TECHNOSPIES

The Secret Network That Spies on You—and You

by Ford Rowan

G. P. Putnam's Sons
New York

© 1978

transferred between cooperating networks with no loss of fidelity." Thus it would be very easy to use a network like the ARPANET for coded secret transmissions.

In 1976 ARPA Director George Heilmeier testified about a joint project with the Navy to develop a secure network to study command and control problems. Heilmeier said it would be a "secure subnet" of the ARPANET, which would involve very powerful computer systems. ARPANET, he said, was "coming of age in an operational sense."

In fact, ARPA is not only sharing its ARPANET with the military services, it is turning over the technology itself for use in upgrading other military communications systems. The Defense Communication Agency's new AUTODIN II, a secure network designed for the entire military, is modeled after the ARPANET. The old AUTODIN broke down so often in Vietnam that soldiers referred to the AUTODIN machines as "auto-dinosaurs." Because of the unreliability of AUTODIN, CIA officers in Vietnam often had to use unsecured telephone lines. The CIA even considered building its own communications system, called PYRAMIDER, so agents could communicate directly with CIA headquarters in Langley, Virginia. The military hopes that the new AUTODIN will solve the problem. ARPA's director testified that the ARPANET "is the complete technology base for AUTODIN II [Automatic Digital Network], the secure DOD military computer-communications network scheduled to begin initial operation in FY 1979."

The intelligence agencies are also upgrading their communications capabilities. Before 1973 special intelligence and special access organization information was sent on the Defense Special Security Communication System. In 1973 this communications system was merged into AUTODIN. But the intelligence agencies were not satisfied with the upgrading of AUTODIN to ARPANET standards. So intelligence officials decided to upgrade one of their own net-

works called COINS, the Community On-Line Intelligence Network. COINS is a secure network serving the Defense Intelligence Agency, the military intelligence agencies, the National Security Agency, the CIA, and the State Department.

With the addition of IMPs and TIPs the COINS network will have the capability of remote retrieval of data stored in military computers. Pentagon officials insist that COINS has never been used to spy on Americans. But the network is designed to share secret intelligence information among the various agencies. "The purpose of the COINS network," a Pentagon Official testified, "is to make sure that a file available in the DIA can be used by an intelligence analyst in the NSA, for example."

There's no guarantee that COINS and the other powerful tools of the intelligence agencies cannot be turned against Americans in the future. The abuses of the CIA and the NSA in the past show that it can happen. In fact, at about the time the CIA began Operation CHAOS to spy on thousands of Americans and the NSA began compiling "watch lists" to eavesdrop on millions of telephone conversations, there was one primitive use of the COINS system. The network was used to relay some information from the Secret Service to the National Security Agency in the late 1960's. According to a former Secret Service official who took part in the transfer, the material was "junk." It was just a "trial run."

COINS and AUTODIN are not the only systems to benefit from ARPANET technology. In 1972 the director of ARPA told a congressional committee that "the Defense Communications Agency has ordered three of ARPA's Interface Message Processors so that a prototype ARPANET operation can be established between three of the WWMCCS computers." WWMCCS is pronounced "Wimmix," and it stands for Worldwide Military Command and Control System. It is a central nerve system for the entire military. One

broke up, were the two Army intelligence officers. They duly filed reports on all they had seen and heard.

The information from the Halloween party and the hundreds of other events covered by 1,500 Army agents in the 1960s was filed away, much of it in computer data banks. Civilian officials in the Pentagon were not fully aware of what was going on until 1970 when the Army spying program was exposed in the press.

Senator Sam Ervin, the chairman of the subcommittee investigating the surveillance, said he "was first told informally that there were no computers; then, that there was one, but that it had been disconnected for this program; then that there were a few more computers that the department had forgotten about or not known about." During the controversy the Pentagon promised to stop spying on civilians and destroy its domestic surveillance files. But as late as 1975 some parts of the files were found in an Army counterintelligence analysis detachment in Washington. The Army had also given much of the data to the CIA, the NSA, and various police department "Red Squads" across the country.

The story of the primitive use of computers in the domestic surveillance of the 1960s and 70s is a chilling taste of what could happen again. If an "emergency" similar to the civil rights and antiwar protests of the past should occur in the future, all of the government agencies will have much more sophisticated computer systems in place. And the likelihood is that the new computer networks will be quickly utilized if government decides to spy on its own citizens.

The Central Intelligence Agency has tried to keep secret a proposal made by CIA Director Richard Helms during the height of the antiwar protests in 1969. Helms recommended using computer networks to share information about American dissidents between the CIA, the FBI, the National Security Agency, and military intelligence units. In one memo

Helms wrote, "I understand that the Office of Computer Service possesses on-line capabilities and other functions which not only would provide vastly improved information storage and retrieval but also affords the possibility of a data link with certain other elements of the security community.

"I would urge the earliest utilization of this capability," Helms added.

In fact, the CIA and the NSA went the farthest in utilizing computers to spy on Americans. In 1969 Director Helms stated, "There is an obvious need for introducing expanded, sophisticated computer support" for the CIA's domestic surveillance program. Operation CHAOS, as the biggest program was code-named, eventually gathered information on 300,000 individuals and the agency collected information from electronic eavesdropping, mail opening, and the penetration by agents of domestic groups. All of it went into a computer system called HYDRA.

The bottom line in a CIA manpower study on Operation CHAOS says this about the HYDRA computer: "Without such computer support, it would have been impossible to run this program . . ." HYDRA was developed to handle the "backlog of undigested raw information" that flowed in during Operation CHAOS. The names of individuals mentioned in intelligence reports were computer indexed. The computer printout on an individual or a group contained references to every file, document, and communications traffic where that name appeared.

The HYDRA computer was designed to categorize information on a "need to know" basis. The computer contained "streams" of data, some more sensitive and secret than others. Special passwords were required for CIA officers using the computer to gain access to information in each stream. It was because of the multistream nature of the computer that it was dubbed HYDRA.

When enough information had been collected on an in-

dividual to warrant special attention, a personality file called a "201" was opened on that person. The least sensitive part of the 201 file contained information on his birthdate, place of birth, occupation, and organizational memberships. More sensitive information would be recorded in another "stream" in HYDRA. Such information about the individual would be more detailed and would show which sources and methods were providing facts about the person.

Operation CHAOS developed nearly 1,000 files on targeted organizations and some 7,200 personality files were stored in HYDRA. A 1972 CIA memo on the HYDRA system states that "since all cable and dispatch correspondence in relation to the program is compartmented for reasons of operational security and sensitivity," it was not processed through regular CIA channels. Instead, the memo stated, "a complex, highly sophisticated system is utilized for the control and retrieval of this information." The memo also said that an additional reason for these advanced procedures was "the receipt of a large volume of reporting from the Federal Bureau of Investigation which requires detailed retrieval capability for pertinent names cited . . . ."

Information was flowing into HYDRA not only from CIA sources but from the FBI, the NSA, Army intelligence, and other government agencies. Every name went into the HYDRA system. If an individual who was being spied upon mentioned the name of a friend, even a casual acquaintance, the name of that person went into the computer as well. Thus people who had no direct participation in protest activities came to be spied upon along with the activists. Every bit of information gathered in Operation CHAOS went into HYDRA with no winnowing out of erroneous information.

The HYDRA system was designed so there could be on-line query and input capability at remote terminals. That meant that a CIA officer using the computer could do so

68

from a terminal in his office rather than having to go to the computer center. HYDRA was an astonishing assemblage of electronic components, including nine IBM 2260 terminals, five IBM 2741 terminals, one Data 100 Offline printer, one Data 100 Card Reader, and an IBM 360/67 computer.

The CIA's computers contained more about Americans than just the information collected in the domestic surveillance program. The CIA, which is supposed to be a *foreign* intelligence operation, has long been accumulating biographical information unrelated to its foreign duties. And many American citizens are listed in the CIA's central index. There are a total of about 15 million biographical references. In recent years there has been an effort to cut down the mass of information. In 1975 there were about 7.5 million names in the CIA computer, of which about 115,000 were those of American citizens. The number of personality 201 files on Americans is estimated to total about 70,000.

In 1974 the CIA issued new regulations to restrict the storage of information about Americans in the data banks. No information would be filed away unless the citizen was involved in "foreign activity detrimental to the national security interests of the United States." But the regulation listed examples of activities which can be interpreted quite broadly, including "espionage, counterintelligence, sabotage, subversion, covert propaganda, psychological or unconventional warfare or paramilitary operations . . . terrorist activity and narcotics trafficking," as well as participating in the "illegal apparatus of foreign Communist parties" or "other international clandestine activity."

The CIA's Office of Security maintains files on some 900,000 people, almost all of them Americans. Most of these files are about people who work for the CIA, but it includes others who simply have a relationship with the agency. The Office of Security is very liberal in deciding what constitutes a relationship. There are files on elected officials,

69

judges, and businessmen. In 1975 the CIA kept dossiers on seventy-five senators and members of the House.

The CIA Office of Security once kept an extensive computer list of about 300,000 persons who had been arrested in cities all over the nation and charged with offenses relating to homosexuality. The CIA claims this list was destroyed in 1973.

The extensive nature of the CIA's computer files shows how all-encompassing record keeping can become. When the CIA feared embarrassing disclosures it terminated Operation CHAOS in 1974, but the agency continued to maintain a mountain of material on American citizens. When Director William Colby ended CHAOS, he issued a directive restricting the collection of information about Americans. But it contained a big loophole. The Colby directive permitted the collection of facts about Americans when incidental to foreign intelligence collection. That was a key exception. From the secret beginning of Operation CHAOS through the period of controversy after its exposure the CIA claimed that the spying on Americans simply had been an incidental part of its foreign intelligence mission.

The Colby directive stated that if information is received by CIA bases on American citizens, "and it is determined that such information is inimical to U.S. interests or the base feels that the incidental information should be reported to headquarters," it should be sent through channels. "Headquarters will make the final determination as to disposition of any information which is received."

So the CIA is still the judge of what it should collect, whom it should tag for surveillance, and which records it should store in its computers. While there is no evidence that the massive surveillance of the antiwar period continues, the HYDRA computers still exist. In fact, the CIA has continued to upgrade its computers.

A CIA officer named Paul sits at the center of this enormous powerhouse. From the CIA's Operations Center on a top floor of the agency's Langley complex, he has access to news moving over the press association teletypes, cables coming on from CIA officers overseas, and messages flowing to and from the agency from the State Department, the FBI, the Treasury, and the White House. "We have to know everything from the status of the Russian fleet to who is cutting down a tree in the demilitarized zone of Korea," Paul explains.

It is essential work, essential to the survival of America in a nuclear age. But in performing its legitimate tasks, the agency has acquired a proficiency that can be turned against American citizens if a domestic emergency, like the antiwar protests of the Vietnam era, suddenly hits home. One can sense the growing technological power of the CIA in a conversation with Paul, who uses the agency's might only for worthwhile foreign purposes.

Paul can describe the new computer terminals linking various intelligence agencies and the White House where lengthy texts of messages can be edited. On his desk sit two telephones, a normal business phone and a special gray phone, the latter instrument part of a system that electronically codes conversations. A notice on the gray phone warns that it must not be used within three feet of the regular phone—to prevent any of the secret conversations from somehow being intercepted. The gray phone links various elements of the national security community.

Down the hall from Paul, in another area of the Operations Center, are the facsimile machines, devices which can transmit photocopies of documents to the White House or the FBI. Newer machines are in the process of being installed for "Wash Fax," as the system is called, Paul explains. But he notes that there are so few of the older facsimile machines in existence that when the Treasury Department was added to the system a couple of years ago, the

FORD ROWAN

only place where the White House could find a "Wash Fax" machine to install in the Treasury was at the home of a former President. "They didn't need it in San Clemente anymore," Paul notes.

All is not perfect at the hub of this powerhouse. Paul recalls how he tried to test the emergency preparedness telephone system late one night. He tried to call a command center like Mount Weather, Paul said, "but the guy who answered the phone said he was a guard at a prison in Virginia."

Despite occasional shortcomings, the CIA has managed to develop communications skills which make it possible to transmit intelligence information quickly and secretly. Few would complain when the intelligence concerns overseas developments. The danger is that the system could be perverted for domestic surveillance in some future Operation CHAOS. There are two haunting lines from those old CIA documents about Operation CHAOS: ". . . the Office of Computer Service possesses on-line capabilities [which] afford the possibility of a data link with certain other elements of the security community. . . . I would urge the earliest utilization of this capability." And, "Without such computer support, it would have been impossible to run this program . . . ."

While the CIA had no business engaging in police functions inside the United States, the Federal Bureau of Investigation has a clear responsibility to protect Americans from crime. To carry out its legitimate domestic role, the FBI has acquired immense record-keeping skills and has amassed voluminous information about Americans. The problem, as one General Accounting Office study confirmed, is that often the FBI uses its skills in ways that do nothing to counter crime.

The GAO found that FBI domestic surveillance opera-

72

Commission. It provides tips on how to get information from trade and professional associations, the Better Business Bureaus, credit agencies, banks, and other private sources. *Where's What* suggests that a skilled investigator check the records written into a family bible.

And here is what *Where's What* has to say about educational records: "The visit to the small college is almost always a pleasant assignment because the setting, the spirit of the students, and the relaxed manner of administrators and faculty are difficult to match in any other type inquiry. The first stop is usually the registrar's office. . . . Some schools will provide a nice little office for the investigator, others will have only counter space. The author remembers one school where a cantankerous old lady never wanted to extract a file from a cabinet as she was concerned that it would not be replaced. She kept all the files in a vault, would open the cabinet, peek at the file and then call off the desired information—never once facing the investigator. When all was finished, the lady would turn around and in her sweetest smile would say, 'Always glad to be of help.'"

And the CIA is supposed to be a foreign intelligence agency! CIA officials insist that just because a lot of filing systems are mentioned in *Where's What* does not mean that CIA agents are regularly poking around in them. But *Where's What* is a "how to" manual. How to snoop.

Where's What recommends that CIA investigators seek the assistance of local police. The policeman, it says, makes it his job to know what is going on, who knows whom, who can be trusted to be discreet, who are the blabbermouths, and who are the "window detectives." *Where's What* concludes, "The modern professional police officer is not the 'flatfoot cop' of many years ago but is a well-educated, intelligent gentleman who wants to cooperate with federal investigators."

Despite its disdain for the word "flatfoot," *Where's What*

still advocates that an investigator use his feet to visit offices and procure files. It is a pre-computer document. The world has changed in the decade since it was written. With computerization, the investigator of the very near future will not need to wear down his feet to the point where he's called a "flatfoot." Tomorrow's investigator may be able to get almost all of the information he wants simply by using the computer terminal at his desk.

The possibility of keeping tabs on individuals electronically will be enhanced with the growth of a banking service known as EFT, Electronic Funds Transfer. With EFT, the customer can give his bank card to a merchant, who inserts it into a terminal, which records the amount at the bank, and transfers money from the customer's account into the merchant's account. Other devices permit bank customers to withdraw cash from machines when banks are closed. These transactions rely on computers and telecommunications. The economies in such EFT systems are apparent, but there are dangers in the movement toward electronic banking.

A great deal of information is recorded about an individual with each EFT transaction—not only is a history built up of his spending habits but each purchase and his whereabouts when he made that purchase are recorded. Such information can be of great value to law enforcement and intelligence officers. Even if a person who has been using an EFT system suddenly decides he wants privacy and elects to spend cash, the EFT computer would record the cash withdrawal—and it would stand out prominently.

In a 1971 experiment a group of specialists in computers, communications, and surveillance was given a strange task. They were asked to describe a system of surveillance which might fit the purposes of the Soviet secret police. The experts were told to come up with a plan which would not be obtrusive. What did they come up with? An EFT system. An

112

113

substantive content of the speech. . . . This will open up entirely new ways for people to interact with devices and control systems of all types."

The question is where will the "control" reside? In free men? Or in the surveillance machines of agencies like the NSA?

A former director of the NSA, General Lew Allen, said that the computerized sorting and analyzing processes can help the agency ignore inappropriate messages that it just happens to intercept. Allen says the procedures are designed so that Americans will not be spied upon because "processing, sorting, and selecting for analysis is conducted . . . to insure immediate and, where possible, automatic rejection of inappropriate messages."

But unfortunately, the NSA's use of computers, buzzwords, and watch lists of targeted individuals can be directed against Americans more easily than these techniques can be used to protect citizens. The NSA's surveillance of Americans in recent years has been an Orwellian harvest of shame. The NSA has used its most secret communications capabilities to spy on American citizens.

Over the years the agency has collected information on thousands of Americans who sent or received messages, spoke on the telephone, or were referred to in conversations intercepted by the NSA. Until those files were destroyed in late 1974, the NSA had information on some 75,000 American citizens in its computers. The mere mention of a name during a transatlantic telephone call could trigger the NSA to open a file on an individual.

The NSA's appetite just grew and grew. And it was willing to share its bountiful harvest with other agencies, like the CIA. Some of the information from the NSA went into the CIA's domestic surveillance program, Operation CHAOS. In the late 1960s the agency was drawn into the systematic monitoring of the protest activities of Americans.

Operation MINARET, for instance, was set up to study foreign influence in U.S. peace and black power movements. In the charter establishing this secret eavesdropping program, MINARET was described as an effort to monitor "communications concerning individuals or organizations involved in civil disturbances, antiwar movements/demonstrations and military deserters involved in antiwar movements."

The FBI, the CIA, the Defense Intelligence Agency, the Secret Service, and the military services all submitted names of American protestors for the MINARET watch list. These people's communications were intercepted and analyzed by the NSA, and reports were furnished to the other agencies. Between 1967 and 1973 some 1,200 Americans were listed on the watch list.

The CIA used the information supplied by the NSA's MINARET to update its CHAOS files. The FBI used it to develop leads on citizens who were later harassed in the COINTELPRO operation. The NSA assisted the Bureau of Narcotics and Dangerous Drugs in an illegal wiretapping program designed to catch Latin American drug traffickers. The BNDD suspected that a public phone in Grand Central Station in New York was being used to arrange illegal drug shipments. The BNDD knew it could not legally wiretap the phone, so it asked the NSA to do the job! Rather than use one agent to listen to calls from one pay telephone booth, the NSA used its electronic monitoring devices and computers to screen virtually all phone conversations between citizens in the United States and Latin America. They didn't catch their drug peddlers.

The NSA discontinued its most blatant eavesdropping on Americans when congressional investigators began asking about the supersecret agency, but it still monitors international communications, including telephone, cable, and computer data traffic, and some domestic long-distance telephone circuits. Because the NSA can monitor virtually

collection of information about a person's life style, politics, religion, or race, on the ground that the law violates the credit firm's freedom of speech.

Businesses sometimes hire private investigative agencies to check out prospective employees. One such firm, the Wachkenhut Corporation, utilized a list drawn up by a Washington man named Barz Lag who kept track of congressional hearings and other government proceedings to sort out "derogatory-type" information on leftists for blacklisting purposes. These lists of "subversives" contained the names of people active in civil rights and antiwar protests in the 1960s. Wachkenhut gave the lists to the "Church League of America," which now claims to hold the largest and most comprehensive files on subversive activity, with the single exception of the FBI. Wachkenhut's investigators still make use of these files.

Very often it is possible to learn a great deal about someone without having to resort to direct surveillance. A remarkable guidebook for gathering personal information about Americans came to light in 1975. It is entitled *Where's What* and it was published as a "confidential" sourcebook by the Central Intelligence Agency. It is now available to the public under the Freedom of Information Act.

In its more than 400 pages *Where's What* lists hundreds of sources of information for investigators, ranging from vital statistics kept at county courthouses to financial records stored in automated files. The book tells how to find information about motor vehicles, education, police actions, and court judgments. Open sources—libraries and old newspaper morgues, for instance—are not overlooked.

Where's What lists the record systems of all federal departments plus twenty-two federal agencies, including the Selective Service System, the Small Business Administration, the Veterans Administration, and the Civil Service

CHAPTER 11

How far has it gone?

Mother lit up another Virginia Slims and peered into the Planter's Punch. Unnoticed underfoot, a small mouse scampered across the faded carpet of the Army & Navy Club in Washington. The talk was of "The Threat." The man was "Mother." He was thinking back two years.

A gaunt, ghostlike character, he has put the fear of God into grown men who have worked for the CIA for more than two decades. Some of them look back over their shoulders when his name is uttered.

James Angleton. Former chief of counterintelligence for the CIA. Master spy. Poet. Horticulturalist. His orchids, it is said, are stunning. For twenty years he was in charge of keeping the CIA's men in line and keeping Communists out of the CIA. He was known around the agency as the "Gray Ghost." But in his later years he obtained a new nickname after two books about the CIA referred to him pseudonymously as "Mother."

Mother is testifying now. In a soft voice. But it cuts like a

scalpel. "It is inconceivable that a secret intelligence arm of the government has to comply with all the overt orders of the government."

The scene is the Old Senate Office Building. The date is September 24, 1975. James Angleton is on the witness stand. It is an unprecedented sight. It is not friendly forum.

"I withdraw that statement," Angleton breathes. It is not his finest moment. Appearing before the Senate Intelligence Committee, he is grilled about his life's work, the secret work, and about his deeply held feelings that there are times when an intelligence agency is not expected to obey the public regulations of the government and the laws of the land.

"Well," Angleton backtracks, "I would say I had been rather imprudent in making those remarks." While his life's experience screamed internally, "It's true," his public front, prodded by Senator Frank Church, capitulated.

Church pressed Angleton about his comment that it is "inconceivable" that the CIA should have to comply with "all the overt orders of the government."

"Do you withdraw that statement?" Church demanded.

"I do." Angleton glared. A lie, perhaps, but one that welled up from the very depths of his personality. Here he was, the CIA's guardian, guardian of the nation's security, before this group of senators, men who could never comprehend that we are in a "secret war," to use Angleton's own term.

How is this war going? Angleton speaks as one who, in his own words, "has given up thirty-one years of life with certain very high ideals for this country. When I left the Army," he explains, "I believed that we were in the dawn of the millennium." He swallows. "When I look at the map today and the weakness of power in this country, that is what shocks me."

FORD ROWAN

How did Angleton fight this "secret war"? "The sum total of counterintelligence activity includes dossiers, identification of individuals, travel control, and a whole series of other dossier items," Angleton explains. These items form a base "from which can be developed a product which is counterespionage," the direct effort to counter the threat.

Angleton struck fear into the hearts of brave men in the CIA. In charge of keeping the agency pure, he watched everyone. No Russian infiltrators or subversives would slip past this slim man. For society at large, Angleton had larger fears. Fears, as Walter Mondale put it, that America's own children were trying to destroy this country.

Yes, Angleton says, the threat seemed so real back in the late 60's and early 70's that agencies like the CIA, NSA, FBI, and Army were called on to protect national security. To Angleton it was an emergency, a threat, a challenge, a crisis, and it required information, intelligence, dossiers, and action.

To Mondale it was paranoia. "Paranoia that the American people were trying to destroy the country," Mondale told Angleton. "I think that attitude," Mondale added, "shows how dangerous it is to have agencies which themselves do not feel that they are bound by the restrictions of the law."

Mother responded softly, "It was not, in my view, paranoia."

Years later, over drinks with a reporter at his club, Angleton relives those hearings, and it is clear that his views have not changed. "America," he intones, "faces a grave threat." His voice rarely raises over a whisper. Straining forward to catch every word, one is pulled gradually into Angleton's world. Despite the gravity of the perceived threat, it is a comfortable world—made easier to comprehend because the enemy is identifiable even as he is everywhere. The threat comes from the left. And Angleton favors strong measures to fight his "secret war."

186

TECHNOSPIES

To understand past episodes of spying on Americans—like Operation CHAOS—or things which could happen in the future, like a more pervasive misuse of surveillance technology, it is necessary to understand men like Angleton.

After several lunches with the man it becomes easier to grasp his fears for the country, to recognize his well-meaning sincerity, to feel friendship for this man who was once so fearsome. He is bitter about the Congressional probes. In response to an offhand remark that former CIA director William Colby was to be commended for always telling the truth to the reporter, Angleton snaps, "He should have lied!"

While the ground rules of these meetings do not permit quotation of other remarks by Angleton, one overriding impression can be conveyed. Here was a man of action, a man dedicated to protecting his country.

The CIA likes to boast of its capability to *analyze* the threat to America, but its personnel have always viewed their role as *protecting* America from the threat. Inside the agency, information gathering and analysis has always been viewed as an adjunct to the CIA's main role. Analysis has taken a back seat to operations. The emphasis has been on covert action.

That's why the CIA worked so hard at destabilizing the democratically elected government of Chile when President Nixon demanded an end to Marxism there. The CIA utilized the full range of covert tactics, including propaganda, press manipulation, bribes to officials, efforts to rig elections, penetration of interest groups, and efforts to foment a military coup. The CIA mounted this campaign despite an interdepartmental intelligence report which concluded that the United States had no vital interests within Chile, the world military balance of power would not be significantly altered by a Marxist victory, and the election of a leftist government would not pose any likely threat to the peace of the region.

187

Another example of the CIA's energetic use of covert action came in Operation MONGOOSE, designed to get rid of Castro. MONGOOSE and related CIA efforts were fueled by the intense desire of President Kennedy and his brother Robert to topple the Cuban Premier. The CIA, in its zeal to remove Castro, contemplated using exotic poisons to kill him, and even enlisted help from Mafia hoodlums.

Under both Presidents Kennedy and Nixon, the CIA considered assassination as a proper tool to counter the threat of Marxism. Was the threat so grave as to justify such tactics? These were not "one-shot" affairs. The CIA even established an "Executive Action" unit, code-named ZR/RIFLE, to develop a capability to neutralize enemies. The CIA claims this capability was never used.

The CIA was not above participating in mass murder. Operation PHOENIX, a military program, involved CIA personnel in operations with South Vietnamese forces which resulted in the deaths of 20,000 Vietnamese civilians. This program of terror utilized computer data banks to help track down Vietcong infiltrators and crack the "infrastructure" of Communist sympathizers in South Vietnam.

This marriage of technology and terror, be it toxins with murder plots or computers with efforts to wipe out an "infrastructure," is a fact of life for the CIA. The CIA uses information and it uses technology. And some of the covert uses can be very dirty.

The CIA has performed most of its covert actions overseas, but the covert mentality has made inroads on domestic agencies, especially the FBI and the IRS, which have used their powers to harass extremists and enemies. And the CIA's covert tactics have been copied in other agencies, specifically in the drug abuse program.

The big push for action came from the White House. President Nixon ordered the CIA to help curb drug abuse and related crimes, which he called "the number-one domestic

188

problem." Overseas the CIA was ordered to help keep track of drug traffic. The NSA monitored telephone calls to catch drug traffickers. Agents followed the trail of drugs right into American cities.

The drug problem in 1971 was not unlike the urban disorders of the 1960s or the antiwar protests of the 1970s, or even the success of Marxists in Latin America. Each was viewed as a danger to the national security. In each case presidential orders called for extraordinary action. The drug menace was seized upon by the Nixon Administration as the cause of the crime wave Nixon had campaigned against in 1968. In short order the antidrug crusade came to be envisioned by White House aides as a force for domestic surveillance and clandestine political repression.

From the beginning, drug abuse proved especially hard to curtail, and President Nixon turned to the most covert of agencies at his disposal. In addition to using the CIA to monitor drug traffic overseas, the Nixon Administration recruited CIA personnel to work for the agencies responsible for coping with drug abuse in the United States. Some sixty former CIA men went to work for the Drug Enforcement Administration. One, Lucian Conein, became a senior official in the DEA. In earlier days, Conein had been a counterinsurgency operative in Vietnam. He was the U.S. embassy's liaison with the cabal of South Vietnamese generals who assassinated President Ngo Dinh Diem. After Conein left the CIA, his old colleague Howard Hunt brought him into the White House, where he was assigned to work on Nixon's number-one domestic problem, drug abuse.

While Conein's role is not fully known, the White House task force went to work under Hunt and Gordon Liddy. It began organizing a team of about 200 former Cuban agents to perform political tasks for Nixon, to fight Castro, and to fight drug abuse. The project, code-named DIAMOND, recruited men skilled in combat and demolition. It was to be

189

the strike force of the White House Plumbers, a special co-vert action unit, ready for instant use against domestic "enemies." This project never went very far.

Conein eventually was moved to head of the Special Operations Branch of the DEA, in charge of carrying out the war on drug pushers. The White House reorganized the antidrug program in DEA and demanded that some way be found to stop the big-time traffickers. Gordon Liddy came up with a way. His suggestion was to kill them.

The DEA set up a network of informers and a computerized system for penetrating the drug "infrastructure" and identifying traffickers. The program resembled the CIA's PHOENIX program in Vietnam. One computer program, known as EPIC, collected intelligence on drug traffic across the Mexican border into Texas. States as far away as Vermont and Washington have used the EPIC data. And the NADDIS computer provided automatic cross-indexing, which permits agents in the field to obtain information on individuals in a hurry.

The Nixon Administration even enlisted Mount Weather in the campaign against drug pushers. During 1972 the White House established a national heroin "hotline" so people could telephone a central number to report drug pushers. The program was hastily put together and the only facility with the necessary telephone equipment which could be found was the underground communications center in Virginia. Personnel of the Office of Emergency Preparedness were put to work answering phones on a twenty-four-hour basis as the calls streamed in to the toll-free number from across the country. The program, however, proved to be only a publicity gimmick. Of the 33,313 phone calls received in the first three months, only 113 provided solid leads for the narcs and only four arrests resulted.

As for the program to assassinate major drug traffickers, it also fell through. Although the CIA took credit for killing

some drug suppliers in Southeast Asia, the program never got off the ground anywhere else. Before any "hits" were attempted, word of the DEA's strange undertaking got into the press. Senator Lowell Weicker disclosed that Conein had examined some unusual weapons that a private firm was trying to sell to the DEA, such things as an exploding telephone and a rocket launcher swagger stick. Conein later explained that he thought he was going to be shown only surveillance devices, not weapons. The publicity put an end to the efforts to murder drug pushers.

But America had come too close to having the techniques of the CIA's PHOENIX program transplanted from the battlefields of Vietnam to the streets of America.

"Let me tell you the story about the dead man who went seeking a decent burial." George smiles, as if he is about to tell a joke, then he looks at the fishpond and frowns. "This is a good place for the story about the dead man." As we walked across the lawn of the old brick mansion, George talked about his days as a pilot. As we stepped through the giant atrium, the conversation shifted to laser research. When we looked at the flower garden, George spoke of computers, the kind which comprehend human speech. As we sat on a wooden garden bench, George spoke of executive action and murder.

Dumbarton Oaks, where an international meeting in the 1940s helped create the United Nations, is a pleasant place. But three hours in the gardens with a spy-soldier-scholar can be an unusual experience. George likes to stroll slowly and soak up the spring beauty. But he understands that things are not always as they appear. And that's why he has a story about a dead man.

"This fellow showed up at a church and asked the priest to bury him," George recounts. "The priest said, 'It's good to make arrangements in advance, farsighted,' but the fel-

low said, 'Farsighted, hell, I've been dead for two weeks!'"
George has a twinkle in his eye. "The priest knew he had a
troubled soul on his hands, but he couldn't convince the fel-
low that he was alive and well." Rather than exorcism,
George laughs, "the priest decided to try a modern form of
witchcraft—he sent the guy to a psychiatrist."

George recounted how the fellow insisted to the psychia-
trist that he was dead. "The doctor got him to talk and talk,
but all he would talk about was his recent 'death,' so in ex-
asperation the shrink turned to logic as a last resort."
George leans over and grabs a hand, like he's acting out the
story.

"The doctor said, 'My man, isn't it true that a corpse that's
been dead for two weeks cannot bleed?'" George paused.
"The fellow answered, 'Well I guess so, a corpse that's been
dead that long wouldn't bleed.'" Then George ran the stem
of his pipe across the hand. "The doctor took a little knife
and nicked the fellow's hand, and of course it bled. 'See,'"
George quoted the doctor, "'you're bleeding.'"

"'What do you know,'" George quoted the fellow,
"'corpses do bleed!'"

Not a bad joke, but what's the point?

"It's a parable, dammit," George shouts, shaking his pipe
so hard the smoldering tobacco spills out onto his pants leg.
"A society that thinks it's dead will view all the evidence in
such a way as to prove it's dead; a society that thinks it's
right will twist all the information showing it's wrong
around to prove it's right."

We all live our lives within the confines of our own mind
sets, our world views. Everyone processes information
through his own frame of reference. Information which con-
flicts with preconceived notions is hard to swallow. As
George pointed out, witness our struggle with civil rights or
the reality of American behavior in Vietnam.

"All the talk about equal rights and equality contradicted

the bigoted world view of many whites. Not to mention the
inferiority complexes of many blacks," George explained.
"Look at Vietnam, the pictures of Americans burning vil-
lages, the stories of Americans killing women and children,
it didn't fit our view of ourselves as honorable victors." Evi-
dence which contradicted our world views produced ten-
sions, George says, but over time attitudes changed.

What George really worries about is that the mind set of
American intelligence operatives and their political superi-
ors is more resistant to change than the average man's, that
the White House, the CIA, the FBI, and the other agencies
cannot comprehend what is happening in America. "Social
change and protest didn't fit their preconceived picture of
what was supposed to happen in the land of the free and
home of the brave.

"The reason the intelligence agencies were unleashed to
spy on Americans," George explains, "is because of a mam-
moth intelligence failure. The guys at the top," he explains,
"were blinded by their own preconceived attitudes. We saw
everything in terms of the Cold War," George adds. "Every-
thing was a crisis, an emergency, a matter of national secu-
rity."

President Johnson and, later, President Nixon clearly be-
lieved they were acting to cope with a pressing national
emergency when they demanded intelligence about racial
riots and antiwar protests. They couldn't believe it was
homegrown protest, so both presidents concluded that for-
eign influence had triggered domestic unrest.

Johnson turned to military intelligence and the CIA to try
to uncover foreign elements fomenting unrest at home. No
one ever found any foreign control. Nixon insisted that the
CIA dig up the facts on foreign influence in the antiwar pro-
tests. Yet every major study conducted by the intelligence
agencies showed no instances of foreign control. Every neg-
ative report was greeted with presidential orders to expand

the spying, to look harder for foreign influence. For nearly a decade powerful military, intelligence, and law enforcement agencies snooped on Americans and made trouble for "troublemakers" because no one in leadership positions could accept the evidence that this was homegrown, legitimate protest.

Both the Johnson and Nixon Administrations criticized the FBI for failing to cope with the demonstrators and dissidents. The bureau had enormous information-gathering operations, but the results seemed meager.

The Johnson Administration wanted to figure out a way to evaluate the FBI's raw data on domestic disorders, so the assistant attorney general for civil rights, John Doar, suggested setting up a new "single intelligence unit" to study data from the FBI, the IRS, and neighborhood, labor, and antipoverty programs. His recommendation was accepted in 1967 by Attorney General Ramsey Clark, who established the Interdivisional Information Unit, the IDIU, which set up a computerized system and accumulated files on 12,000 citizens.

In 1969 President Nixon's Attorney General, John Mitchell, included the CIA in the Interdivisional Information Unit. The IDIU computer now processed more than 30,000 reports each year from the FBI, military intelligence, and all the other sources enlisted in the fight against domestic unrest. The IDIU encouraged the sharing of surveillance information among agencies. By 1970 it was producing weekly computer printouts of all intelligence on black activities, campus disturbances, and other disorders. In 1971 Assistant Attorney General Robert Mardian, who would later be tried for Watergate offenses, issued new guidelines for the IDIU. "IDIU must analyze and monitor all information relating to past civil disorders as well as information relating to the potential for civil disorder," Mardian instructed.

Unhappy with the failure to predict violence, the Nixon

Administration established the Intelligence Evaluation Committee in 1971. This led to the so-called Huston Plan, hatched by White House aide Tom Charles Huston, to coordinate the domestic activities of the FBI, the CIA, the NSA, and military intelligence units. The Huston plan sought the presidential seal of approval on the illegal surveillance activities by intelligence agencies that were already under way. It called for intensified electronic eavesdropping, mail openings, and break-ins. The Huston memo noted that those tactics were "clearly illegal."

The heads of the CIA, the NSA, and the Defense Intelligence Agency and President Nixon endorsed Huston's plan, but it was scrapped when FBI Director Hoover objected, apparently because it intruded onto his bureaucratic turf. Nonetheless, many of the illegal surveillance activities continued.

The IDIU, the IEC, and the Huston Plan were top-level responses to the need for good analysis of what was happening. Yet the White House was never satisfied with the analytical product it received.

Because the analysis failed to measure up, the emphasis shifted to operations. In place of analytical deficiencies, the White House ordered dubious operations. The result was even greater efforts by the White House and the intelligence agencies to gather facts about Americans and mount operations against them.

It is a big mistake to chalk up the Huston Plan and Watergate as extraordinary events brought about by a corrupt administration. They were only part of a long-term trend toward the centralization of intelligence analysis and operations. Surveillance grew by leaps and bounds because of the emergency mentality that still persists throughout these agencies. And throughout the decade of the protests there was increased dependence upon new technology for surveillance purposes. Army Intelligence was enlisted in the

FORD ROWAN

cause because the military had nationwide communications superior to the FBI's. The CIA was brought in because its computers, more sophisticated than the FBI's, could perform analytical functions. The CIA, the NSA, and the DIA were involved in the Huston Plan because they were the fellows with the big computers and the most sophisticated techniques.

After it was all disclosed, Huston himself conceded that the risks had been too great. "The risk was that you would get people who would be susceptible to political considerations as opposed to national security considerations, or would construe political considerations to be national security considerations, to move from the kid with a bomb to the kid with a picket sign, and from the kid with the picket sign to the kid with the bumper sticker of the opposing candidate, and you just keep going down the line."

"Imagine," the privacy expert asked, "what Watergate might have been if its adventures had taken place not in 1972, when automation was still in roughly an early stage, but in 1980, or 1984?" Dr. Alan Westin warned Congress that when more governmental and private files are computerized, when the Social Security number is used more and more to identify people, and when some central government unit has the security plans and data access keys to all sorts of computers, then it will be possible to pull off a successful Watergate-type operation.

"By 1980 or 1984, of course, the White House would have been well staffed with systems experts and computer information specialists," Westin said. "Instead of a basement room with tape recorders, the White House would have had video display terminals linked to a computer in Camp David." Westin added, "This would have held some 'enemies files,' such as 500,000 political opponents to be systematically harried by federal discretionary authority. . . ." West-

196

in listed other files which could be made accessible to the White House, including computer records of "leakers" to the press, and files on "disloyal" radicals.

"In such a Watergate 1984 setting, the Plumbers of 1972 would have become the filers of 1984, and the dossiers," Westin said, "would have been produced far more effectively than by such crude measures as wiretaps, break-ins, and double agents." Westin warned, "We cannot allow secret files to be built under the cover of national security, files that can be easily used to harass political opponents, dissident groups, and the press."

Westin, testifying in 1974, said that computerized information systems had not grown to that full dimension of danger when Watergate occurred. But what he and almost everyone else did not know is that the Nixon Administration had begun the process of centralizing computer communications at the White House.

The May, 1971, memo is on CREEP stationery. It is stamped "Confidential." It reads, "To: Gordon Strachan. From: Jeb Magruder. Subject: White House Computer." The memo discusses ways the Committee for the Re-Election of the President could utilize the government's computer resources. The proposal lists eighteen potential uses, including using the computer to maintain information on registered voters on a precinct-by-precinct basis for the entire nation. The memo includes a map showing how the computer can be used for "simulation mapping of demographic data."

The CREEP officials were ready to utilize government computers for blatantly political purposes. A June, 1971, memo discusses ways to use each agency to control patronage. Patronage is defined broadly to include jobs, contracts, grants, subsidies, social programs, public works programs, and public relations. One form of "patronage" is listed in the memo this way: "Execution of federal law (resides

197

mainly in the Department of Justice whose interpretive power touches every vested interest)."

With that kind of attitude it is not surprising that the White House wanted to upgrade communications and computer capabilities. An earlier memo on the campaign states that the White House Communications Agency and "other people with technical know-how" will be asked to devise "various telephonic and electronic devices" to provide communications between the White House and its political operatives.

The first computer the Nixon Administration turned to was the one operated by the Emergency Preparedness staff at Mount Weather. Remote terminals in the White House and the nearby Executive Office Building permitted White House officials to use the computer for personnel purposes.

The Mount Weather computer was used by the White House to maintain three files: the Executive Branch Presidential Appointees File, the Incumbent File, and the Talent Bank. About three thousand names were included in each file. The Talent Bank contained facts on a person's ethnic background, sex, political affiliation, work experience, education, and performance rating. These files were used by the Nixon Administration to keep track of its own personnel and job applicants, but sources say there were plans to expand it to include political "enemies" of the administration, so they would not be able to get government jobs or contracts.

"It was an itch on our part to get friends in the departments rather than the people that we found there," John Ehrlichman explained. The Nixon Administration considered establishing Talent Banks at every department to screen people applying for jobs—even nonpolitical jobs supposedly protected by civil service merit rules. "It was a large-scale intensive effort to undermine merit hiring for civil service jobs," according to one investigator. Joseph
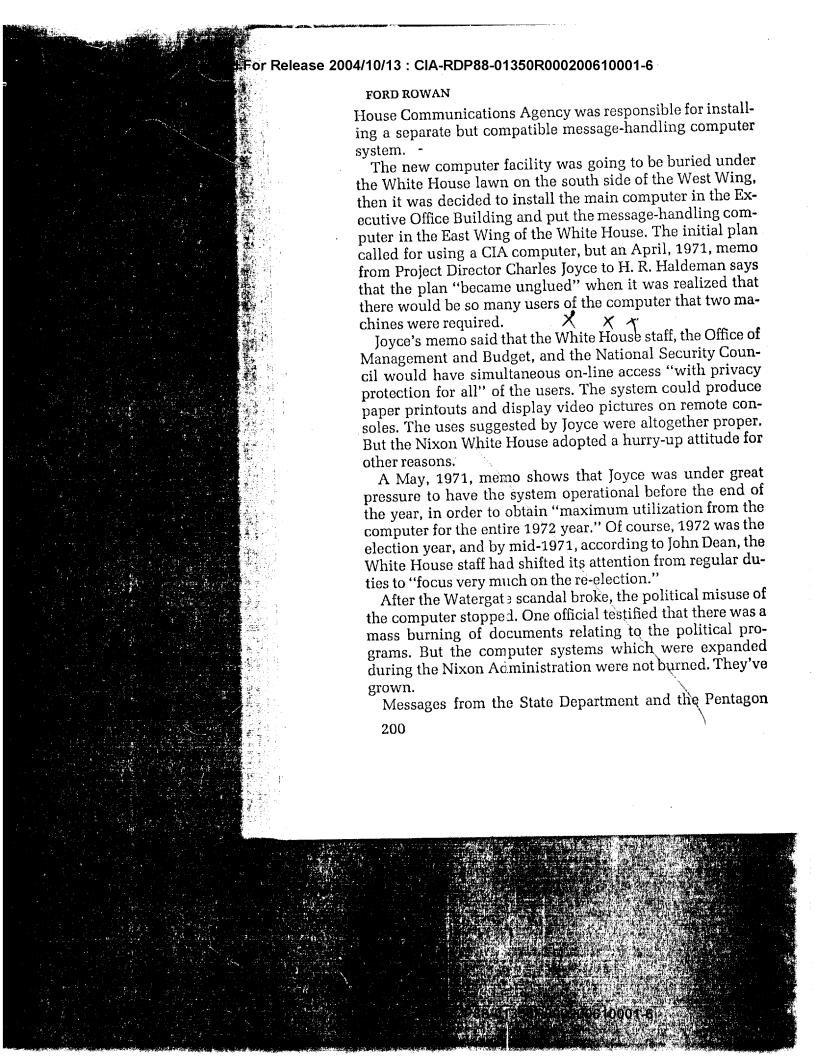
198

once worked for the Civil Service Commission, but he quit when he couldn't get anyone to do anything about the abuses he uncovered. He's willing to "go public" only if he's subpoenaed by a congressional committee, but so far none has dared call him. That's because he knows a lot about how representatives and senators of both parties abused the system.

"On some occasions," Joseph recounts, "applicants for civil service jobs were cleared through the White House personnel office." He recalls references to secret political clearances for jobs. "The system rated everybody on political criteria," he says, "and it was computerized at the White House."

Actually the computer was buried deep beneath the hills of Virginia at Mount Weather. The preparedness officials were happy to share their computer capability because they could use the lists of presidential appointees in an emergency to help keep the government running. The danger, of course, is that such a secret system could be used to ban "enemies" from government jobs during normal conditions. Furthermore, the Mount Weather computer has a large memory capacity and could be used to store intelligence data on dissidents. Preparedness officials deny that that has ever happened.

But in 1971, before Watergate forced a cutback to the most ambitious political schemes, the White House was considering ways to utilize technology. In that year a major program code-named ZENITH was instituted to modernize the White House situation room and expand the computer facilities available to the President and his staff. ZENITH was budgeted at $2 million for the first two years and involved several agencies. The Defense Communications Agency was responsible for the design and installation of the computer equipment. The General Services Administration was responsible for finding space for the equipment. The White

199

FORD ROWAN

House Communications Agency was responsible for installing a separate but compatible message-handling computer system. -

The new computer facility was going to be buried under the White House lawn on the south side of the West Wing, then it was decided to install the main computer in the Executive Office Building and put the message-handling computer in the East Wing of the White House. The initial plan called for using a CIA computer, but an April, 1971, memo from Project Director Charles Joyce to H. R. Haldeman says that the plan "became unglued" when it was realized that there would be so many users of the computer that two machines were required.

Joyce's memo said that the White House staff, the Office of Management and Budget, and the National Security Council would have simultaneous on-line access "with privacy protection for all" of the users. The system could produce paper printouts and display video pictures on remote consoles. The uses suggested by Joyce were altogether proper. But the Nixon White House adopted a hurry-up attitude for other reasons.

A May, 1971, memo shows that Joyce was under great pressure to have the system operational before the end of the year, in order to obtain "maximum utilization from the computer for the entire 1972 year." Of course, 1972 was the election year, and by mid-1971, according to John Dean, the White House staff had shifted its attention from regular duties to "focus very much on the re-election."

After the Watergate scandal broke, the political misuse of the computer stopped. One official testified that there was a mass burning of documents relating to the political programs. But the computer systems which were expanded during the Nixon Administration were not burned. They've grown.

Messages from the State Department and the Pentagon

200

CHAPTER 13

What's next?

The young woman did as she was told. She sat still and looked straight ahead, not glancing to the side to see what was happening at the end of all those wires that connected to her body. Jennifer was on "the box." The operator, a man who had seen thousands like Jennifer come and go, went down the list of questions. When he asked, "Have you ever used drugs?" the needles on the machine jiggled even before she finished lying. Before long the man had extracted a confession that Jennifer and her boyfriend smoked pot from time to time.

A half hour after Jennifer had arrived for her polygraph test in a suburb of Washington, D.C., the man had good news for her. Despite the drug episode, Jennifer had "passed" the lie detector test. "It was scary being strapped to that machine," Jennifer said, relieved that she had made it through.

This was not a scene from the Langley, Virginia, head-quarters of the Central Intelligence Agency, although it

219

would fit right in. Jennifer is a teenager. She had applied for a summer job as checkout clerk at a local drugstore. The drugstore required all prospective employees to take a polygraph test.

This is the story of the technological inquisition, which is still in its infancy, with the "lie detector" its most common manifestation. Ongoing research attempts to link computerized techniques with new medical, psychological, and sociological insights in order to understand and manipulate human behavior. Combined with other surveillance techniques, behavior modification may become the most intrusive form of government activity in the future. Government agencies have invested millions of dollars in research to find out how people behave. Modern inquisitors have considered almost everything from using mind-control drugs to implanting computer devices in peoples' brains. It is not such a big jump from spying on peoples' behavior to trying to change their behavior. Because of the advances in technology, it is completely possible that America could slip into the everyday use of behavior monitoring and modification in the future.

It is increasingly common for American businesses to screen prospective employees and make spot checks of employees' honesty from time to time with polygraphs. Some 300,000 job-connected lie detector tests are given each year.

A former employee of a milk store chain in Georgia told how he was given lie detector tests every three months. During his last test he conceded that he had consumed some soft drinks and milk without paying. The examiner used abusive language in an attempt to intimidate the man into confessing he had taken more than he had admitted. The man called the lie detector "the newest form of torturing confessions out of citizens."

The American Civil Liberties Union, which considers polygraphs to be of "unproven reliability," says that one out

of every four potential employees tested by companies may be barred from a job because of recommendations by polygraph examiners.

The ACLU wants to ban the use of polygraphs as an invasion of privacy. Thirteen states already restrict business use of such devices. The Congressional Subcommittee on Information and Individual Rights also recommended that "the use of polygraphs and similar devices be discontinued by all government agencies for all purposes." The Privacy Protection Study Commission recommended in 1977 that a new law be enacted to prohibit private employers from using any kind of "truth verification" device.

Nevertheless, the use of such devices is on the increase and the variety of lie detecting machines is growing. They can measure psychological stress in a person's voice and how fidgety a person is (this device is known as the "wiggle seat"). There is a microwave respiration monitor, and a machine which measures the dilation of the pupil of the eye.

"The box," the standard polygraph machine, measures blood pressure, pulse, respiration, perspiration, and changes in the skin's resistance to electricity. It requires considerable equipment, including a blood pressure cuff for the arm, a bellows for the chest, wires for fingertips, and so on. The theory is that when a person tries to conceal or lie about something there are measurable physiological changes in his body.

The Subcommittee on Information and Individual Rights, however, said that "there is no 'lie detector,' neither machine nor human. People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood."

"I sure can tell if you're lying," Mike insists. Mike is a polygraph operator who has worked for police and security outfits in Virginia, just outside of Washington. He is an energetic man, a Polish-American who has adorned his office

FORD ROWAN

TECHNOSPIES

wall with cartoons about "Polacks" and squiggly graphs made by a stress evaluator stylus. One graph measures the stress of a mooning calf; another measures the stress of a calf being castrated. There is a discernible difference between the patterns.

Mike says that psychological stress can be measured by devices like the polygraph and the voice-stress analyzer. "It works," he insists. Others believe that the key to the success of any polygraph is the operator or examiner who administers the test. A good examiner gets subjective clues from watching the person being grilled, the argument goes, and the machine gives him clues only to the person's mental state. Mike, who appears to be a shrewd judge of men, does not buy the argument that it is all subjective, but he agrees that the skill of the operator makes a difference. There have been reports that only 20 percent of polygraph operators are competent. Mike doesn't think it is that bad, but he does scorn polygraph operators who ask a few questions then announce to an employer that someone lied or "flunked."

Mike is now working with voice-stress analyzers, and he says that operators of these devices must be properly trained. The voice analyzer does not require the cumbersome equipment of the polygraph machine. Answers to questions can be taped for later testing on the machine. One of the most controversial demonstrations of the voice-stress analyzer was its use by George O'Toole on tape recordings of Lee Harvey Oswald's remarks after he was arrested in Dallas in connection with the murder of President Kennedy. O'Toole concluded that the stress levels in Oswald's voice indicated he was not lying when he denied killing Kennedy.

Proponents of the voice-stress analyzer say that one advantage of the device is that it can be used surreptitiously. The person being tested need not know his voice is being recorded. Newspapers like the *National Enquirer* have used

it to evaluate the recorded comments of politicians. It has resulted in headlines like this one: "Exclusive—Scientific Evidence Proves: Ted Told the Truth About Chappaquiddick."

But does it work? The CIA, the military, and the FBI have been cautious about using voice-stress analyzers, even though alumni of those organizations developed the machines. A study made by a Fordham University psychologist for the Army in 1974 concluded that there was a "clear inferiority of voice analysis . . . not only to the polygraph but also to judgments made on the basis of simply observing subjects' behavior." Proponents of the analyzer say that it does accurately measure stress but that it does not necessarily show that someone is lying. Mike, who uses the machine regularly, says that stress might result because of a personal problem or nervousness about a particular subject rather than because the subject is lying. "But if there is no stress in an answer," Mike says, "that's a good indication the fellow is telling the truth." Other users of voice analyzers are less cautious in their claims. One Seattle, Washington, operator announced, "I am declaring war on liars, and I don't care what problems with invasion of privacy there are."

In Israel a new "microwave respiration monitor" is being tested by the police and military. The Israeli policemen aim their machine at the solar plexus of an Arab walking up to the Allenby Bridge checkpoint. As soldiers question the Arab, the microwave signal tells the police if he is breathing more rapidly than normal. If the Arab appears too nervous, the police radio the soldiers and the Arab is turned away.

Another device developed at Kent State University is supposed to tell if someone is lying even if the individual says nothing. It measures changes in the size of the pupil of the human eye as the person is asked questions. The small eye changes are supposed to show his reaction to the questions, even if he refuses to comment.

222

223

The Central Intelligence Agency is a big user of polygraphs. So many tests are made that the agency uses a computer to categorize stress measures on the individual polygraph charts. The CIA recently disclosed that over a ten-year period more than 60 percent of its job applicants were rejected as a result of lie detector tests. About half had already completed all the other security screening and been provisionally approved for employment. "Without the polygraph program," Director George Bush said in 1976, "the disqualifying information on these cases would have remained unknown." Bush defended the CIA's polygraph screening, claiming that it deters unsuitable persons from applying and keeps out foreign agents who would like to penetrate the CIA.

The debate over lie detection techniques, their accuracy and propriety, is likely to continue as their use increases and new devices become available for surreptitious testing of individuals. But one major reason for their use was summed up by Richard Nixon on a White House tape recording. "I don't know anything about polygraphs," Nixon said, "and I don't know how accurate they are, but I know they'll scare the hell out of people."

Classified CIA behavior research files show that the agency developed computerized polygraph techniques to try to test the truthfulness of its own agents and Communist defectors. The effort to use machines to test whether someone was telling the truth evolved into an effort to use drugs to force someone to tell the truth. The CIA's exotic research program shows how technology and medicine can be commandeered for surveillance and control. Most of the experiments of the past three decades fell short of the CIA's goals; one reason most of them failed was that computer techniques were still in their infancy.

* * *

224

Perhaps the most bizarre experiment ever paid for by the U.S. government was code-named MIDNIGHT-CLIMAX. The Central Intelligence Agency outfitted apartments in San Francisco and New York City in the 1950s with fancy red drapes, paintings of can-can girls, two-way mirrors, and recording equipment.

Prostitutes were hired to pick up men in local bars and lure them to the apartments, where the women gave them drinks spiked with LSD, and CIA psychologists watched what happened through two-way mirrors. But the men were not all lonely barflies. In the words of one CIA memo the tests involved "individuals from all social levels, high and low, native Americans and foreign nationals."

Many CIA counterintelligence officers are skeptical about Russian and other defectors. They suspect that defectors may have been given the mission of misleading American intelligence officials. The agency has invested significant time, energy and money into ways of testing their truthfulness, including experiments with "truth serums."

The idea was that drugs could be used to elicit honest answers not only from defectors but from the CIA's own employees, from prisoners of war, and even from people who had no idea they were being drugged. The development of truth drugs, however, was only a start. It turned out to be an easy step from research into ways of monitoring behavior to research into ways of modifying and controlling behavior.

The CIA was not the only agency involved in drug experimentation. In 1948 the CIA, the FBI, and the military services established Project CHATTER to find a drug that would force people to talk against their will. Over the years the FBI dropped out, but the CIA and the Army steamed full speed ahead.

Everyone is aware of the arms race, but few people know that there was a behavior control race. In the early 1950s the

225

Soviet Union was believed to have a mushroom that induced hallucinations, so the CIA started trying to grow a fungus that induced hallucinations.

CIA behavior research was stepped up during the Korean War. The agency was worried about Communist efforts to brainwash American soldiers captured in Korea. Some American POW's had a memory lapse, a period of disorientation, after passing through Manchuria. The CIA wanted to subject the returning POW's to interrogation with truth serum, but the Army refused permission. So the CIA set up the ARTICHOKE team to develop behavior control techniques using drugs, electro-shocks, aphrodisiacs, lie detectors, hypnosis, and extrasensory perception. It arranged to buy 100 million doses of LSD.

ARTICHOKE was renamed Project ULTRA, and from 1952 until 1967 drug experiments were conducted at eighty institutions—colleges, prisons, hospitals, research companies. Knockout drugs were tested on unwitting patients suffering from terminal cancer. Prisoners were given drugs which caused loss of speech, loss of memory, loss of will power, and had the capability of putting them in a catatonic stupor. Hallucinogens were slipped into the mixed drinks of unsuspecting people. Exotic toxins were developed which could inflict instant death. At least two people died because of the tests. The CIA conceded later that some of the research was "considered to be professionally unethical." Twenty years after research along these lines was begun, the Army surgeon general said that some of the experiments on military facilities violated the Nuremberg war crimes codes, which require that people subjected to experiments first give their consent.

In 1962 Congress enacted a law to safeguard people involved in drug tests. The law provided that the Food and Drug Administration monitor the experiments. The law was aimed at research by private drug companies, but it was

226

clear it referred to all testing, including government-sponsored tests.

The CIA simply ignored the law. And the military actually drafted a memo saying it was exempt from the law. This 1964 "Memorandum of Understanding" was drawn up so that if the military approved a secret drug test it "will automatically exempt the drug" from the application of the law. The memorandum was signed by then Deputy Defense Secretary Cyrus Vance. Accompanying regulations which implemented this "exemption" were signed by then Director of Defense Research Harold Brown.

This arrangement to escape FDA scrutiny was later labeled as illegal by the General Accounting Office. Vance was named Secretary of State by President Carter; Brown was named Secretary of Defense. While there is no evidence either Brown or Vance knew about the unusual drug experiments, no official inquiry has ever been undertaken on how high up the Pentagon chain of command the drug tests were evaluated.

Permitting the military and agencies like the CIA to experiment with behavior-altering drugs is especially dangerous to a free society. Monitoring is only the first step for a covert intelligence outfit. As night follows day, covert operations follow intelligence collection in an agency like the CIA.

The operational side of the CIA has dominated the side that gathers information. In the CIA covert action came to be more important than the analysis of the information which was collected. This trend has affected not only foreign intelligence but the FBI's domestic intelligence operations as well. COINTELPRO disruption programs became more important than the evaluation of information about what was actually happening in the ghettos and on campuses.

In behavior research the emphasis also shifted from ways to monitor behavior to ways to manipulate it. The CIA's Proj-

227

FORD ROWAN

ect ULTRA was designed to consider "possible means for controlling human behavior of which drugs were only one aspect. . . ." Other means included "radiation, electro-shock, psychology, psychiatry, sociology, anthropology, graphology, harassment substances, and paramilitary devices and materials."

ULTRA was the research program and DELTA was the operational program, designed in the words of one CIA memo "for the use of biochemicals in clandestine operations."

A 1963 report by the CIA's inspector general noted "major accomplishments both in research and operational employment" of ULTRA and DELTA techniques. The inspector general reported that the CIA had developed "chemical, biological, and radiological materials capable of employment in clandestine operations to control human behavior." This is an incredible power for any agency, especially a clandestine agency, to possess. We have learned a great deal about the experimental programs of ULTRA, but almost nothing has been revealed about DELTA.

The CIA insists it halted the drug testing program in the 1960s. But a 1975 CIA memo documented the agency's continuing interest in behavior control, affirming that the agency conducts "a many-disciplined research program encompassing activities in the physical, life, and social sciences. Research activities include life sciences research, in behavior sciences, physiology, and the related physical science materials with emphasis on assessment, health, bionics, narcotics, and biological and chemical warfare materials."

Although the most odious drug experiments have been stopped, the CIA continues to show an interest in behavioral techniques to control or change the way people act and think.

*　*　*

228

Glossary

ARPA—The Defense Advanced Research Projects Agency is a foremost sponsor of research into computers and surveillance systems.

ARPANET—An advanced computer network set up by ARPA to link universities, think tanks, and military research installations; it has served as a model for new telecommunications systems.

ARS—The Advanced Record System was designed by the General Services Administration to handle messages for government agencies; shortcomings in the system have prompted proposals to upgrade the ARS for computer communications.

Biocybernetics—The study of ways to link men and computers is now being sponsored by ARPA and other government agencies.

CHAOS—The Central Intelligence Agency code-named its domestic surveillance program of the antiwar period Operation CHAOS; facts were gathered on 300,000 Americans.

COINS—One of the communications links which connect computers in the various agencies of the U.S. intelligence community is code-named COINS; the system is being upgraded to ARPANET standards.

Cointelpro—The FBI's counterintelligence program resulted in the disruption and harassment of American citizens who were considered radical or extremist by the bureau's leadership.

Covert Action—This term usually refers to the CIA's secret operations overseas, but it also applies to FBI operations like Cointelpro.

DAME, DASE—These terms are used by Army Intelligence to refer to methods of defending against break-ins (DAME), and electronic surveillance (DASE); but agents who were trained in these methods say they were actually taught how to conduct burglaries and wiretaps.

DOMS—The Pentagon's Division of Military Support coordinates the Armed Forces planning and operations to suppress domestic insurrection in the United States.

EFTS—Electronic Fund Transfer Systems are being used by banking and credit card companies to permit merchants and customers in widely dispersed areas to use central computers to handle financial transactions without cash.

Elsur—Electronic Surveillance comes in three basic forms: Bugging picks up conversations via hidden microphones, wiretapping picks up conversations directly from telephone lines, and radio interception picks up messages sent by air—including long-distance phone calls relayed by microwave towers.

FEDNET—In the 1960s the General Services Administration proposed upgrading a communications system to serve

various government agencies, but critics managed to get this computer network killed because they feared it would be a threat to personal privacy.

FPA—The Federal Preparedness Agency, like its predecessor the Office of Emergency Preparedness, is in charge of coordinating the government's readiness for emergency; it runs hidden headquarters like Mount Weather.

Garden Plot—The Pentagon's plan for coping with civil disturbances in the United States is code-named Garden Plot; the plan has been put in effect to handle racial incidents.

Gram Metric—This term was used as the code-name of one of the Pentagon's biggest command post exercises in which a war game simulated conditions of domestic unrest in American cities.

Harvest—The National Security Agency has a mammoth computer operation which harvests, correlates, and stores information gathered from electronic eavesdropping.

HYDRA—The Central Intelligence Agency put the information gathered during its domestic surveillance program into a computer system which it called HYDRA because the machine could process multiple streams of information.

Huston Plan—During the Nixon Administration a White House aide named Tom Charles Huston drew up a proposal for the President outlining illegal intelligence operations which secretly were being carried out by government agencies inside the United States.

IEC—The Intelligence Evaluation Committee was one of several coordinating bodies set up during the antiwar period to try to impose some central planning and operational control over the domestic activities of the FBI, the CIA, and other intelligence operations.

IDIU—The Inter-Divisional Information Unit attempted to coordinate domestic intelligence activities and centralize information into computerized form in the Justice Department.

IDRS—The Internal Revenue Service maintains a nationwide system so tax collectors can check out information in computers about taxpayers; it's known as the Integrated Data Retrieval System.

IGRS—During the period of antiwar protests, the Internal Revenue Service used to run something called the Information Gathering and Retrieval System, which stored intelligence information about 465,442 people.

KBE—During the period of racial protest the FBI kept a list of black civil rights leaders which it called the Key Black Extremist Index.

Message Switching—New computer technology has made it possible for telecommunications networks to transmit and store messages across the country; the FBI wants to utilize this technology to coordinate state and local police data communications.

Microwave—From ovens to telephones, the technology of using microwaves is making life more efficient; but when microwaves are used to relay long-distance telephone calls it becomes very easy for anyone with the proper radio equipment to listen in.

MINARET—During the protests against the Vietnam War, the National Security Agency instituted a watch list of Americans involved in protest activities so that their communications with persons overseas could be monitored and given to the CIA and FBI for evaluation.

Mount Weather—One of several underground bunkers which the federal government maintains in the mountains to the west of the nation's capitol to be used as a headquarters in the event of an emergency.

NCIC—The FBI's National Crime Information Center is a

FORD ROWAN

computerized system which local and state police departments can use for such purposes as checking on wanted persons and stolen cars.

OTP—The Office of Telecommunications Policy in the White House had been in charge of coordinating communications planning; the Carter Administration has shifted this responsibility to the Commerce Department.

Polygraph—Electric devices which monitor physiological changes in an individual who is being interrogated are widely used in an effort to detect lies; their accuracy, however, is questionable.

Rabble Rouser Index—The Federal Bureau of Investigation maintained a variety of lists of suspected subversives during the directorship of J. Edgar Hoover; the Rabble Rouser Index contained hundreds of names of social activists.

SAD—The Special Analysis Division of the emergency preparedness program was in charge of developing ways to control information and impose censorship in America.

Security Index—The FBI's most important list of suspected subversives totaling thousands of names was secretly maintained for four decades; shortly before it was abolished in the mid-1970s the list was computerized.

Special Service Staff—The Internal Revenue Service established this staff during the period of antiwar protests as part of the interagency effort to keep track of and disrupt protesters.

Tiger Teams—This term is used to describe teams of military computer experts who test the security of computers by trying to penetrate —and usually succeeding in doing so—supposedly secure systems.

Zenith—This code-name was used to describe the efforts during the Nixon Administration to upgrade the White House Computer operation.

254