FORVM GEOPOLITICA
Independent Commentary on a Fractured World

Encryption and Cyber Insecurity

Russia, China, and North Korea did not fall into a trap set by the U.S., but 120 other nations did! And be warned: Encryption is unsafe and cyber-security is a myth!

Felix Abt

Sat 28 Oct 2023

Short introduction by Peter Hanseler

We are once again pleased that Felix Abt has provided us with a more than interesting article. Felix Abt is the editor of the blog easternangle.com.

Introduction

For Crypto AG, the Swiss company that, according to The Economist, "*rose to dominate the global market for cipher machines after the Second World War*" and was for decades the leading manufacturer of cipher equipment for voice communications and digital data networks, Hans Bühler was the top salesman, accounting for about 40% of the company's sales.

A life-threatening turn in the career of a very successful businessman: who and what is behind it?

He provided numerous nations, particularly those in the Middle East, including Iran, with cipher devices. On his 25th visit to Teheran, he was detained and imprisoned on March 18, 1992. He spent nine months in solitary confinement in the Evin jail in Tehran, where he was interrogated for five hours every day.

Iran charged Bühler with disclosing their encryption keys to Western intelligence. Bühler was released in January 1993 because Crypto AG posted bail of $1 million to Iran, despite his complete ignorance of any problem in the equipment. Bühler's company sacked him shortly after his release, and they went after him personally to get the $1 million bail money back.

CIA controlled global encryption company for decades, says report

Swiss government orders inquiry after revelations Crypto AG was owned and operated by US and German intelligence

'It was the intelligence coup of the century,' the CIA report concluded. Photograph: Saul Loeb/AFP/Getty Images

"It was the intelligence coup of the century," reported Britain's Guardian. Screenshot of the headline from The Guardian, February 11, 2020

A few years later, I met Hans Bühler, a tall, slender person who spoke and explained calmly and confidently: "*Until my arrest in Tehran, I believed in the integrity of my company. But the Iranians knew things I didn't. Obviously, they found out that secrets they thought were safe on Crypto's machines were going to countries that were hostile to them. And they probably knew even then that Western government agencies had hijacked the company to use it as an espionage tool against them.*"

Hans Bühler answering questions by reporters after his release from Iran. Image: Handelszeitung, Zurich

Total deception: the business model of a CIA-controlled company

Bühler's firm bet their name and the security concerns of their clients on their home country's neutrality, and 120 countries, including the Vatican, had purchased the most advanced and ostensibly safe encryption technology from them. Since many nations were understandably wary of the cryptographic equipment sold in NATO nations, they resorted to Switzerland, a neutral third party. Few nations, like China, Russia, and North Korea, continued to be wary of potentially purchasing a Trojan horse in the West and opted to create their own enciphering technology instead. Their suspicions were founded because these gadgets were in fact employed to eavesdrop on their gullible users. For instance, the Washington Post and German state broadcaster ZDF both reported that "*the U.S. intelligence community actively monitored for decades the diplomatic and military communications of numerous Latin American nations through encryption machines supplied by a Swiss company that was secretly owned by the CIA and the German intelligence agency*."

Hans told me that he believed his clients were given an honest sales pitch when he assured them that their messages would be entirely secure as they traveled from their capitals to embassies, military attaches, trade offices, and espionage hotspots throughout the globe and back. He and his clients were shocked to learn that they weren't!

From a bygone era when the media still investigated and reported critically

After Hans Bühler was released from prison, journalists continued their investigation into his case and spoke with him. Reports began to surface on German magazines like Der Spiegel, German Radio International, Swiss Television, and all the main Swiss newspapers. They were looking for information on whether and how Western spy agencies had tampered with Crypto AG's hardware. They spoke with other Crypto AG personnel and continued to delve more and farther. To put an end to the narrative and silence Hans Bühler and other employees, Crypto AG filed a lawsuit in response. However, it was unsuccessful in keeping the media from learning what transpired at the time. They continued to make efforts to determine the circumstances: They discovered that agents from the NSA, America's surveillance agency, frequently paid Crypto AG a visit. NSA cryptographer Nora L. Mackebee, for example, attended a secret workshop at Crypto AG in August 1975 to present a new prototype encryption device. She was listed as an independent "consultant" to disguise her true role as a participant on behalf of NSA.

Additionally, solid proof of a covert agreement between Crypto AG and the NSA from 1951 onwards has been provided by previously classified papers that were partially revealed by the NSA in 2014. There is no doubt that the CIA and the BND, Germany's intelligence service and a longtime collaborator of the US government, agreed to buy Crypto in 1970. However, out of fear of being exposed, the BND sold its stake in the company to the US in the early 1990s. The Washington Post reported that the CIA exploited the business up until 2018, when it sold the business's assets to two private firms.

Now compare this to the way the same media recently handled the worst act of terrorism in Europe since World War II, the Nordstream gas lifeline bombing, and failed to seriously investigate: They would surely react just as shabbily if Buhler were still alive and had returned from Iranian custody at the present time.

The world's most massive industrial-scale espionage program

The US has routinely intercepted and decoded top-secret encrypted messages from 120 different countries for decades. The BND and NSA codebreakers could use the key to decipher any communication sent by any of Crypto AG's 120 countries clients once the cipher machines had been modified to incorporate the secret decryption key. As simply as they might read the morning newspaper, NSA analysts

could analyze the communication flow. Additionally, the CIA thoroughly penetrated and tainted Omnisec, the main rival of Crypto AG, another Swiss-based business, to ensure that nothing slipped their eyes and ears.

Stasi (State security) files from former East Germany that made their way to Iran are likely to have given the Iranians information about the American encryption hacking.

Information stolen from unsuspecting friends and enemies are systematically used against them

According to the revelations, the U.S. used Argentina's reliance on Crypto AG's encryption technology to its advantage during the Falklands War by passing intercepted conversations about Argentine military plans to allied Britain. The breach of the Argentine diplomatic rules was publicly acknowledged by former British Foreign Office minister Ted Rowlands.

Alternatively, the U.S. was able to monitor all of Egyptian President Sadat's communications with Cairo when he met with Israeli Prime Minister Begin and U.S. President Carter at Camp David in 1978 to arrange a peace treaty between Egypt and Israel.

The U.S. had also repeatedly demanded the purchase of certain equipment as a condition for receiving benefits. Pakistan received military loans from the U.S. in return for the purchase of its encryption technology from Crypto AG.

The US and its allies have benefited from 50 years of intercepted communication in terms of trade, diplomacy, economics, and strategy. They have been able to influence international treaties and negotiations by learning the "bottom line" negotiating positions of foreign governments – both "friends" and "enemies." For instance, they would be aware of the king of Saudi Arabia's exact health status, the president of Argentina's covert financial dealings, the negotiating position of South Africa's trade delegation at the World Trade Organization, the South Korean president's attitude toward American troop presence in his country, or the Pope's anti-abortion stance. Such information, which is daily provided to the president and secretary of state in their intelligence briefings, is very helpful and enables the US to play high-stakes diplomatic poker with a mirror behind everyone else's back.

The world's largest surveillance state deflects attention from itself by pointing the finger at China

Ironically, the U.S. government and its partners in the mainstream media often pretend to be outraged by surveillance in China, even though the U.S. has built the most comprehensive and global surveillance state, unmatched by China, which allegedly still uses spy balloons. One China insider even asks the legitimate question, "*In Western scaremongering, the alleged Chinese social credit system or social credit score is played up, but does it even exist?*" The U.S. government spies on people all over the world, including heads of state it calls "allies" and "friends," as well as its own citizens. Even if your cell phone is turned off, it can know when you fart in bed at night, no matter what bed or where.

Lie, cheat, steal: the modus operandi of the most powerful government in the world

In 2018, the year Hans Bühler passed away, the CIA lost interest in Crypto AG after it was revealed that it was a clandestine CIA project. However, it is unquestionably still interested in purposefully degrading encryption techniques so that it may exploit them to snoop on its consumers. And it will undoubtedly uphold the principles that Mike Pompeo, a former head of the CIA, echoed: *"We lied, we cheated, we stole!"* To that end, it most likely owns or has gained access to a number of other businesses.

How easy is it to infiltrate your devices?

The CIA and the NSA also add backdoors to apps they create or purchase in order to ensure that not only governments but also businesses and private citizens can be thoroughly spied on.

End-to-end encryption, such as that used by Zoom, Signal, Telegram, and WhatsApp, cannot be bypassed unless a party has access to the content of the transmission or obtains the keys or ciphers. This can only be done through hacking. But the endpoints (smartphone, PC, or other device) are the weakest link in the chain, as they are almost certainly insecure and can be compromised in an infinite number of ways. Users of software that purports to provide security for end-to-end communications should be aware of this. And even if encryption prevents the content of your messages from being read, the metadata is not hidden or encrypted, which means it is possible to determine who you sent messages to and potentially infer the content. Even if you perfectly protect all your devices and are sure that no

one has access to the messages on them, you cannot be sure that the device of the person you are talking is not compromised. It could also send you malware. End-to-end encryption is no help there.

As for by far the largest and most privacy-invasive government surveillance actor, the NSA has used its supercomputers to crack much more complicated encryption algorithms and decrypt systems on seized hardware and/or communications from foreign intelligence agencies. With this capability, there is probably nothing the NSA can't hack, and it will if it wants to. For example, it can easily decrypt iPhone communications without obtaining the keys from Apple.

ARTICLE TAGS:

Analysis Bühler, Hans China North Korea Russia Switzerland US Crypto AG Pompeo, Michael Der Spiegel Central Intelligence Agency (CIA) NATO The Washington Post National Security Agency (NSA)