CIA Secretly Owned Global Encryption Provider, Built Backdoors, Spied On 100+ Foreign Governments: Report

Davey Winder ⋮ 6-8 minutes ⋮ 2/12/2020

New revelations reveal how the CIA secretly owned a global encryption provider and spied upon secret ... [+] government communications

LightRocket via Getty Images

More than 100 countries across the globe relied for decades upon encryption equipment from a Swiss provider, Crypto AG, to keep their top-secret communications, well, top-secret. For decades, it is alleged, U.S. intelligence agencies were able to read those encrypted communications.

The Swiss company that global governments trusted with their most sensitive of conversations for more than fifty years was actually owned by the U.S. Central Intelligence Agency (CIA) in partnership with the West German BND intelligence service, according to an investigation based on CIA documents obtained by the reporters.

Operation Rubicon, as it became known, was both brazen in nature and breathtaking in scope. Foreign governments paid top dollar for the equipment that was being used to spy upon them by both the U.S. and West Germany, and potentially other nation-states that were part of what is known as the Five Eyes alliance: the U.K., Australia, Canada and New Zealand.

Operation Rubicon: How the CIA 'owned' encryption

The *Washington Post* has got access to internal CIA accounts of the intelligence operation known as

Rubicon, and the revelations confirm what has been rumored for many years. Namely that the CIA and BND partnership added backdoors into the Crypto AG encryption products and used these for intelligence gathering purposes across the years. Intelligence gathering, it would appear, from both adversaries and allies. According to the CIA report quoted by the Washington Post, Rubicon was the "intelligence coup of the century."

The idea of a nation-state being able to introduce vulnerabilities into communications equipment that enable eavesdropping into sensitive and supposedly highly encrypted conversations may sound familiar. It's at the heart of the U.S. Government argument to prevent telecoms equipment made by Huawei from being used. Indeed, the revelation that the U.S. apparently has "evidence" of a Huawei capability to do just this is currently being widely reported and continues to stoke the flames of fear. Fear, one must suggest, that could be based upon a been there, done that, had been hiding the t-shirt mentality of U.S. intelligence agencies.

The most detailed evidence of Operation Rubicon so far

The idea of backdoors in Crypto AG ciphering machines has surfaced repeatedly over the decades, the earliest reporting I could find being that of Scott Shane and Tom Browne in the Baltimore Sun back in 1995. However, until now, these reports were based upon hearsay. The *Washington Post* investigation puts the meat back onto the bone with the most detailed CIA history of events to date using leaked "secret" documents.

That history suggests that the company was secretly purchased by the CIA and BND in 1970, with the BND selling its share to the U.S. sometime in the early 1990s. The Washington Post investigation concludes that the CIA might have been able to exploit Crypt AG backdoors until as recently as 2018 when the company was eventually sold to private buyers.

In the meantime, more than 100 governments around the world, possibly as many as 120, purchased and employed the backdoored equipment. China and the Soviet Union, as it was then, weren't amongst the buyers. However, Egypt was, and this apparently enabled the U.S. to monitor communications between Anwar Sadat and Cairo during the Egypt-Israel peace accord meeting at Camp David in 1978. So was Iran, and this was exploited by the U.S. during the 1979 hostage crisis, for example. The U.K. benefited from U.S. intelligence garnered from Argentinian communications during the Falklands War, the report reveals. Other countries that were customers of the company included India, Iraq, Nigeria, Pakistan, Saudi Arabia, Syria and the Vatican.

The *Washington Post* reports that neither of the companies which purchased the "dismembered" Crypto AG assets in 2018 has any "ongoing connection to any intelligence service."

The Swiss government has started an investigation into the reports, having first been made aware of the revelations in November 2019.

The military intelligence expert view

"The intelligence services from any country using legitimate companies as a front is a tactic that has been used for many many years," Philip Ingram, a former Colonel in British Military Intelligence, says, "international cooperation on a bilateral basis again is nothing new what is interesting is this is Germany and the U.S. at a time when it was the U.S. and the U.S. leading cryptology." While in the early days of encryption it was under the control of governments and subject to the same export restrictions as weapons, in 1977, the U.S. International Traffic in Arms Regulation Code was used to raise concerns about the publication and distribution of crypto research. "As the government-led and owned crypto monopoly become more and more fragile with the development of commercial cryptography the intelligence agencies will have done everything they can to try and maintain the edge," Ingram says, "losing visibility, even for a short period of time, is an agencies worst nightmare."

Ian Thornton-Trump, CISO at Cyjax and a former member of the Canadian Forces Military Intelligence

Branch, says that the revelation is "completely in line with the American intelligence community desire for encryption backdoors dating back to World War Two." While arguing that you could spend "zillions of dollars" to break crypto like the allies' efforts back then with Enigma, Thornton-Trump says, "it's so much easier and orders of magnitude less expensive to 'pre-break' encryption at the supply chain level." The problems start when trying to act upon that intelligence. "When you have good intelligence on something really bad about to happen, even though you could counter it, you can't as it may reveal the covert access you have established," he says. Historically, Thornton-Trump says, covert access like this has to be used in a very limited capacity. "Knowing all the things," he concludes, "does not mean you can act on all the things."