« عملیات روبیکان »

فهرست مطالب

APA-IUTcert

کودتای اطلاعاتی قرن

اسناد سیا : « این کودتای اطلاعاتی قرن است».

حدود نیم قرن است که دولت‌های سراسر جهان برای حفظ امنیت و محرمانگی ارتباطات دیپلمات‌ها، مقامات، جاسوس‌ها و ... به یک شرکت واحد اعتماد کرده‌اند: **Crypto AG**

شرکت سوئیسی کریپتو با فروش تجهیزات رمزنگاری به بیش از ۱۲۰ کشور جهان تا قرن ۲۱، میلیون‌ها دلار درآمد کسب کرد. از مشتریان مهم این شرکت می‌توان به کشورهایی در خاورمیانه، نیروهای نظامی حاضر در آمریکای لاتین، پاکستان و هند و حتّی واتیکان اشاره کرد. هیچ‌یک از مشتریان نمی‌دانستند که شرکت کریپتو، درواقع تحت مالکیت محرمانه‌ی آژانس اطلاعاتی آمریکا و آلمان، یعنی CIA و BND قرار داشت. آژانس‌های اطلاعاتی، دستگاه‌های شرکت را مهندسی و دست‌کاری می‌کردند تا با سوءاستفاده از آن‌ها، پیام‌های محرمانهٔ سایر کشورها را به آسانی شنود کنند.

جزئیات برنامه‌ی سوءاستفاده از شرکت کریپتو با عمری به‌اندازه‌ی چند دهه که شامل اسرار طبقه‌بندی شده‌ی جنگ سرد هم می‌شود، در تاریخچه‌ای جامع و محرمانه از عملیات سیا نگه‌داری شده است. اسناد به‌دست آمده، حتی نام مقام‌های آمریکایی مرتبط با پرونده و مدیران اجرایی حاضر در شرکت کریپتو را فاش می‌کند. اطلاعاتی از ریشه‌های شرکت سوئیسی و همکاری با آژانس‌های اطلاعاتی و حتی درگیری‌های داخلی و نهایتاً پایان کار آن در اسناد سیا وجود دارد.اسناد محرمانه نشان می‌دهد که چگونه آمریکا از اعتماد کشورها(حتّی کشورهای دوست) به شرکت کریپتو سوءاستفاده کند. دی این اسناد، این عملیات ابتدا به‌نام **Thesaurus** و سپس با عنوان **Rubicon** شناخته می‌شد.

روبیکان نام رودی در ایتالیا است که به عنوان خط مرزی استفاده می‌شد و ۴۹ سال پیش از میلاد مسیح، سزار برای حمله به روم باستان از آن گذر کرد. انتخاب این کد عملیاتی از آن جهت بود که ایالات متحده و آلمان می‌دانستند در این عملیات، از مرز اطلاعاتی کشورهای دوست و دشمن خود عبور خواهند کرد.

در بخشی از اسناد سیا آمده است: « دولت‌های خارجی پول خوبی به ایالات متحدهٔ آمریکا و آلمان غربی به دلیل داشتن امتیاز خواندن ارتباطات بسیار محرمانه‌شان توسط حداقل دو (و احتمالاً پنج یا شش) کشور خارجی پرداخت می‌کردند.»

APA-IUT.ir

از سال ۱۹۷۰ به بعد، سازمان سیا و آژانس امنیت ملی[1](NSA) ایالات متحده به همراه همتایان آلمانی خود، تقریباً تمامی فعالیت‌های شرکت کریپتو را کنترل می‌کردند. به عبارت دیگر کلیهٔ تصمیمات استخدامی، طرّاحی فنّاوری شرکت، خرابکاری الگوریتم‌ها و حتّی مدیریت اهداف فروش، تحت مدیریت ایالات متحده و آلمان صورت می‌پذیرفت. با مرور زمان نقش آن‌ها کمتر و به شنود محدود شد.

این جاسوسیِ اطلاعات، گستره‌ای وسیع از ارتباطات ایران در زمان تسخیر سفارت‌خانهٔ آمریکا در سال ۱۹۷۹، پشتیبانی اطلاعاتی انگلستان در مورد ارتش آرژانتین در جریان جنگ فالکلندز[2]، دنبال کردن اطلاعات پیرامون ترور سران آمریکای جنوبی تا تبریکات مقامات لیبی به یکدیگر در بمب‌گذاری برلین در سال ۱۹۸۶ را شامل می‌شود.

هر چند عملیات روبیکان، محدودیت‌هایی نیز داشت. برای مثال مهم‌ترین رقبای ایالات متحده آمریکا همچون اتحاد جماهیر شوروی و چین، هرگز مشتریان شرکت کریپتو نبودند. ظن درست آن‌ها به شرکت سوئیسی به سپر اطلاعاتی آن‌ها تبدیل شد. هر چند عملاً اطلاعاتی که بین این کشورها و سایر کشورهای طرف قرارداد کریپتو ردوبدل می‌شد در اختیار آمریکا و آلمان قرار داشت.

همچنین چندین گاف امنیتی، اعتمادپذیری شرکت سوئیسی را زیر سؤال برد. برای مثال در دهه ۱۹۷۰، اسناد بسیاری از مکاتبات سران NSA و بنیان‌گذاران شرکت منتشر شد. به علاوه برخی مقامات کشوری ایالات متحده همچون رونالد ریگان با اظهارنظرات خود، شک رقبای خود را برانگیختند. بیشتر آن که دستگیری فروشندهٔ محصولات کریپتو در ایران، موج عمومی‌سازی عملیات را قوّت بخشید. با این وجود ارتباطات گستردهٔ شرکت با سیا و همتای آلمانی‌ش تا امروز فاش نشده بود. آژانس جاسوسی آلمان که احتمال افشای عملیات را زیاد می‌دانست اوایل دهه ۹۰ میلادی از پروژه خارج شد. سیا با خرید سهم آلمان به عملیات اطلاعاتی خود تا سال ۲۰۱۸ ادامه و نهایتاً در آن سال کلیهٔ دارایی‌های شرکت را فروخت.

با توسعهٔ فناوری رمزنگاری مبتنی بر نرم‌افزار، از اهمیّت شرکت کریپتو کاسته شد. الگوریتم‌های پیچیدهٔ رمزنگاری که روزی تحت قدرت و مالکیت دولت‌ها و شرکت‌های بزرگ بودند؛ اکنون در حد برنامه‌های کاربردی تلفن هوشمند، همه‌گیر شده‌اند. با این وجود عملیات روبیکان به خرابکاری مدرن گره خورده است. مدت زمان وحجم عملیات، سیری‌ناپذیری ایالات متحده برای نظارت جهانی را نشان می‌دهد. همچنین ردپایی شبیه کریپتو در ارتباط شرکت‌های مطرح و بین‌المللی و دولت‌ها وجود دارد که شک‌برانگیز است. شرکت‌هایی مانند ضدبدافزار روسی کسپراسکای، برنامهٔ پیام کوتاه و امارات و غول ارتباطات چین یعنی هواوی.

گزارش پیش رو مبتنی بر تاریخچهٔ سیا و BND و مصاحبه‌هایی است که با برخی مقامات اطلاعاتی سابق و کارمندان شرکت کریپتو صورت پذیرفته است. بسیاری از مصاحبه‌شوندگان با توجه به حساسیت موضوع تنها به صورت ناشناس حاضر به افشای اطلاعات شدند.

اطلاعات مربوط به این عملیات بی‌سابقه است.سازمان‌های CIA و BND هیچ اظهارنظری درباره‌ی اطلاعات افشاشده نداشته‌اند، اما هیچ‌یک نیز ادعایی علیه اعتبار اسناد نکردند. سند اول، گزارشی ۹۶ صفحه‌ای از عملیات در سال ۲۰۰۴، توسط سیا در شاخهٔ پیشینهٔ داخلی نوشته شده است. سند دوم پیشینه‌ای شفاهی در سال ۲۰۰۸ است که توسط مقامات اطلاعاتی آلمان بیان شده است.

[1] The National Security Agency
[2] The Falklands War

دو سند با وجود هم‌پوشانیِ اطلاعاتی نشان می‌دهند که دو شریک پروژه پیرامون درآمد مالی، کنترل عملیات و محدودیت‌های اخلاقی، اختلاف نظر داشته‌اند(شکل زیر). در بخش‌هایی از سند دوم دیده می‌شود که طرف آلمانی، از اشتیاق شدید همتایان آمریکایی خود در هدف قرار دادن کشورها، مبهوت می‌شده‌اند.

(S) German and American case officers who had worked together remember the days of MINERVA with fondness. For almost everyone it was the highlight of their careers. Even during periods of disagreement, there was a recognition that the greater good of Western intelligence required that the project continue to run smoothly. Cultural differences, and the divergent interests of the two countries, were overcome, again and again, to fashion the most profitable intelligence venture of the Cold War.

هر دو سازمان CIA و BND، عملیات را موفّق و ماورای پیش‌بینی‌هایشان توصیف کرده‌اند. برای مثال در دهه ۸۰ میلادی، بالغ بر ۴۰ درصد اطلاعات NSA از ارتباطات مقامات دیپلماتیک دنیا با استفاده از تجهیزات شرکت کریپتو بدست آمده است و برای آلمان ۹۰ درصد گزارشات ارتباطات دیپلماتیک از این تجهیزات به دست آمده است(شکل زیر).

(TS) The American-German partnership on MINERVA had continued for over twenty years. To the Americans it represented over 40 percent of NSA's total machine decryptions, and was regarded as an irreplaceable resource. To the Germans, however, it was even more important, accounting for 90 percent of the BND's diplomatic product reports. The BND regarded it as the linchpin of its highly productive intelligence relationship with the Americans.

به علاوه میلیون‌ها دلار سود خالص شرکت کریپتو، بین دو شریک اطلاعاتی تقسیم و به سایر عملیات‌ها تزریق می‌شد که این خود دستاورد قابل‌توجّهی بود.

متاسفانه محصولات کریپتو همچنان در ده‌ها کشور در سراسر جهان استفاده می‌شوند و هنوز لوگوی نارنجی و سفید شرکت، بالای مقر اصلی آن در نزدیکی شهر زوگ سوئیس می‌درخشد.

شرکت کریپتو در سال ۲۰۱۸ توسط سهام‌دارانی که هویّت آنها با توجّه به قوانین تجاری لیختن‌اشتاین، برای حفظ اسرار مالی مخفی مانده است، منحل شد. دارایی‌های این شرکت توسط دو شرکت خریداری شد. شرکت اول، CyOne Security است که محصولات امنیتی خود را عمدتاً به دولت سوئیس می‌فروشد و شرکت دیگر شرکت Crypto International که از برند شرکت کریپتو برای تجارت بین‌الملل استفاده می‌کند. اگر چه هر دوی این شرکت‌ها، ارتباط با سرویس‌های اطلاعاتی را رد می‌کنند؛ اما تنها یکی از آن‌ها، از مالکیت سازمان سیا اظهار بی‌اطلاعی کرده است.

شرکت CyOne Security لینک بیشتری با شرکت منحل‌شده‌ی کریپتو دارد. مدیرعامل این شرکت به‌مدّت دو دهه و در زمان مالکیت سیا، مدیرعامل کریپتو بوده است. با این وجود سخنگوی CyOne می‌گوید: «هیچ ارتباطی با هیچ سرویس اطلاعاتی خارجی ندارد.» آندره لیند[3]،رئیس شرکت سابق کریپتو که اکنون حق مالکیت محصولات و تجارت آن را در شرکت Crypto International دارد، می‌گوید کاملاً از ارتباطات شرکت کریپتو و سازمان‌های CIA و BND بی‌اطلاع بوده و به تازگی آگاه شده است!

او در مصاحبه‌ای گفت: «ما در Crypto International هیچ ارتباطی با CIA یا BND نداریم و لطفا سخن من را نقل کنید ... چرا که اگر چیزی که شما می‌گویید درست باشد؛ من احساس خیانت می‌کنم و خانواده‌ام احساس خیانت می‌کنند و من می‌دانم کارمندان بسیاری احساس خیانت خواهند کرد و حتی مشتریان.»

دولت سوئیس، سه‌شنبه چهارم فوریه از بازرسی ارتباطات شرکت کریپتو با CIA و BND خبر داد. به‌علاوه آن‌ها مجوز صادرات شرکت Crypto International را نیز باطل کردند. زمان‌بندی اقدامات دولت سوئیس، جالب‌توجّه است چرا که اسناد CIA و BND ادعا می‌کنند که مقامات سوئیسی ده‌ها سال از ارتباط شرکت با سازمان‌های آمریکایی و آلمانی خبر داشته‌اند. به نظر می‌رسد آن‌ها پس از آغاز افشای اطلاعاتی رسانه‌ها، تصمیم به مداخله گرفته‌اند.

اسناد تاریخچهٔ سیا به اینکه این سازمان چه موقع و یا اصلاً دخالت خود را تمام کرده است یا خیر، اشاره‌ای نمی‌کند. این اسناد، روایت متعصبانهٔ طراحان و معماران عملیات روبیکان است. آن‌ها روبیکان را عملیات جاسوسی موفّقی می‌دانند که به ایالات متحده کمک کرده است تا در جنگ سرد پیروز شود، از رژیم‌های استبدادی اخّاذی کند و منافع خود و هم‌پیمانانش را حفظ کند. به علاوه این اسناد سؤالات ناخوشایندی مثل اینکه ایالات متحده چه چیزی می‌دانسته و در قبال آن چه کار کرده یا نکرده است را نیز پاسخ نمی‌دهد. آن‌ها در بسیاری موارد از نقشه‌های ترور، نسل‌کشی و نقض حقوق بشر آگاه بوده‌اند و فقط نظاره کرده‌اند. همچنین این اسناد به مهم‌ترین مسأله اخلاقی این عملیات اشاره نمی‌کند، یعنی فریب و سوءاستفاده از مخالفان، متحدان و صدها کارمند شرکت کریپتو که ناآگاهانه به سراسر جهان سفر کرده و محصولات شرکت را به فروش می‌رساندند.

در مصاحبه‌های اخیر، کارمندانِ فریب‌خورده ابراز کردند که با انتشار اسناد شرکت به شدّت احساس خیانت به خودشان و مشتریانشان دارند. برای مثال یورگ اسپورندی[4]، مهندس برقی که ۱۶ سال برای شرکت کار کرده است، می‌گوید: « فکر می‌کنید که کار خوبی انجام می‌دهید و چیزی را امن می‌سازید و سپس متوجّه می‌شوید که به مشتریان خود خیانت کرده‌اید».

در مقابل، مسئولان اجرای عملیات ابداً پشیمان نیستند. برای مثال بابی ری‌اینمان[5]، مدیر NSA و معاون CIA در اواخر دههٔ ۷۰ و اوایل دههٔ ۸۰ میلادی می‌گوید:

[3] Andreas Linde
[4] Juerg Spoerndli
[5] Bobby Ray Inman

« آیا ناراحت هستم؟ هرگز... عملیات، منبع بسیار ارزشمند ما از ارتباطات بخش اعظمی از جهان و برای سیاست گذاران ایالات متحده بسیار بااهمیّت بود».

APA-IUTcert

شروع عملیات

داستان عملیات روبیکان از نیاز ارتش آمریکا به دستگاه رمزنگاری آغاز شد.

بوریس هایلین[6]، بنیان‌گذار شرکت کریپتو، کارآفرین و مخترع روسی بود که برای ادامهٔ تحصیل به سوئد رفت. وی که از خانواده‌ای متموّل بود با انقلاب روسیه و قدرت گرفتن بولشوویک‌ها[7] در روسیه، نتوانست به روسیه بازگردد(شکل زیر) و در خلال جنگ جهانی، زمانی که ارتش نازی نروژ را اشغال کرد به ایالات متحده آمریکا رفت.

(U) Boris Caesar Wilhelm Hagelin was raised under very different circumstances. Born in Adschikent, a small town near Baku in Azerbaijan, on July 2, 1892, he was the son of a wealthy Swedish industrialist who managed the Baku oilfields for the Nobel family. His father was a personal friend of Emanuel Nobel, who then headed the family, and it was assumed that Boris would someday assume management of the Nobel oil interests in Russia. After early schooling in Russia, Boris was sent to Sweden to finish his education, and graduated from the Royal Technical University in Stockholm in 1914 with a degree in mechanical engineering. He entered employment with ASEA (Allmanna Svenska Elektriskz Aktiebolaget), the General Electric of Sweden, to apprentice for his presumed management role in the Nobel enterprises. But as the Russian Revolution so inconveniently intervened, it would not have been politic, or even possible, for him to go back to Baku, so he spent a year in the United States, marking time.

او یک ماشین رمزنگاری، شبیه به جعبهٔ موسیقی را با خود به آمریکا برد. این دستگاه شامل یک میل‌لنگ در کنار و دنده‌های فلزی و چرخ‌دنده‌ها درون جعبه بود.

[6] Boris Hagelin
[7] The Bolsheviks

ماشین رمزنگاری هایلین به اندازه ماشین‌های انیگما[8] که توسط ارتش نازی استفاده می‌شدند؛ امن نبود ولی این ماشین که با نام M-209 شناخته می‌شد وزن کمتر و قابلیت جابه‌جایی بیشتری داشت به علاوه برای استفاده از آن نیازی به برق نبود(شکل زیر). هنوز هم از چندین ماشین رمز هایلین در موزهٔ خصوصی آیندهوفن[9] هلند نگهداری می‌شود.

(U) The Story of the M-209

(U) The C-36, which eventually became known as the M-209 in American circles, was ideal for battlefield use. It was light, easy to carry, required no electricity, and could produce enciphered characters at the rate of almost one every two seconds. In 1937 Hagelin journeyed to the United States to peddle his wares, and there he first met William Friedman. The two men immediately hit it off -- they enjoyed similar interests, and stayed in touch with each other. Hagelin was again in the United States in 1939, trying to sell the C-36 and its successor, the C-38, and showed Friedman the improved machine.

ارسال پیام با دستگاه رمز هایلین کمی دشوار بود. فرستنده پیام، حرف به حرف دستگاه را تنظیم و میل‌لنگ را پائین می‌کشید. چرخ‌دنده‌های داخل جعبه، پیام رمزشده را روی یک نوار کاغذی چاپ می‌کرد. یک افسر ارتش، پیام رمزشده را با استفاده از کد مورس ارسال می‌کرد و نهایتاً گیرندهٔ پیام عملیات رمزگشایی را با استفاده از دستگاه به صورت معکوس انجام می‌داد.

امنیت پیام رمزشده با دستگاه M-209 کم بود. به گونه‌ای که دشمن با صرف زمان(معمولاً چند ساعت) می‌توانست آن را رمزگشایی کند. هرچند از آنجا که از آن برای رمزنگاری پیام‌های تاکتیکی در مورد حرکت نیروها استفاده می‌شد؛ زمانی که نازی‌ها سیگنال را کدگشایی می‌کردند، پیام فاقد ارزش بود.

بالغ بر ۱۴۰ هزار دستگاه M-209 زمان جنگ در کارخانهٔ Smith Corona typewriter در سیراکیوز نیویورک ساخته شد. این حجم تولید، تحت قراردادی به ارزش ۸.۶ میلیون دلار بین ارتش ایالات متحده و کریپتو صورت پذیرفت. پس از جنگ، هایلین کارخانه‌اش را در سوئد بازگشایی کرد در حالی که ثروتی عظیم و حس وفاداری ابدی به ایالات متحده را نیز با خود به سوغات آورده بود.

با این وجود جاسوسان آمریکایی محتاطانه وی را زیر نظر داشتند. اوایل دههٔ ۵۰ میلادی، هایلین نسخهٔ پیشرفته‌تر دستگاه خود را ساخت. در ماشین جدید از توالی مکانیکی نامنظّمی استفاده می‌شد که کدشکن‌های آمریکایی نتوانستند پیام رمزشده با آن را رمزگشایی کنند. قابلیت‌های دستگاه جدید که بعداً CX-52 نام گرفت، مقامات آمریکا را به فکر فرو برد.

طبق اسناد سیا(شکل زیر)، آن زمان «دوران تاریک رمزنگاری آمریکا» بود. به اقرار سازمان سیا، اتحاد جماهیر شوروری، چین و کرهٔ شمالی از سیستم‌های رمزی استفاده می‌کردند که غیرقابل نفوذ و شکستن بودند. با ظهور CX-52، آمریکا نگران بود که سایر کشورهای جهان نیز با خرید آن، نفوذناپذیر شوند.

[8] Enigma
[9] Eindhoven

(S) When, in 1950, North Korean forces attacked the south, Army codebreakers cracked the North's communications security like a nut in a vise. A year later that effort, too, was in tatters, a victim of North Korean communications security improvements. The codebreakers were to read none of the enemy's high-level systems for the rest of the war.

(S) And so American codebreaking entered into a period that CIA official Charles Collins once called "the Dark Ages of American cryptology." When Dwight Eisenhower became president, American cryptologists were reading none of the high-level ciphers of their three principal enemies.

امّا ایالات متحده چندین برگ برنده در بازی با هایلین داشت: اوّل تمایل عقیدتی هایلین و حس مثبت او به این کشور، دوم تلاش هایلین برای حفظ آمریکا به عنوان مشتری همیشگی و سودآور خود و نهایتاً این که هایلین نگران بود که ایالات متحده با عرضهٔ دستگاه‌های M-209 که از جنگ باقیمانده بود؛ شهرت او را لکّه‌دار کند.

امّا مهم‌ترین برگ برنده برای ایالات متحده، داشتن ویلیام فریدمن[10] بود. فریدمن که به عنوان پدر رمزنگاری آمریکا شناخته می‌شود با هایلین را از دههٔ ۱۹۳۰ میلادی آشنا بود. از آنجا که هایلین و فریدمن هر دو روس‌تبار با عقبه و علایق مشترک و شیفتهٔ پیچیدگی‌های رمزنگاری بودند؛ دوستی عمیقی با یکدیگر داشتند. اگر دوستی هایلین و فریدمن نبود؛ ممکن بود که عملیات روبیکان نیز نباشد. سال ۱۹۵۱ در کلوبی در واشنگتن، ویلیام فریدمن در قراری پنهانی با بوریس هایلین، به او پیشنهاد کرد تا دستگاه‌های پیچیدهٔ خود را به کشورهای خاص و دستگاه‌های قابل‌نفوذ را به سایر کشورها بفروشد(شکل زیر). در عوض به عنوان جبران خسارت فروش به هایلین بیش از ۷۰۰۰۰۰ دلار پرداخت شد.

(S) When Hagelin arrived in Washington, he and Friedman went to dinner at Friedman's favorite haunt, the exclusive Cosmos Club. Over dinner, Friedman set forth quite a different menu. Would it be possible, Friedman asked, to control the sale of the new machines in such a way that only certain countries could purchase the newer, more secure, machines? Hagelin sounded interested, and agreed to hear what Friedman's organization, the Armed Forces Security Agency (AFSA), had to offer.

سال ۱۹۶۰، سازمان سیا و هایلین قرارداد خود را تحت توافقنامه‌ای به نام «توافق صدور مجوز[11]» تمدید کردند(شکل زیر). برای تجدید تعهدّات هایلین ۸۵۵۰۰۰ دلار پیش‌پرداخت به وی پرداخت شد. به‌علاوه سالانه ۷۰۰۰۰ دلار کمک‌هزینه و ۱۰۰۰۰ دلار نیز برای فعالیت‌های بازاریابی به هاگلین پرداخت شد تا بیشتر دولت‌های جهان با وی قرارداد بسته و سایر شرکت‌های حوزهٔ رمزنگاری توان رقابت با او را نداشته باشند.

[10] William Friedman
[11] Licensing Agreement

(S) The Licensing Agreement was not much different, technically, from the Gentlemen's Agreement, but it was in writing. Hagelin could sell any machine to any NATO countries, plus Switzerland and Sweden. As for the rest, the agreement had an attached chart showing who could buy what. It was to last for five years, with automatic renewals annually past 1965 for another ten years. After 1975, renewals would require specific concurrence from both parties. The United States would have patent rights to all Hagelin equipment (except for the pocket device, which Bo still possessed) for the duration of the agreement.

هدف از این قرارداد این بود که هیچ سلاح و فناوری اطلاعاتیی که خارج از کنترل و نظارت آمریکا باشد به دست دشمنان این کشور نرسد. این قرارداد شروع همکاری شرکت کریپتو (که به سوئیس نقل مکان کرده بود) و سازمان اطلاعات آمریکا بود.

APA-IUT.ca

رویکرد حریصانه

در رویکردی جدید مقامات ایالات متحده مایل بودند به هایلین پیشنهاد کنند تا اجازه دهد ماشین‌های رمزنگاری توسط متخصصان آمریکایی دستکاری شود. ولی فریدمن آن‌ها را منصرف و متقاعد کرد که هایلین این پیشنهاد را نخواهد پذیرفت و آن را زیاده‌روی می‌داند.

اواسط دهه ۶۰ میلادی، روزنهٔ امیدی برای سازمان CIA و NSA ظاهر شد. با رشد وتوسعهٔ مدارهای الکترونیکی، هایلین مجبور به پذیرش کمک از بیرون شرکت برای اتّخاذ فناوری جدید شد. در غیر اینصورت شرکت ورشکست می‌شد چرا که محصولات کریپتو، ماشین‌هایی مکانیکی بودند. به طور مشابه NSA نیز نگران فناوری نوظهور در حوزهٔ رمز بود زیرا به نظر می‌رسید عصر رمزنگاریِ غیرقابل‌شکست آغاز شده است. در این بین تحلیل‌گر ارشد NSA به نام پیتر جنکس[12]، آسیب‌پذیری بالقوه‌ای را شناسایی کرد.

نظر جنکس این بود که اگر مبنای ریاضی محصولات کریپتو به دقّت طراحی شود؛ دستگاه می‌تواند به گونه‌ای به نظر آید که رشته‌ای از کاراکترهای رندوم تولید می‌کند. حال آن که در واقع خروجی دستگاه، رشتهٔ دارای الگویی است که کارشناسان رمزنگاری NSA می‌توانند آن را کدگشایی کنند. دو سال بعد، سال ۱۹۶۷، شرکت کریپتو دستگاه جدید و تمام-الکترونیک خود موسوم به H-460 (شکل زیر) را بیرون داد که تماماً توسط NSA طراحی شده بود. نفوذ به شرکت کریپتو و مجاب کردن آن‌ها به فروش ابزار دلخواه آمریکا، رویکردی حریصانه بود که از نظر مقامات ایالات متحده، موفّقیتی بزرگ به حساب می‌آید.

سازمان NSA یک در پشتی خام یا برنامه‌ای که کلیدهای رمزنگاری را استخراج کند، روی دستگاه نصب نکرده بود و آژانس همچنان با مشکل تفسیر و کدگشایی ارتباطات سایر دولت‌ها روبرو بود- چه سیگنال در هوا پخش شود و چه مانند سال‌های اخیر،

[12] Peter Jenks

از طریق کابل‌های فیبر نوری ارسال شود. با این وجود دستکاری الگوریتم‌ها و طراحی ماشین‌های کریپتو، زمان فرآیند کدگشایی که می‌توانست ماه‌ها به طول بیانجامد، کاهش داده و در مواردی به چند ثانیه رسانده بود.

شرکت کریپتو همواره دو نسخه از هر مدل از محصولات خود را تولید می‌کرد: یکی برای فروش به دولت‌های دوست و دیگری برای سایر کشورهای دنیا. بدین ترتیب مشارکت ایالات متحده و کریپتو تکامل یافته بود به گونه‌ای که هایلین دستگاه‌های دارای آسیب‌پذیری را به مشتریانش می‌فروخت و آگاهانه به آن‌ها خیانت می‌کرد. با شیفت کامل محصولات شرکت و توسعهٔ فعالیت‌های تجاری آن، هایلین به رابطه با آمریکا معتاد شده بود. دولت‌های خارجی با عطش بسیار، سیستم‌های رمزنگاری الکترونیک را به جای دستگاه‌های مکانیکی از شرکت کریپتو تقاضا می‌کردند. دستگاه‌هایی که در ظاهر بهتر از پیشینیان مکانیکی خود بودند ولی در اصل رمزگشایی آن‌ها برای جاسوسان آمریکایی ساده‌تر بود.

APA-IUT.ir

شکل‌گیری دوگانهٔ آلمان و آمریکا

اواخر دههٔ ۶۰ میلادی، هایلین که نزدیک به ۸۰ سال سن داشت، بابت آیندهٔ شرکت خود با بیش از ۱۸۰ کارمند، نگران بود. مقامات سیا نیز به طور مشابه نگران آیندهٔ عملیات بودند. هایلین یک بار ابراز امیدواری کرده بود که کنترل شرکت را به پسرش بو[۱۳]، بسپارد. لیکن مقامات اطلاعاتی آمریکا او را ریسکی برای عملیات دانسته و مشارکتشان را از او پنهان کرده بودند. در سال ۱۹۷۰ بو هایلین در یک تصادف مشکوک در کمربندی واشنگتن کشته شد!

مقامات اطلاعاتی آمریکا مدت‌ها پیرامون خرید شرکت کریپتو بحث می‌کردند ولی اختلافات داخلی دو سازمان CIA و NSA، مانع خرید شده بود. تا آن که دو سازمان جاسوسی دیگر وارد بازی شدند: فرانسه و آلمان غربی. این دو کشور و سایر سرویس‌های اطلاعاتی اروپا، کمابیش در مورد ارتباطات کریپتو و ایالات متحده مطلّع شده بودند و مایل بودند معامله‌ای مشابه با شرکت داشته باشند.

سال ۱۹۶۷، سرویس اطلاعاتی فرانسه و آلمان خرید شرکت را به هایلین پیشنهاد کردند. هایلین پیشنهاد آن‌ها را رد و به سازمان CIA گزارش کرد. دو سال بعد، آلمان‌ها با اشاره به حفظ منافع آمریکا، پیشنهاد خود را مجدداً مطرح کردند. در نشستی اوایل سال ۱۹۶۹ در سفارت‌خانهٔ آلمان غربی در واشنگتن، رئیس رمز کشور آلمان غربی، ویلهلم گوئنگ[۱۴]، پیشنهادیهٔ خود را به آمریکا تقدیم و نسبت به مشارکت در عملیات ابراز علاقه‌مندی کرد. چند ماه بعد، یکی از مدیران سیا به نام ریچارد هلمس[۱۵] برای مذاکره با آلمان غربی به پایتخت آن یعنی بون[۱۶] اعزام شد تا با مقامات آلمان غربی مذاکره کند. این مذاکرات یک پیش‌شرط داشت، فرانسه باید از بازی حذف می‌شد. آلمان غربی، سلطهٔ آمریکا را در بازی قدرت پذیرفته و ژوئن سال ۱۹۷۰، قراردادی بین دو آژانس اطلاعاتی CIA و BND نوشته شد(شکل زیر).

(S) The sale was made on 4 June, and the agreement with the BND was contained in a 12 June 1970 memorandum of understanding between CIA and the BND. For CIA, COB Munich Tom Lucid signed, in a hand made shaky by Parkinson's disease, while the BND signature was illegible. It specified that the BND, operating through Deutsche Truehand Gesellschaft-Munich (DTG-M), would purchase AEH. The sale price was 25 million Swiss Francs, 8.5 million to be paid at contract closing, and the remainder to be paid in two equal installments on 1 June 1971 and 1 June 1972. Hagelin had remarried in 1969, and insisted that a pension be provided for his new wife -- Elsa Hagelin (nee Svensson), his late wife's former nurse -- after his death. All decisions would be subject to joint CIA-BND concurrence.

نهایتاً هر دو سازمان سهمی مساوی از تقریباً 5.75 میلیون دلار به هایلین پرداختند. سازمان سیا اینکه چگونه ردپایی از دو سازمان در این قرارداد و تراکنش‌ها باقی نماند را به آلمان واگذار کرد. یک شرکت حقوقی در لیختن‌اشتاین به نام Marxer and Goop، کمک کرد که هویت مالکین جدید کریپتو مخفی بماند. این شرکت دستمزدی سالانه از آن‌ها دریافت می‌کرد که به نقل مستقیم

[13] Bo
[14] Wilhelm Goeing
[15] Richard Helms
[16] Bonn

از BND، «بیشتر حقّ‌السکوت بود تا برای کاری که کرده بودند». شرکت فوق‌الذکر که اکنون Marxer and Partner نام دارد؛ هیچ نظری در مورد رسوایی کریپتو نداشت.

پس از خرید شرکت، هیئت مدیرهٔ جدیدی برای کنترل شرکت تشکیل شد. از هیئت مدیرهٔ سابق، تنها یک عضو به نام استور نایبرگ[17] از مالکیت سیا آگاه بود. سال ۱۹۷۶، نایبرگ شرکت را ترک کرد و از وضعیت فعلی او هیچ اطلاعی در دست نیست.

سازمان‌های CIA و BND، جلسات منظّمی پیرامون نحوهٔ مدیریت عملیات داشتند. ملاقات دو سازمان ابتدا در مقر مخفی سازمان سیا در مونیخ صورت می‌پذیرفت و سپس به اتاقی در ساختمان مجاور کنسولگری آمریکا در این شهر منتقل شد. آن‌ها روی مجموعه‌ای از اسامی رمز توافق کرده بودند. برای مثال شرکت کریپتو، مینِروا[18]، الههٔ خرد و جنگ استراتژیک در روم باستان(شکل زیر)، خوانده می‌شد.

نایبرگ به نام بَل[19] و همکارش اُسکار استوارزینگر[20]، سیگفرید[21] خوانده می‌شدند. همچنین کد سازمان CIA، EOS، سازمان BND، GAMMA و آژانس NSA، HOCKEY بود. نام عملیات ابتدا Thesaurus بود که در دههٔ ۸۰ میلادی به روبیکان تغییر داده شد(شکل زیر).

(S) To cover the whole arrangement, CIA and the BND agreed to a special cryptonym series. CAG would always be referred to as MINERVA, so as not to have to use the true company name. Foreign players in the game got cryptonyms. Nyberg, the only original CAG player who was witting, was named BALL, while his technical, but unwitting, counterpart, Oscar Stuerzinger, was called SIEGFRIED.

(S) Each major organization got a cryptonym: thus, CIA was EOS, NSA was HOCKEY, BND was GAMMA, ZfCh was SIGMA, and Siemens was OLYMPIA. The American firm Motorola, which had been brought into the MINERVA equation in the 1960s, was called NAVAHO. AEH, the holding company that owned Crypto AG, was called GOLF. Even DTG, the accounting firm, had a cryptonym. It was called FIDELIO.

(S) The Partners named their joint project THESAURUS. In the late 1980s they changed the name to RUBICON. They held periodic conferences to establish or change policy. Essentially, the conferences undertook the role of a covert board of directors.

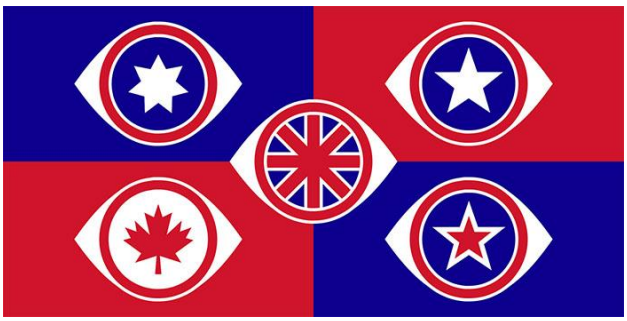
[17] Sture Nyberg
[18] Minerva
[19] BALL
[20] Oscar Stuerzinger
[21] SIEGFRIED

هر سال دو کشور، سود حاصل از کریپتو را تقسیم می‌کردند. طبق اسناد آلمانی، BND پول سازمان سیا را در یک پارکینگ زیرزمینی به آن‌ها تحویل می‌داد. با مرور زمان، اختلافات و تنش‌های بین دو سازمان بالا گرفت. از طرفی سیا به BND خرده می‌گرفت که چرا دائماً به فکر سودآوری بوده و دید عملیاتی خود را از دست داده است. طرف آلمانی نیز به حرص آمریکا نسبت به جاسوسی از همه حتّی نزدیک‌ترین هم‌پیمانانش از جمله اعضای ناتو مثل اسپانیا، یونان، ترکیه و ایتالیا معترض بود(شکل زیر).

(S) Cipher readability was a vexing question. Why produce readable and nreadable equipment, NSA officers asked themselves, if they could sell readable equipment to everyone? So as time went on, the American position began to change. Americans became less and less agreeable to selling secure equipment to anyone. Why secure Spanish communications if they were yielding useful information? Why, indeed, secure the communications of some of the NATO countries? Greece and Turkey were taken off the "secure" list at a very early date, even though they were NATO partners. The list of protected nations became shorter by the year.

(S) Germany, with a Eurocentric outlook, strongly supported the two-cryptologies approach. The BND did not like to sell readable equipment to its allies. According to bilateral MINERVA agreements, the BND had to concur in all CAG sales. But NSA remained tenacious, and in the long run, only a handful of NATO nations directly or indirectly involved in MINERVA, plus Sweden and Switzerland, remained protected.

دو سازمان CIA و BND، با آگاهی از محدودیت‌های تکنیکال خود برای مدیریت شرکتی با تکنولوژی بالا، شرکت‌های بزرگی مثل زیمنس و موتورولا را وارد عملیات کردند. آلمان‌ها، ۵ درصد از فروش شرکت را برای دریافت مشاورهٔ تجاری و فنی با شرکت زیمنس مبادله کردند. از آمریکا، شرکت موتورولا برای دستکاری محصولات وارد شد.به این ترتیب تقریباً برای رؤسای شرکت موتورولا محرز شد که این کار را برای سازمان‌های اطلاعاتی آمریکا انجام می‌دهند. مسئولین هر دو شرکت مذکور از اظهار نظر پیرامون این عملیات خودداری کردند.



با مشارکت در این عملیات، آلمان که هرگز نتوانسته بود به پیمان دیرینهٔ اطلاعاتی «پنج چشم» شامل آمریکا، بریتانیا، استرالیا، نیوزیلند و کانادا(شکل زیر) اضافه شود؛ به شدت به آمریکا نزدیک شده بود.

همچنین با پشتیبانی دو آژانس اطلاعاتی و دو شرکت پیشرو در فناوری اطلاعات، تجارت شرکت کریپتو شکوفا شد. اسناد سازمان سیا(شکل زیر) به وضوح نشان می‌دهد که فروش شرکت از ۱۵ میلیون فرانک سوئیسی در سال ۱۹۷۰ به بیش از ۵۱ میلیون فرانک سوئیسی یا ۱۹ میلیون دلار، افزایش یافت.

APA-IR

Table 3
(S) Crypto AG: Sales and Profits, 1970-1975

Year	Sales (SFr)	Profits (SFr)	Profit as a Percentage of Sales
1970	15.17	1.38	9%
1971	15.86	.83	5%
1972	19.17	3.47	18%
1973	27.59	2.90	10%
1974	34.48	4.12	12%
1975	51.27	4.41	8.6%

امّا سود خالص آمریکا، دو دهه دسترسی بی‌سابقهٔ اطلاعاتی به ارتباطات دولت‌های خارجی بود.

APA-IUT.ir

عملیات بین‌المللی

اهداف شنود NSA از نظر جغرافیایی به سه گروه شوروی با کد A، آسیا با کد B و سایر کشورها با کد G تقسیم می‌شدند. اوایل دهۀ ۸۰ میلادی بیش از نیمی از اطلاعات جمع‌آوری‌شده از گروه G از طریق ماشین‌های کریپتو به دست می‌آمدند و وابستگی سازمان‌های آمریکا به این اطلاعات روز به روز بیشتر می‌شد. از جمله در سال ۱۹۷۸، زمانی که سران کشورهای مصر و آمریکا و رژیم اسرائیل برای مذاکرات صلح در کمپ دیوید، گرد آمده بودند؛ آژانس NSA مخفیانه ارتباطات رئیس جمهور مصر، اَنوَر سادات[۲۲] با قاهره را شنود می‌کرد. یک سال بعد، پس از تسخیر لانۀ جاسوسی آمریکا، ارتباطات ایران و الجزایر(واسط بین ایران و آمریکا در آن زمان) شنود می‌شد. مدیر وقت NSA، اینمان می‌گوید جیمی کارتر، رئیس‌جمهور وقت آمریکا مرتباً با آژانس تماس می‌گرفت و اطلاعات می‌خواست. اینمان در این زمینه می‌گوید: « ما در ۸۵ درصد موارد، قادر بودیم به او اطلاعات دهیم». چرا که هر دو کشور ایران و الجزیره از دستگاه‌های کریپتو استفاده می‌کردند. به گفتۀ اینمان دستگاه‌های کریپتو برای آمریکا بسیار حیاتی بود و برای رئیس جمهور، امکان استفادۀ مؤثر از موقعیت و مدیریت مذاکرات را فراهم می‌کرد. (شکل زیر).

(TS) The negotiations to repatriate the American hostages in Iran dominated the late Carter years. To President Carter, it was critical to know what the Iranians were up to, and since the Algerians were acting as intermediaries, that information came from Algerian diplomatic communications. Admiral Bobby Inman, then DIRNSA, recalled in an interview that the President would frequently call him at his office at Fort Meade to request information that NSA could gain through Algerian communications. Those communications, Inman said, were MINERVA-enabled, and this was the "absolutely critical ingredient" in enabling the President to appreciate the situation and manage the negotiations.

اینمان می‌گوید این عملیات او را در یکی از سخت‌ترین شرایطی که در ارائۀ خدمات دولتی داشت، قرار داده بود. زمانی که با رمزگشایی ارتباطات لیبی، فاش شد که برادر رئیس‌جمهور، بیلی کارتر[۲۳]، حامی منافع لیبی در واشنگتن است و از رهبر لیبی یعنی معمّر قذافی دستمزد دریافت می‌کند. اینمان، موضوع را به دپارتمان عدالت گزارش می‌کند. اف‌بی‌آی بیلی کارتر را بازجویی کرده و او به دروغ، دریافت پول از لیبی را رد می‌کند. در پایان برادر رئیس‌جمهور محاکمه نشد ولی عنوان «عامل خارجی» در پروندۀ وی ثبت می‌شود.

مثالی دیگر از دخالت ایالات متحده با کمک گرفتن از تجهیزات کریپتو، کودتای پینوشه در شیلی سال ۱۹۷۳ میلادی است. سال ۱۹۷۰ سالوادور آلنده[۲۴] به عنوان رئیس‌جمهور شیلی انتخاب شد. جناح راست شیلی مخالف او بود و با ابراز وفاداری به آمریکا از این کشور خواست تا به آن‌ها در سرنگونی آلنده کمک کند. اسناد سیا نشان می‌دهد که وفاداری شیلی به ماشین‌های کریپتو کمک بزرگی به کودتای پینوشه بود. ۱۷ سال دیکتاتوری پس از آن، شامل دستگیری و شکنجۀ بیرحمانۀ مخالفان، کشته شدن بیش از ۳۰۰۰ و فرار بسیاری از شهروندان شیلی از این کشور، نتیجۀ دخالت آشکارا و فعال آمریکا بود.

[22] Anwar Sadat
[23] Billy Carter
[24] Salvador Allende

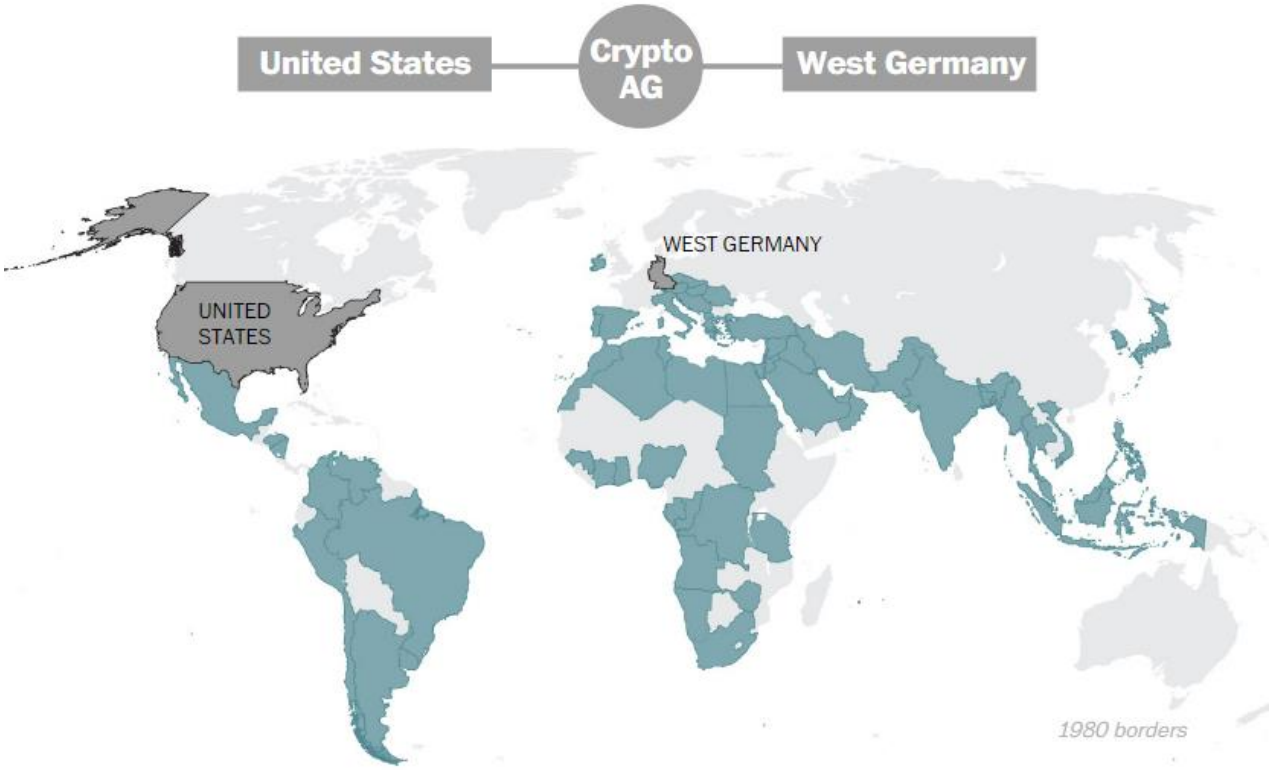
لیست مشتریان کریپتو در دهۀ ۸۰ میلادی، جالب توجّه است. در سال ۱۹۸۱، عربستان سعودی بزرگترین مشتری شرکت کریپتو بود و ایران، ایتالیا، اندونزی، عراق، لیبی ، اُردن و کرۀ جنوبی پس از آن قرار داشتند. برای حفظ مشتریان خود و بیرون راندن سایر شرکت‌ها از میدان رقابت، کریپتو و مالکین مخفی آن، انواع روش‌ها از جمله پرداخت رشوه به مقامات دولتی را اتخاذ می‌کردند. برای مثال طبق اسناد بدست‌آمده، کریپتو یکی از مدیران اجرایی خود را با ۱۰ عدد ساعت رولکس[۲۵] به ریاض فرستاد و بعداً از مقامات سعودی برای شرکت در یک برنامۀ آموزشی در سوئیس دعوت کرد که به نقل مستقیم، در آن «سرگرمی موردعلاقۀ مهمانان سعودی، بازدید از فاحشه‌خانه‌ها بود که هزینۀ آن نیز بر عهدۀ شرکت بود». در برخی موارد این مشوّق‌ها موجب خرید بی‌استفادۀ دولت‌ها می‌شد. برای مثال پس از دو سال که نیجریه محمولۀ بزرگی از محصولات شرکت را خریداری کرده بود؛ هیچ اطلاعاتی از ارتباطات آن در دست نبود. شرکت برای بررسی بیشتر، نمایندۀ فروش خود را به نیجریه اعزام کرد. طبق اسناد آلمان « او تجهیزات خریداری‌شده را در انبار پیدا کرد در حالی که هنوز بسته‌بندی آن‌ها باز نشده بود».

در سال ۱۹۸۲، دولت ریگان از اتکای آرژانتین به ماشین‌های کریپتو سوءاستفاده کرده و در جریان جنگ انگلستان و آرژانتین بر سر جزایر فالکلند، اطلاعات راهبردی آرژانتین را در اختیار انگلستان قرار می‌داده است. نخست‌وزیر وقت انگلستان مارگارت تاچر[۲۶]، با استفاده از اطلاعات رسیده از عملیات دستور به حمله به کشتی کروز آرژانتینی بلگرانو را صادر کرد. در این حمله ۳۰۰ نفر غرق شدند.

سال ۱۹۸۹ در حمله ایالات متحده به پاناما، حاکم وقت این کشور یعنی مانوئل نوریگا[۲۷] در سفارت‌خانۀ واتیکان در پاناما پنهان شده بود. آمریکا با رمزگشایی ارتباطات واتیکان که از محصولات کریپتو استفاده می‌کرد؛ سفارت واتیکان را محاصره و روز سوم ژانویۀ سال ۱۹۹۰ نوریگا را دستگیر کرد. نوریگا پس از دستگیری به جرم قاچاق مواد مخدر به ۴۰ سال حبس محکوم شد.

[25] Rolex
[26] Margaret Thatcher
[27] Manuel Noriega

طبق اسناد سازمان‌های CIA و BND، بیش از ۱۲۰ کشور دهه‌ها از تجهیزات شرکت کریپتو استفاده می‌کردند. از بین این ۱۲۰ کشور نام ۶۲ کشور به صورت صریح در اسناد سری این دو سازمان لیست شده است. همچنین طبق اسناد حداقل چهار کشورِ اسرائیل، سوئد، سوئیس و انگلستان، از عملیات مطّلع و حتّی از اطلاعات آن استفاده می‌کرده‌اند.



THE AMERICAS
Argentina
Brazil
Chile
Colombia
Honduras
Mexico
Nicaragua
Peru
Uruguay
Venezuela

EUROPE
Austria
Czechoslovakia
Greece
Hungary
Ireland
Italy
Portugal
Romania
Spain
Turkey
Vatican City
Yugoslavia

AFRICA
Algeria
Angola
Egypt
Gabon
Ghana
Guinea
Ivory Coast
Libya
Mauritius
Morocco
Nigeria
Rep. of the Congo
South Africa
Sudan
Tanzania
Tunisia
Zaire
Zimbabwe

MIDDLE EAST
Iran
Iraq
Jordan
Kuwait
Lebanon
Oman
Qatar
Saudi Arabia
Syria
U.A.E.

REST OF ASIA
Bangladesh
Burma
India
Indonesia
Japan
Malaysia
Pakistan
Philippines
South Korea
Thailand
Vietnam

معمّای جادوگر شهر اُز

یکی از مهم‌ترین دغدغه‌های CIA و BND این بود که کارمندان شرکت از آن چه پشت پرده اتفّاق می‌افتد باخبر نشوند. آن‌ها رویکرد هایلین در مدیریت شرکت را حفظ کرده و با پرداخت حقوق بالا و مزایایی شامل سرگرمی‌های لوکس مثل دسترسی به قایق بادبانی در دریاچهٔ زوگ نزدیک دفتر شرکت، سعی در راضی نگه داشتن کارمندان داشتند. با این وجود، بر شک کارمندانی که از نزدیک درگیر مسائل مرتبط با رمزنگاری بودند، روز به روز افزوده می‌شد. به علاوه الگوریتم‌هایی که از بیرون به ماشین‌ها قالب می‌شدند، توسط مهندسین و طراحانِ مسئولِ ساخت نمونه‌های اولیّه مورد سؤال قرار می‌گرفت.

مدیران اجرایی کریپتو اغلب طراحی الگوریتم‌های رمز را به عنوان بخشی از قرارداد مشاورهٔ زیمنس توجیه می‌کردند. ولی همچنان برای کارمندان شرکت سؤال بود که چرا برخی الگوریتم‌ها آسیب‌پذیری‌هایی دارند که به سادگی می‌توان از آن‌ها سوءاستفاده کرد و چرا نباید آن‌ها را وصله یا برطرف کنند؟

سال ۱۹۷۷، ناگهان ترافیک دیپلماتیک سوریه برای آژانس NSA غیرقابل خواندن شد و این آژانس به شرکت شکایت کرد. علّت این امر آن بود که مهندسی به نام پیتر فروتیگر[۲۸] که به همکاری کریپتو و سازمان اطلاعات آلمان شک داشت، پس از اعلام نارضایتی از تجهیزات از دمشق، چندین بار به سوریه سفر کرده و بدون اجازهٔ شرکت، آسیب‌پذیری تجهیزاتشان را رفع کرده بود. هاینز واینر[۲۹]، مدیر اجرایی کریپتو که از نقش سازمان‌های CIA و BND در این شرکت مطلّع بود؛ این مهندس خوش‌نام شرکت را اخراج کرد. طبق اسناد سیا: « فروتیگر از راز مینِروا[۳۰] آگاه شده بود و دیگر کار با او مطمئن نبود». فروتیگر از مصاحبه پیرامون این رسوایی اجتناب کرد.

مقامات آمریکا همچنین زمانی که واینر، مهندس برقی به نام منجیا کفلیش[۳۱] را استخدام کرد به وی هشدار دادند. کفلیش سال‌ها در ایالات متحده در دانشگاه مریلند تحقیقاتی در حوزهٔ سیگنال داشت و در سال ۱۹۷۸ به وطن خود سوئیس بازگشته بود. واینر هشدار مقامات NSA در مورد کفلیش، مبنی بر اینکه «او خیلی باهوش‌تر از آن است که بی‌اطلاع بمان» را نادیده گرفت و او را استخدام کرد(شکل زیر).

(S) Early the following year Wagner hired a bright new engineer, Dr. Mengia Caflisch -- again, without consulting the Partners. NSA quickly realized that she was too bright to remain unwitting, and frantically tried to cancel the hiring. Wagner was unmoved, and Caflisch stayed. But NSA had been right. She was too bright, and soon broke the new 500 cryptology through a known plain text attack. She went on to expose the cryptographic weaknesses of other CAG products, and proceeded to design her own, unbreakable, cryptologics. Her technical brilliance attracted a following among several CAG engineers.

[28] Peter Frutiger
[29] Heinz Wagner

[۳۰] نام عملیاتی کریپتو

[31] Mengia Caflisch

هشدارها درست بودند و کفلیش خیلی زود شروع به ارزیابی آسیب‌پذیری محصولات شرکت کرد. او و یکی از همکارانش به نام اشپوردلی[۳۲] در دپارتمان تحقیقات چندین تست و حمله از نوع متنِ آشکار[۳۳] بر دستگاه‌های مدل HC-570 اعمال کردند. اشپوردلی در مصاحبه‌ای گفته بود که تنها با مقایسهٔ ۱۰۰ کاراکتر متن پیام اصلی و پیام رمز، توانستند کد را بشکنند که یعنی امنیت دستگاه‌ها بسیار پائین بود.

کفلیش شروع به حل مشکل کرد. او الگوریتمی بسیار قوی طراحی کرد و آن را بدون اجازهٔ شرکت، روی ۵۰ دستگاهِ مدل HC-740 پیاده‌سازی کرد. مقامات NSA که آگاه شدند به شدّت نگران بودند که خروجی الگوریتم کفلیش قابل خواندن نباشد. شرکت پس از شکایت NSA و اطلاع از ماجرا به کفلیش اخطار داد که «آزاد نیست هر کاری که می‌خواهد انجام دهد». کفلیش که در آن زمان بسیار مشکوک شده بود در مصاحبه‌ای در ژانویهٔ ۲۰۲۰ با واشنگتن‌پست گفت:«من فقط با خودم فکر می‌کردم که بعضی چیزها در شرکت خیلی عجیب هستند».

به مرور زمان ظن کفلیش به سایر کارمندان سرایت کرد. آن‌ها می‌پنداشتند که فناوری شرکت در اختیار دولت آلمان است و از مالکیت ایالات متحده بی‌خبر بودند. شرکت کریپتو شبیه به سرزمین اُز شده بود و کارمندان به دنبال پیدا کردن جادوگری بودند که دانش بسیاری در زمینهٔ رمزنگاری داشت و تمام دستگاه‌ها را با جادوی خود آسیب‌پذیر کرده بود.

مقامات سازمان‌های CIA و BND در تلاش برای مخفی کردن ردپای خود، درصدد معرفی آژانس اطلاعاتی دوستانشان به عنوان پوشش برای فعالیت‌هایشان بودند. از بین کشورهای کاندید، سوئد با توجّه به پیشینهٔ هایلین، انتخاب شد. خلِ-اُف ویدمَن استاد ریاضیات در استکهلم سوئد، در اروپا در زمینهٔ رمز به شهرت رسیده بود و سابقهٔ خدمت نظامی و همکاری با مقامات اطلاعاتی سوئد را نیز داشت. به علاوه او به ایالات متحده به واسطهٔ تحصیل در ایالت واشنگتن، تعلّق خاطر داشت. از آن جا که تلفظ نام او برای دوستان آمریکایی‌اش مشکل بود؛ او را هِنری(نامی که برای همیشه با او ماند) صدا می‌کردند. البته نام عملیاتی او آتِن یاد بود. (شکل زیر).

(S) Unable to pronounce his name, his American friends called him Henry. Widman carried this name with him for the rest of his life, and was known informally to MINERVA teammates as Henry. His cryptonym became ATHENA, the goddess of wisdom (and war).

ویدمَن به عنوان «مشاور علمی» در شرکت استخدام شد و مستقیماً به واینر گزارش می‌داد. او هر ۶ هفته یک‌بار زوگ را برای شرکت در جلساتی با CIA و BND ترک می‌کرد. آن‌ها موافقت کردند که برای اصلاح وجههٔ شرکت الگوریتم‌ها و روش‌های رمزنگاری را تغییر دهند. ویدمن طرح دلخواه این دو سازمان را به مهندسین تحویل می‌داد و هر بار نقص و آسیب‌پذیری‌ها را به گونه‌ای توجیه می‌کرد. در اسناد سیا آمده است که او «فرد غیرقابل‌جایگزین» و «مهم‌ترین استخدام در تاریخ مینروا» بوده است. عقبهٔ فنی او، مانع از آن بود که کارمندان شرکت او را به چالش کشند. به علاوه ظن کشورها(در صورت وجود شک) بیشتر به سوئد می‌رفت. از طرفی طراحان الگوریتم‌های رمز در NSA رویکرد خود را تغییر داده از روش‌های رمزنگاریی استفاده می‌کردند

[32] Spoerndli

[۳۳] حملهٔ متن آشکار حمله‌ای است که در آن مهاجم پیام اصلی و رمزشدهٔ آن را دارد و با مقایسهٔ آن‌ها می‌تواند الگوهای رمزنگاری را شناسایی کرده نهایتاً کلید الگوریتم را بدست آورد.

که «با تست‌های معمول آماری قابل شکستن نباشند» و حتّی اگر به احتمال ناچیز شکسته شدند توجیه «اشتباه در پیاده‌سازی و یا خطای انسانی» باشد.

چنانچه گفته شد در سال ۱۹۸۲، ارتباطات آرژانتین رمزگشایی و پیام‌های محرمانه‌شان برای انگلستان ارسال می‌شد. ظن آرژانتین به شدّت به تجهیزات کریپتو بود. برای توجیه و آرام کردن اوضاع، ویدمن به بوینس‌آیرس اعزام شد و به آن‌ها توضیح داد که اشکال از دستگاه ازرده‌خارج‌شده‌ای بوده است. دستگاهی که در زمان جنگ آرژانتین استفاده و NSA توانسته به آن نفوذ کند. او در ادامه مقامات آرژانتین را متقاعد کرد که سایر دستگاه‌هایی که آرژانتین از کریپتو خریداری کرده است شامل CAG 500 «غیرقابل‌نفوذ» هستند. طبق اسناد سیا(شکل زیر) لاف ویدمن عمل کرد و آرژانتین به خرید از کریپتو ادامه داد.

(S) When faced with customer revolt, he would get on a plane, sometimes alone, sometimes with Wagner, and fly off to confront the customer. This tactic led to several trips to Latin America to calm the waters. Chile continued to complain about weak CAG cryptologics, and Henry was afraid that the Chilean navy was just inches away from breaking its own 503 machine. When the Chileans threatened to buy Datotek equipment, Henry assured them that Datotek could not get an export license. (Since Chuck Kinney was himself the approving authority, Henry was on solid ground.) Instead, Henry assured the suspicious Chileans that he would provide a more secure cryptologic just for them. Chile was thus saved as a CAG customer.

(S) After the Falkland Islands War, the Argentines discovered that the British and Americans had broken their systems. The furious Argentines summoned Henry to Buenos Aires to explain. The matter was not simple, said Henry, but it appeared that NSA had broken an analog speech system -- these systems were notoriously weak, he said, but the CAG 500 systems were unbreakable. The bluff worked. The Argentines swallowed hard, but kept buying CAG equipment.

ویدمَن اکنون مدت‌ها است که بازنشسته شده و در استکهلم زندگی می‌کند. اگر چه او از اظهار نظر در ارتباط با رسوایی اخیر اجتناب کرده است؛ سال‌ها پس از استخدامش به یکی از مقامات آمریکایی گفته بود: « احساس می‌کند درگیر عملیاتی حساس به نفع سرویس‌های اطلاعاتی غربی است» و این که:

« این مأموریتِ او در زندگی بوده است».

(S) Rick Schroeder was then introduced in his true CIA colors, and they talked awhile longer. Henry said he was willing, and they shook hands. When they entered the garden where the luncheon was in progress, it was thumbs up. There was much congratulating and Gemutlichkeit. The luncheon became an event.

(S) Years later, Henry recalled the lunch. He felt that he had been welcomed into a secret society, and had learned the secret handshake. These people had become colleagues engaged in a critical struggle for the benefit of Western intelligence. These were people he could work with. It was, he said, the moment in which he felt at home. This was his mission in life.

ظن ایران به عملیات

اظهار نظر ریگان در سال ۱۹۸۶ در جریان بمب‌گذاری یک دیسکو در برلین غربی (که بین نیروهای آمریکایی محبوب بود)، عملیات روبیکان را به خطر انداخت. در این بمب‌گذاری دو سرباز آمریکایی و یک زن از ترکیه کشته شده بودند. ده روز پس از بمب‌گذاری، ریگان رئیس‌جمهور ایالات متحده با بیان اینکه شواهدی «مستقیم، دقیق و غیرقابل‌انکار» از دست داشتن لیبی در بمب‌گذاری وجود دارد؛ دستور به حملات تلافی‌جویانه علیه لیبی داد. در این حملات یکی از دختران قذافی نیز کشته شد. مدارکی که ریگان به آن‌ها اشاره کرده بود شامل دستور حمله از لیبی به سفارت خود در شرق برلین، یک هفته قبل از حمله و سپس گزارش بمب‌گذاری یک روز پس از آن است. طبق اسناد سیا: « آن‌ها به طرابلس گزارش کردند که مأموریت با موفقیّت انجام شد».

سخنان بی‌پروای ریگان برای لیبی روشن ساخت که ارتباطات طرابلس و سفارت‌خانه شنود و رمزگشایی شده است. امّا لیبی تنها کشوری نبود که سرنخ‌هایی که ریگان فراهم کرده بود را مورد توجّه قرار داد. ایران که می‌دانست لیبی هم از تجهیزات کریپتو در ارتباطات محرمانهٔ خود استفاده می‌کند؛ به شدّت نگران ارتباطات خود شد ولی تا شش سال ظن خود را مخفی کرد.

در سال ۱۹۹۲ ایران مطابق با ظن خود به شرکت کریپتو، یکی از فروشندگان شرکت را بازداشت کرد. هانس بوئلر[۳۴]، یکی از بهترین فروشندگان شرکت بود. از آن جا که ایران از مهم‌ترین کشورهای طرف قرارداد کریپتو بود؛ بوئلر مرتباً به ایران سفر می‌کرد.

سال ۱۹۹۲، شش سال پس از ماجرای بمب‌گذاری دیسکوی برلین و حملات موشکی آمریکا به لیبی در سال ۱۹۸۶، بوئلر بازداشت و توسط مقامات ایرانی بازجویی شد. مقامات وقت کنسولگری سوئیس اجازه داشتند تا او را ملاقات کنند. طبق گزارشات او در «شرایط بد روحی» قرار داشت. نُه ماه بعد، در ازای یک میلیون دلار که توسط سازمان BND(شکل زیر) فراهم شده بود؛ بوئلر آزاد شد. سازمان سیا از این که سهم خود را بپردازد سر باز زد چرا که آن را باج به ایران می‌دانست.

[34] Hans Buehler

(S) The next day Munich was informed that the White House had rejected the "bail" sophistry. It was clearly "ransom," and could not be paid. BND President Konrad Porzner was to be informed that no American money was to be used to secure Buehler's release.

(S) When informed of the American stance, Porzner decided that if necessary Germany would proceed alone, and pay the entire $1 million. Perhaps the Americans could be talked into paying their share later, but even if they could not, this was too important a matter to let a peculiarly American prohibition stop the release of Buehler. Germany was under no such prohibition, and would do what it believed was necessary.

بوئلر که به نظر می‌رسید چیزی راجع به روابط کریپتو و سازمان‌های CIA و BND و آسیب‌پذیری‌های دستگاه‌های شرکت، نمی‌دانست با شک به جایی که برای آن کار می‌کرد به سوئیس بازگشت. او با سازمان‌های خبری سوئیس چندین مصاحبه کرده و در مورد ظن و گمان خود به شرکت کریپتو سخن گفت.

در آن زمان، نظرها دوباره به سرنخ‌های ازیادرفتهٔ «پروژهٔ بوریس» جلب شد. این سرنخ‌ها از مجموعهٔ اسناد و اطلاعات فریدمن بدست آمده بود که پس از مرگ او در سال ۱۹۶۹ به موسسهٔ نظامی ویرجینیا اهدا شده بود. این اسناد که ۷۲ جعبه از کپی مکاتبات او و هایلین بود؛ اوضاع کریپتو را بحرانی کرد.

در سال ۱۹۹۴ بحران کریپتو جدی‌تر شد. زمانی که بوئلر در تلویزیون سوئیس حاضر و گزارشی ارائه کرد که به داستان فروتیگر- مهندسی که به دلیل تعمیر و اصلاح سیستم‌های رمز سوریه، اخراج شده بود- اشاره کرد. هر چند فروتیگر سخنان او را تأیید یا رد نکرد. برای فرو نشاندن حرف و حدیث‌ها، میشل گروپ[۳۵] از مدیران اجرایی شرکت در یک برنامهٔ تلویزیونی حاضر و سخنان بوئلر را رد کرد. اسناد سیا(شکل زیر) نشان می‌دهد که لفاظی‌ها و توجیهات گروپ، «عملیات را نجات داد».

(S) Grupe appeared on camera, interviewed by a Swiss journalist. He bluntly denied the allegations, terming them warmed-over claims by disgruntled employees. Buehler was fired because company management had lost trust, and because he refused to turn over his lawyer's files to the firm. He dismissed as "insanity" the allegations that the Germans were manipulating the gear. CAG sold in Germany, he pointed out, and in Switzerland, which had given the company a "clean bill of health." The whole thing was utter nonsense. As to allegations that foreign intelligence organizations were known to visit CAG, of course they had. They were customers, and good ones. They trusted the security of CAG gear.

(S) Grupe's appearance cast enough doubt on Buehler's allegations to blur the issue. Langley hoped that viewers would come away at least a little confused about charges that had seemed so clear in pre-program and pre-book publicity. Grupe's performance was credible, and may have saved the program.

با این وجود بحران ادامه داشت چرا که در سال ۱۹۹۵، مجموعه‌ای از مدارک پیرامون ارتباط آژانس NSA و کریپتو منتشر شد. این اسناد، سفر مقامات NSA به زوگ اواسط دههٔ ۱۹۷۰ برای ملاقات‌های سرّی با مسئولین کریپتو را نشان می‌داد.

[35] Michael Grupe

عمومی‌سازی این اطلاعات و اسناد باعث شد که برخی از کارمندان شرکت به دنبال جای دیگری برای کار باشند. همچنین چندین کشور، شامل آرژانتین، ایتالیا، عربستان سعودی، مصر و اندونزی قرارداد خود با کریپتو را لغو کردند.
جالب آن که ایران همچنان به کار با این شرکت ادامه داد(شکل زیر)!

(S) For customers, the Buehler affair came as a shock. The Argentine Navy threatened to buy everything from other suppliers, and a government decision to make a major purchase from CAG was immediately placed under review. The Italians, always a little skittish about CAG products, seemed likely to fly out of the CAG orbit. The Saudis, the single biggest customers, halted orders pending clarification. The CAG salesman in Indonesia was having trouble defending CAG products, and appeared to have his own suspicions. Egypt began peppering the company with questions about crypto security. One of the few countries that showed little reservation was Iran. It resumed its purchase of CAG equipment almost immediately.

این در حالی است که اسناد آژانس‌های جاسوسی ایالات متحده نشان می‌دهند که اطلاعات بسیار زیادی از ارتباطات ایران، از طریق ماشین‌های کریپتو داده‌کاوی و رمزگشایی می‌شدند. برای مثال در زمان جنگ هشت‌سالهٔ ایران و عراق، بالغ بر ۱۹۰۰۰ ارتباط ایران از طریق تجهیزات کریپتو شنود شده است. طبق اسناد سازمان سیا(شکل زیر)،

---

۸۰ تا ۹۰ درصد ارتباطات ایران، قابل خواندن بوده است.

(TS) The most lucrative target using influenced crypto was Iran. The Iranian target was 80-90 percent readable, thanks to the Iranian penchant for buying from MINERVA. In 1988, over 19,000 Iranian decrypts were turned into product reports, covering everything from hostage issues to the Iranian conflicts with other Gulf States.

جدایی آلمان از عملیات

سال‌ها مقامات BND و همتایان آمریکایی خود بر سر فروش تجهیزاتِ دارای آسیب‌پذیری به کشورهای متحّد و دوست، بحث و مجادله داشتند. بحث بر سر این بود که کدام کشورها، شایستگی دریافت نسخه‌های اَمن را دارند و از نظر ایالات متحده، هیچ کس(چه دوست و چه دشمن) این شایستگی را نداشت. نظر آمریکا این بود: « در دنیای اطلاعات، هیچ دوستی وجود ندارد».

جنگ سرد به پایان رسید و دیوار برلین فروریخت و آلمان یکی شد. ظن ایرانیان و ماجرای بوئلر زنگ خطر را برای آلمان یکپارچه به صدا درآورد. آن‌ها به این فکر می‌کردند که اگر بحران کریپتو ادامه یافته و رسوایی به بار آورد؛ چه پیامدهای سیاسی و اقتصادی در سطح اروپا خواهد داشت. در سپتامبر سال ۱۹۹۳ آلمان با فروش سهم خود به ارزش ۱۷ میلیون دلار به آمریکا، عملیات را ترک کرد.

با جدایی آلمان از عملیات، مقامات اطلاعاتی دیگر دسترسی به منابع پشت پرده نداشتند و نگران بودند که آیا هنوز «جزء معدود کشورهایی که اطلاعاتشان توسط آمریکا خوانده نمی‌شود»، هستند؟! مدارک منتشرشده توسط ادوارد اسنودِن نشان داد که جواب سوال آن‌ها منفی است و سال‌ها اطلاعات مقامات آلمان از جمله تلفن صدراعظم آلمان آنجلا مرکل شنود شده است. به این ترتیب مقامات اطلاعاتی آلمان، سیاست‌مداران این کشور را به دلیل جدایی زودهنگام از عملیات سرزنش می‌کردند.

ثبت رویدادها در سند تاریخچهٔ سیا پیرامون عملیات روبیکان، با رفتن آلمان خاتمه یافته و در سال ۲۰۰۴ تمام شد. هر چند عملیات همچنان ادامه داشت. در این اسناد آمده است که دستگیری بوئلر « جدی‌ترین نقض امنیت تاریخ برنامه» بود ولی با این وجود « در پایان قرن بیستم، مینِروا[۳۶] همچنان زنده و سرحال است».

(S) The HYDRA affair was the most serious security breach in the history of the program, and its aftershocks continued to rumble through the end of the decade. But it did not cause its demise, and at the turn of the century MINERVA was still alive and well. It was a very narrow escape.

[۳۶] نام عملیاتی شرکت کریپتو

پایان عملیات

پس از سال‌ها، روزهای سوددهی کریپتو رو به افول بود. با افزایش ظن و گمان‌ها و پس از کاهش تعداد مشتریان، خط تولید و درآمد شرکت کاهش یافت. با این همه به دلیل اهمال برخی دولت‌ها(اکثراً از کشورهای کمتر توسعه‌یافته) در تغییر دستگاه‌های کریپتو، اطلاعات همچنان به سازمان‌های اطلاعاتی ایالات متحده جریان داشت.

با رفتن BND از عملیات، سازمان سیا کمپانی‌های حوزهٔ رمزنگاری خود را با استفاده از سود حاصل از کریپتو، توسعه داد. طبق اسناد، سیا دو شرکت دیگر حوزهٔ رمز را از آن خود کرد. متأسفانه اطلاعاتی پیرامون این شرکت‌ها در اختیار نیست. البته سند BND به خرید رقیب دیرینهٔ کریپتو یعنی شرکت گرتاگ[۳۷] واقع در سوئیس توسط یک آمریکایی اشاره دارد. شرکتی که در سال ۲۰۰۴ پس از تغییر نام منحل شد.

به تدریج شرکت کریپتو که روزی از جعبه‌های آهنی به مدارهای الکترونیکی و از ماشین‌های تله‌تایپ به سیستم‌های صوتی رمز، اُروج کرده بود؛ در انقلاب صنعت رمز از سخت‌افزار به نرم‌افزار، زمین خورد. به نظر می‌رسد که مقامات اطلاعاتی آمریکا به کریپتو اجازهٔ مرخص شدن دادند و در عوض سرمایه‌شان را به راه‌حل‌های جدید مثل گوگل، مایکروسافت، وریزون و سایر غول‌های صنعت فناوری اطلاعات معطوف کرده‌اند.

سال ۲۰۱۷ مقر همیشگی کریپتو در شهر زوگ و سال ۲۰۱۸ تمامی مایملک آن به فروش رفت. تنها مشتری شرکت CyOne که امتیاز تجارت کریپتو را خریده بود؛ دولت سوئیس است. کشوری که در زمان عملیات نیز، تجهیزات امن کریپتو به آن می‌رسید.

[37] Gretag AG