a news conference, acknowledged that "within the last number of years, because of the radio transmission of telephone conversations, the intercept on a passive basis of these kinds of transmissions has become a common ability for nations to pursue."[1]

How did this happen? How do they do this?

Since 1950, telephone companies have increasingly sent conversations—both between people and between computers—from city to city by microwaves. These are radio waves beamed on a line of sight from a transmitter through several relay towers, usually perched atop hills about 25 miles apart, to the receiver.

Radio is easy to intercept. Each relay radiates enough energy for an eavesdropper to pick up the microwave signal five to ten miles away. The antenna for this would have to be a ten-foot dish, but "the interceptor can make use of a number of innocent-appearing structures such as apartments, houses, sheds, barns or a specially outfitted van," says a recent study made for the White House.[2] If the interceptor can get closer to the beam, he can use smaller and less obtrusive equipment. None of this is either very difficult or very costly—around $60 000, according to the study. The real problem arises in trying to pluck a particular person's conversations out of the incredible welter of calls.

The evolution of computers made individual targeting feasible. A computer can count the clicks of a telephone dial or the beedledybeeps of multifrequency pushbutton calling as they pour in torrents over the microwaves. It compares that number with a list stored in its memory. If it finds no match, it discards the call and passes to the next. But if a match exists, the system "drops" the intercept onto a tape recorder for human analysis.

The Soviet Union, acting through disguised intermediaries, has almost certainly rented houses near important microwave routes and filled them with the sophisticated electronic gear needed for interception. Senator Daniel Moynihan has said that the Russians are listening in their consulate in San Francisco, their mission to the United Nations in New York, and their apartment house in the Riverdale section of the Bronx. The two locations in New York, he states, provide "extraordinary access to telephone traffic in the whole of the New York metropolitan area, and in particular to that of the financial, commercial, and legal communities of Manhattan."

---

[1] *Public Papers of the Presidents of the United States: Jimmy Carter, 1977*, vol. II. Washington, DC: GPO, 1978, p. 1234.

[2] Mitre Corporation, McLean, Virginia, *Study of Vulnerability of Electronic Communication Systems to Electronic Interception*, prepared for the Office of Telecommunications Policy, January 1977, Department of Commerce: National Technical Information Service, PB 264447 and PB 264448. vol. I, p. 17.

Cartoon by Bob Englehart; reprinted courtesy of the artist.

Though the aerials on the present Soviet embassy on 16th Street in Washington a few blocks north of the White House are designed for legitimate shortwave transmissions and not for interceptions, the Russians got lucky with their new embassy on Tunlaw Road, on one of the highest hills in Washington. When they were assigned the land, private telephone monitoring was unknown, and no one took into account that the site bestrides some important microwave beams. A primary telephone trunk group for the eastern seaboard runs close by on the relay between microwave towers in Arlington, Virginia and Gambrills, Maryland. A Defense Department digitized voice circuit from the Pentagon to Western Union's Tenley Tower on Wisconsin Avenue passes almost directly over the site.

Late in 1977, the Soviet Union added another new and important mode of interception when it installed big antennas in Cuba to monitor communications sent by satellite. These comprise telephone calls, telegrams, and computer data moving between the United States and 55 other nations. The messages are directed upward to one of seven satellites hovering 22 300 miles above the Atlantic; the satellite then retransmits them back down toward a receiving station on the ground, usually on the other side of the ocean. But the downward beam spreads widely, and even from outside its fairly large "footprint" on the surface of the earth it is easy to pick up its signals, though the cost of a steerable 30-m dish for such interception has been estimated at $1.5 million.

All this seems an extraordinary effort to gain information that on its face does not seem very important. Why does the Soviet Union do it?

One reason is that codebreaking no longer yields the quantities of central information it once did. The transistor and large-scale integration of electronic circuits, which make pocket calculators so cheap, have placed excellent cipher machines within the price range of more countries than ever before. This means fewer codebreaking results, and this reduction has driven the Soviet Union, as well as the United States, to gather information from the unencrypted, plain language messages—both human and computer—that pass over telephone circuits. Though plain language intercepts seldom provide the insight that cryptanalyzed ones do, they have their strengths. "Anyone listening in to a senator's telephone conversations for two weeks would own him," says one senatorial aide with tongue only halfway in cheek.

Another reason for the shift to telephone eavesdropping is that it can provide quantities of a kind of information that is becoming more and more important: eco-

nomic intelligence. Information that might warn of dollar or energy crises is becoming as critical as military and diplomatic information. The Soviet Union, for example, is reported to have used its intercepts of American grain dealers' telephone conversations to advantage in its big grain purchase. Monitoring the data flowing by microwave and satellite in domestic and international time-sharing computer networks could reveal financial transactions of giant multinationals.

The United States, too, is seeking economic intelligence through interception. In its leaked 1976 report, the House Intelligence Committee said that American signals intelligence "in this area has rapidly developed since 1972, particularly in reaction to the Arab oil embargo" and the Soviet grain deal success. Recently it was reported that intercepts of oil-producing nations' messages warned the U.S. government of their intention to raise oil prices.

Almost certainly, too, the United States eavesdrops extensively on communications within the Soviet Union. Monitors at the embassy on Tchaikovsky Street in Moscow are known to have listened in on the limousine radiotelephones of Soviet leaders, even though they apparently got only scraps of intelligence (including, according to a columnist, views on the ability of a favorite masseuse). It seems likely that such activities are targeted as extensively as possible on other Soviet internal communications, particularly those of a sort that would be between private citizens in America. No doubt the Western powers get fewer intercepts from East European countries and the Soviet Union than those powers obtain in the West, but because information is harder to come by in the communist closed societies, the West's intercepts are more valuable.

The National Defense

As these new techniques become known, the two superpowers are taking steps to close them off. And these steps have generated some of the new controversy and discussion. What are they?

The Soviet Union has flooded the American embassy with nonsignal-carrying microwaves, apparently to jam the American eavesdropping devices.

But that is not a solution in the United States, as much for environmental as for technical reasons; nor is a proposal by Senator Moynihan, who grew incensed about the apparent double standard applied against interceptions. "We are standing around in the Rose Garden pinning medals on one another for having discovered that the FBI is tapping somebody's telephone," he said, but nobody is doing anything about the Soviet intrusions. He introduced a bill that calls upon the President to declare *persona non grata* any individual with diplomatic immunity who is "willfully engaging in electronic surveillance on behalf of a foreign power."

One problem with this idea is that the Russians might retaliate in the same way against American eavesdropping. Another is that expelling a foreign eavesdropper might cause more loss than gain. For the United States has apparently learned about Soviet eavesdropping mainly by "piggybacking," or intercepting Soviet transmissions of their urgent American intercepts back to Russia for analysis. To reveal details officially might compromise the source.

Probably for these reasons, the executive branch has rejected the Moynihan proposal. What then is the United States doing to deprive the Soviet Union of this intelligence? It is undertaking a multimillion-dollar program to protect American domestic communications. On February 15, 1979, the White House issued a three-page, single-spaced National Telecommunications Protection Policy directive. It divides messages into three categories and specifies different safeguards for each.

The U.S. apparently intercepts Soviet transmissions back to Russia of their intercepts of American messages.

"Government classified information relating to national defense and foreign relations"—military and diplomatic messages—will come, as before, under the control of the National Security Agency, the government's cryptologic body. It has already transferred many sensitive telephone circuits from microwaves to buried cable, and is expanding the Electronic Secure Voice Network. This uses telephone scramblers.

The other two categories will be handled by a new Special Project office in the Commerce Department's National Telecommunications and Information Administration. Associate Administrator Donald Jansky has an annual budget of $2 million and 20 experts for the job, the main part of which he expects will last 5 years. His teams have already spoken to almost a dozen telecommunication common carriers on how to protect messages in the second category: "unclassified information transmitted by and between government agencies and contractors that would be useful to an adversary." Some companies are looking into such matters as the practicability of bulk encryption to scramble all messages transmitted over a particular microwave link. The teams will also survey the needs of government agencies and will recommend particular cipher systems to them.

The third category consists of "nongovernmental information that would be useful to an adversary." Examples that Jansky gives include the strategy to be used by American firms in negotiations against foreign competitors, changes in the prime interest rate, crop forecasts, the availability of critical materials, and developments in advanced technologies. The White House directive requires that such information "be identified and the private sector informed of the problem and encouraged to take appropriate measures." Jansky's office will draw up guidelines for evaluating types of protection systems that the firms will probably buy.

The entire program comes under a National Security Council subcommittee that will settle jurisdictional disputes between Commerce and NSA. It marks the first time that any government has ever dispensed advice on codes and ciphers to the public. Jansky predicts that for the carriers and private firms the cost will reach "probably in the billions."

Protecting Private Citizens' Records

The new program is linked to the rising debate on cryptology in another way as well. One of the cipher systems that it will recommend to some government bodies and contractors lies right in the crossfire of the argument over whether foreign code-cracking intelligence is more important than protecting citizens' privacy by giving them good ciphers. The cipher is known as the DES, or Data Encryption Standard. As bank cash-dispensing machines grew in number, bank officers became concerned that the wires between these machines and the central office computer could be tapped to gain information and then used to "tickle" a money machine to make it disgorge its average cash holdings of $20 000. So the International Business Machines Corporation devised a cipher to encrypt the identifications, amounts and account numbers passing over these wires. Modern semiconductor techniques enabled it to be extremely complex and yet embodied on an integrated-circuit ceramic "chip" the size of a thumbnail: it is the tiniest known "cipher machine" ever produced.

In 1973, the National Bureau of Standards, responding to the increasing public concern about data privacy—such as the confidentiality of individuals' Internal Revenue Service files—solicited for a standard cipher. Government agencies would have to use it when encrypting personal files, and private firms would have to use it when communicating with these agencies in secret mode. By far the best system submitted was IBM's.

It was, in fact, so good that a miniature debate seems to have broken out in secret between the two halves of the National Security Agency, which was advising the Bureau of Standards. The codebreaking side wanted to make sure that the cipher was weak enough for NSA to solve it when used by foreign nations and companies. The codemaking side wanted any cipher it was certifying for use by Americans to be truly good. The upshot was a bureaucratic compromise. Part of the cipher—the "S-boxes" that performed a substitution—was strengthened. Another part—the key that varied from one pair of users to another—was weakened. In this form the government proposed its adoption as the Data Encryption Standard for nonnational security messages and files and for interfacing with the private sector.

Defense secrecy needs vie with public demand for protection of each individual's computerized records.

At once a storm of controversy broke. Computer scientists and mathematicians clamored that the DES was still too weak. NSA, they contended, had no right unilaterally to decide a question of such importance to so many people. They also said it was possible that IBM and the code agency had built a "trap door" into the cipher that it alone could spring to reach a solution, and argued that lengthening the key was necessary to afford proper protection to personal records. The Bureau replied that the cipher was strong enough and that lengthening the key would increase the cost of encipherment unacceptably. So vociferous did this first national debate on cryptology become that the Standards Bureau set up two workshops on the DES. These vented some of the criticism but otherwise nothing changed. As of July 15, 1977, the DES became the official government civilian cipher.[3]

Later the Senate Intelligence Committee Staff investigated the matter. It issued a report saying that no one had exercised any improper influence on anyone else and noting that the NSA had recommended the cipher for use by the Federal Reserve Board. For the present, the furor has abated. DES chips are now being manufactured by half a dozen firms, and it is a sign of the new interest in secret communications that the DES bids fair to become what no other cipher ever has been: profitable in sales to business. The American Banking Association has endorsed it. (The protection of the security of financial transfers is, of course, a matter of grave private concern. But there is also a possibility that hostile elements or terrorists, if they could break into the system, might introduce spurious messages designed to throw the whole financial system into chaos.)

But in five or ten years advances in computer technology will so greatly reduce the time needed to crack the DES—a time now measured in years, even with the fastest computers—that the cipher will have to be strengthened. The debate will resume. It will again bring into confrontation the needs of national security through codebreaking and those of individual liberties through codemaking.

Free Inquiry into Cryptology Versus National Security

Another great debate in cryptology continues to simmer. Should free inquiry be allowed in the field, or are its implications for national security so great and so sensitive that research should be controlled by the government?

For a long time this issue did not really exist. The only cryptologists outside NSA, with its squadrons of brilliant

[3]Department of Commerce, National Bureau of Standards, *Data Encryption Standard*, Federal Information Processing Standards Publication 46, Department of Commerce: National Technical Information Service, January 15, 1977.

dedicated mathematicians and engineers backed by banks of the biggest and fastest computers, were a few hundred hobbyists who solved pencil-and-paper cryptogram puzzles. The spread of computers and of data communications began changing that. Whereas stealing a paper file required physical access to it, stealing data that were stored and transmitted electronically could be done by copying them at a remote terminal. Computer crime, wiretapping, and terrorism made this threat real. One defense was encryption, and computer scientists in many firms and universities began studying it; the DES is a product of this interest. Very rapidly the quantity and quality of information on cryptology being circulated outside of government channels exceeded by far what it had ever been before.

The expansion was accelerated by Stanford University scientists' development of public key cryptography, the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance. Unlike standard cryptosystems, such as the DES, in which the same key serves both to encrypt a message and to decrypt it, public key cryptography employs one key to encrypt and another to decrypt. The two keys are mathematically related to one another, and each user possesses a pair. He makes one key public. The other he keeps secret. Suppose user *A* wants to communicate secretly with user *B*. He looks up *B*'s public key and encrypts his message to *B* in it. *B* applies his private key to decrypt the message. Thus anyone can send *B* a secret message, but only he can read it. This asymmetry can eliminate one of the most vexing problems in practical cryptography: distributing keys to a correspondent before secret communication can be started with him. A twist makes possible what has never been possible before with electronic messages: unforgeable signatures.

The seeming impossibility of these schemes, their boldness, and their elegance have attracted numbers of first-rate mathematicians to cryptology. There is now, for the first time, an informal network of scientists who can do sophisticated mathematical cryptology.

Suddenly the nation is faced with a problem it has never had before—an information explosion in cryptology. NSA worries that any mention of codebreaking might make other nations change their codes. This happens far less often than the agency likes to think. In 1941, for example, Japan did not change its principal diplomatic cipher despite an unequivocal report that the United States had broken it. Nor did the German navy alter its systems in World War II, despite much suspicion. Several of the countries named by the defectors Martin and Mitchell in 1960 as having had their codes broken by NSA did not change them thereafter. But more cautious nations do replace their cryptosystems upon suspicion of solution, and NSA fears that all the new activity in cryptology may not only dry up the flow of foreign intelligence but also inadvertently expose principles used in American ciphers. All of this has caused it to ask whether the right of unrestricted inquiry is worth the national security losses. The issue has surfaced in three recent episodes.

One dealt with inventors of cryptographic systems. Dr. George I. Davida, a bright and articulate Professor of Electrical Engineering and Computer Science at the University of Wisconsin, had applied for a patent for a cipher device using advanced mathematical techniques. The law requires that, if competent government authority deems that disclosure of an invention "would be detrimental to the national security," the Commissioner of Patents "shall withhold the grant of a patent." On the advice of NSA, the commissioner ordered that Davida's invention be kept secret. The University's Milwaukee Chancellor protested that the secrecy order had "a chilling effect on academic freedom." The NSA Director argued, on the other hand, that the decision to seek a patent implied a profit motive, not academic freedom. "If the individual had elected to publish in academic journals there would have been no question of a secrecy order," he said. But this dodged the fundamental issue of whether publication of Davida's work would have impaired the government's cryptologic operations.

NSA fears other nations may change their codes due to the information explosion in cryptology.

While this matter was working its way through the government and university bureaucracies, the Commissioner of Patents imposed another secrecy order. This was against a "phaserphone" voice scrambler which would let CB and telephone users who had it chat without being overheard by others. The four estimated that the device could sell for $100 and could have a large commercial market. The leader, Carl R. Nicolai of Seattle angrily charged that the secrecy order "appears part of a general plan by the NSA to limit the privacy of the American people. They've been bugging people's telephones for years and now someone comes along with a device that makes this a little harder to do and they oppose this under the guise of national security." (The 1974-1975 investigations revealed that NSA had in fact listened to the conversations of 1650 Americans and had intercepted millions of private telegrams up to the mid-1970's.)

The storm of publicity led to a quick about-face by NSA. It lifted the secrecy orders on both applications. But the agency's vacillation suggested that it had not resolved within itself the issue of freedom versus security that the incidents had raised.

The third episode began when an eccentric NSA employee, J.A. Meyer, wrote on his own a letter to the Institute of Electrical and Electronics Engineers, Inc., which was holding a session on cryptology as part of a symposium in Ithaca, New York. Meyer warned the IEEE that the session and articles on cryptology that it had

published might violate the government's International Traffic in Arms Regulations.[4] These implement the law authorizing the President "to control the import and the export of defense articles and defense services." On the U.S. Munitions List that enumerates these articles, which include guns, ammunition, and warships, are, in Category XIII(b), "speech scramblers, privacy devices, cryptographic devices," and ancillary equipment.

To export a warplane or a cipher machine, the exporter must apply for a license, which the State Department grants or denies after consultation with the Defense Department. (It is easy to evade these controls for cipher devices, some manufacturers note. They ship the mechanisms to the foreign country's Washington embassy, which then sends them home by diplomatic pouch.) But the regulations also require a license to export "technical data" touching these "implements of war." "Technical data" are defined very broadly. They cover "any unclassified information that can be used . . . in the design, production . . . [or] operation" of any Munitions List items as well as "any technology which advances the state of the art or establishes a new art in an area of significant military applicability." At the same time, the regulations in effect define "export" very broadly. Before publishing something in a periodical with subscribers outside of the country, the writer must seek government approval, the regulations say. They declare that "an export occurs whenever technical data . . . is disclosed to foreign nationals in the United States (including plant visits and participation in briefing and symposia)." This seems to mean that every time someone publishes a paper or gives a talk at a conference on cryptology or on any of the other items on the Munitions List without government approval, he is breaking the law. These regulations seem never to have been tested in court.

When Meyer's letter reached IEEE, officials cravenly urged authors of papers on cryptology to clear them with the government. As a consequence, some of the speakers conferred with their universities' lawyers, and the Massachusetts Institute of Technology suspended distribution of a monograph on public key cryptography. There was a flurry of news stories. But in the end, all the papers were read—though one tenured professor read papers by two of his graduate students to protect them—and the mailings resumed.

For a while, many people thought that NSA was behind the Meyer move. But the Senate Intelligence Committee cleared the agency of this charge. What has not been clarified is the threat of government crippling of research posed by the arms regulations. The present Director of the NSA, Admiral Bobby Inman, is seeking first to calm the waters. "I am striving," he said, "to open up a dialogue" between the agency and industry and academia. He is doing so by talking to private researchers, giving interviews to the press, and making a speech in public. No other Director has ever thus come out officially from behind NSA's triple barbed-wire electrified fence at its Fort Meade, Maryland, headquarters; Admiral Inman says he is doing so out of concern that a bad press might harm recruitment.

[4] *Code of Federal Regulations*, Title 22, ch. 1, subch. M.

"THE LINE FORMS AT THE REAR, PAL!"

Cartoon by Doug Marlette; reprinted courtesy of the artist.

Inman's substantive proposals on cryptologic research flow from his "deep convictions that the national security missions entrusted to the agency are in peril." He is considering imposing restrictions "on domestic dissemination of nongovernmental technical information relating to cryptology," although he would limit this to "a central core of critical cryptologic information that is likely to have a discernible adverse impact on the national security." It is rumored that he is seeking a law for cryptology analogous to the Atomic Energy Act, which places under government control not just government-generated secrets but "all data" concerning atomic

Who can foresee where future critical areas may lie?

weapons and "special nuclear material." Present laws on cryptology deal only with government secrets. NSA has sought to have cryptology included among the "critical technologies" whose export would be controlled under law.

But George Davida, his erstwhile opponent in the patent secrecy dispute, sees many problems in this approach. Who can foresee where the critical areas are? Microprocessors—which put practically an entire computer on a single chip—may confer greater cryptologic ability on a country than all the seminar papers ever given. Yet they are not cryptologic in themselves. Mathematicians working with no thought of cryptology may find that their work touches upon it directly. Complexity theory, which deals with how hard some problems are to solve, is a current example. "How are you going to clamp down on complexity theory?" Davida asks. "And to turn a complexity theorem into encryption is trivial. If Inman is trying to monitor everything, he'll find it very hard. In universities, where we have to keep up with new developments in computing science for our livelihoods, we find it hard."

Nor are the problems confined to the United States. They are as universal as science. Several nations, among them France and West Germany, have passed laws requiring that stored or transmitted personal data be encrypted where necessary. Work is under way to create effective protocols.

Another problem is the variability of practice among governments in dealing with encrypted information coming into their territories by cable or radio. Some countries impose no restrictions; others require knowing the cryptosystem used. Some countries insist upon this for domestic communications as well. For most nations, the new public awareness of cryptology has not yet become a major concern of their governments. Even in Britain, where the most public work is being done, persons studying cryptology have not gotten the feeling that the government cryptologic agency is trying to discourage the activity. But there seems little doubt that such concerns will eventually emerge.

The Future: An Ongoing Debate

Davida and Inman, at odds on a number of points, agree on others: cryptology is no longer a government monopoly; the debate is just beginning; it will be political; it will attract many participants. Davida thinks that the question of government regulation in the field is a matter that "each person must decide for himself." Inman says that the question has to be "fully examined by the executive branch, the Congress, and the interested segments of the public."

But the examination itself may raise more difficulties than it settles. Is it paradoxical to seek public resolution of a matter that deals in secrets? Will it be done by legislation or executive order—or not at all? How can one balance the conflicting demands of national security and individual freedom?

The problems are almost impossible to predict. Will the experts in the National Security Agency (who are reported to have invented their own type of public key cryptography some years ago), be able to stay a step ahead of the inventors, or will their closed work system eventually be matched (as it may have been in that case) and even surpassed by the open interactive community of bright scientists who refuse the restrictions and nonrecognitions of work in a clandestine agency? Will the study of cryptology become an epidemic that even all the government's resources will be unable to stem?

So cryptology, in 1945 a nation's most closely held secret, has gone public. But not even the procedures or forums for coming to grips with the new problems have been settled on. Their evolving substance will be harder still to resolve.

David Kahn was born in New York City in 1930 and received the B.A. in social science in 1951 from Bucknell University, Lewisburg, PA. After graduation he became a reporter for the Long Island daily *Newsday*, working there from 1955 to 1963. His hobby had been cryptology since the age of 13; he has been a member of the amateur American Cryptogram Association since 1943. In 1960, an article on codes and ciphers in *The New York Times Magazine* that documented the defection of two Americans from the National Security Agency led to a contract for the book that eventually became *The Codebreakers: The Story of Secret Writing*. Kahn quit *Newsday* to write the book and, when it was nearly completed, moved to Paris and took a job there on the international edition of the *New York Herald Tribune*. He returned to New York after two years, when, in 1967, Macmillan published the book, which has been called "the classic in its field."

After beginning the study of German at Berlitz, Kahn went to Freiburg-im-Breisgau in 1969 to examine documents in the German military archives for a book on German military intelligence. While in Germany, he interviewed more than 100 former producers and consumers of intelligence. He did much of the writing during his two years at St. Antony's College, Oxford, where the skeleton of the study served as a Ph. D. dissertation; the University awarded the doctorate in 1974. The book was published in 1978 as *Hitler's Spies: German Military Intelligence in World War II* (Macmillan, 1978).

A coeditor of the new journal *Cryptologia* (published at Albion College, Albion, MI), he has written on cryptology for publications as varied as *Playboy* and *Scientific American*. Kahn is now assistant Viewpoints Editor at *Newsday*. Married and the father of two boys, he lives in Great Neck.