IL “COLPO DEL SECOLO” A PROPOSITO DI SPIONAGGIO

Greg Miller
***The Washington Post*, 11 febbraio 2020**
trad. it. di David Arboit

Per più di mezzo secolo, i governi di quasi tutto il mondo si sono affidati a una unica azienda per gestire le comunicazioni segrete delle proprie spie, dei militari e dei diplomatici.
La società, la Crypto AG, ottenne la prima opportunità grazie a un contratto per la costruzione di macchine per la produzione di codici di criptazione per le truppe statunitensi durante la seconda guerra mondiale. Rapidamente ebbe un sacco di commesse, divenne il produttore leader nei dispositivi di crittografia per decenni, riuscendo a restare sulla cresta dell’onda durante le successive fasi di sviluppo della tecnologia, dagli ingranaggi meccanici ai circuiti elettronici e, infine, ai chip e al software al silicio.
La società svizzera ha guadagnato milioni di dollari vendendo attrezzature in oltre 120 paesi fino al XXI secolo. Tra i suoi clienti c’erano [oltre all’Italia] l’Iran, le Giunte militari in America Latina, India e Pakistan, due Stati avversari nel settore nucleare, e persino il Vaticano.
Ma nessuno dei suoi clienti ha mai saputo che Crypto AG era segretamente proprietà della CIA con una partnership top secret con i servizi segreti della Germania occidentale [BND]. Queste due agenzie di spionaggio hanno truccato i dispositivi prodotti dall’azienda in modo da poter facilmente violare i codici utilizzati dai paesi per inviare messaggi segreti crittografati.
L’accordo decennale, uno dei segreti più nascosti e custoditi della Guerra fredda, è statao rivelato in un rapporto CIA completo e segreto che narra l’operazione, rapporto ottenuto dal quotidiano *The Washington Post* e da ZDF, una emittente tedesca, che hanno realizzato un reportage congiunto.
Il rapporto identifica gli ufficiali della CIA che hanno avviato il programma e i dirigenti dell’azienda incaricati di eseguirlo. Traccia l’origine dell’azienda nonché i conflitti interni che quasi l’hanno fatta deragliare. Descrive come gli Stati Uniti e i suoi alleati hanno sfruttato l’ingenuità di altre nazioni per anni, prendendo i loro soldi e rubando i loro segreti. L’operazione, conosciuta prima con il nome in codice “Thesaurus” e successivamente “Rubicon”, è tra le più audaci nella storia della CIA.
“Fu il colpo spionistico del secolo” conclude il documento CIA che racconta l’operazione. “I governi stranieri – si legge nel documento – stavano pagando dei bei soldi agli Stati Uniti e alla Germania occidentale per avere il privilegio di far leggere le loro comunicazioni segrete ad almeno due (e forse fino a cinque o sei [probabilmente i Five Eyes + Israele]) paesi stranieri”.
Dal 1970 in poi, la CIA e il suo fratello craccatore di codici, la National Security Agency [NSA], hanno messo sotto stretta sorveglianza ogni aspetto delle operazioni Crypto gestendo con i loro partner tedeschi l’assunzione di decisioni, progettando la tecnologia, sabotando i suoi algoritmi e gestendo i suoi obiettivi commerciali. Poi le spie degli Stati Uniti e della Germania occidentale si sedevano e ascoltavano.
Hanno tenuto sotto controllo i mullah iraniani durante la crisi degli ostaggi del 1979, hanno fornito informazioni sull’esercito argentino alla Gran Bretagna durante la guerra delle Falkland, hanno seguito i dittatori sudamericani durante le loro azioni di sterminio degli oppositori e hanno ascoltato i funzionari libici congratularsi con sé stessi per l’attentato del 1986 a una discoteca di Berlino.
Il programma aveva però dei limiti. I principali avversari dell’America, inclusi l’Unione Sovietica e la Cina, non furono mai clienti Crypto. Sospettando i legami della società con l’Occidente, russi e cinesi si sono protetti, anche se il documento CIA che narra l’operazione ci insegna che le spie statunitensi hanno imparato molto lo stesso su russi e cinesi tenendo sotto controllo le comunicazioni di Mosca e Pechino con i Paesi che erano clienti Crypto.

Ci sono state anche fughe di notizie che hanno messo Crypto nella condizione di essere circondata da un alone di sospetto. I documenti prodotti negli anni '70 mostrano una fitta corrispondenza sospetta tra un pioniere della NSA e il fondatore di Crypto.
A volte gli obiettivi stranieri spiati sono stati informati a proposito del loro essere target da dichiarazioni rilasciate sbadatamente da funzionari pubblici, incluso il presidente Ronald Reagan.
L'arresto nel 1992 di un venditore Crypto in Iran, che non sapeva di vendere attrezzature truccate, scatenò una devastante campagna pubblica sulla questione. Ma la vera portata del rapporto della Crypto con la CIA, e con la sua controparte tedesca, non è stata fino ad oggi mai rivelata.
Quando i servizi segreti tedeschi, la BND, cominciarono a pensare che il rischio di essere smascherati fosse ormai troppo grande, lasciarono l'operazione nei primi anni '90. La CIA ha allora acquistato la partecipazione tedesca nell'azienda e ha semplicemente continuato, utilizzando per sé la Crypto con tutta la sua capacità di spionaggio fino al 2018, quando l'Agenzia ha venduto le partecipazioni della società. L'importanza dell'azienda per il mercato globale della sicurezza era ormai diminuita, superata dalla diffusione della tecnologia di crittografia dell'online. Un tempo specialità dei governi e delle grandi società, la crittografia avanzata è ora onnipresente, come le app, sui telefoni cellulari.
Anche se ormai conclusa, l'operazione Crypto è importante per lo spionaggio moderno. La sua portata e la sua durata aiutano a spiegare come gli Stati Uniti abbiano sviluppato un appetito insaziabile per la sorveglianza globale, cosa che è stata rivelata e confermata nel 2013 da Edward Snowden.
Ci sono anche echi della vicenda Crypto nei sospetti che oggi circondano continuamente le aziende moderne che hanno presunti collegamenti con i governi stranieri, tra cui la società russa antivirus Kaspersky, un'app di messaggistica legata agli Emirati Arabi Uniti e al colosso cinese delle telecomunicazioni Huawei.
Questa storia si basa su quanto narrato in un documento CIA che racconta l'operazione, e in un resoconto parallelo del BND, anch'esso ottenuto dal *Post* e da ZDF, e su interviste fatte a funzionari dell'intelligence occidentale attuale e passata, nonché con i dipendenti Crypto. Molti hanno parlato in condizione di anonimato perché si tratta di un tema sensibile.
La straordinarietà di questi racconti della CIA e del BND non è stata certamente sopravvalutata.
I file sensibili dei servizi segreti vengono periodicamente declassificati e pubblicati. Ma accade raramente, o forse è un evento senza precedenti, di avere la possibilità di dare un'occhiata ai resoconti interni di un'intera operazione segreta. Il *Post* ha potuto leggere tutti i documenti, ma la fonte ha insistito affinché fossero pubblicati solo degli estratti.
La CIA e il BND hanno rifiutato di commentare, sebbene i funzionari statunitensi e tedeschi non abbiano contestato l'autenticità dei documenti.
Il primo è un resoconto di 96 pagine sull'operazione completato nel 2004 dal Centro per lo Studio dell'Intelligence della CIA, un ramo storico interno dell'Agenzia. Il secondo è una testimonianza orale compilata da funzionari dell'intelligence tedesca nel 2008.
Comparando i resoconti si evidenziano attriti tra i due partner a proposito del denaro, del controllo e dei limiti etici, con i tedeschi occidentali spesso stupiti dall'entusiasmo con cui le spie statunitensi spesso prendevano di mira i loro alleati.
Entrambe le parti descrivono l'operazione come riuscita al di là delle loro più ottimistiche previsioni. A volte, anche negli anni '80, la Crypto gestiva circa il 40 percento delle comunicazioni diplomatiche e di altre trasmissioni riservate di governi stranieri, comunicazioni che i crittografi dell'NSA decodificavano regolarmente e da cui estraevano informazioni.
Nello stesso tempo, Crypto ha generato milioni di dollari di profitti che la CIA e il BND hanno diviso e investito in altre operazioni.
I prodotti di Crypto sono ancora in uso in oltre una dozzina di Paesi in tutto il mondo e il suo simbolo bianco e arancione si trova ancora in cima al vecchio quartier generale dell'azienda vicino a Zugo, Svizzera. Ma la società è stata smembrata nel 2018, liquidata da azionisti le cui identità

sono state permanentemente protette dalle leggi bizantine del Liechtenstein, una piccola nazione europea che ha una reputazione simile alle Isole Cayman per quanto riguarda il segreto bancario.
Due società hanno acquistato la maggior parte degli asset di Crypto. La prima, CyOne Security, è stata creato da manager che hanno rilevato una parte delle quote di Crypto e ora vende i sistemi di sicurezza esclusivamente al governo svizzero. L'altra, la Crypto International, ha rilevato il marchio e gli affari internazionali della società precedente.
Ciascuna delle due società ha insistito sul fatto che non ha alcuna connessione in corso con i servizi di intelligence, ma solo una ha affermato di non essere a conoscenza del fatto che l'azienda fosse di proprietà della CIA. Le dichiarazioni erano in risposta alle domande di *Post*, ZDF e dell'emittente svizzera SRF, che ha avuto anch'essa accesso ai documenti.
La società CyOne Security ha collegamenti più sostanziali con l'ormai ex società Crypto AG, incluso il fatto che l'amministratore delegato della nuova società ha ricoperto la stessa posizione in Crypto per quasi due decenni durante il periodo proprietà della CIA. Il portavoce di CyOne ha rifiutato di fare dichiarazioni su qualsiasi aspetto della storia di Crypto AG, ma ha affermato che la nuova società "non ha legami con alcun servizio di intelligence straniero".
Andreas Linde, il presidente dell'azienda che ora detiene i diritti sui prodotti e sulle attività internazionali di Crypto, ha dichiarato che non era a conoscenza del rapporto della società con la CIA e il BND prima di avere letto questo articolo. "Noi di Crypto International non abbiamo mai avuto rapporti con la CIA o BND, e per favore scrivilo – ha detto in un'intervista. "Se quello che stai dicendo è vero, allora mi sento tradito e la mia famiglia si sente tradita, e sento che ci saranno molti dipendenti e clienti che si sentiranno traditi."
Martedì il governo svizzero ha annunciato che avrebbe avviato un'indagine sui legami di Crypto AG con la CIA e il BND. All'inizio di questo mese, i funzionari svizzeri hanno revocato la licenza di esportazione a Crypto International.
Il tempismo della iniziativa svizzera risulta curioso. I documenti della CIA e del BND indicano che i funzionari svizzeri devono aver saputo per decenni dei legami di Crypto con i servizi di spionaggio statunitensi e tedeschi, ma gli svizzeri sono intervenuti solo dopo aver appreso che i giornalisti stavano per pubblicare la notizia dell'accordo.
Le ricostruzioni storiche, non affrontano il punto del se e quando la CIA ha messo fine al suo coinvolgimento, perché i documenti scritti contengono le inevitabili manipolazioni prodotte dal punto di vista di chi ha architettato l'operazione. Descrivono infatti l'operazione Rubicon come un trionfo dello spionaggio, che ha aiutato gli Stati Uniti a prevalere nella Guerra Fredda, a tenere sotto controllo dozzine di regimi autoritari e a proteggere gli interessi degli Stati Uniti e dei suoi alleati.
I documenti in gran parte evitano di affrontare le questioni più inquietanti, tra cui ciò che gli Stati Uniti sapevano – e che cosa hanno fatto oppure non hanno fatto – nei paesi che usavano le macchine Crypto ed erano impegnati a organizzare omicidi, campagne di pulizia etnica e violazioni dei diritti umani.
Le rivelazioni contenute nei documenti possono fornire ragioni per rivedere il comportamento degli Stati Uniti in alcune questioni internazionali, per valutare se fossero in grado di intervenire, o almeno di informare sulle atrocità commesse in alcuni Paesi esteri, e se a volte hanno scelto di non fare nulla per preservare il segreto del accesso a preziose fonti di intelligence.
I documenti, inoltre, non trattano gli ovvi problemi etici che sono al centro dell'operazione: per esempio l'aver ingannato e sfruttato avversari, alleati e centinaia di dipendenti Crypto che non sapevano nulla della operazione. Molti dipendenti hanno viaggiato in tutto il mondo vendendo o facendo assistenza ai sistemi truccati senza avere la minima idea del fatto che lo facevano mettendo a rischio la propria personale sicurezza.
Nelle recenti interviste, i dipendenti ingannati – anche quelli che avevano cominciato a sospettare durante la loro permanenza presso Crypto che la società stesse collaborando con i servizi segreti occidentali – hanno affermato che le rivelazioni nei documenti hanno acuito la sensazione di essere stati traditi sia loro sia i loro clienti. "Pensi di fare un buon lavoro e di rendere sicuro qualcosa", ha

detto Juerg Spoerndli, un ingegnere elettrico che ha trascorso 16 anni in Crypto. “E poi ti rendi conto di aver imbrogliato i tuoi clienti.”
Chi gestiva il programma clandestino non è pentito e non è per niente dispiaciuto. “Ho qualche scrupolo? Zero!”, ha dichiarato Bobby Ray Inman, che è stato direttore della NSA e vicedirettore della CIA alla fine degli anni '70 e all’inizio degli anni '80. “Era una fonte di informazioni molto preziosa su regioni del mondo significativamente importanti, importanti per i politici statunitensi”.

Una operazione di interdizione
Questa sofisticata e tentacolare operazione è nata perché i militari statunitensi avevano bisogno di disporre di un dispositivo di crittografia semplice ma compatto.
Boris Hagelin, il fondatore di Crypto, era un imprenditore e inventore nato in Russia e fuggito in Svezia quando i bolscevichi presero il potere. Fuggì poi di nuovo negli Stati Uniti quando i nazisti occuparono la Norvegia nel 1940. Portava con sé una macchina da crittografia che sembrava un grosso carillon, con una robusta manovella sul lato e un gruppo di ingranaggi e rotelle di metallo, in una custodia di metallo duro.
Non era un sistema elaborato, o sicuro, come le macchine Enigma utilizzate dai nazisti. Ma l’M-209 di Hagelin, nome con cui divenne noto, era portatile, azionato a mano e perfetto per le truppe in movimento. Le foto mostrano i soldati con le scatole da otto libbre – aveva le dimensioni di un grosso libro – legato alle loro ginocchia. Molti dei dispositivi di Hagelin sono stati conservati in un museo privato a Eindhoven, nei Paesi Bassi.
L’invio di un messaggio sicuro con il dispositivo era faccenda lunga e noiosa. L’utente ruotava un quadrante, lettera per lettera, e spingeva verso il basso la manovella. Gli ingranaggi nascosti giravano e sputavano un messaggio cifrato su una striscia di carta. Un ufficiale di segnalazione doveva quindi trasmettere quel messaggio criptato con il codice Morse a un destinatario che avrebbe invertito la sequenza.
La sicurezza di questo sistema era così debole che si presumeva che quasi tutti i nemici avrebbero potuto decifrare il codice impiegando un po’ di tempo. Ma ci volevano ore. E poiché la macchina era usata principalmente per messaggi tattici sui movimenti delle truppe in battaglia, quando i nazisti riuscivano a decodificare una comunicazione questa non aveva più alcun valore.
Nel corso della guerra, circa 140.000 macchine M-209 furono costruite nella fabbrica di macchine da scrivere Smith Corona a Syracuse, New York, con un contratto dell’esercito degli Stati Uniti del valore di 8,6 milioni di dollari affidato a Crypto. Dopo la guerra, Hagelin tornò in Svezia per riaprire la sua fabbrica, portando con sé una fortuna personale e un senso di lealtà permanente nei confronti degli Stati Uniti.
Fu così che le spie americane tennero d’occhio le sue iniziative nel dopoguerra. All’inizio degli anni '50, sviluppò una versione più avanzata della macchina dell’epoca della guerra, con una nuova sequenza “irregolare” meccanica che mise fuori strada per un breve periodo gli specialisti di decriptazione americani. Allarmati dalle capacità del nuovo CX-52 e di altri dispositivi concepiti da Crypto, i funzionari statunitensi iniziarono a discutere di quello che chiamavano il “problema Hagelin”.
Questo fu “il periodo nero” della crittografia americana, secondo il documento CIA che racconta l’operazione. I sovietici, i cinesi e i nordcoreani stavano usando sistemi di codifica quasi impenetrabili. Le agenzie di spionaggio statunitensi erano preoccupate che anche il resto del mondo diventasse oscuro e impenetrabile se i paesi avessero potuto acquistare le macchine sicure da Hagelin.
Ma gli americani con Hagelin potevano far leva su molte punti: la sua affinità ideologica con gli USA, la speranza che gli Stati Uniti potessero restare un grande cliente e la velata minaccia di poter danneggiare le sue prospettive economiche inondando il mercato con la vendita delle vecchie M-209.
Gli Stati Uniti avevano infine un altro elemento di vantaggio cruciale: William Friedman. Ampiamente considerato il padre della crittografia americana, Friedman conosceva Hagelin dagli

anni '30. Avevano stretto una solidissima amicizia perché avevano un background e degli interessi condivisi, compresa il loro passato russo e la passione per le complessità della crittografia.
Non ci sarebbe mai stata un'operazione Rubicon se i due uomini non si fossero stretti la mano quando fu stipulato il primo accordo segreto tra Hagelin e l'intelligence degli Stati Uniti durante una cena al Cosmos Club di Washington nel 1951.
L'accordo prevedeva che Hagelin, che aveva trasferito la sua azienda in Svizzera, limitasse le vendite dei suoi modelli più sofisticati ai paesi per i quali gli Stati Uniti davano la loro approvazione. Le nazioni non incluse nell'elenco USA avrebbero avuto sistemi più vecchi e più deboli. Hagelin sarebbe stato compensato in anticipo per le sue mancate vendite, con un massimo di 700.000 dollari.
Ci vollero anni perché gli Stati Uniti concludessero l'accordo, perché i massimi funzionari della CIA e il predecessore della NSA bisticciavano sui termini e sulla saggezza del piano. Ma Hagelin ha rispettato l'accordo fin dall'inizio, e nei successivi due decenni, la sua relazione segreta con le agenzie di intelligence statunitensi si è approfondita.
Nel 1960, la CIA e Hagelin hanno stipulato un "accordo di uso esclusivo" a favore degli USA, e sono stati pagati 855.000 dollari per rinnovare l'impegno del vecchio accordo della stretta di mano. L'Agenzia gli ha pagato 70.000 dollari all'anno di acconto e ha iniziato a dare alla sua azienda iniezioni di contanti di 10.000 dollari per spese di "marketing" per garantire che Crypto – e non altre start-up nel settore della crittografia – mettesse in sicurezza i contratti con la maggior parte dei governi del mondo.
Era una classica "operazione di interdizione" nel linguaggio dell'intelligence, una strategia progettata per impedire agli avversari di acquisire armi o tecnologia che avrebbero offerto loro un vantaggio. Ma era solo l'inizio della collaborazione di Crypto con l'intelligence degli Stati Uniti. Nel giro di un decennio, l'intera operazione apparteneva alla CIA e al BND.

Uno straordinario mondo nuovo

I funzionari CIA statunitensi avevano giocato fin dall'inizio con l'idea di chiedere a Hagelin se sarebbe stato disposto a lasciare che i criptologi statunitensi controllassero le sue macchine. Ma Friedman si oppose, convinto che Hagelin avrebbe visto la cosa come una invasione di campo.
A metà degli anni '60 la CIA e la NSA videro aprirsi una breccia nel rifiuto di Hagelin, quando la diffusione dei circuiti elettronici lo costrinse ad accettare aiuti esterni per adattarsi alla nuova tecnologia e per non rischiare l'estinzione rimanendo fedele alla produzione di macchine meccaniche.
Anche criptologi della NSA erano preoccupati per il potenziale impatto dei circuiti integrati, che sembrava rendere possibile una nuova era di una crittografia indecifrabile. Ma uno degli analisti senior dell'Agenzia, Peter Jenks, identificò una potenziale vulnerabilità.
Se "accuratamente progettato da un cripto-matematico intelligente", disse, un sistema basato su circuiti potrebbe essere realizzato in modo da fare sembrare che stia producendo flussi infiniti di caratteri generati casualmente, mentre in realtà si ripeterebbero a intervalli sufficientemente brevi da consentire agli esperti della NSA – e i loro potenti computer – di decifrare lo schema.
Due anni dopo, nel 1967, Crypto lanciò un nuovo modello di macchina completamente elettronico, l'H-460, i cui meccanismi interni furono completamente progettati dalla NSA.
Il documento CIA che racconta l'operazione, quasi gongola quando narra come fu superata questa soglia: "Immaginate l'idea del governo americano che convince un produttore straniero a truccare delle attrezzature a suo favore", dice il documento. "Stiamo parlando di un mondo nuovo e straordinario".
L'NSA non ha installato semplici "backdoor" o programmato segretamente i dispositivi perché sputassero fuori le loro chiavi di crittografia. E l'Agenzia si trovava ancora di fronte il difficile compito di intercettare le comunicazioni degli altri governi, sia che si trattasse di beccare i segnali dall'etere o, negli anni successivi, di collegarsi a cavi in fibra ottica.

Ma la manipolazione degli algoritmi di Crypto semplificava il processo di violazione del codice, a volte riducendo a pochi secondi il tempo di un'attività che altrimenti avrebbe richiesto mesi. La società ha sempre realizzato almeno due versioni dei suoi prodotti: modelli sicuri che sarebbero stati venduti a governi amici e sistemi truccati per il resto del mondo.
Così facendo, la collaborazione tra Stati Uniti e Hagelin si è trasformata da rifiuto a partecipazione attiva al progetto NSA. Crypto non si limitava più a vendere le sue migliori attrezzature soltanto a pochi, ma prendeva parte attiva al progetto spionistico USA vendendo dispositivi già progettati per tradire i propri acquirenti.
Il vantaggio è andato oltre la diffusione dei dispositivi. Il passaggio di Crypto ai prodotti elettronici ha fatto crescere così tanto il valore degli affari da fare diventare la ditta dipendente dalla sua dipendenza dalla NSA. I governi stranieri chiedevano a gran voce sistemi di criptazione che sembravano chiaramente superiori ai vecchi e goffi dispositivi meccanici, ma che in realtà erano più facili da leggere per le spie statunitensi.

I partenariato tra tedeschi e americani
Alla fine degli anni '60, Hagelin aveva quasi 80 anni e si preoccupò di assicurare un futuro per la sua azienda, che era cresciuta e aveva ssunto più di 180 dipendenti. Allo stesso modo i funzionari della CIA erano preoccupati per ciò che sarebbe accaduto all'operazione se Hagelin avesse improvvisamente venduto o fosse morto.
Hagelin sperava di passare il controllo dell'azienda a suo figlio, Bo. Ma i funzionari dell'intelligence degli Stati Uniti lo consideravano una "wild card" [persona dal comportamento imprevedibile] e hanno fatto in modo di tenerlo all'oscuro della partnership. Bo Hagelin è stato ucciso in un incidente d'auto sulla Beltway di Washington nel 1970. Non ci sono informazioni tali da far ipotizzare un gioco scorretto della CIA.
I funzionari dell'intelligence degli Stati Uniti hanno discusso dell'idea di acquistare Crypto per anni, ma il conflitto tra CIA e NSA ha impedito loro di agire fino a quando altre due agenzie di spionaggio sono entrate nella mischia.
I servizi di intelligence francesi, tedeschi occidentali e altri servizi segreti europei erano stati informati dell'accordo tra gli Stati Uniti e la Crypto, oppure lo avevano scoperto da soli. Alcuni erano comprensibilmente invidiosi e cercavano modi per combinare per se l'affare.
Nel 1967, Hagelin fu contattato dal servizio di intelligence francese con un'offerta di acquisto dell'azienda in collaborazione con l'intelligence tedesca. Hagelin respinse l'offerta e la riferì ai suoi gestori della CIA. Ma due anni dopo, i tedeschi tornarono cercando di fare una successiva offerta con la benedizione degli Stati Uniti.
In un incontro all'inizio del 1969 presso l'ambasciata della Germania Ovest a Washington, il capo del servizio di cifratura di quel paese, Wilhelm Goeing, delineò la proposta e chiese se gli americani "fossero interessati a diventare anche partner".
Mesi dopo, il direttore della CIA Richard Helms approvò l'idea di acquistare Crypto e inviò un subordinato a Bonn, la capitale della Germania occidentale, per negoziare i termini con un avvertimento importante: i francesi, dissero funzionari della CIA a Goeing, dovevano essere tenuti fuori dall'affare.
La Germania occidentale acconsentì a questo gioco di potere americano e un accordo tra le due agenzie di spionaggio fu registrato in un promemoria del giugno 1970 con la firma traballante di un ufficiale della CIA a Monaco che stava vivendo le prime fasi del morbo di Parkinson e lo scarabocchio illeggibile del suo controparte del BND.
Le due agenzie hanno concordato di mettere una medesima fiche per acquistare l'azienda di Hagelin equivalente a un valore di circa 5,75 milioni di dollari, ma la CIA ha lasciato in gran parte ai tedeschi il compito di capire come impedire che qualsiasi traccia della transazione diventasse pubblica.
Uno studio legale con sede nel Liechtenstein, Marxer e Goop, ha contribuito a nascondere le identità dei nuovi proprietari di Crypto attraverso una serie di "scatole cinesi" e azioni "al

portatore" che non richiedevano nomi nei documenti di registrazione. Alla Marxer è stato fatto uno versamento annuale "non per la quantità di lavoro erogato ma più per il loro silenzio e accettazione", racconta la BND. L'azienda, ora denominata Marxer e Partner, non ha risposto a una richiesta di commento da parte dei giornalisti.

Fu istituito un nuovo consiglio di amministrazione per governare la società. Solo un membro del consiglio di amministrazione, Sture Nyberg, al quale Hagelin si era affidato per la gestione quotidiana, era a conoscenza del coinvolgimento della CIA. "È stato attraverso questo meccanismo", osserva il documento CIA che racconta l'operazione, "che BND e la CIA hanno controllato le attività" di Crypto. Nyberg lasciò la compagnia nel 1976. Il *Post* e ZDF non sono riusciti a localizzarlo e capire se sia vivo o morto.

Le due agenzie di spionaggio hanno tenuto le proprie riunioni regolarmente per discutere che cosa fare con il loro acquisto. La CIA utilizzava una base segreta a Monaco, inizialmente in una installazione militare impiegata dalle truppe americane e successivamente nella soffitta di un edificio adiacente al Consolato degli Stati Uniti, come quartier generale per il suo coinvolgimento nell'operazione.

La CIA e il BND hanno concordato una serie di nomi in codice per il programma e le sue varie componenti. Crypto è stato chiamato "Minerva", che è anche il titolo del documento CIA che racconta l'operazione. L'operazione fu inizialmente denominata in codice "Thesaurus", sebbene negli anni '80 il nome fu cambiato in "Rubicon".

Ogni anno, la CIA e il BND dividevano tutti i profitti realizzati da Crypto, secondo quanto raccontato dai tedeschi, e il BND gestiva la contabilità e consegnava i contanti dovuti alla CIA in un garage sotterraneo.

Fin dall'inizio, la partnership è stata tormentata a causa di piccoli disaccordi e tensioni. Agli agenti della CIA, il BND sembrava soprattutto preoccupato di realizzare un profitto e gli americani "ricordavano costantemente ai tedeschi che si trattava di un'operazione di intelligence, non di una impresa per fare soldi". I tedeschi furono colti di sorpresa dalla volontà degli americani di spiare tutti a parte i loro più stretti alleati [il gruppo dell'anglosfera, i cosiddetti Five Eyes], con obiettivi che comprendevano anche i membri della NATO come Spagna, Grecia, Turchia e Italia.

Consapevoli dei limiti delle loro competenze per dirigere una società high-tech, le due agenzie hanno introdotto nell'azienda degli outsider. I tedeschi arruolarono la Siemens, un gruppo industriale con sede a Monaco, per fornire consulenza a Crypto su questioni commerciali e tecniche in cambio del 5% dei profitti dell'azienda. Gli Stati Uniti in seguito hanno portato Motorola a riparare prodotti che non funzionavano, chiarendo al CEO di Motorola che ciò veniva fatto per l'intelligence degli Stati Uniti. Interrogati dal *Post* Siemens ha rifiutato di commentare e i funzionari Motorola non hanno risposto a una richiesta di commento.

Con suo grande disappunto, la Germania non fu mai ammessa al tanto decantato gruppo dei "Five Eyes", un patto di intelligence di lunga data che coinvolgeva Stati Uniti, Gran Bretagna, Australia, Nuova Zelanda e Canada. Ma con la partnership di Crypto, la Germania si avvicinò alla sacra Chiesa americana dello spionaggio più di quanto non sarebbe sembrato possibile dopo la seconda guerra mondiale. Con il supporto segreto di due delle principali agenzie di intelligence del mondo e il supporto di due delle più grandi società del mondo, l'attività di Crypto è cresciuta.

Una tabella nel documento CIA che racconta l'operazione mostra che le vendite sono cresciute da 15 milioni di franchi svizzeri nel 1970 a oltre 51 milioni nel 1975, ovvero di 19 milioni di dollari. Il libro paga dell'azienda è stato ampliato assumendo più di 250 dipendenti.

"L'acquisto di Minerva ha prodotto una fortuna", dice il documento CIA che racconta l'operazione parlando di questo periodo. L'operazione ha dato per due decenni un accesso senza precedenti alle comunicazioni dei governi stranieri.

La diffidenza iraniana

L'impero dell'origliare realizzato dalla NSA è stato organizzato per molti anni attorno a tre principali obiettivi geografici, ciascuno con il proprio codice alfabetico: A per i sovietici, B per l'Asia e G per praticamente ovunque.

All'inizio degli anni '80, oltre la metà dell'intelligence raccolta dal gruppo G proveniva dalle macchine Crypto, un potenziale a cui i funzionari statunitensi si affidavano crisi dopo crisi.

Nel 1978, mentre i leader di Egitto, Israele e Stati Uniti erano riuniti a Camp David per negoziare un accordo di pace, l'NSA stava monitorando segretamente le comunicazioni del presidente egiziano Anwar al Sadat con il Cairo.

L'anno seguente, dopo che i militanti iraniani avevano assaltato l'ambasciata degli Stati Uniti e preso 52 ostaggi americani, l'amministrazione Carter cercò di farli rilasciare grazie a comunicazioni riservate con l'Algeria fuori dalla trattativa ufficiale. Inman, che all'epoca ricopriva il ruolo di direttore dell'NSA, ha affermato di aver regolarmente ricevuto chiamate dal presidente Jimmy Carter per chiedere come il regime ayatollah Khomeini stesse reagendo agli ultimi messaggi.

"Siamo stati in grado di rispondere alle sue domande circa l'85 percento delle volte", ha dichiarato Inman. Questo perché gli iraniani e gli algerini stavano usando i dispositivi Crypto.

Inman ha detto che l'operazione lo ha messo anche in uno degli intrecci più complicati che avesse mai incontrato durante il suo servizio al governo. Ad un certo punto, la NSA ha intercettato le comunicazioni libiche che indicavano che il fratello del presidente, Billy Carter, stava favorendo gli interessi della Libia a Washington ed era sul libro paga del leader Moammar Gheddafi.

Inman ha riferito la questione al Dipartimento di Giustizia. L'FBI ha avviato un'indagine su Carter, che ha detto il falso negando di avere avuto i pagamenti. Alla fine, non è stato processato ma ha accettato di definirsi come agente straniero.

Durante gli anni '80, l'elenco dei principali clienti di Crypto può essere letto come il libro aperto dei punti di crisi mondiali. Nel 1981, l'Arabia Saudita era il principale cliente di Crypto, seguito da Iran, Italia, Indonesia, Iraq, Libia, Giordania e Corea del Sud.

Per proteggere la sua posizione di mercato, secondo i documenti, Crypto e i suoi proprietari segreti si sono impegnati in campagne diffamatorie, discrete e riservate, contro le società rivali e hanno corrotto funzionari del governo con tangenti. Crypto ha inviato un dirigente a Riyadh, in Arabia Saudita, con 10 orologi Rolex nel suo bagaglio, dice la documentazione del BND, e in seguito ha organizzato un programma di formazione per i sauditi in Svizzera, dove il "passatempo preferito dai partecipanti era visitare i bordelli, che l'azienda ha anche finanziato".

A volte, gli incentivi hanno portato a vendite in paesi non in grado di utilizzare sistemi complicati. La Nigeria acquistò una grossa spedizione di macchine Crypto, ma due anni dopo, quando non era ancora stato ottenuto un corrispondente profitto in termini di intelligence, un rappresentante della società fu inviato per indagare e "ha trovato l'attrezzatura in un magazzino ancora nella sua confezione originale", racconta il documento tedesco che narra l'operazione.

Nel 1982, l'amministrazione Reagan ha approfittato della dipendenza dell'Argentina dalle apparecchiature Crypto, per passare informazioni di intelligence alla Gran Bretagna durante la breve guerra tra i due paesi sulle Isole Falkland, ma il documento CIA che racconta l'operazione non fornisce alcun dettaglio su quale tipo di informazione fosse passato a Londra. I documenti in genere discutono dell'intelligence prodotta dall'operazione in termini generali e forniscono poche informazioni su come poi è stata utilizzata.

Reagan sembra aver messo a repentaglio l'operazione Crypto dopo che la Libia fu implicata nell'attentato del 1986 quando una bomba esplose in una discoteca di Berlino Ovest molto frequentata dalle truppe americane di stanza nella Germania occidentale. Due soldati statunitensi e una donna turca furono uccisi a seguito all'attacco.

Reagan ordinò attacchi di ritorsione contro la Libia 10 giorni dopo. Tra le vittime segnalate c'era una delle figlie di Gheddafi. In un discorso al Paese in cui annunciava gli attacchi, Reagan affermò che gli Stati Uniti avevano prove della complicità della Libia "dirette, precise, e indiscutibili".

Le prove, disse Reagan, hanno dimostrato che l'ambasciata libica a Berlino Est ha ricevuto l'ordine di eseguire l'attacco una settimana prima che accadesse. Quindi, il giorno dopo l'attentato, "hanno riferito a Tripoli del grande successo della loro missione".
Le parole di Reagan chiarirono che le comunicazioni di Tripoli con la sua stazione a Berlino Est erano state intercettate e decifrate. Ma la Libia non fu il solo governo a prendere nota degli indizi forniti da Reagan.
L'Iran, che sapeva che anche la Libia utilizzava macchine Crypto, cominciò sempre più a preoccuparsi per la sicurezza delle sue attrezzature. Ma Teheran reagì a questi sospetti soltanto sei anni dopo.

Un uomo insostituibile
Dopo l'acquisizione di CIA e BND, uno dei problemi più fastidiosi per i due partner segreti era garantire che la forza lavoro di Crypto rimanesse collaborativa e non sapesse nulla dell'operazione. Anche se lontano dagli sguardi dei dipendenti, le agenzie hanno fatto di tutto per mantenere il comportamento benevolo con cui Hagelin gestiva la proprietà dell'azienda. I dipendenti erano ben pagati e godevano di numerosi vantaggi, incluso l'uso di una piccola barca a vela sul lago di Zugo vicino alla sede dell'azienda.
Ma a un certo punto sembrava che coloro che lavoravano a stretto contatto con i progetti di crittografia si avvicinassero sempre più alla scoperta del segreto principale dell'operazione. Gli ingegneri e i progettisti responsabili dello sviluppo di prototipi di modelli hanno spesso messo in dubbio alcune forme di algoritmo che venivano imposte da una misteriosa entità esterna.
I dirigenti di Crypto spesso cercavano di far credere ai dipendenti che alcune decisioni di progetto fossero fornite nell'ambito dell'accordo di consulenza con Siemens. Ma fosse stato anche così, i dipendenti si chiedevano perché erano presenti difetti di crittografia così facili da individuare e perché gli ingegneri di Crypto erano regolarmente bloccati quando tentavano di correggerli?
Nel 1977, Heinz Wagner, amministratore delegato di Crypto, che conosceva il vero ruolo della CIA e del BND, licenziò bruscamente un ingegnere ribelle quando la NSA si lamentò del fatto che il traffico diplomatico proveniente dalla Siria era diventato improvvisamente illeggibile. L'ingegnere, Peter Frutiger, da tempo sospettava che Crypto stesse collaborando con i servizi segreti tedeschi. Aveva fatto più viaggi a Damasco per rispondere ai reclami sui prodotti Crypto e, forse senza l'autorizzazione della sede centrale, aveva risolto le loro vulnerabilità eliminandole.
Frutiger "aveva scoperto il segreto di Minerva e non si poteva più essere sicuri di lui", secondo i documenti CIA che raccontano dell'operazione. Anche così, l'agenzia si arrabbio con Wagner per aver licenziato Frutiger piuttosto che trovare un modo per farlo tacere utilizzando il libro paga dell'azienda. Frutiger ha rifiutato di dare ai giornalisti un commento su questa storia.
I funzionari statunitensi si allarmarono ancora di più quando Wagner assunse un ingegnere elettrico di talento nel 1978 di nome Mengia Caflisch. Aveva trascorso diversi anni negli Stati Uniti a lavorare come ricercatrice di radioastronomia per l'Università del Maryland prima di tornare nella sua nativa Svizzera e fare domanda di lavoro presso la Crypto. Wagner ha colto al volo l'occasione di assumerla. Ma i funzionari della NSA hanno immediatamente comunicato la loro preoccupazione perché a loro pareva fosse "troppo intelligente per rimanere inconsapevole".
Il segnale di pericolo dei funzionari Usa si è rivelato premonitore poiché presto Caflisch ha iniziato a sondare le vulnerabilità dei prodotti dell'azienda. Lei e Spoerndli, una collega del dipartimento di ricerca, hanno eseguito vari test e "attacchi in chiaro" su dispositivi, tra cui un modello di telescrivente, l'HC-570, che è stato costruito utilizzando la tecnologia Motorola. Spoerndli in un'intervista ha dichiarato "Abbiamo esaminato le operazioni interne e le dipendenze di ogni passaggio", ha affermato Spoerndli, e ci siamo convinti di poter decifrare il codice confrontando solo 100 caratteri di testo crittografato con un messaggio sottostante non crittografato. Era un livello di sicurezza sorprendentemente basso, ha detto Spoerndli in un'intervista il mese scorso, ma tutt'altro che insolito.
"Gli algoritmi", ha detto, "sembravano sempre poco chiari".

Negli anni seguenti, Caflisch ha continuato a porre problemi. Ad un certo punto, ha progettato un algoritmo a così alto livello di sicurezza che i funzionari della NSA si sono preoccupati perché era indecifrabile. Il progetto è stato realizzato in 50 macchine HC-740 che sono uscite dalla fabbrica prima che i dirigenti dell'azienda scoprissero lo sviluppo e lo interrompessero.
"Avevo solo avuto l'idea che qualcosa potesse essere strano", ha detto Caflisch in un'intervista il mese scorso, a proposito dell'origine dei suoi sospetti. Ma fu chiaro che indagare sulla questione non era cosa gradita, ha detto. "Non tutte le domande sembravano essere ben accette."
La società ha ripristinato l'algoritmo taroccato per il resto della produzione e ha venduto i 50 modelli sicuri alle banche per tenerle fuori dal controllo dei governi stranieri. Poiché questi e altri sviluppi erano così difficili da difendere, Wagner ad un certo punto disse a un gruppo selezionato di membri dell'unità di ricerca e sviluppo che Crypto "non era del tutto libera di fare ciò che voleva". L'aver ammesso il fatto sembrò limitare le pretese degli ingegneri, che lo interpretarono come una conferma del fatto che la tecnologia dell'azienda era soggetta ai vincoli imposti dal governo tedesco. Ma la CIA e il BND divennero sempre più convinti che mantenere la loro abituale interferenza sotto copertura fosse insostenibile.
Crypto era diventata qualcosa di simile a una "operazione mago di Oz" con i dipendenti che sondavano per vedere cosa c'era dietro il sipario. Alla fine degli anni '70, i partner segreti decisero di trovare una figura magica che potesse aiutare a escogitare debolezze più profonde – e meno rilevabili – negli algoritmi, qualcuno che avesse sufficienti competenze crittografiche da addomesticare il dipartimento di ricerca.
Le due agenzie si sono rivolte ad altri servizi di spionaggio per verificare potenziali candidati prima di accettare un individuo presentato dal servizio di intelligence della Svezia. A causa dei legami di Hagelin con il paese, la Svezia era stata tenuta al corrente dell'operazione sin dall'inizio.
Kjell-Ove Widman, professore di matematica a Stoccolma, si era fatto conoscere negli ambienti accademici europei con le sue ricerche sulla crittografia. Widman era anche un riservista dell'esercito che aveva lavorato a stretto contatto con funzionari dell'intelligence svedese.
Per la CIA, Widman aveva un attributo ancora più importante: una simpatia e affinità per gli Stati Uniti che si era formata mentre trascorreva un anno nello stato di Washington come studente per uno scambio internazionale. La famiglia che lo ospitava aveva problemi a pronunciare il suo nome svedese e per questo lo chiamarono "Henry", un soprannome che in seguito usò con i suoi contatti della CIA.
I funzionari coinvolti nel reclutamento di Widman raccontano che fu molto facile arruolarlo. Dopo essere stato preparato da funzionari dell'intelligence svedese, fu portato a Monaco nel 1979 per quella che si presumeva essere una serie di interviste con dirigenti di Crypto e Siemens. La finzione fu mantenuta mentre Widman affrontò le domande di una mezza dozzina di uomini seduti attorno a un tavolo in una sala conferenze dell'hotel. Mentre il gruppo si scioglieva per andare a pranzo, due uomini chiesero a Widman di rimanere per una conversazione privata.
"Sai cos'è ZfCh?" gli chiese Jelto Burmeister, un ufficiale del BND, usando l'acronimo per il servizio di cifratura tedesco. Quando Widman rispose affermativamente, Burmeister disse: "Ora, hai capito chi possiede davvero Crypto AG?"
A quel punto Widman fu presentato a Richard Schroeder, un ufficiale della CIA di stanza a Monaco per gestire il coinvolgimento dell'agenzia in Crypto. Widman affermò poi agli storici dell'Agenzia che in quel momento il "mondo era caduto in pezzi". Vista la situazione, non ha esitato ad arruolarsi nell'operazione.
Senza nemmeno lasciare la stanza, Widman sigillò il suo reclutamento con una stretta di mano. Mentre i tre uomini si unirono al resto del gruppo a pranzo, il segnale di "pollice in alto" trasformò il raduno in una celebrazione.
Crypto installò Widman in azienda come "consulente scientifico" che riferiva direttamente a Wagner. Era diventato l'agente delle spie nascosto all'interno. Lasciava Zugo ogni sei settimane per incontri clandestini con i rappresentanti della NSA e ZfCh. Schroeder, l'ufficiale della CIA, avrebbe partecipato ma senza ascoltare le loro chiacchiere tecniche.

Si sarebbero accordati sulle modifiche e la elaborazione di nuovi schemi di crittografia. Quindi Widman avrebbe consegnato i progetti agli ingegneri Crypto. I documenti CIA che raccontano dell'operazione lo chiamano "l'uomo insostituibile" e il "reclutamento più importante nella storia del programma Minerva".
Il suo prestigio intimoriva i subordinati, investendolo "di una competenza tecnica che nessuno in CryptoAG poteva sfidare". Ha anche contribuito a sviare le inchieste dei governi stranieri. Quando Widman si insediò, i partner segreti adottarono una serie di principi per algoritmi truccati, secondo quanto racconta il BND. Dovevano essere "non rilevabili dai consueti test statistici" e, se scoperti, dovevano "essere facilmente mascherati come errori di implementazione o umani". In altre parole, messi alle strette, i dirigenti di Crypto davano la colpa o ai dipendenti sciatti o agli utenti incapaci.
Nel 1982, quando l'Argentina si convinse che la sua attrezzatura Crypto aveva tradito rivelando messaggi segreti e aiutato le forze britanniche nella guerra delle Falkland, Widman fu inviato a Buenos Aires. Widman disse che probabilmente l'NSA aveva violato un dispositivo di decodifica vocale obsoleto che l'Argentina stava usando, ma che il prodotto principale acquistato da Crypto, il CAG 500, era rimasto "impenetrabile".
"Il bluff ha funzionato", dice il documento CIA che racconta l'operazione. "Gli argentini ingoiarono il rospo a fatica, ma continuarono ad acquistare attrezzature CryptoAG."
Widman è in pensione da tempo ormai e vive a Stoccolma. Chiamato dai giornalisti ha rifiutato di commentare. Anni dopo il suo reclutamento, ha detto ai funzionari degli Stati Uniti che si vedeva "impegnato in una difficile lotta per favorire l'intelligence occidentale", scrive il documento CIA che racconta l'operazione. "È stato, ha detto, il momento in cui si è sentito a casa. Questa era la sua missione nella vita."
Nello stesso anno, Hagelin, allora novantenne, si ammalò durante un viaggio in Svezia e fu ricoverato in ospedale. Si riprese abbastanza bene per tornare in Svizzera, ma i funzionari della CIA erano preoccupati dell'ampia raccolta di documenti aziendali e personali di Hagelin che si trovavano nel suo ufficio di Zugo. Schroeder, con il permesso di Hagelin, arrivò con una valigetta e passò diversi giorni a esaminare i file. Fu presentato come uno storico interessato a tratteggiare la vita di Hagelin. Schroeder tirò fuori i documenti "che erano pericolosi", dice la storia CIA, e li rimandò al quartier generale della CIA, "dove risiedono fino ad oggi".
Hagelin è rimasto invalido fino alla sua morte nel 1983. Il *Post* non è riuscito a localizzare Wagner o sapere se è ancora vivo. Schroeder si è ritirato dalla CIA più di dieci anni fa e insegna part-time alla Georgetown University. Contattato da un giornalista del *Post*, ha rifiutato di commentare.

La crisi Hydra
Crypto ha avuto per diversi anni perdite economiche nel corso degli anni '80, ma le informazioni di intelligence continuavano ad arrivare in gran quantità. Le agenzie di spionaggio statunitensi hanno intercettato più di 19.000 comunicazioni iraniane inviate tramite macchine Crypto durante la guerra decennale di quella nazione con l'Iraq, estraendone informazioni su vari argomenti come i legami di Teheran con il terrorismo e i tentativi di colpire i dissidenti.
Le comunicazioni dell'Iran erano "dall'80 al 90 percento dei casi leggibili" per le spie statunitensi, secondo il documento della CIA, una quantità che probabilmente sarebbe precipitata a un numero a una cifra se Teheran non avesse più usato i dispositivi taroccati di Crypto.
Nel 1989, l'uso in Vaticano di dispositivi Crypto si è rivelato cruciale nella caccia all'uomo attuata dagli Stati Uniti nei confronti del leader panamense Manuel Antonio Noriega. Quando il dittatore cercò rifugio nella Nunziatura Apostolica – l'equivalente di un'ambasciata papale – la sua posizione fu rivelata dai messaggi della missione indirizzati a Città del Vaticano.
Nel 1992, tuttavia, l'operazione Crypto ha affrontato la sua prima grande crisi: l'Iran, anche se in ritardo rispetto ai suoi sospetti di vecchia data, ha arrestato un venditore della società.
Hans Buehler, che allora aveva 51 anni, era considerato uno dei migliori venditori dell'azienda. L'Iran era uno dei maggiori contratti della compagnia e Buehler aveva viaggiato da e per Teheran per anni. C'erano già stati momenti di tensione, anche quando era stato a lungo interrogato nel 1986

da funzionari iraniani dopo l'attentato alla discoteca e gli attacchi missilistici degli Stati Uniti sulla Libia. Ma poi era stato rilasciato.
Sei anni dopo, salì a bordo di un volo Swissair per Teheran ma non riuscì a rientrare nei tempi previsti. Quando non si presentò, Crypto chiese aiuto alle autorità svizzere che gli dissero che era stato arrestato dagli iraniani. I funzionari consolari svizzeri autorizzati a visitare Buehler riferirono che si trovava in una "cattiva forma mentale", secondo quanto raccontato dal documento CIA.
Buehler fu finalmente rilasciato nove mesi dopo quando Crypto accettò di pagare 1 milione di dollari agli iraniani, una somma che è stata segretamente fornita dal BND. La CIA ha rifiutato di intervenire, citando la politica degli Stati Uniti contro il cedimento alla richiesta di riscatto di ostaggi.
Buehler non sapeva nulla della relazione di Crypto con CIA e BND o delle vulnerabilità nei suoi dispositivi. Ma è tornato traumatizzato e diffidente rispetto al fatto che l'Iran sapesse di più di lui sulla compagnia per cui lavorava. Buehler iniziò a parlare alle organizzazioni di stampa svizzere del suo calvario e dei suoi crescenti sospetti. La pubblicità della questione ha portato una nuova attenzione nei confronti di altri indizi dimenticati da tempo, compresi i riferimenti a un "progetto Boris" citato nella vasta raccolta di documenti personali di Friedman, che erano stati donati al Virginia Military Institute quando morì nel 1969. Tra le 72 scatole consegnate a Lexington, in Virginia, c'erano copie della sua continua corrispondenza con Hagelin.
Nel 1994, la crisi si è approfondita quando Buehler è apparso sulla televisione svizzera in un resoconto che parlava anche di Frutiger, la cui identità era nascosta. Buehler è morto nel 2018.
Frutiger, l'ingegnere che era stato licenziato per aver riparato i sistemi di crittografia della Siria anni prima, non ha risposto alle richieste di commento dei giornalisti.
Michael Grupe, che era subentrato a Wagner come amministratore delegato, accettò di apparire alla televisione svizzera e contestò quelle che sapeva essere accuse reali. "Le performance di Grupe sono state credibili e potrebbero aver salvato il programma", afferma il documento della CIA.
Grupe non ha risposto alle richieste di commento dei giornalisti.
Anche così, ci sono voluti diversi anni perché la controversia si spegnesse. Nel 1995, il quotidiano Baltimore Sun ha pubblicato una serie di storie investigative sulla NSA, tra cui una chiamata "Rigging the Game" che ha messo in luce aspetti della relazione dell'agenzia con Crypto.
L'articolo riportava che funzionari della NSA si erano recati a Zugo a metà degli anni '70 per incontri segreti con i dirigenti di Crypto. I funzionari si sono presentati come consulenti per una società di facciata denominata "Intercomm Associates", ma poi hanno iniziato a presentarsi con i loro nomi reali, che sono stati registrati nelle note della riunione tenuta da un dipendente della società.
Nel bel mezzo della campagna di stampa, alcuni impiegati hanno iniziato a cercare lavoro altrove. E almeno una mezza dozzina di paesi – tra cui Argentina, Italia, Arabia Saudita, Egitto e Indonesia – hanno annullato o sospeso i loro contratti con Crypto. Sorprendentemente, l'Iran non era tra questi, secondo il file della CIA, e ha ripreso il suo acquisto di attrezzature CryptoAG quasi immediatamente".
La principale vittima della crisi "Hydra", il nome in codice dato al caso Buehler, è stata la partnership CIA-BND.
Per anni, i funzionari del BND avevano rifiutato di seguire i loro omologhi americani che non distinguevano gli avversari dagli alleati. I due partner hanno spesso litigato su quali paesi meritassero di ricevere le versioni sicure dei prodotti Crypto, con i funzionari degli Stati Uniti che insistevano spesso sul fatto che le attrezzature truccate fossero inviate a quasi tutti, alleati o meno, che potevano essere raggirati nell'acquisto.
Nei documenti tedeschi che narrano l'operazione, Wolbert Smidt, ex direttore del BND, si è lamentato del fatto che gli Stati Uniti "volevano trattare con gli alleati proprio come trattavano con i paesi del Terzo mondo". Un altro funzionario del BND ha ripreso quel commento dicendo che per gli americani, "nel mondo dell'intelligence non c'erano amici".

La guerra fredda era finita, il muro di Berlino era caduto e la Germania riunificata aveva diverse sensibilità e priorità. I tedeschi si sono visti molto più direttamente esposti ai rischi dell'operazione Crypto. Idra aveva scosso i tedeschi, che temevano che la divulgazione del loro coinvolgimento avrebbe scatenato l'indignazione europea e causato enormi ricadute politiche ed economiche.
Nel 1993, Konrad Porzner, il capo del BND, chiarì al direttore della CIA James Woolsey che il supporto alla operazione nelle alte sfere del governo tedesco stava calando e che i tedeschi avrebbero potuto desiderare di uscire dal partenariato Crypto. Il 9 settembre, il capo della stazione della CIA in Germania, Milton Bearden, raggiunse un accordo con i funzionari BND, per conto della CIA, per l'acquisto delle azioni tedesche per 17 milioni di dollari, secondo quanto riportato nei documenti CIA che raccontano della operazione.
I funzionari dell'intelligence tedesca hanno rimpianto il fatto di avere abbandonato un'operazione che avevano in gran parte contribuito a elaborare. Nei documenti tedeschi che raccontano l'operazione, alti funzionari dell'intelligence incolpano i leader politici di aver posto fine a uno dei programmi di spionaggio di maggior successo di cui il BND abbia mai fatto parte.
Con la loro partenza, i tedeschi furono presto esclusi dalle informazioni e dall'intelligence che gli Stati Uniti continuarono a raccogliere. Burmeister, citato nei documenti tedeschi, si chiede se la Germania appartenesse ancora "a quel piccolo numero di nazioni che non sono "lette" dagli americani". I documenti pubblicati da Snowden hanno fornito una risposta inquietante, dimostrando che le agenzie di intelligence statunitensi non solo consideravano la Germania come un obiettivo, ma monitoravano il cellulare del cancelliere tedesco Angela Merkel.

Vivi e vegeti

La storia raccontata nel documento CIA si conclude essenzialmente con l'uscita della Germania dal programma, anche se è stata completata nel 2004 e contiene chiare indicazioni sul fatto che l'operazione era ancora in corso. Nota, ad esempio, che il caso Buehler è stato "la più grave violazione della sicurezza nella storia del programma "ma non è stato fatale. Non ne ha causato la sua scomparsa", dice la storia, "e al volgere del secolo Minerva era ancora viva e vegeta".
In realtà, l'operazione sembrava essere entrata in un lungo periodo di declino. A metà degli anni '90, "i giorni dei profitti erano molto lontani", e Crypto "sarebbe andato fuori mercato se non fosse stato per le iniezioni di denaro del governo degli Stati Uniti".
Di conseguenza, sembra che la CIA abbia sostenuto per anni un'operazione che era più vitale come piattaforma di intelligence che come impresa economica. La sua linea di prodotti si è ridotta e le entrate e la base di clienti sono diminuite.
Ma da Crypto le informazioni continuarono ad arrivare, sostengono i funzionari CIA attuali e passati, anche a causa dell'inerzia dei burocrati. Molti governi non sono mai riusciti a passare a sistemi di crittografia più recenti, che sono stati prodotti numerosi dagli anni '90 in poi, e non sono riusciti a sostituire i loro dispositivi Crypto. Questo è accaduto in particolare nelle nazioni meno sviluppate, dicono i documenti dell'Agenzia.
La maggior parte dei dipendenti identificabili nei documenti CIA e BND che raccontano l'operazione ha circa 70 o 80 anni, e alcuni di loro sono morti. Nelle interviste fatte in Svizzera il mese scorso, diversi ex lavoratori Crypto citati nei documenti hanno espresso disagio per il loro coinvolgimento nell'azienda.
Non erano mai stati informati delle relazioni dell'azienda con i servizi di intelligence. Ma avevano fondati sospetti e sono ancora oggi alle prese con le implicazioni etiche delle loro decisioni di rimanere in un'azienda che immaginavano impegnata nell'inganno.
"O te ne andavi o dovevi accettare in qualche modo la situazione", ha detto Mengia Caflisch, ora 75enne, che ha lasciato l'azienda nel 1995 ma continua a vivere alla periferia di Zugo in una ex fabbrica tessile ristrutturata dove lei e la sua famiglia per molti anni hanno messo in scena opere teatrali semiprofessionali. "Avevo delle ragioni per lasciare", ha detto, compreso il disagio per i suoi dubbi su Crypto e il suo desiderio di essere più a casa con i suoi figli. Dopo le ultime rivelazioni, ha detto: "Mi chiedo se avrei dovuto andare via prima".

Spoerndli ha dichiarato di essersi pentito di quello che ha fatto. “A volte mi sono detto che era meglio che i bravi ragazzi negli Stati Uniti sapessero che cosa sta succedendo tra i dittatori del Terzo mondo”, ha detto. “Ma è un modo conveniente per autoassolversi. Alla fine, non è così.”
La storia raccontata dai documenti CIA dice che la maggior parte dei dirigenti direttamente coinvolti nell’operazione era motivata da obiettivi ideologici e ha rifiutato qualsiasi tipo pagamento che non fosse i loro stipendi Crypto. Widman era una delle eccezioni. “Con l’avvicinarsi della pensione, il suo compenso segreto fu notevolmente aumentato, dice la storia della CIA. Ha anche ricevuto una medaglia con il sigillo della CIA.
Dopo la partenza del BND, la CIA ha ampliato la sua collezione clandestina di aziende del settore della crittografia, secondo gli ex funzionari dell’intelligence occidentale. Usando i soldi accumulati con l’operazione Crypto, l’Agenzia ha segretamente acquisito una seconda azienda e poi una terza. I documenti non rivelano alcun dettaglio su queste due nuove entità. Ma la storia del BND osserva che una delle rivali di lunga data di Crypto – la Gretag AG, anch’essa con sede in Svizzera – è stata “rilevata da un americano” e, dopo un cambio di denominazione nel 2004, è stata liquidata”.
La stessa Crypto come azienda zoppicava. Era sopravvissuto alla transizione dalle scatole di metallo ai circuiti elettronici, passando dalle macchine telescriventi ai sistemi vocali cifrati. Ma ha faticato a mantenere la propria posizione mentre il mercato della crittografia si spostava dall’hardware al software. Le agenzie di intelligence statunitensi sembrano essersi accontentate di lasciare che l’operazione Crypto proseguisse e uscisse lentamente di scena, mentre l’attenzione dell’NSA si è spostata sulla ricerca di modi per sfruttare la portata globale di Google, Microsoft, Verizon e altre tipologie di potenti strumenti tecnologici statunitensi.
Nel 2017, il quartier generale di Crypto, vicino a Zugo, è stato venduto a una società immobiliare commerciale. Nel 2018, le attività rimanenti dell’azienda – le parti principali dell’attività di crittografia avviata quasi un secolo prima – sono state frazionate e vendute. Le transazioni sembravano progettate per garantire una copertura per l’uscita dalla CIA.
L’acquisto della parte svizzera del business da parte di CyOne è stato strutturato come un buyout fatto dai manager che avevano la gestione, consentendo ai dipendenti Crypto di trasferirsi in una nuova società isolata dai rischi di spionaggio e con una fonte di entrate affidabile. Il governo svizzero, al quale sono state sempre vendute versioni sicure dei sistemi Crypto, è ora l’unico cliente di CyOne.
Giuliano Otth, che è stato CEO di Crypto AG dal 2001 fino alla sua smembramento, ha assunto la stessa posizione in CyOne dopo aver acquisito le attività svizzere. Dato il suo incarico alla Crypto, è probabile che fosse consapevole della proprietà CIA dell’azienda, proprio come lo erano stati tutti i suoi predecessori che avevano la medesima posizione.
“Né CyOne Security AG né Mr. Otth hanno commenti da fare sulla storia di Crypto AG”, ha dichiarato la società in una nota.
I beni mobili e immobili di Crypto sono stati venduti ad Adreas Linde, un imprenditore svedese, che proviene da una famiglia benestante con partecipazioni immobiliari commerciali.
In un incontro tenutosi a Zurigo il mese scorso, Linde ha affermato di essere stato attratto dall’azienda in parte dalla sua eredità e dal suo legame con Hagelin, un passato che ha ancora un eco in Svezia. Dopo aver preso il controllo delle attività dell’azienda, Linde ha persino spostato alcune delle attrezzature storiche di Hagelin dal magazzino in una vetrina all’ingresso della fabbrica.
Di fronte alle prove del fatto che Crypto era di proprietà della CIA e del BND, Linde è sembrato visibilmente scosso e ha detto che durante la trattativa non aveva mai saputo della identità degli azionisti dell’azienda. Ha chiesto quando la storia sarebbe stata pubblicata, dicendo che aveva dipendenti all’estero e che esprimeva preoccupazione per la loro sicurezza.
In una successiva intervista, Linde ha dichiarato che la sua azienda sta indagando su tutti i prodotti che vende per determinare se hanno delle vulnerabilità nascoste. “Dobbiamo tagliare il più presto possibile con tutto ciò che è stato collegato a Crypto”, ha detto.

Quando gli è stato chiesto perché non si fosse confrontato con Otth e altri coinvolti nella transazione sul fatto che ci fosse qualche verità nelle accuse che da lungo tempo venivano fatte a Crypto, Linde ha affermato di aver considerato queste accuse "solo voci". Ha detto che era rassicurato dal fatto che Crypto aveva continuato ad avere contratti importanti con i governi stranieri, paesi che supponeva avessero verificato attentamente i prodotti dell'azienda e che non li avrebbero più utilizzati se fossero risultati compromessi.
"Ho perfino acquisito il marchio Crypto", ha affermato, sottolineando la sua fiducia nella redditività dell'azienda. Date le informazioni che stanno venendo alla luce, ha detto, questa "è stata probabilmente una delle decisioni più stupide che io abbia mai preso nella mia carriera".
La liquidazione della società è stata gestita dallo stesso studio legale del Liechtenstein che ha fornito copertura per la vendita di Hagelin alla CIA e BND 48 anni prima. I termini della transazione del 2018 non sono stati resi noti, ma i funzionari attuali e passati hanno stimato il valore complessivo della operazione tra 50 milioni e 70 milioni di dollari
Per la CIA, i soldi sono stati il guadagno finale da Minerva.