

The Spy Game That Shook the World



In February 2020, a shocking article in the Washington Post exposed a decades-long scandal: Crypto AG, a seemingly innocuous Swiss encryption company, was secretly owned by the CIA and West German intelligence (BND). This revelation not only exposed a major intelligence coup but also raised serious questions about the role of government manipulation in global communications security.

Crypto AG: A Trojan Horse in Plain Sight

Crypto AG, founded in 1952, established itself as a trusted provider of encryption devices to governments and militaries worldwide. Unbeknownst to its customers, however, the company was a covert operation run by the CIA and BND. Through backdoor access built into the devices, Western intelligence agencies could effortlessly decrypt communications passing through them, effectively granting them a window into the diplomatic and military secrets of dozens of nations.

Key Players in the Espionage Game

William F. Friedman: An American cryptologist who, along with his team, cracked many ciphers during World War II.

Boris Hagelin: The Swedish founder of Crypto AG, who remained largely oblivious to the company's true ownership. Hagelin's focus on quality and security inadvertently built a Trojan horse that would be used for decades to compromise global communications.

Decision-Making Flawed by Incompetence and Trust

While the technical brilliance of the operation is undeniable, the Crypto AG affair also exposes significant failures in decision-making on the part of the buying nations. Many governments, particularly those in developing countries, lacked the technical expertise or resources to independently assess the security of the Crypto AG devices. They relied heavily on the reputation of the company and the perceived trustworthiness of Western nations.

This affair is a stark reminder of the dangers of blindly trusting security technology, especially if you do not deeply understand it.

In an audacious secret operation "Rubicon", the CIA and West German intelligence turned the tables on over 120 countries. They covertly owned Crypto AG, a Swiss firm that sold encryption devices worldwide. Unbeknownst to these countries, their most secret communications were being intercepted and decoded. This was not a mere breach of trust, but a monumental intelligence coup.

The agencies exploited the devices to decipher the codes of their customers, including nations like Iran, India, Pakistan, and even the Vatican. This operation was also a glaring spotlight on the incompetence of decision makers in the customer countries. Their inability to detect or halt this spying operation raises serious questions about their judgment and capabilities.