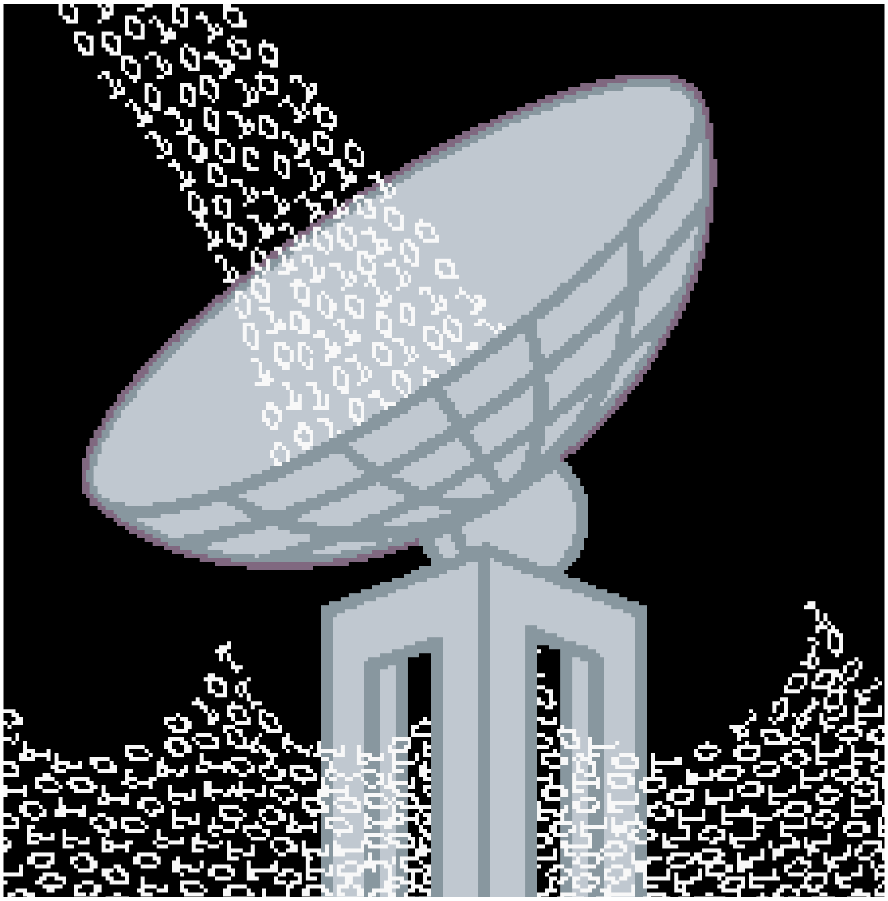
ANNALS OF NATIONAL SECURITY

THE INTELLIGENCE GAP

How the digital age left our spies out in the cold.

BY SEYMOUR M. HERSH



CHRISTOPH NIEMANN

The National Security Agency, whose Cold War research into code breaking and electronic eavesdropping spurred the American computer revolution, has become a victim of the high-tech world it helped to create. Through mismanagement, arrogance, and fear of the unknown, the senior military and civilian bureaucrats who work at the agency's headquarters, in suburban Fort Meade, Maryland, have failed to prepare fully for today's high-volume flow of E-mail and fibre-optic transmissions—even as nations throughout Europe, Asia, and the Third World have begun exchanging diplomatic and national-security messages encrypted in unbreakable digital code.

The N.S.A.'s failures don't make the headlines. In May, 1998, India's first round of nuclear tests, which took place in Pokharan, southwest of New Delhi, caught Washington by surprise, and provoked criticism of the Central Intelligence Agency from the press and from Congress. But it was the N.S.A., in the days and weeks before the detonations, that did not detect signs of increased activity or increased communications at Pokharan. "It's a tough problem," one nuclear-intelligence expert told me, because India's nuclear-weapons establishment now sends encrypted digital messages by satellite, using small dishes that bounce signals beyond the stratosphere through a system known as VSAT ("very small aperture terminal")—a two-way version of the system widely used for DirecTV.

Similarly, the North Koreans, with the help of funds from the United Nations, according to one United States intelligence official, have bought encrypted cell phones from Europe, high-speed switching gear from Britain, and up-to-date dialling service from America—a system that the N.S.A. cannot readily read. The official said of the North Koreans, "All their military stuff went off ether into fibre"—from high-frequency radio transmission to fibre-optic cable lines, which transmit a vast volume of digital data as a stream of light. A former high-level Defense Department official told me, "It's a worldwide problem. You could wire up all of Africa for less than two billion dollars." This former official, like most of the two dozen signals-intelligence (SIGINT) experts interviewed for this account, agreed to speak only after being assured of anonymity. A 1951 federal law prohibits any discussion or publication of communications intelligence.

The decline of the N.S.A. is widely known in Washington's national-security community. "The dirty little secret is that fibre optics and encryption are kicking Fort Meade in the nuts," a recently retired senior officer in the C.I.A.'s Directorate of Operations told me. "It's over. Everywhere I went in the Third World, I wanted to have someone named Ahmed, a backhoe driver, on the payroll. And I wanted to know where the fibre-optic cable was hidden. In a crisis, I wanted Ahmed to go and break up the cable, and force them up in the air"—that is, force communications to be broadcast by radio signals. The number of daily satellite-telephone calls in the Arab world, many of which are encrypted, is in the millions, creating severe difficulties for eavesdroppers. The mobile-telephone system used by Saddam Hussein at the height of Iraq's dispute last year with a United Nations arms-control inspection team operated on more than nine hundred channels. Each channel was separately encrypted, with multiple keys, and Saddam's conversations bounced from channel to channel with each call. A U.N. intelligence team eventually gained access to the telephone system's technical manuals and other data, and was able to record the encrypted conversations, but without these materials it could not have made sense of the intercepts. The code-makers are leaving the code-breakers far behind.

IN its heyday, during the Cold War, the N.S.A. had nearly ninety-five thousand employees, more than half of them in the military, monitoring communications from hundreds of sites around the world. It played a dominant role in American intelligence gathering behind the Iron Curtain and elsewhere, producing by the end of the nineteen-sixties more than a thousand intelligence reports a day. The N.S.A.'s intercepts were the government's most reliable and important sources of intelligence on the Soviet Union—far outstripping the intelligence collected by the C.I.A. and its agents abroad. In Western Europe, N.S.A. linguists and Army G.I.s sat in unmarked vans monitoring the daily conversations of Soviet tank units on the other side of the Berlin Wall. In the Pacific, Air Force radiomen and N.S.A. technicians, in specially configured Boeing 707s, flew huge figure eights over the ocean, copying Morse-code transmissions from North Korea and the Soviet Far East. In the Mediterranean, Navy signalmen worked hectic shifts with their N.S.A. colleagues, eavesdropping on government communications in the Middle East. Many of the most sophisticated Soviet codes were broken, including the diplomatic traffic to Moscow from its Embassy in Washington. By the time President Nixon was in office, the agency was listening to telephone conversations of Soviet leaders as they were driven in limousines to and from the Kremlin. In the upper reaches of the United States government, access to the agency's daily top-secret "take" was a sign of importance and success. Henry A. Kissinger, Nixon's national-security adviser, went as far as to order the agency to scan the diplomatic traffic from Washington, isolate references to him, and deliver the cables to his office, without any further distribution inside the government. Many of his successors have received the same service.

These successes were the payoff for years of painstaking technical research. In the nineteen-fifties and sixties, the N.S.A.'s engineers, working closely with the American computer industry, coördinated and financed much of the early work in telecommunications, underwriting research on semiconductors, high-speed circuitry, and transistorized computers. With its research into microelectronics, the agency also helped to develop the early guidance systems for intercontinental ballistic nuclear missiles. And the agency's team of mathematicians—aided by outside advisers, many of whom were tenured at places such as Harvard, Dartmouth, and Princeton—steadily tore through the Soviet cipher systems.

By the mid-seventies, as the world began routinely communicating by microwave, the agency maintained its edge with innovative use of satellite intelligence, and its mathematicians and computer experts were sometimes able to thwart the Russians' attempts to scramble their signals. Even undersea and underground coaxial cables—the most secure means then of relaying telephone conversations and electronic communications—could be intercepted. Books and newspaper articles have described the penetration of Soviet cables at sea by N.S.A. units aboard Navy submarines as some of the most daring intelligence operations of the Cold War.

The collapse of Communism, in 1989, and the collapse of the Soviet Union, in 1991, led to a revised mission for the N.S.A., with more focus on international terrorism and drug dealing—both highly elusive targets. The agency's budget was cut back. In the early nineties, as more nations turned to fibre optics, the N.S.A. shut down twenty of its forty-two radio listening posts around the world. (In some cases, equipment was left behind to be monitored remotely.) The agency's overseas military personnel have been reduced by half.

The N.S.A.'s status within the government has also been diminished. Last year, Richard Lardner, a reporter for the Washington newsletter *Inside the Pentagon*, revealed that the agency had been "reined in" and would no longer be authorized to report directly to the Secretary of Defense. The N.S.A. was ordered instead to report through an Assistant Secretary. In recent years, according to a congressional study, the N.S.A.'s contribution to the President's daily intelligence brief—a secret summary prepared at the C.I.A. every morning for the White House—has fallen by nearly twenty per cent. The N.S.A. was being jarred by the difficulties of tracking terrorism, and by the rapid spread of unbreakable codes. The agency also discovered that it had few advocates in the White House and among those officials at the Office of Management and Budget who control the flow of money to the top-secret world. The agency was not allowed to keep the funds it had saved by reducing manpower and drastically cutting overseas stations.

The N.S.A. is also getting very little help from its colleagues in the American intelligence community. One legislative aide told me that George Tenet, the director of Central Intelligence, who has nominal responsibility for all intelligence gathering, had expressed alarm upon taking office about the N.S.A.'s weakness, and told congressmen of his desire to rescue the agency from what appeared to be a "precipitous calamity." But, the aide added, "he didn't do it."

The N.S.A.'s strongest supporters—the members and staffs of the Senate and House intelligence committees—are also its most vocal critics. The agency is now facing the most caustic congressional scrutiny in its history, amid much pessimism that it can right itself without major changes in its management. Staff members of the intelligence-oversight committees traditionally prefer not to be quoted by name, but John Millis, a former C.I.A. officer who is staff director of the House intelligence committee, openly discussed the N.S.A.'s problems in the fall of 1998 at a luncheon meeting with a group of retired C.I.A. officers. "Signals intelligence is in a crisis," Millis told his former colleagues, who reprinted the speech in a newsletter. "We have been living in the glory days of SIGINT over the last fifty years, since World War II." He went on, "Technology has been the friend of the N.S.A., but in the last four or five years technology has moved from being the friend to being the

enemy." Millis also made it clear that any significant increase in the agency's budget was made more difficult by the fact that "there is no management of the intelligence community. There is no one in a position to make the tradeoffs within the intelligence community that will make a coherent, efficient organization that will function as a whole. So we end up doing it on Capitol Hill. And I've got to tell you, if you are depending on Capitol Hill to do something as important as this, you're in trouble."

Senator Robert Kerrey, of Nebraska, the ranking Democrat on the Senate's intelligence committee, told me that there was little he could add to Millis's assessment, because most information dealing with the agency and its work is highly classified. Kerrey also pointed out that secrecy "does not equal security," and can be self-defeating. For example, the agency is in desperate need of more money to get started on information-retrieval programs for the Internet which should have been under way years ago. "But I can't tell you how much they need," Kerrey said, "and I can't tell you how much they have. The public doesn't know about the N.S.A., or what it is. There are no editorials in the New York *Times*, no advocates. Does the public know that the nation might be more secure if more was invested? Out of sight, out of mind."

Last July, during a little-noticed Senate colloquy on an intelligence-spending bill, Kerrey hinted at the N.S.A.'s problems. "The signals are becoming more complex and difficult to process," he said. "And they are becoming more and more encrypted." Because of the sophistication of current encryption systems for E-mail and other communications, he said, "we will find our people on the intelligence side coming back and saying, 'Look, I know something bad happened . . . I couldn't make sense of the signal. We intercept, and all we get is a buzz and background noise. We cannot interpret. We can't convert it.' "

Kerrey says that his concern was heightened by a report on the N.S.A. that was filed last year by an unusual study group that he and Senator Richard C. Shelby, Republican of Alabama and the committee's chairman, had put together. Secret congressional studies are routine, but the Senate team, known as the Technical Advisory Group, included a number of prominent outsiders—men who were in charge of research and technology for major American high-tech corporations, such as George Spix, of Microsoft, Bran Ferren, of the Walt Disney Company, and a nuclear-weapons physicist, Dr. Lowell Wood, of the Lawrence Livermore National Laboratory. The outsiders were given full clearance and access to many of the most sensitive areas at the Fort Meade headquarters. Their conclusions were devastating. "We told them that unless you totally change your intelligence-collection systems you will go deaf," one involved official told me. "You've got ten years."

The advisory group put much of the blame for the agency's problems on the stagnation and rigidity of the senior civilian management. "The N.S.A.'s party line to Congress is 'We're fine. We don't need to change,' " the official told me. "It's like a real Communist organization. Free thought is not encouraged" among the managers. Referring to the senior bureaucracy, the official said that the agency would "have to fire almost everyone." This official and others singled out Barbara A. McNamara, the current N.S.A. deputy director, as someone especially resistant to change. "She's leading a cohort of thirty-year veterans who go back to radio"—a reference to high-frequency radio transmissions—"and think nothing is needed," the official said. In secret testimony this fall before Congress, he added, McNamara talked about "how good the N.S.A. is—how it caught this and that drug guy. They got a whole bunch of horseshit from Barbara."

In subsequent interviews, many former N.S.A. managers endorsed the advisory group's findings. One former official described the civilian leadership as "a self-licking ice-cream cone," with little tolerance for dissent or information it did not wish to hear. "If you didn't support their position, you weren't considered a team player," this person told me. "You couldn't go into a meeting, put your best ideas on the table, have it out, get the best idea, and then go have a beer." McNamara's authority stems from her longevity: the admirals and generals who serve the agency director remain on the job for an average of three years before retiring or going on to other military assignments. The agency's top civilians have worked together, in many cases, for nearly thirty years, and inevitably share the same insular points of view. Another recently retired official told me that the N.S.A. has become a dynastic bureaucracy, in which the fathers have made room for their sons, with the wives and mothers of favored employees hired as mid-level staff in the human-resources office. "The place is full of warlords and fiefdoms," the former official said. "Now we're getting to the *grandchildren*." Such insider hiring has led to the quip, which I heard from a number of officials, that the N.S.A. functions as a "Glen Burnie W.P.A. project." Glen Burnie is a nearby suburb, and home to many N.S.A. employees. Questions also were raised during my interviews about the effectiveness of many of the senior military officers who are routinely assigned to the N.S.A. for two-, three-, or four-year tours of duty. Some perform brilliantly, but far too many find themselves put in charge of units for which they are unqualified, and end up relying extensively on their civilian staffs. "We call them the summer help," a former manager told me, adding that the smart ones generally seek to get reassigned as soon as possible.

The Technical Advisory Group urged that the agency immediately begin a major reorganization, and start planning for the recruitment of several thousand skilled computer scientists. One of their missions would be to devise software and write information-retrieval programs that would enable the agency to make sense of the data routinely sucked up by satellite and other interception devices. The vast majority of telephone calls, E-mails, and faxes are not encrypted—almost all are sent as plain text—but the N.S.A. has been overwhelmed by the sheer volume of the intercepted data, much of which is irrelevant. "They're still collecting a lot of digital," one of the agency's consultants told me, "and can't do anything with it." The consultant added that agency managers recently estimated that Fort Meade had three years' worth of storage capacity for intercepted Internet traffic. "They filled it in eleven months," he said.

"The bottom line is they've got to retool," the advisory-group official said. "It will take a lot of money and effort—like starting the N.S.A. again." Far from being able to retool, the agency has suffered a severe brain drain in recent years, losing mid-career managers to the high pay and upward mobility of private industry. One former senior official described the process as self-defeating: the agency's recognized need for more outside contact with, and stimulation by, the computer world is offset by the fact that its budding young experts "meet new people and then get hired away by them."

The N.S.A.'s current alienation from the computer gurus in industry and academia might not have occurred if two Californians with a fascination for the mathematics of cryptoanalysis hadn't decided to compare notes more than two decades ago. A 1951 law gave the government the right to classify as secret any invention considered potentially harmful to national security, but in November, 1976, Whitfield Diffie, a computer scientist, and Martin E. Hellman, a Stanford University electrical engineer, published a revolutionary technical paper on what has become known as public key cryptography. Before their work, an encrypted message could be understood only if the sender and receiver had the same key, or decoder, to turn the scrambled letters into readable text. The beauty of the Diffie-Hellman breakthrough was its simplicity: the message would have two keys—one could be registered in a public directory (today it might be on the Internet) and the other would be known only to the intended recipient. One key would be used to encipher the message and the other to decipher it. A senior N.S.A. official has described the Diffie-Hellman concept as a series of computations that are easy to do but hard to reverse, like breaking a window.

To the agency's dismay, the world now had access to a sophisticated level of cryptography that had not been previously fully understood even by N.S.A. analysts. In 1978, when George I. Davida, a computer scientist at the University of Wisconsin, tried to patent an encryption device he had invented, the N.S.A. invoked the 1951 secrecy law. Davida took his case to the media, and the agency, prodded by attorneys in the Carter Administration, eventually backed down, but the message was clear—the agency would do all it could to prevent public access to encryption techniques.

By the early nineties, the telephone system had been deregulated, the computer market was booming, and the Internet was beginning its ride, but the N.S.A.'s policy remained static: encryption was defined as a "weapons system" whose export was controlled by the government. The debate over encryption was now a public controversy, with the government arrayed against privacy advocates, academics, and a computer industry that was bemoaning the annual loss of billions of dollars to foreign manufacturers whose computers included high-powered encryption.

In 1993, law-enforcement officials further infuriated the computer industry by beginning a criminal investigation of Philip R. Zimmermann, a software engineer then living in Boulder, Colorado. Zimmermann's crime was being a free-spirited hacker; he cobbled together a cryptography program called P.G.P.—for Pretty Good Privacy—and gave it away. P.G.P. was the agency's nightmare—it offered the average computer user a nontechnical and nonthreatening entry into easy, daily use of cryptography. P.G.P. soon found its way to the Internet, and it quickly spread around the world—making Zimmermann, in the government's view, an exporter of munitions. A grand-jury inquiry began. The computer industry rallied around Zimmermann, and after three years the case was dropped. Zimmermann eventually explained to a Senate committee, "I wrote P.G.P. from information in the open literature.... This technology belongs to everybody." By the mid-nineteen-nineties, the Software Publishers Association was telling journalists that the number of cryptographic products being sold by foreign companies had reached three hundred and forty.

President Clinton and his senior advisers, under pressure from the law-enforcement and national-security communities, tried to compromise on the issue. The export of encryption for computers could go forward, the government said, if the industry agreed to install a government-approved encryption chip, known as the Clipper Chip, that could be directly accessed by law-enforcement officers. Under another proposal, American computer manufacturers would have been permitted to export new encryption products if a spare set of decoding keys were accessible to the government. The proposals, known as key recovery or key escrow, were assailed by privacy proponents, who demanded to know whether the Clinton Administration would have dared to advocate that citizens be required to give the keys to their house or safety-deposit box to a third person.

The cultural divide between Fort Meade and Silicon Valley was widening. The agency's senior managers were unable to comprehend what every programmer and researcher in academia and industry intuitively understood: encryption could not be stopped. The managers had ample warning. In 1991, a secret study predicted that the use of encryption would grow exponentially—a prediction largely ignored by the agency's senior management. A former N.S.A. director recalled that in the early nineties he had had a series of conversations with the civilian managers, urging them not to insist on their version of key recovery. "I couldn't believe their proposals," he said, adding that he had warned the managers that, given the public's attitude toward privacy, key recovery "could not work if the government held the key. They were so arrogant. They knew all there was to know."

"Export control is a legitimate concern to the agency," one former senior official told me, but the issue made the top managers "paralyzed and afraid to move into the future." He and many colleagues had argued for a two-prong approach—continuing to do all that was possible to maintain export controls while also planning for a fully encrypted world. The agency's long fight against encryption delayed its widespread use by many years, but the agency's senior managers spent those years "holding on to what we have today" instead of seeking ways to lessen encryption's impact. The official lamented, "We were squandering time" while continuing to make more enemies inside the computer industry.

Today, the encryption fight is all but over. The Commerce Department is scheduled to issue new export regulations on December 15th that, many experts believe, will permit American computer companies to include advanced cryptography, with fewer restrictions, on equipment sold worldwide. "We've won," Phil Zimmermann told me, jubilantly. "And they tried to put me in prison! Now we can export strong crypto and they can't stop us. We can do whatever we wish."

The N.S.A.'s short-term solution to the encryption dilemma has been to urge the C.I.A. to go back to the world of dirty tricks and surreptitious entry. According to a 1996 congressional staff study, the next century will require a clandestine agency that "breaks into or otherwise gains access to the contents of secured facilities, safes and computers" and "steals, compromises and influences foreign cryptographic capabilities so as to make them exploitable" by the N.S.A.

Such information theoretically could help Washington's policymakers disrupt future terrorist activity, intercept illicit shipments of nuclear arms, or uncover acts of espionage against American defense corporations. Unfortunately, several C.I.A. officers I spoke with found the proposal too ambitious. One retired case officer told me that while he was on a clandestine assignment years ago in the Third World, "I was designated to get a certain black box. I worked on it for three and a half years, and I got nowhere. If I had worked on it for ten years, and with a true stroke of luck, I might have gotten within ten feet of it." Another retired operations officer, similarly skeptical of the C.I.A.'s chances of obtaining cryptological intelligence, told me that sometimes the clandestine operatives in the field have to report back, "This is too hard. "

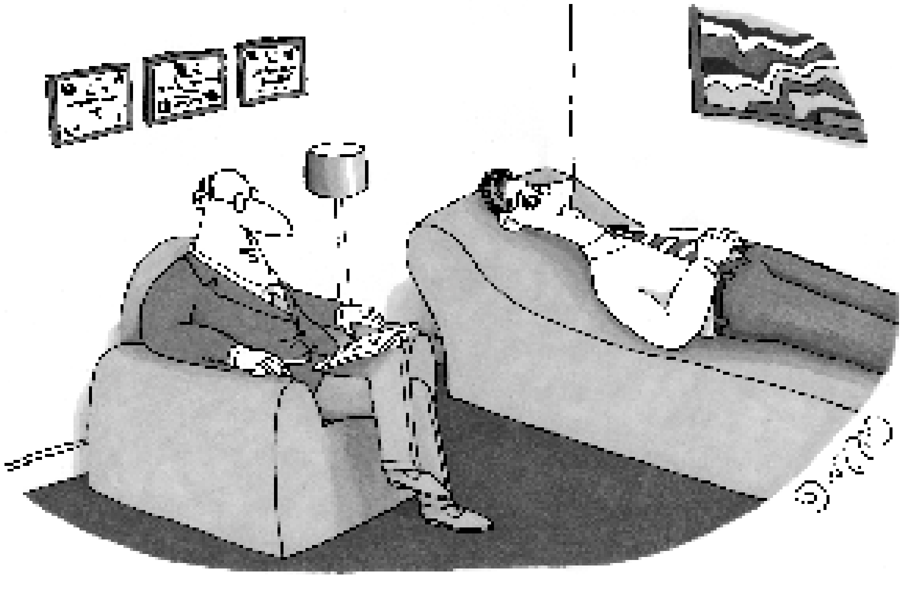
MANY Americans, of course, are deeply distrustful of the N.S.A.—a view reflected in recent Hollywood movies like "Enemy of the State" and "Mercury Rising." The traditional American belief in privacy and constitutional protection is at odds with a superspy agency capable of monitoring unencrypted telephone conversations and E-mail exchanges anywhere in the world. Abuses have occurred. In the nineteen-seventies, the Senate intelligence committee revealed that the agency had systematically violated the law by surveilling American citizens, including more than twelve hundred antiwar and civil-rights activists. The revelations led to a public outcry and to the 1978 Foreign Intelligence Surveillance Act, which made monitoring of American targets illegal without a warrant from a special federal court. (The court rarely turns down such requests from the government.) The act, and a supporting executive order, set rules for the handling of intercepts or other intelligence involving Americans who were overheard or picked up in the course of legitimate foreign surveillance.

The N.S.A.'s bitter fight over encryption, with its tell-all computer chips and key-recovery proposals, has renewed longstanding fears that one of the agency's satellite-data collection programs, codenamed ECHELON, is routinely collecting and analyzing unencrypted telephone conversations and Internet chatter around the world. ECHELON was launched, in the mid-nineteen-seventies, to spy on Soviet satellite communications. "Imagine," the BBC exclaimed last month—one of hundreds of such reports in the past ten years—"a global spying network that can eavesdrop on every single phone call, fax, or E-mail, anywhere on the planet. It sounds like science fiction, but it's true." The agency does routinely collect vast amounts of digital data, and it is capable of targeting an individual telephone line or computer terminal in many places around the world. But active and retired N.S.A. officials have repeatedly told me that the agency does not yet have the software to make sense out of more than a tiny fraction of the huge array of random communications that are collected. If the agency *were* able to filter through the traffic, the officials noted, international terrorists like Osama bin Laden would not be able to remain in hiding. The fact is that ECHELON, far from being one of the N.S.A.'s secret weapons, as some believe, is viewed as a fiscal black hole by the Senate and House intelligence committees.

John Millis, in his private talk to the retired C.I.A. agents, complained that the United States was spending "incredible amounts of money" on satellite collection. "It threatens to overwhelm the intelligence budget." Using satellites to sweep up communications indiscriminately, he said, "doesn't make a lot of sense. . . . You shouldn't be spending one more dollar than we do to try and intercept communications from space." Millis's point was that the data collected from sate lites, like the data collected from the Internet, cannot be sorted or analyzed in any meaningful way.

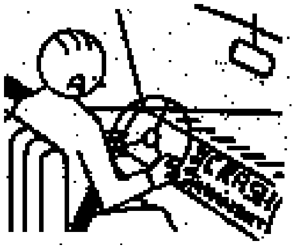
THE agency's critics, in and out of the government, told me that they see a glimmer of hope for the N.S.A. in the appointment, last May, of Lieutenant General Michael Hayden as its new director. Hayden, who joined the Air Force after earning a master's degree in American history at Duquesne University, in Pittsburgh, has been praised for his intelligence and open-mindedness. "Hayden gets it," one intelligence-committee aide told me. "But he's parachuted in there, and faced with a deputy director whose job is to foil what the director wants to do. There's no question that it's the hardest job in the intelligence community. He's got to manage a multibillion-dollar corporation that has a blue-collar mentality."

General Hayden's initial goal will be to convince Congress and the White House that he can do what his predecessors did not—develop a specific



"I'll say a normal word, then you say the first sick thing that pops into your head."

management plan and a budget for analyzing intelligence from the Internet and other digital sources. "We've criticized the N.S.A. for not having a well-coördinated strategy," one legislative aide told me, "but we're not in a position to tell them where to go." The issues, of course, are highly technical, and it's not clear that more money—even billions of dollars—will get the job done. The amount of data flowing through the Internet is growing exponentially, and skilled computer scientists are at a premium. The agency's war against encryption has left a legacy of bitterness throughout the computer industry, and today's technical advances are taking place not at Fort Meade but on university campuses and in corporation laboratories across America. Those computer whizzes who might have been attracted to high-level government work are instead being attracted by the far higher pay scales offered by private industry.



There also is little evidence that President Clinton and his national-security team view the agency's signals-intelligence plight as significant. This year's classified Defense Department budget request included a boost of nearly two hundred million dollars for the agency, with the funds earmarked for long-range research into signals intelligence. The money never made it through the White House's Office of Management and Budget, however. "George Tenet didn't support it," a former congressional aide explained. A similar secret request, for four hundred million dollars or more to modify the Jimmy Carter, a Seawolf-class nuclear submarine, for top-secret agency intelligence work, was approved—evidence that the White House believes that more covert operations will solve the nation's coming intelligence problems.

Hayden also will have to contend with those, in and out of the government, who remain dubious about the N.S.A. One firm skeptic is the encryption expert Whitfield Diffie, who is now at Sun Microsystems. Diffie, a leading advocate of computer privacy, was quick to suggest that the current alarm in the N.S.A. may be a self-interested ruse. When I brought up the N.S.A.'s problems with new technology, he replied, "What bothers me is that you are saying what the agency *wants* us to believe—they used to be great, but these days they have trouble reading the newspaper, the Internet is too complicated for them, there is so much traffic and they can't find what they want. It *may* be true, but it is what they have been 'saying' for years. It's convenient for N.S.A. to have its targets believe it is in trouble. That doesn't mean it isn't in trouble, but it is a reason to view what spooky inside informants say with skepticism."

Shortly after his appointment, Hayden assembled a group of highly regarded mid-level managers and gave them free rein to evaluate the agency. He also began a series of meetings, outside Fort Meade, to get independent advice. The evaluations were consistently "brutal," according to one official, in terms of the ongoing management problems. On November 15th, Hayden announced to the N.S.A. workforce that he was beginning what he called One Hundred Days of Change. The next day, he made his move against the establishment. He dissolved the agency's leadership structure, despite a bitter protest from Barbara McNamara, and announced the formation of a five-member executive group, under his leadership, which would be responsible for decision-making.

Last month, General Hayden agreed to speak to me, at his unpretentious top-floor offices at Ops 2, the N.S.A. headquarters building. He is an affable spymaster, who laughs easily, offers no slogans, and promises no quick fixes for the agency's problems. He seemed to understand that his new troops—computer gurus and mathematicians—are unlike any others he had commanded before.

When I brought up the agency's long-standing war against the export of encryption, Hayden quickly dismissed it as yesterday's lost battle. He also took issue with those who criticized Barbara McNamara and other civilian managers for their failure to anticipate the communications upheaval. "Barbara McNamara has been a good deputy to me," he said. "But I make the decisions."

Hayden emphasized that the personnel problems are far less significant than the technological ones: "The issue is not people but external changes. For the N.S.A., technology is a two-edged sword. If technology in the outside world races away from us—at breakneck speed—our mission is more difficult. It can be our enemy."

When I asked Hayden about the agency's capability for unwarranted spying on private citizens—in the unlikely event, of course, that the agency could somehow get the funding, the computer scientists, and the knowledge to begin making sense out of the Internet—his response was heated. "I'm a kid from Pittsburgh with two sons and a daughter who are closet libertarians," he said. "I am not interested in doing anything that threatens the American people, and threatens the future of this agency. I can't emphasize enough to you how careful we are. We *have* to be so careful—to make sure that America is never distrustful of the power and security we can provide."

General Hayden made no effort to minimize his agency's plight. During the Cold War, he said, the N.S.A. was "technologically more adept than our adversary. Now it's harder to predict where America's interests will need to be in the future." His goal in the near future, he added, speaking carefully, is to determine which of the agency's past practices are applicable to today's high-tech world—"and which of them may be counterproductive."

"A lot of the choices are Sophie's choices," he said. "The trade-off is between modernization" (recruiting computer scientists and beginning long-range programs to tackle the Internet) "and readiness"—that is, meeting the hectic operational needs of the Defense Department and the White House for immediate intelligence. "We have a high ops tempo," he added, "but choices have to be made." In other words, he made clear, some ongoing N.S.A. intelligence-collection programs will have to be curtailed, or eliminated, so that funds are available for futuristic research.

"In its forty-year struggle against Soviet Communism," Hayden noted, "the N.S.A. was thorough, stable, and focussed." Then he asked "What's changed?" and he answered, "All of that." ♦

With our powers of reasoning, rich memories and the ability to imagine what the future might hold, human intelligence is unequalled in the animal kingdom. Our closest relatives, chimpanzees, are adept problem solvers, making their own tools to reach food, for example.Â Thomas Suddendorf, a psychologist at the University of Queensland, describes this as the gap â€“ the cognitive gulf that separates us from animals. But it was not always so wide, he says in the video above. The Cybersecurity Information Security Act is trying to bridge the intelligence gap between all the various entities government, public, etc. without breaking or modifying the laws that are in place today around competitive information sharing. The Act itself is still going through its due process but outlines a lot of work effort: Requiring Homeland Security, Department of Defense, Department of Justice and the Director of gap intelligence strives to do our very best to support the local community and those in need. Through our community outreach team, the 3Ts, we attempt to do just that. 3Ts stands for Time, Talent, and Treasure and is our way to give back to others.Â Join gap intelligence for a free webinar to learn about how the current climate is affecting appliance, consumer electronic, and print industries. The first half of 2020 brought drastic changes to the industries covered by gap intelligence. The gap exists, and is due to people having complex language and communication skills. All types of intelligence involve information gathering, storage, analysis and decision making. Communication is in essence information gathering. Animals main venue for information gathering is individual independent observation. Whereas for us, Communication allows us to gather information beyond our scope of observation.