The NSA-Crypto AG Sting

For years US eavesdroppers could read encrypted messages without the least difficulty

Ludwig De Braeckeleer (ludwig)
CONTRACT REPORTER

Published 2007-12-29 06:53 (KST)

For decades, the US National Security Agency (NSA) has been reading effortlessly ultra sensitive messages intercepted from all parts of the world. This extraordinary feat was not the consequence of the work of some genius cyber mathematician. Nor was it the result of the agency dominance in the field of super computers, which allegedly have outpaced their most direct rivals by orders of magnitude. The truth is far simpler and quite troubling. The game was rigged.

For half a century, Crypto AG, a Swiss company located in Zug, has sold to more than 100 countries the encryption machines their officials rely upon to exchange their most sensitive economic, diplomatic and military messages. Crypto AG was founded in 1952 by the legendary (Russian born) Swedish cryptographer Boris Hagelin. During World War II, Hagelin sold 140,000 of his machine to the US Army.

TODAY'S TOP STORIES

- Russia-Iran Ties: A Necessary Evil?
- Revolution and Reaction: Cit-J in Hungary
- Internet Scams Growing in Africa
- We Can Wipe You Off the Map
- Remembering the Millennium New Year

FROM THE SECTION

- Bhutto's Son Chosen to Lead Party
- Internet Scams Growing in Africa
- Pakistan Considering Poll Delay
- Revolution and Reaction: Cit-J in Hungary
- Russia-Iran Ties: A Necessary Evil?

"In the meantime, the Crypto AG has built up long standing cooperative relations with customers in 130 countries," states a prospectus of the company. The home page of the company Web site says, "Crypto AG is the preferred top-security partner for civilian and military authorities worldwide. Security is our business and will always remain our business."

And for all those years, US eavesdroppers could read these messages without the least difficulty. A decade after the end of WWII, the NSA, also known as No Such Agency, had rigged the Crypto AG machines in various ways according to the targeted countries. It is probably no exaggeration to state that this 20th century version of the "Trojan horse" is quite likely the greatest sting in modern history.

In effect, US intelligence had spies in the government and military command of all these countries working around the clock without ever risking the possibility of being unmasked.

An Old and Venerable Company

In the aftermath of the Islamic revolution, Iran, quite

understandably, would no longer trust encryption equipment provided by companies of NATO countries.

The Swiss reputation for secrecy and neutrality lured Iranians to Crypto AG, an old and venerable company. They never imagined for a moment that, attached to the encrypted message, their Crypto machines were transmitting the key allowing the description of messages they were sending. The scheme was perfect, undetectable to all but those who knew where to look.

Crypto AG, of course, denied the allegations as "pure invention." In 1994, the company issued a message in the Swiss press, stating that "manipulation of Crypto AG equipment is absolutely excluded."

On the Wikipedia page of Crypto AG, one can read: "Crypto AG rejected these accusations as pure invention, asserting in a press release that in March 1994, the Swiss Federal Prosecutor's Office initiated a wide-ranging preliminary investigation against Crypto AG, which was completed in 1997. The accusations regarding influence by third parties or manipulations, which had been repeatedly raised in the media, proved to be without foundation."

However, meetings between a NSA cryptographer and Crypto AG personnel to discuss the design of new machines have been factually established. The story was also confirmed by former employees and is supported by company documents. Boris Hagelin is said to have acted out of idealism. What is certain is that the deal for Crypto AG was quite juicy. In return for rigging their machines, Crypto AG is understood to have been granted export licenses to all entities controlled by the NSA.

Early Hints

A book published in 1977 by Ronald Clark (*The Man Who Broke Purple: The Life of Colonel William F. Friedman*) revealed that William F. Friedman, another Russian-born genius in the field of cryptography (he deciphered the Japanese code in World War II) and onetime special assistant to the NSA director, had visited Boris Hagelin in 1957. Friedman and Hagelin met at least on two other occasions. Clark was urged by the NSA not to reveal the existence of these meetings for national security reasons. In 1982, James Bamford confirmed the story in his book on the NSA: *The Puzzle Palace*. The operation was codenamed the "Boris project." In effect, Friedman and Hagelin had reached an agreement that was going to pave the way to cooperation of Crypto AG with the NSA.

Despite these very obvious hints, countries such as Iran, Iraq and Libya continued using the Crypto AG machines for encrypting their messages. And so did the Vatican, among many other entities.

Persian Suspicions

In 1987, ABC News Beirut correspondent Charles Glass was taken hostage for 62 days in Lebanon by Hezbollah, the Shi'ite Muslim group widely believed to have been founded by Ali Akbar Mohtashemi, when he was Iranian ambassador to Syria in the early 1980s.

Washington claimed that NSA had intercepted coded Iranian diplomatic cables between Iran's embassies in Beirut and the Hezbollah group. Iranians began to wonder how the US intelligence could have broken their code.

After the USS Vincennes shot down an Iranian Airbus over the Persian Gulf on July 3, 1988, "Iran vowed that the skies would

- Obscurity and confinement for migrants in Europe

Weekly Top Ten Views

- The NSA-Crypto AG Sting
- A Vile 'Aliens vs. Predator: Requiem'
- We Can Wipe You Off the Map
- Bhutto Coffin Flown to Her Hometown
- Netizens Censored in South Korean Presidential Election
- British Media Exploited by Intel Agencies
- Personal and Global Reflections on 2007
- 'There Will Be Blood' a Masterpiece
- The Coming Age of Mass Atheism
- Charlie Chaplin Is Back as a Cat

rain with American blood." A few months later, on Dec. 21, a terrorist bomb brought down Pan Am Flight 103 over Lockerbie, Scotland.

Once more, NSA intercepted and decoded a communication of Iranian Interior Minister Ali Akbar Mohtashemi linking Iran to the bombing of Pan Am 103.

One intelligence summary, prepared by the US Air Force Intelligence Agency, was requested by lawyers for the bankrupt Pan American Airlines through the Freedom of Information Act.

"Mohtashemi is closely connected with the Al Abas and Abu Nidal terrorist groups. He is actually a long-time friend of Abu Nidal. He has recently paid 10 million dollars in cash and gold to these two organizations to carry out terrorist activities and was the one who paid the same amount to bomb Pan Am Flight 103 in retaliation for the US shoot-down of the Iranian Airbus."

Moreover, Israeli intelligence intercepted a coded transmission between Mohtashemi in Teheran and the Iranian Embassy in Beirut concerning the transfer of a large sum of money to the Popular Front for the Liberation of Palestine-General Command, headed by Ahmed Jibril, as payment for the downing of Pan Am 103.

The Iranians were now at a loss to explain how Western and Israeli intelligence agencies could so easily defeat the security of their diplomatic traffic. The ease with which the West was reading Iranian coded transactions strongly suggested that some may have possessed the decryption keys.

The Bakhtiar Murder

In April 1979, Shahpour Bakhtiar was forced to leave Iran as the last prime minister of the Shah. He returned to France where he lived in the west Paris suburb of Suresnes. In July 1980, he narrowly escaped an assassination attempt. On Aug. 6, 1991, Bakhtiar and his personal secretary Katibeh Fallouch were murdered by three assassins.

Two of them fled to Iran, but the third, Ali Vakili Rad, was apprehended in Switzerland. One of the six alleged accomplices, Zeyal Sarhadi was an employee of the Iranian Embassy in Berne and a great-nephew of former president of Iran Hasemi Rafsanjani. Both men were extradited to France for trial.

On the day of his assassination and one day before his body was found with his throat slit, the Teheran headquarters of the Iranian Intelligence Service, the VEVAK, transmitted a coded message to Iranian diplomatic missions in London, Paris, Bonn and Geneva. "Is Bakhtiar dead?" the message asked.

Switzerland's *Neue Zurcher Zeitung* reported that the U.S. had provided the contents of encrypted Iranian messages to France to assist Investigating Magistrate Jean Louis Bruguiere in the conviction of Ali Vakili Rad and one of his alleged accomplices Massoud Hendi. This information was confirmed by *L' Express*.

The NSA interception and decoding of the message led to the identification of the murderers before the murder was discovered. From the Swiss and French press reports, Iranians now knew that British and American SIGINT operators had intercepted and decoded the crucially embarrassing message. Something was definitely wrong with their encryption machines.

The Buehler Arrest

Hans Buehler was a top Crypto AG salesman who had worked at the Zug company for 13 years. In March 1992, Buehler, a strongly built cheerful man in his 50s, was on his 25th trip to Iran on behalf of Crypto AG.

Then, on March 18, he was arrested. Iranian intelligence agents accused him of spying for the United States as well as Germany. Buehler was held in solitary confinement in the Evin prison located in the north of Tehran. He was interrogated everyday for five hours for more than nine months.

"I was never beaten, but I was strapped to wooden benches and told I would be beaten. I was told Crypto was a spy center that worked with foreign intelligence services."

Buehler never confessed any wrongdoing on his part or on the part of Crypto AG. It appeared that he had acted in good faith and the Iranians came to believe him. "I didn't know that the equipment was bugged, otherwise the Iranians would have gotten it out of me by their many methods."

Back to Switzerland

In January 1993, after nine months of detention, Crypto AG [or was it Siemens?] paid US$1 million to secure Buehler's freedom. During the first weeks after his return to Switzerland, Buehler's life was once again beautiful. The euphoria did not last long. Once more, his life came to an abrupt change. Crypto fired him and demanded repayment of the $1 million provided to Tehran for his liberation.

Back to Zug, Buehler began to ask some embarrassing questions about the Iranian allegations. And the answers tended to back up Iranian suspicions. Soon, reports began to appear on Swiss television and radio. Major Swiss newspapers and German magazines such as *Der Spiegel* picked up the story. Most, if not all, came to the conclusion that Crypto AG's equipment had been rigged by one or several Western intelligence services.

Buehler was bitterly disappointed. He felt nothing short of having been betrayed by his former employer. During all these years, Buehler never thought for a second that he had been unknowingly working for spies. Now, he was sure that he had done so.

Buehler contacted several former Crypto AG employees. All admitted to him, and eventually to various media, that they believed that the company had long cooperated with US and German intelligence agencies.

The Truth Emerges

One of these former engineers told Buehler that he had learned about the cooperation from Boris Hagelin Jr., the son of the company's founder and sales manager for North and South America. In the 1970s, while stranded in Buenos Aires, Boris Hagelin Jr. confided that he thought his father had been wrong to accept rigging the Crypto AG machines.

Stunned by the revelation, the engineer decided to take this matter directly to the head of Crypto AG. Boris Hagelin confirmed that the encryption methods were unsafe.

"Different countries need different levels of security. The United States and other leading Western countries required completely secure communications. Such security would not be appropriate for the Third World countries that were Crypto's customers," Boris

Hagelin explained to the baffled engineer. "We have to do it."

The NSA-Crypto AG Collaboration

A Crypto AG official document describes an August 1975 meeting set up to demonstrate the capacity of a new prototype. The memorandum lists among the participants Nora L. Mackebee, who, like her husband, was an NSA employee. Asked about the meeting, she merely replied: "I cannot say anything about it."

During the '70s, Motorola helped Crypto AG in making the transition from mechanical to electronic machines. Bob Newman was among the Motorola engineers working with Crypto AG. Newman remembers very well Mackebee but says that he ignored that she was working for the NSA.

Juerg Spoerndli left Crypto AG in 1994. He helped design the machines in the late '70s. "I was ordered to change algorithms under mysterious circumstances" to weaker machines," says Spoerndli who concluded that NSA was ordering the design change through German intermediaries.

"I was idealistic. But I adapted quickly … the new aim was to help Big Brother USA look over these countries' shoulders. We'd say 'It's better to let the USA see what these dictators are doing,'" Spoerndli says.

"It's still an imperialistic approach to the world. I do not think it's the way business should be done," Spoerndli adds.

Ruedi Hug, another former Crypto AG technician, also believes that the machines were rigged.

"I feel betrayed. They always told me that we were the best. Our equipment is not breakable, blah, blah, blah. Switzerland is a neutral country."

Crypto AG vs. Buehler

Crypto AG called these allegations "old hearsay and pure invention." When Buehler began to suggest openly that there may be some truth to them, Crypto AG not only dismissed him on the spot, but also filed a legal case against him.

Yet Crypto AG settled the case out of court, in November 1996, before other former Crypto AG employees could provide evidence in court that was likely to have brought embarrassing details to light.

No one has heard from Buehler since the settlement. "He made his fortune financially," whispers an insider.

A Fuzzy Ownership

The ownership of Crypto AG has been to a company in Liechtenstein, and from there back to a trust company in Munich. Crypto AG has been described as the secret daughter of Siemens but many believe that the real owner is the German government.

Several members of Crypto AG's management had worked at Siemens. At one point in time, 99.99 percent of the Crypto AG shares belonged to Eugen Freiberger, the head of the Crypto AG managing board in 1982. Josef Bauer was elected to the managing board in 1970. Bauer, as well as other members of Crypto AG management, stated that his mandate had come from the German company Siemens.

The German secret service, the Bundesnachrichtendienst (BND), is believed to have established the Siemens' connection. In October 1970, a secret meeting of the BND had discussed how the Swiss company Graettner could merge with it. "The Swedish company Ericsson could be influenced through Siemens to terminate its own cryptographic business," reads the memo of the meeting.

A former employee of Crypto AG reported that he had to coordinate his developments with the "central office for encryption affairs" of the BND, also known as the "people from Bad Godesberg."

American "watchers" demanded the use of certain encryption codes and the "central office for encryption affairs" instructed Crypto AG what algorithms to use to create these codes.

Bakhtiar Murder Trial

"In the industry everybody knows how such affairs will be dealt with," says a former Crypto engineer. "Of course such devices protect against interception by unauthorized third parties, as stated in the prospectus. But the interesting question is: Who is the authorized fourth?"

On Dec. 6, 1994, a special French terrorism court convicted two Iranians of murdering Bakhtiar. Vakili Rad was sentenced to life in prison. But, to the dismay of all observers, Sarhadi was acquitted.

"Justice has not been entirely served for reasons of state," complained Bakhtiar's widow.

It appears indeed that France, Switzerland, the German BND and the NSA decided to let Sarhadi go free in order to preserve the "secrecy" of the Crypto AG cooperation with the NSA.

In 1991, the US and the U.K. indicted two Libyans for the bombing of Pan Am 103. To the surprise of many observers, the indictment did not mention those believed to have contracted the act of terror in spite of the fact that their guilt had been established by the interception of official communications by several intelligence agencies.

To many observers, justice was not served at the Lockerbie trial. Could it be that the US and U.K. governments decided to sacrifice the truth in order to preserve the (in)efficiency of their intelligence apparatus?

Notes

Ludwig De Braeckeleer has a Ph.D. in nuclear sciences. He teaches physics and international humanitarian law. He blogs on "The GaiaPost."

» Other articles by reporter Ludwig De Braeckeleer

Input number 81

Post

9. UN-FSO-DPKO-UNTSO	Jeff Smith , 2007-12-31 14:01	0	1
8. How the Iraq/Iran War Got Started	bill payne , 2007-12-31 07:31	0	1
7. some observations	The mole , 2007-12-31 05:21	0	1
6. Good for the NSA	Kev , 2007-12-31 04:42	0	1
5. A small error	James Fletcher , 2007-12-31 04:26	0	
4. Zug Heil(1)	amanfromMars , 2007-12-30 15:41	1	2

View Chronologically View Approvals