The Washington Post

National Security

'The intelligence coup of the century'

For decades, the CIA read the encrypted communications of allies and adversaries.

By Greg Miller   Feb. 11, 2020

f   (twitter)   (email)

F or more than half a century, governments all over the world trusted a single company to keep the communications of their spies, soldiers and diplomats secret.

The company, Crypto AG, got its first break with a contract to build code-making machines for U.S. troops during World War II. Flush with cash, it became a dominant maker of encryption devices for decades, navigating waves of technology from mechanical gears to electronic circuits and, finally, silicon chips and software.

Read more:
Compromised encryption machines gave CIA window into major human rights abuses in South America

As the U.S. spied on the world, the CIA and NSA bickered

The Swiss firm made millions of dollars selling equipment to more than 120 countries well into the 21st century. Its clients included Iran, military juntas in Latin America, nuclear rivals India and Pakistan, and even the Vatican.

But what none of its customers ever knew was that Crypto AG was secretly owned by the CIA in a highly classified partnership with West **German** intelligence. These spy agencies rigged the company's devices so they could easily break the codes that countries used to send encrypted messages.

The decades-long arrangement, among the most closely guarded secrets of the Cold War, is laid bare in a classified, comprehensive CIA history of the operation obtained by The Washington Post and ZDF, a **German** public broadcaster, in a joint reporting project.

The account identifies the CIA officers who ran the program and the company executives entrusted to execute it. It traces the origin of the venture as well as the internal conflicts that nearly derailed it. It describes how the United States and its allies exploited other nations' gullibility for years, taking their money and stealing their secrets.

The operation, known first by the code name "Thesaurus" and later "Rubicon," ranks among the most audacious in CIA history.

"It was the intelligence coup of the century," the CIA report concludes. "Foreign governments were paying good money to the U.S. and West Germany for the privilege of having their most secret communications read by at least two (and possibly as many as five or six) foreign countries."

From 1970 on, the CIA and its code-breaking sibling, the National Security Agency, controlled nearly every aspect of Crypto's operations — presiding with their German partners over hiring decisions, designing its technology, sabotaging its algorithms and directing its sales targets.

Then, the U.S. and West German spies sat back and listened.

They monitored Iran's mullahs during the 1979 hostage crisis, fed intelligence about Argentina's military to Britain during the Falklands War, tracked the assassination campaigns of South American dictators and caught Libyan officials congratulating themselves on the 1986 bombing of a Berlin disco.

Left: A Royal Navy helicopter takes off after transporting Royal Marines to Darwin, Falkland Islands, in 1982. During the Falklands War, U.S. spies fed intelligence about Argentina's military to Britain. (Paul Haley/Imperial War Museums/Getty Images) **Right:** An American hostage is guided outside the U.S. Embassy compound in Tehran in 1979, after students stormed the embassy and took its diplomatic staff hostage. Using Crypto, the United States monitored Iran's mullahs during the crisis. (Kaveh Kazemi/Getty Images)

The program had limits. America's main adversaries, including the Soviet Union and China, were never Crypto customers. Their well-founded suspicions of the company's ties to the West shielded them from exposure, although the CIA history suggests that U.S. spies learned a great deal by monitoring other countries' interactions with Moscow and Beijing.

There were also security breaches that put Crypto under clouds of suspicion. Documents released in the 1970s showed extensive — and incriminating — correspondence between an NSA pioneer and Crypto's founder. Foreign targets were tipped off by the careless statements of public officials including President Ronald Reagan. And the 1992 arrest of a Crypto salesman in Iran, who did not realize he was selling rigged equipment, triggered a devastating "storm of publicity," according to the CIA history.

But the true extent of the company's relationship with the CIA and its **German** counterpart was until now never revealed.

The **German** spy agency, the BND, came to believe the risk of exposure was too great and left the operation in the early 1990s. But the CIA bought the **German**s' stake and simply kept going, wringing Crypto for all its espionage worth until 2018, when the agency sold off the company's assets, according to current and former officials.

The company's importance to the global security market had fallen by then, squeezed by the spread of online encryption technology. Once the province of governments and major corporations, strong encryption is now as ubiquitous as apps on cellphones.

Even so, the Crypto operation is relevant to modern espionage. Its reach and duration help to explain how the United States developed an insatiable appetite for global surveillance that was exposed in 2013 by Edward Snowden. There are also echoes of Crypto in the suspicions swirling around modern companies with alleged links to foreign governments, including the Russian anti-virus firm Kaspersky, a texting app tied to the United Arab Emirates and the Chinese telecommunications giant Huawei.

This story is based on the CIA history and a parallel BND account, also obtained by The Post and ZDF, and interviews with current and former Western intelligence officials as well as Crypto employees. Many spoke on the condition of anonymity, citing the sensitivity of the subject.

It is hard to overstate how extraordinary the CIA and BND histories are. Sensitive intelligence files are periodically declassified and released to the public. But it is exceedingly rare, if not unprecedented, to glimpse authoritative internal histories of an entire covert operation. The Post was able to read all of the documents, but the source of the material insisted that only excerpts be published.

📄 Click any underlined text in the story to see an excerpt from the CIA history.

The CIA and the BND declined to comment, though U.S. and German officials did not dispute the authenticity of the documents. The first is a 96-page account of the operation completed in 2004 by the CIA's Center for the Study of Intelligence, an internal historical branch. The second is an oral history compiled by German intelligence officials in 2008.

The overlapping accounts expose frictions between the two partners over money, control and ethical limits, with the West Germans frequently aghast at the enthusiasm with which U.S. spies often targeted allies.

But both sides describe the operation as successful beyond their wildest projections. At times, including in the 1980s, Crypto accounted for roughly 40 percent of the diplomatic cables and other transmissions by foreign governments that cryptanalysts at the NSA decoded and mined for intelligence, according to the documents. 📄

All the while, Crypto generated millions of dollars in profits that the CIA and BND split and plowed into other operations.
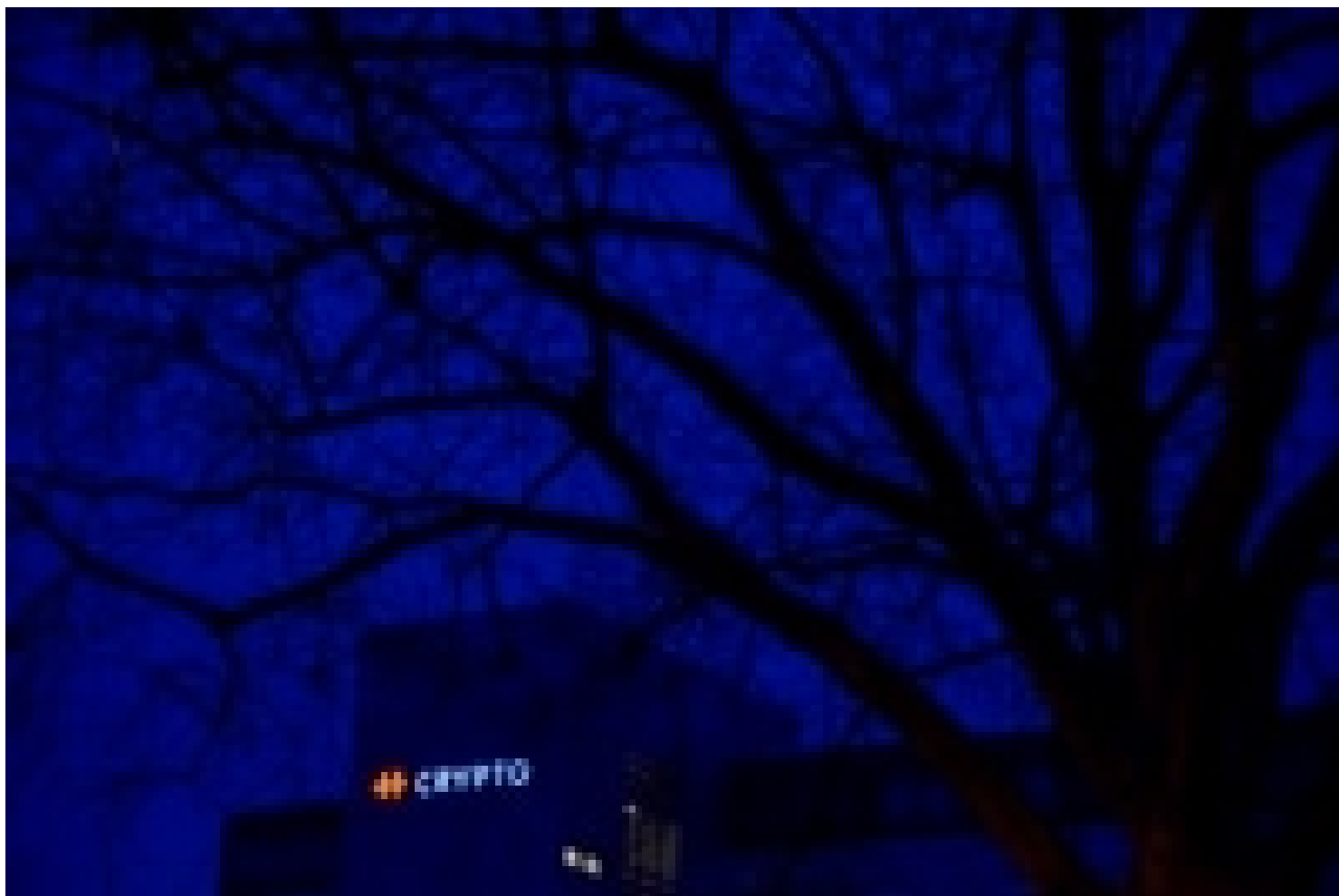
Crypto's sign is still visible atop its longtime headquarters near Zug, Switzerland, though the company was liquidated in 2018. (Jahi Chikwendiu/The Washington Post)

Crypto's products are still in use in more than a dozen countries around the world, and its orange-and-white sign still looms atop the company's longtime headquarters building near Zug, Switzerland. But the company was dismembered in 2018, liquidated by shareholders whose identities have been permanently shielded by the byzantine laws of Liechtenstein, a tiny European nation with a Cayman Islands-like reputation for financial secrecy.

Two companies purchased most of Crypto's assets. The first, CyOne Security, was created as part of a management buyout and now sells security systems exclusively to the Swiss government. The other, Crypto International, took over the former company's brand and international business.

Each insisted that it has no ongoing connection to any intelligence service, but only one claimed to be unaware of CIA ownership. Their statements were in response to questions

from The Post, ZDF and Swiss broadcaster SRF, which also had access to the documents.

CyOne has more substantial links to the now-dissolved Crypto, including that the new company's chief executive held the same position at Crypto for nearly two decades of CIA ownership.

A CyOne spokesman declined to address any aspect of Crypto AG's history but said the new firm has "no ties to any foreign intelligence services."

Andreas Linde, the chairman of the company that now holds the rights to Crypto's international products and business, said he had no knowledge of the company's relationship to the CIA and BND before being confronted with the facts in this article.

"We at Crypto International have never had any relationship with the CIA or BND — and please quote me," he said in an interview. "If what you are saying is true, then absolutely I feel betrayed, and my family feels betrayed, and I feel there will be a lot of employees who will feel betrayed as well as customers."

The Swiss government announced on Tuesday that it was launching an investigation of Crypto AG's ties to the CIA and BND. Earlier this month, Swiss officials revoked Crypto International's export license.

Post Reports | Podcast

The CIA's 'coup of the century'

Subscribe

0:00　　　　⟲ 15　　　　15 ⟳　　　　32:01

The timing of the Swiss moves was curious. The CIA and BND documents indicate that Swiss officials must have known for decades about Crypto's ties to the U.S. and **German** spy services, but intervened only after learning that news organizations were about to expose the arrangement.

The histories, which do not address when or whether the CIA ended its involvement, carry the inevitable biases of documents written from the perspectives of the operation's architects. They depict Rubicon as a triumph of espionage, 🗎 one that helped the United States prevail in the Cold War, keep tabs on dozens of authoritarian regimes and protect the interests of the United States and its allies.

The papers largely avoid more unsettling questions, including what the United States knew — and what it did or didn't do — about countries that used Crypto machines while engaged in assassination plots, ethnic cleansing campaigns and human rights abuses.

The revelations in the documents may provide reason to revisit whether the United States was in position to intervene in, or at least expose, international atrocities, and whether it opted against doing so at times to preserve its access to valuable streams of intelligence.

Nor do the files deal with obvious ethical issues at the core of the operation: the deception and exploitation of adversaries, allies and hundreds of unwitting Crypto employees. Many traveled the world selling or servicing rigged systems with no clue that they were doing so at risk to their own safety.

Juerg Spoerndli is an electrical engineer who spent 16 years working at Crypto. Deceived employees said the revelations about the company have deepened a sense of betrayal, of themselves and customers. (Jahi Chikwendiu/The Washington Post)

In recent interviews, deceived employees — even ones who came to suspect during their time at Crypto that the company was cooperating with Western intelligence — said the revelations in the documents have deepened a sense of betrayal, of themselves and customers.

"You think you do good work and you make something secure," said Juerg Spoerndli, an electrical engineer who spent 16 years at Crypto. "And then you realize that you cheated these clients."

Those who ran the clandestine program remain unapologetic.

"Do I have any qualms? Zero," said [Bobby Ray Inman](), who served as director of the NSA and deputy director of the CIA in the late 1970s and early 1980s. "It was a very valuable source of communications on significantly large parts of the world important to U.S. policymakers."

Boris Hagelin, the founder of Crypto, and his wife arrive in New York in 1949. Hagelin fled to the United States when the Nazis occupied Norway in 1940. (Bettmann Archive)

A denial operation

This sprawling, sophisticated operation grew out of the U.S. military's need for a crude but compact encryption device.

Boris Hagelin, 📄 Crypto's founder, was an entrepreneur and inventor who was born in Russia but fled to Sweden as the Bolsheviks took power. He fled again to the United States when the Nazis occupied Norway in 1940.

He brought with him an encryption machine that looked like a fortified music box, with a sturdy crank on the side and an assembly of metal gears and pinwheels under a hard metal case.

It wasn't nearly as elaborate, or secure, as the Enigma machines being used by the Nazis. But Hagelin's M-209, as it became known, was portable, hand-powered and perfect for troops on the move. Photos show soldiers with the eight-pound boxes — about the size of a thick book — strapped to their knees. Many of Hagelin's devices have been preserved at a private museum in Eindhoven, the Netherlands.

Left: Marc Simons and Paul Reuvers founded the Crypto Museum in Eindhoven, Netherlands. The virtual museum has preserved many of Hagelin's devices. (Jahi Chikwendiu/The Washington Post) **Right:** Hagelin's M-209 encryption machine had a crank on the side and an assembly of metal gears and pinwheels under a hard metal case. Portable and hand-powered, it was used mainly for tactical messages about troop movements. (Jahi Chikwendiu/The Washington Post)

Sending a secure message with the device was tedious. The user would rotate a dial, letter by letter, and thrust down the crank. The hidden gears would turn and spit out an enciphered message on a strip of paper. A signals officer then had to transmit that scrambled message by Morse code to a recipient who would reverse the sequence.

Security was so weak that it was assumed that nearly any adversary could break the code with enough time. But doing so took hours. 🗎 And since these were used mainly for tactical messages about troop movements, by the time the Nazis decoded a signal its value had probably perished.

Over the course of the war, about 140,000 M-209s were built at the Smith Corona typewriter factory in Syracuse, N.Y., under a U.S. Army contract worth $8.6 million to Crypto. After the war, Hagelin returned to Sweden to reopen his factory, bringing with him a personal fortune and a lifelong sense of loyalty to the United States.

Even so, American spies kept a wary eye on his postwar operations. In the early 1950s, he developed a more advanced version of his war-era machine with a new, "irregular" mechanical sequence that briefly stumped American code-breakers.

Marc Simons, co-founder of Crypto Museum, a virtual museum of cipher machines, explains how secret messages were created using the Hagelin CX-52. (Stanislav Dobak/The Washington Post)

Alarmed by the capabilities of the new CX-52 and other devices Crypto envisioned, U.S. officials began to discuss what they called the "Hagelin problem."

These were "the Dark Ages of American cryptology, 🗎" according to the CIA history. The Soviets, Chinese and North Koreans were using code-making systems that were all but impenetrable. U.S. spy agencies worried that the rest of the world would also go dark if countries could buy secure machines from Hagelin.

The Americans had several points of leverage with Hagelin: his ideological affinity for the country, his hope that the United States would remain a major customer and the veiled

threat that they could damage his prospects by flooding the market with surplus M-209s from the war.

The U.S. Army's Signals Intelligence Service was headed by William Friedman, center, in the mid-1930s. Other members, from left: Herrick F. Bearce, Solomon Kullback, U.S. Army Capt. Harold G. Miller, Louise Newkirk Nelson, seated, Abraham Sinkov, U.S. Coast Guard Lt. L.T. Jones and Frank B. Rowlett. (Fotosearch/Getty Images)

The United States also had a more crucial asset: William Friedman. Widely regarded as the father of American cryptology, Friedman had known Hagelin since the 1930s. They had forged a lifelong friendship over their shared backgrounds and interests, including their Russian heritage and fascination with the complexities of encryption.

There might never have been an Operation Rubicon if the two men had not shaken hands on the very first secret agreement between Hagelin and U.S. intelligence over dinner at the Cosmos Club in Washington in 1951. 📄

The deal called for Hagelin, who had moved his company to Switzerland, to restrict sales of his most sophisticated models to countries approved by the United States. Nations not on that list would get older, weaker systems. Hagelin would be compensated for his lost sales, as much as $700,000 up front.

It took years for the United States to live up to its end of the deal, as top officials at the CIA and the predecessor to the NSA bickered over the terms and wisdom of the scheme. But Hagelin abided by the agreement from the outset, and over the next two decades, his secret relationship with U.S. intelligence agencies deepened.

In 1960, the CIA and Hagelin entered into a "licensing agreement 🗎" that paid him $855,000 to renew his commitment to the handshake deal. The agency paid him $70,000 a year in retainer and started giving his company cash infusions of $10,000 for "marketing" expenses to ensure that Crypto — and not other upstarts in the encryption business — locked down contracts with most of the world's governments.

It was a classic "denial operation" in the parlance of intelligence, a scheme designed to prevent adversaries from acquiring weapons or technology that would give them an advantage. But it was only the beginning of Crypto's collaboration with U.S. intelligence. Within a decade, the whole operation belonged to the CIA and BND.

In 1967, Crypto released the H-460, an all-electronic machine whose inner workings were designed by the NSA. (Jahi Chikwendiu/The Washington Post)

A brave new world

U.S. officials had toyed since the outset with the idea of asking Hagelin whether he would be willing to let U.S. cryptologists doctor his machines. But Friedman overruled them, convinced that Hagelin would see that as a step too far.

The CIA and NSA saw a new opening in the mid-1960s, as the spread of electronic circuits forced Hagelin to accept outside help adapting to the new technology, or face extinction clinging to the manufacturing of mechanical machines.

NSA cryptologists were equally concerned about the potential impact of integrated circuits, which seemed poised to enable a new era of unbreakable encryption. But one of

the agency's senior analysts, Peter Jenks, identified a potential vulnerability.

If "carefully designed by a clever crypto-mathematician," he said, a circuit-based system could be made to appear that it was producing endless streams of randomly generated characters, while in reality it would repeat itself at short enough intervals for NSA experts — and their powerful computers — to crack the pattern.

Two years later, in 1967, Crypto rolled out a new, all-electronic model, the H-460, whose inner workings were completely designed by the NSA.

The CIA history all but gloats about crossing this threshold. "Imagine the idea of the American government convincing a foreign manufacturer to jimmy equipment in its favor," the history says. "Talk about a brave new world."

The NSA didn't install crude "back doors" or secretly program the devices to cough up their encryption keys. And the agency still faced the difficult task of intercepting other governments' communications, whether plucking signals out of the air or, in later years, tapping into fiber optic cables.

But the manipulation of Crypto's algorithms streamlined the code-breaking process, at times reducing to seconds a task that might otherwise have taken months. The company always made at least two versions of its products — secure models that would be sold to friendly governments, and rigged systems for the rest of the world.

In so doing, the U.S.-Hagelin partnership had evolved from denial to "active measures." No longer was Crypto merely restricting sales of its best equipment but actively selling devices that were engineered to betray their buyers.

The payoff went beyond the penetration of the devices. Crypto's shift to electronic products buoyed business so much that it became addicted to its dependence on the NSA. Foreign governments clamored for systems that seemed clearly superior to the old clunky mechanical devices but in fact were easier for U.S. spies to read.

German and American partners

By the end of the 1960s, Hagelin was nearing 80 and anxious to secure the future for his company, which had grown to more than 180 employees. CIA officials were similarly anxious about what would happen to the operation if Hagelin were to suddenly sell or die.

Hagelin had once hoped to turn control over to his son, Bo. But U.S. intelligence officials regarded him as a "wild card" and worked to conceal the partnership from him. Bo Hagelin was killed in a car crash on Washington's Beltway in 1970. There were no indications of foul play.

U.S. intelligence officials discussed the idea of buying Crypto for years, but squabbling between the CIA and NSA prevented them from acting until two other spy agencies entered the fray.

The French, West German and other European intelligence services had either been told about the United States' arrangement with Crypto or figured it out on their own. Some were understandably jealous and probed for ways to secure a similar deal for themselves.

In 1967, Hagelin was approached by the French intelligence service with an offer to buy the company in partnership with German intelligence. Hagelin rebuffed the offer and reported it to his CIA handlers. But two years later, the Germans came back seeking to make a follow-up bid with the blessing of the United States.

In a meeting in early 1969 at the West German Embassy in Washington, the head of that country's cipher service, Wilhelm Goeing, outlined the proposal and asked whether the Americans "were interested in becoming partners too."

Months later, CIA Director Richard Helms approved the idea of buying Crypto and dispatched a subordinate to Bonn, the West German capital, to negotiate terms with one major caveat: the French, CIA officials told Goeing, would have to be "shut out."

West Germany acquiesced to this American power play, and a deal between the two spy agencies was recorded in a June 1970 memo 📄 carrying the shaky signature of a CIA case officer in Munich who was in the early stages of Parkinson's disease and the illegible scrawl of his BND counterpart.

The two agencies agreed to chip in equally to buy out Hagelin for approximately $5.75 million, but the CIA left it largely to the Germans to figure out how to prevent any trace of the transaction from ever becoming public.

A Liechtenstein law firm, Marxer and Goop, helped hide the identities of the new owners of Crypto through a series of shells and "bearer" shares that required no names in registration documents. The firm was paid an annual salary "less for the extensive work but more for their silence and acceptance," the BND history says. The firm, now named Marxer and Partner, did not respond to a request for comment.

A new board of directors was set up to oversee the company. Only one member of the board, Sture Nyberg, to whom Hagelin had turned over day-to-day management, knew of CIA involvement. "It was through this mechanism," the CIA history notes, "that BND and CIA controlled the activities" of Crypto. Nyberg left the company in 1976. The Post and ZDF could not locate him or determine whether he is still alive.

The two spy agencies held their own regular meetings to discuss what to do with their acquisition. The CIA used a secret base in Munich, initially on a military installation used by American troops and later in the attic of a building adjacent to the U.S. Consulate, as the headquarters for its involvement in the operation.

The CIA and BND agreed on a series of code names for the program and its various components. Crypto 📄 was called "Minerva," which is also the title of the CIA history. The operation was at first code-named "Thesaurus," though in the 1980s it was changed to "Rubicon."

Each year, the CIA and BND split any profits Crypto had made, according to the **German** history, which says the BND handled the accounting and delivered the cash owed to the CIA in an underground parking garage.

From the outset, the partnership was beset by petty disagreements and tensions. To CIA operatives, the BND often seemed preoccupied with turning a profit, and the Americans "constantly reminded the **German**s that this was an intelligence operation, not a money-making enterprise." The **German**s were taken aback by the Americans' willingness to spy on all but their closest allies, 📄 with targets including NATO members Spain, Greece, Turkey and Italy.

Mindful of the limitations to their abilities to run a high-tech company, the two agencies brought in corporate outsiders. The **German**s enlisted Siemens, a Munich-based conglomerate, to advise Crypto on business and technical issues in exchange for 5 percent of the company's sales. The United States later brought in Motorola to fix balky products, making it clear to the company's CEO this was being done for U.S. intelligence. Siemens declined to comment. Motorola officials did not respond to a request for comment.

To its frustration, **German**y was never admitted to the vaunted "Five Eyes," a long-standing intelligence pact involving the United States, Britain, Australia, New Zealand and Canada. But with the Crypto partnership, **German**y moved closer into the American espionage fold than might have seemed possible in World War II's aftermath. With the secret backing of two of the world's premier intelligence agencies and the support of two of the world's largest corporations, Crypto's business flourished.

A table in the CIA history 📄 shows that sales surged from 15 million Swiss francs in 1970 to more than 51 million in 1975, or $19 million. The company's payroll expanded to more than 250 employees.

"The Minerva purchase had yielded a bonanza," the CIA history says of this period. The operation entered a two-decade stretch of unprecedented access to foreign governments' communications.

Egyptian President Anwar Sadat and President Jimmy Carter meet during the Egyptian-Israeli peace negotiations at Camp David in September 1978. During the negotiations, the NSA was secretly monitoring Sadat's communications back to Cairo. (White House/CNP/Getty Images)

Iranian suspicions

The NSA's eavesdropping empire was for many years organized around three main geographic targets, each with its own alphabetic code: A for the Soviets, B for Asia and G for virtually everywhere else.

By the early 1980s, more than half of the intelligence gathered by G group was flowing through Crypto machines, a capability that U.S. officials relied on in crisis after crisis.

In 1978, as the leaders of Egypt, Israel and the United States gathered at Camp David for negotiations on a peace accord, the NSA was secretly monitoring the communications of Egyptian President Anwar Sadat with Cairo.

A year later, after Iranian militants stormed the U.S. Embassy and took 52 American hostages, the Carter administration sought their release in back-channel communications 📄 through Algeria. Inman, who served as NSA director at the time, said he routinely got calls from President Jimmy Carter asking how the Ayatollah Khomeini regime was reacting to the latest messages.

"We were able to respond to his questions about 85 percent of the time," Inman said. That was because the Iranians and Algerians were using Crypto devices.

Inman said the operation also put him in one of the trickiest binds he'd encountered in government service. At one point, the NSA intercepted Libyan communications indicating that the president's brother, Billy Carter, was advancing Libya's interests in Washington and was on leader Moammar Gaddafi's payroll.

Inman referred the matter to the Justice Department. The FBI launched an investigation of Carter, who falsely denied taking payments. In the end, he was not prosecuted but agreed to register as a foreign agent.

Throughout the 1980s, the list of Crypto's leading clients read like a catalogue of global trouble spots. In 1981, Saudi Arabia was Crypto's biggest customer, followed by Iran, Italy, Indonesia, Iraq, Libya, Jordan and South Korea.

To protect its market position, Crypto and its secret owners engaged in subtle smear campaigns against rival companies, according to the documents, and plied government officials with bribes. Crypto sent an executive to Riyadh, Saudi Arabia, with 10 Rolex watches in his luggage, the BND history says, and later arranged a training program for the Saudis in Switzerland where the participants' "favorite pastime was to visit the brothels, which the company also financed."

At times, the incentives led to sales to countries ill-equipped to use the complicated systems. Nigeria bought a large shipment of Crypto machines, but two years later, when there was still no corresponding payoff in intelligence, a company representative was sent

to investigate. "He found the equipment in a warehouse still in its original packaging," according to the German document.

In 1982, the Reagan administration took advantage of Argentina's reliance on Crypto equipment, funneling intelligence to Britain during the two countries' brief war over the Falkland Islands, according to the CIA history, which doesn't provide any detail on what kind of information was passed to London. The documents generally discuss intelligence gleaned from the operation in broad terms and provide few insights into how it was used.

Plainclothes U.S. military officers walk around the scene of the bombing at the La Belle disco in West Berlin, which killed two U.S. soldiers and a Turkish woman in 1986. In an address, Reagan appears to have jeopardized the Crypto operation by citing evidence of Libya's complicity in the attack. (Andreas Schoelzel/Associated Press)

Reagan appears to have jeopardized the Crypto operation after Libya was implicated in the 1986 bombing of a West Berlin disco popular with American troops stationed in West

Germany. Two U.S. soldiers and a Turkish woman were killed as a result of the attack.

Reagan ordered retaliatory strikes against Libya 10 days later. Among the reported victims was one of Gaddafi's daughters. In an address to the country announcing the strikes, Reagan said the United States had evidence of Libya's complicity that "is direct, it is precise, it is irrefutable."

The evidence, Reagan said, showed that Libya's embassy in East Berlin received orders to carry out the attack a week before it happened. Then, the day after the bombing, "they reported back to Tripoli on the great success of their mission."

Reagan's words made clear that Tripoli's communications with its station in East Berlin had been intercepted and decrypted. But Libya wasn't the only government that took note of the clues Reagan had provided.

Iran, which knew that Libya also used Crypto machines, became increasingly concerned about the security of its equipment. Tehran didn't act on those suspicions until six years later.

1980 borders
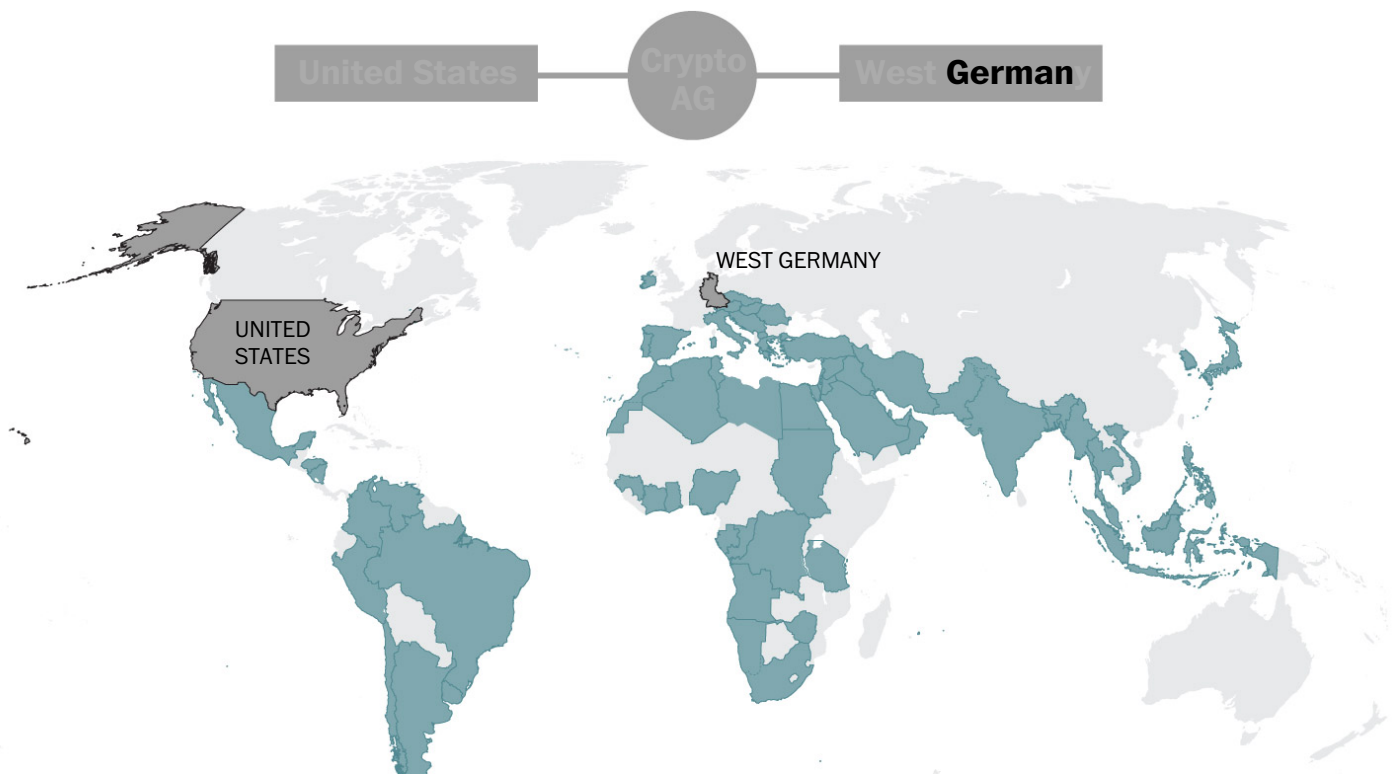
Documents indicate that more than 120 countries used Crypto AG encryption equipment from the 1950s well into the 2000s. The files don't include a comprehensive list but identify at least 62 customers.

THE AMERICAS	EUROPE	AFRICA	MIDDLE EAST	REST OF ASIA
Argentina	Austria	Algeria	Iran	Bangladesh
Brazil	Czechoslovakia	Angola	Iraq	Burma
Chile	Greece	Egypt	Jordan	India
Colombia	Hungary	Gabon	Kuwait	Indonesia
Honduras	Ireland	Ghana	Lebanon	Japan
Mexico	Italy	Guinea	Oman	Malaysia
Nicaragua	Portugal	Ivory Coast	Qatar	Pakistan
Peru	Romania	Libya	Saudi Arabia	Philippines
Uruguay	Spain	Mauritius	Syria	South Korea
Venezuela	Turkey	Morocco	U.A.E.	Thailand
	Vatican City	Nigeria		Vietnam
	Yugoslavia	Rep. of the Congo		
		South Africa		
		Sudan		
		Tanzania		
WORLDWIDE ORGANIZATION		Tunisia		
United Nations		Zaire		
		Zimbabwe		

The records show that at least four countries — Israel, Sweden, Switzerland and the United Kingdom — were aware of the operation or were provided intelligence from it by the United States or West Germany.

The irreplaceable man

After the CIA and BND acquisition, one of the most vexing problems for the secret partners was ensuring that Crypto's workforce remained compliant and unsuspecting.

Even while hidden from view, the agencies went to significant lengths to maintain Hagelin's benevolent approach to ownership. Employees were well paid and had abundant perks including access to a small sailboat on Lake Zug near company headquarters.

And yet, those who worked most closely with the encryption designs seemed constantly to be getting closer to uncovering the operation's core secret. The engineers and designers responsible for developing prototype models often questioned the algorithms being foisted on them by a mysterious external entity.

Crypto executives often led employees to believe that the designs were being provided as part of the consulting arrangement with Siemens. But even if that were so, why were encryption flaws so easy to spot, and why were Crypto's engineers so routinely blocked from fixing them?

In 1977, Heinz Wagner, the chief executive at Crypto who knew the true role of the CIA and BND, abruptly fired a wayward engineer after the NSA complained that diplomatic traffic coming out of Syria had suddenly became unreadable. The engineer, Peter Frutiger, had long suspected Crypto was collaborating with German intelligence. He had made multiple trips to Damascus to address complaints about their Crypto products and apparently, without authority from headquarters, had fixed their vulnerabilities.

Frutiger "had figured out the Minerva secret and it was not safe with him," according to the CIA history. Even so, the agency was livid with Wagner for firing Frutiger rather than finding a way to keep him quiet on the company payroll. Frutiger declined to comment for this story.

Mengia Caflisch, circa 1990s. After she was hired by Crypto, Caflisch, a gifted electrical engineer, began probing the vulnerabilities of the company's products. (Obtained by The Washington Post)

U.S. officials were even more alarmed when Wagner hired a gifted electrical engineer in 1978 named Mengia Caflisch. She had spent several years in the United States working as a radio-astronomy researcher for the University of Maryland before returning to her native Switzerland and applying for a job at Crypto. Wagner jumped at the chance to hire her. But NSA officials immediately raised concerns that she was "too bright to remain unwitting." 🖹

The warning proved prescient as Caflisch soon began probing the vulnerabilities of the company's products. She and Spoerndli, a colleague in the research department, ran various tests and "plaintext attacks" on devices including a teletype model, the HC-570, that was built using Motorola technology, Spoerndli said in an interview.

"We looked at the internal operations, and the dependencies with each step," Spoerndli said, and became convinced they could crack the code by comparing only 100 characters of enciphered text to an underlying, unencrypted message. It was an astonishingly low level of security, Spoerndli said in an interview last month, but far from unusual.

"The algorithms," he said, "always looked fishy."

In the ensuing years, Caflisch continued to pose problems. At one point, she designed an algorithm so strong that NSA officials worried it would be unreadable. The design made its way into 50 HC-740 machines rolling off the factory floor before company executives discovered the development and stopped it.

"I just had an idea that something might be strange," Caflisch said in an interview last month, about the origin of her suspicions. But it became clear that her probing wasn't appreciated, she said. "Not all questions appeared to be welcome."

The company restored the rigged algorithm to the rest of the production run and sold the 50 secure models to banks to keep them out of the hands of foreign governments. Because these and other developments were so hard to defend, Wagner at one point told a select group of members of the research and development unit that Crypto "was not entirely free to do what it wanted."

The acknowledgment seemed to subdue the engineers, who interpreted it as confirmation that the company's technology faced constraints imposed by the German government. But the CIA and BND became increasingly convinced that their routine, disembodied interference was unsustainable.

Crypto had become an Oz-like operation with employees probing to see what was behind the curtain. As the 1970s came to a close, the secret partners decided to find a wizard figure who could help devise more advanced — and less detectable — weaknesses in the algorithms, someone with enough cryptological clout to tame the research department.

The two agencies turned to other spy services for potential candidates before settling on an individual put forward by Sweden's intelligence service. Because of Hagelin's ties to the country, Sweden had been kept apprised of the operation since its outset.

Kjell-Ove Widman, a mathematics professor in Stockholm, had made a name for himself in European academic circles with his research on cryptology. Widman was also a military reservist who had worked closely with Swedish intelligence officials.

To the CIA, Widman had an even more important attribute: an affinity for the United States that he had formed while spending a year in Washington state as an exchange student.

His host family had such trouble pronouncing his Swedish name 📄 that they called him "Henry," a moniker he later used with his CIA handlers.

Officials involved in Widman's recruitment described it as almost effortless. After being groomed by Swedish intelligence officials, he was brought to Munich in 1979 for what purported to be a round of interviews with executives from Crypto and Siemens.

The fiction was maintained as Widman faced questions from a half-dozen men seated around a table in a hotel conference room. As the group broke for lunch, two men asked Widman to stay behind for a private conversation.

"Do you know what ZfCh is?" asked Jelto Burmeister, a BND case officer, using the acronym for the German cipher service. When Widman replied that he did, Burmeister said, "Now, do you understand who really owns Crypto AG?"

At that point, Widman was introduced to Richard Schroeder, a CIA officer stationed in Munich to manage the agency's involvement in Crypto. Widman would later claim to agency historians that his "world fell apart completely" in that moment.

If so, he did not hesitate to enlist in the operation.

Without even leaving the room, Widman sealed his recruitment with a handshake. As the three men joined the rest of the group at lunch, a "thumbs up" signal transformed the gathering into a celebration.

Crypto installed Widman as a "scientific advisor" reporting directly to Wagner. He became the spies' hidden inside agent, departing Zug every six weeks for clandestine meetings with representatives of the NSA and ZfCh. Schroeder, the CIA officer, would attend but tune out their technical babble.

They would agree on modifications and work up new encryption schemes. Then Widman would deliver the blueprints to Crypto engineers. The CIA history calls him the "irreplaceable man," and the "most important recruitment in the history of the Minerva program."

His stature cowed subordinates, investing him "with a technical prominence that no one in CAG could challenge." It also helped deflect the inquiries of foreign governments. As Widman settled in, the secret partners adopted a set of principles for rigged algorithms, according to the BND history. They had to be "undetectable by usual statistical tests" and, if discovered, be "easily masked as implementation or human errors."

In other words, when cornered, Crypto executives would blame sloppy employees or clueless users.

In 1982, when Argentina became convinced that its Crypto equipment had betrayed secret messages and helped British forces in the Falklands War, Widman was dispatched to Buenos Aires. Widman told them the NSA had probably cracked an outdated speech-scrambling device that Argentina was using, but that the main product they bought from Crypto, the CAG 500, remained "unbreakable."

"The bluff worked," 🗎 the CIA history says. "The Argentines swallowed hard, but kept buying CAG equipment."

Widman is long-retired now and living in Stockholm. He declined to comment. Years after his recruitment, he told U.S. officials that he saw himself as "engaged in a critical struggle for the benefit of Western intelligence," 🗎 according to the CIA document. "It was, he said, the moment in which he felt at home. This was his mission in life."

That same year, Hagelin, then 90 years old, became ill on a trip to Sweden and was hospitalized. He recovered well enough to return to Switzerland, but CIA officials became worried about Hagelin's extensive collection of business records and personal papers at his office in Zug.

Schroeder, with Hagelin's permission, arrived with a briefcase and spent several days going through the files. To visitors, he was introduced as a historian interested in tracing Hagelin's life. Schroeder pulled out the documents "that were incriminating," according to the history, and shipped them back to CIA headquarters, "where they reside to this day."

Hagelin remained an invalid until he died in 1983. The Post could not locate Wagner or determine whether he is still alive. Schroeder retired from the CIA more than a decade ago and teaches part-time at Georgetown University. When contacted by a reporter from The Post, he declined to comment.

The Hydra crisis

Crypto endured several money-losing years in the 1980s, but the intelligence flowed in torrents. U.S. spy agencies intercepted more than 19,000 Iranian communications sent via Crypto machines during that nation's decade-long war with Iraq, mining them for reports on subjects such as Tehran's terrorist links and attempts to target dissidents.

Iran's communications were "80 to 90 percent readable" 🗎 to U.S. spies, according to the CIA document, a figure that would probably have plunged into the single digits had Tehran not used Crypto's compromised devices.

In 1989, the Vatican's use of Crypto devices proved crucial in the U.S. manhunt for Panamanian leader Manuel Antonio Noriega. When the dictator sought refuge in the Apostolic Nunciature — the equivalent of a papal embassy — his whereabouts were exposed by the mission's messages back to Vatican City.

In 1992, however, the Crypto operation faced its first major crisis: Iran, belatedly acting on its long-standing suspicions, detained a company salesman.

Hans Buehler, then 51, was considered one of the company's best salesmen. Iran was one of the company's largest contracts, and Buehler had traveled in and out of Tehran for years. There were tense moments, including when he was questioned extensively in 1986 by Iranian officials after the disco bombing and U.S. missile strikes on Libya.

Six years later, he boarded a Swissair flight to Tehran but failed to return on schedule. When he didn't show, Crypto turned for help to Swiss authorities and were told he had been arrested by the Iranians. Swiss consular officials allowed to visit Buehler reported that he was in "bad shape mentally," according to the CIA history.

Buehler was finally released nine months later after Crypto agreed to pay the Iranians $1 million, 🗎 a sum that was secretly provided by the BND, according to the documents. The CIA refused to chip in, citing the U.S. policy against succumbing to ransom demands for hostages.

Buehler knew nothing about Crypto's relationship to the CIA and BND or the vulnerabilities in its devices. But he returned traumatized and suspicious that Iran knew more about the company he worked for than he did. Buehler began speaking to Swiss news organizations about his ordeal and mounting suspicions.

Left: William Friedman in Switzerland in 1957 with his wife and fellow cryptanalyst, Elizebeth Friedman, left, and Annie Hagelin, Boris Hagelin's wife. (George C. Marshall Foundation) **Right:** Boris Hagelin in 1972. (George C. Marshall Foundation)

The publicity brought new attention to long-forgotten clues, including references to a "Boris project" in Friedman's massive collection of personal papers, which were donated to Virginia Military Institute when he died in 1969. Among the 72 boxes delivered to Lexington, Va., were copies of his lifelong correspondence with Hagelin.

In 1994, the crisis deepened when Buehler appeared on Swiss television in a report that also featured Frutiger, whose identity was concealed from viewers. Buehler died in 2018. Frutiger, the engineer who had been fired for fixing Syria's encryption systems years earlier, did not respond to requests for comment.

Michael Grupe, who had succeeded Wagner as chief executive, agreed to appear on Swiss television and disputed what he knew to be factual charges. "Grupe's performance was credible, and may have saved the program," 🗎 the CIA history says. Grupe did not respond to requests for comment.

Even so, it took several years for the controversy to die down. In 1995, the Baltimore Sun ran a series of investigative stories about the NSA, including one called "Rigging the Game" that exposed aspects of the agency's relationship with Crypto.

The article reported NSA officials had traveled to Zug in the mid-1970s for secret meetings with Crypto executives. The officials were posing as consultants for a front company called "Intercomm Associates" but then proceeded to introduce themselves by their real names — which were recorded on notes of the meeting kept by a company employee.

Amid the publicity onslaught, some employees began to look elsewhere for work. And at least a half-dozen countries — including Argentina, Italy, Saudi Arabia, Egypt and Indonesia — either canceled or suspended their Crypto contracts.

Astonishingly, Iran was not among them, according to the CIA file, and "resumed its purchase of CAG equipment almost immediately." 📄

The main casualty of the "Hydra" crisis, the code name given to the Buehler case, was the CIA-BND partnership.

For years, BND officials had recoiled at their American counterpart's refusal to distinguish adversaries from allies. The two partners often fought over which countries deserved to receive the secure versions of Crypto's products, with U.S. officials frequently insisting that the rigged equipment be sent to almost anyone — ally or not — who could be deceived into buying it.

In the German history, Wolbert Smidt, the former director of the BND, complained that the United States "wanted to deal with the allies just like they dealt with the countries of the Third World." Another BND official echoed that comment, saying that to Americans, "in the world of intelligence there were no friends."

The Cold War had ended, the Berlin Wall was down and the reunified Germany had different sensitivities and priorities. They saw themselves as far more directly exposed to the risks of the Crypto operation. Hydra had rattled the Germans, who feared the disclosure of their involvement would trigger European outrage and lead to enormous political and economic fallout.

In 1993, Konrad Porzner, the chief of the BND, made clear to CIA Director James Woolsey that support in the upper ranks of the German government was waning and that the Germans might want out of the Crypto partnership. On Sept. 9, the CIA station chief in Germany, Milton Bearden, reached an agreement with BND officials for the CIA to purchase Germany's shares for $17 million, according to the CIA history.

German intelligence officials rued the departure from an operation they had largely conceived. In the German history, senior intelligence officials blame political leaders for ending one of the most successful espionage programs the BND had ever been a part of.

With their departure, the Germans were soon cut off from the intelligence that the United States continued to gather. Burmeister is quoted in the German history wondering whether Germany still belonged "to this small number of nations who are not read by the Americans."

The Snowden documents provided what must have been an unsettling answer, showing that U.S. intelligence agencies not only regarded Germany as a target but monitored German Chancellor Angela Merkel's cellphone.

Alive and well

The CIA history essentially concludes with Germany's departure from the program, though it was finished in 2004 and contains clear indications that the operation was still underway.

It notes, 🖹 for example, that the Buehler case was "the most serious security breach in the history of the program" but wasn't fatal. "It did not cause its demise," the history says, "and at the turn of the century Minerva was still alive and well."

In reality, the operation appears to have entered a protracted period of decline. 🗎 By the mid-1990s, "the days of profit were long past," and Crypto "would have gone out of business but for infusions from the U.S. government."

As a result, the CIA appears to have spent years propping up an operation that was more viable as an intelligence platform than a business enterprise. Its product line dwindled and its revenue and customer base shrank.

But the intelligence kept coming, current and former officials said, in part because of bureaucratic inertia. Many governments just never got around to switching to newer encryption systems proliferating in the 1990s and beyond — and unplugging their Crypto devices. This was particularly true of less developed nations, according to the documents.

Most of the employees identified in the CIA and BND histories are in their 70s or 80s, and some of them have died. In interviews in Switzerland last month, several former Crypto workers mentioned in the documents described feelings of unease about their involvement in the company.

They were never informed of its true relationship to intelligence services. But they had well-founded suspicions and still wrestle with the ethical implications of their decisions to remain at a firm they believed to be engaged in deception.

"Either you had to leave or you had to accept it in a certain way," said Caflisch, now 75, who left the company in 1995 but continues to live on the outskirts of Zug in a converted weaving factory where she and her family for many years staged semiprofessional operas in the barn. "There were reasons I left," she said, including her discomfort with her doubts at Crypto and her desire to be home more for her children. After the latest revelations, she said, "It makes me wonder whether I should have left earlier."

Spoerndli said he regrets his own rationalizations.

"I told myself sometimes it may be better if the good guys in the United States know what is going on between these Third World dictators," he said. "But it's a cheap self-excuse. In the end, this is not the way."

Most of the executives directly involved in the operation were motivated by ideological purpose and declined any payment beyond their Crypto salaries, according to the documents. Widman was among several exceptions. "As his retirement drew near, his covert compensation was substantially increased," the CIA history says. He was also awarded a medal bearing the CIA seal.

After the BND's departure, the CIA expanded its clandestine collection of companies in the encryption sector, according to former Western intelligence officials. Using cash amassed from the Crypto operation, the agency secretly acquired a second firm and propped up a third. The documents do not disclose any details about these entities. But the BND history notes that one of Crypto's longtime rivals — Gretag AG, also based in Switzerland — was "taken over by an 'American' and, after a change of names in 2004, was liquidated."

Crypto itself hobbled along. It had survived the transitions from metal boxes to electronic circuits, going from teletype machines to enciphered voice systems. But it struggled to maintain its footing as the encryption market moved from hardware to software. U.S. intelligence agencies appear to have been content to let the Crypto operation play out, even as the NSA's attention shifted to finding ways to exploit the global reach of Google, Microsoft, Verizon and other U.S. tech powers.

In 2017, Crypto's longtime headquarters building near Zug was sold to a commercial real estate company. In 2018, the company's remaining assets — the core pieces of the encryption business started nearly a century earlier — were split and sold.

The transactions seemed designed to provide cover for a CIA exit.

CyOne's purchase of the Swiss portion of the business was structured as a management buyout, enabling top Crypto employees to move into a new company insulated from the

espionage risks and with a reliable source of revenue. The Swiss government, which was always sold secure versions of Crypto's systems, is now CyOne's only customer.

Giuliano Otth, who served as CEO of Crypto AG from 2001 until its dismemberment, took the same position at CyOne after it acquired the Swiss assets. Given his tenure at Crypto, it is likely he was witting to the CIA ownership of the company, just as all of his predecessors in the job had been.

"Neither CyOne Security AG nor Mr. Otth have any comments regarding Crypto AG's history," the company said in a statement.

Crypto's international accounts and business assets were sold to Linde, a Swedish entrepreneur, who comes from a wealthy family with commercial real estate holdings.

In a meeting in Zurich last month, Linde said he had been drawn to the company in part by its heritage and Hagelin connection, a past that still resonates in Sweden. Upon taking over operations, Linde even moved some of Hagelin's historic equipment from storage into a display at the factory entrance.

When confronted with evidence that Crypto had been owned by the CIA and BND, Linde looked visibly shaken, and said that during negotiations he never learned the identities of the company's shareholders. He asked when the story would be published, saying he had employees overseas and voicing concern for their safety.

In a subsequent interview, Linde said his company is investigating all the products it sells to determine whether they have any hidden vulnerabilities. "We have to make a cut as soon as possible with everything that has been linked to Crypto," he said.

When asked why he failed to confront Otth and others involved in the transaction about whether there was any truth to the long-standing Crypto allegations, Linde said he had regarded these as "just rumors."

He said he took assurance from the fact that Crypto continued to have substantial contracts with foreign governments, countries he assumed had tested the company's products vigorously and would have abandoned them if they were compromised.

"I even acquired the brand name, 'Crypto,' " he said, underscoring his confidence in the company's viability. Given the information now coming to light, he said, this "was probably one of the most stupid decisions I've ever made in my career."

The company's liquidation was handled by the same Liechtenstein law firm that provided cover for Hagelin's sale to the CIA and BND 48 years earlier. The terms of the 2018 transactions have not been disclosed, but current and former officials estimated their aggregate value at $50 million to $70 million.

For the CIA, the money would have been one final payoff from Minerva.

Reporting for this article was done in collaboration with Peter F. Mueller, a journalist and documentary filmmaker based in Cologne, Germany. Julie Tate in Washington contributed to this report.

Greg Miller

Greg Miller is a national security correspondent for The Washington Post and a two-time winner of the Pulitzer Prize. He is the author of "The Apprentice," a book on Russia's interference in the 2016 U.S. presidential race and the fallout under the Trump administration.

About this story

Editing by Peter Finn. Copy editing by Emily Codik. Design and development by Lucio Villa. Photography by Jahi Chikwendiu. Photo editing and research by Bronwen Latimer. Video by Stainislav Dobak. Video editing by Jason Aldag. Graphics by Aaron Steckelberg. Project management by Julie Vitkovskaya.

1.2k Comments

More stories

During Cold War, CIA used 'Doctor Zhivago' as a tool to undermine Soviet Union

The spy agency labored long and hard to bring the novel's anti-Soviet themes to the Russian people.

The Nazis were closing in on a spy known as 'The Limping Lady.' She fled across mountains on a wooden leg.

Virginia Hall, one of history's most audacious, yet little-known spies, has a CIA training facility named after her and may become the subject of a movie.

Most Read

1　Why outbreaks like coronavirus spread exponentially, and how to 'flatten the curve'
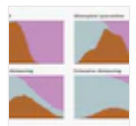
2　Chevy Chase is 74, sober and ready to work. The problem? Nobody wants to work with him.

3　How the CIA used Crypto AG encryption devices to spy on countries for decades

4　How epidemics like covid-19 end (and how to end them faster)

5   Extreme climate change in the United States: Here are America's fastest-warming places

Follow Post Graphics

Twitter	Facebook	Tumblr

Terms of use

Policies and Standards

Digital Products Terms of Sale

Print Products Terms of Sale

Terms of Service

Policies and Standards

Privacy Policy

Submissions and Discussion Policy

RSS Terms of Service

Ad Choices

Do Not Sell My Info