**RUBICON and revelation:**

**The curious robustness of the "secret" CIA-BND operation with Crypto AG.**

ABSTRACT 100 WORDS

For over 50 years, America and Germany read much of the world's communications. With "Operation Rubicon", the CIA and the BND undermined the security of the encryption of foreign governments by controlling the Swiss technology company, Crypto AG. Puzzlingly, investigative journalists and customers increasingly identified Crypto AG's relationship with Western intelligence as well as the vulnerabilities of products on multiple occasions. Yet, Rubicon continued to succeed and produced dividends for over half a century despite repeated revelations. This article asks why? Answering this question, it argues that geopolitical influences on targets, the consumer's limited resources, and individual brilliance by CIA-BND agents within Crypto AG combined to enable operational longevity - where other sigint operations would have failed.

Key words: sigint, media, security, NSA, CIA, BND, Germany

Who told Cong[ress] about Cry[pto] AG?

William Odom, DIRNSA, 6 Nov 1986.[1]

## Introduction

In 1970, the Central Intelligence Agency (CIA) and the Bundesnachrichtendienst (BND) formalised their secret purchase of Crypto AG, one of the world's premier manufacturers of

encryption machines. The agreement, made between German and American intelligence at the highest levels, paved the way for secret exploitation of Crypto AG products by weakening their encryption. As the journalists Scott Shane and Tom Bowman neatly put it in 1995, the partners were "rigging the game".[2] With the help of the National Security Agency (NSA) seemingly invulnerable machines were made more exploitable to US codebreakers, and indeed other countries with high-grade computing. This joint takeover of the company from founder Boris Hagelin was known as the "Minerva purchase" and lasted until 1993 when the BND sold its stake to the CIA. The CIA continued to own a stake in the company into the twenty-first century. Initially known as Operation Thesaurus before being renamed Rubicon, this active measures operation replaced an initial decade-long denial operation where US intelligence simply asked Hagelin to refrain from selling the most secure equipment to target countries.[3] Remarkably, Rubicon managed to outlive the partnership, but not without experiencing several crises during which, in the most serious case, the operation was disclosed in all but name.

Somehow Rubicon survived and continued to thrive after being blown. The operation was not only exposed by investigative journalists and disgruntled employees, but also periodically uncovered by technically competent customers. The users of the devices discovered vulnerabilities as their knowledge of cryptology increased. Yet customers returned to Crypto AG and bought more of their expensive machines, even though their communications security had clearly been compromised. What underpinned the longevity and resilience of this operation? This article explores the episodes where the operation was put at risk and suggests that several factors allowed for the continued success at Crypto AG. The most prominent factors included the choice of and performance of particular individuals whom were witting of the operation and who convinced customers that periodic problems were being addressed. There were also wider lessons of Cold War politics. For some states, regional geopolitical concerns tended to be of greater importance than western centric priorities. Then there were limited choices for customers because the cost of building indigenous cryptography, both in terms of capital and expertise, was prohibitive. This left them reliant on commercial based products such as those designed by Crypto AG or its competitors such as, Racal, Phillips, Mils Electronics, and Datotek.[4] All they could do was test their own systems to ensure that any insecurity in the design of the devices was patched up, since there was no guarantee that an alternative firm was not also working with the United States. Indeed, by the late 1990s, the likelihood that many firms had been controlled in a similar way was widely suspected by the global club of cryptographic cognoscenti.[5]

The academic consensus suggests that when a communications intelligence capability is exposed it is no longer exploitable. Once the target knows that they are being listened to they will likely change channels or further secure their communications, often by enhancing encryption.[6] The history of communications intelligence is littered with examples, most famously the British government's flagrant use of decrypted Russian messages in the House of Commons to justify the Arcos Raid in 1927.[7] Elaborate security precautions surrounded the use of both Magic and Ultra during the Second World War designed to convince the enemy that intelligence had been obtained by human agents or overhead photography rather than codebreaking. In 1979, NSA lost its ability to read South Korean diplomatic communications after *The New York Times* published that the agency had intercepted evidence that Members of Congress had received favours and bribes from South Korea.[8] In 2013, the head of the three UK security agencies gave public testimony that the Snowden revelations had damaged GCHQ's ability to read terrorist messages.[9] These are just a few examples of communications intelligence operations losing their ability due to exposure. Moreover, this is why signals intelligence agencies around the world have operated under the tightest possible security, associating eye-watering secrecy with success.[10] However, Operation Rubicon, with many of its targets in the Global South, seems to challenge this consensus, suggesting a model of greater resilience that may be underpinned by a more regional dynamic.

## Towards a typology of revelations

During the thirty years following the 1970 purchase agreement, the relationship between intelligence agencies and Crypto AG was "unearthed" repeatedly. But secrecy and exposure are not a simple binary and instead constitute a layered process. Crypto AG was hardly a "deep secret" in the sense that the nature of its work and products was widely known; one might even say that speculation about its affiliation might have been expected.[11] The Soviet Union was likely aware of the weaknesses in the communications of Global South. Shortly after Friedman and Hagelin concluded their "Gentleman's' Agreement", NSA experienced a number of defectors and those who sold information to the Soviet Union, including William Martin and Bernon Mitchell, Kalugin's unnamed spy in the mid-1960s.Later there was Ronald Pelton as well as whistleblowing from Perry Fellwock in *Ramparts*. Each divulged NSA targets and capabilities to the USSR providing some direction to avenues for exploitation.[12] Since the USSR had used stolen Hagelin machines in the late-1940s they had some experience in their early designs. Moreover, Desmond Ball and Robert Windrem argued that

the USSR by the end of the Cold War boasted the 'most extensive and most comprehensive signals intelligence (sigint) capabilities in the world'.[13] It is likely that by the 1980s, the KGB sigint teams were able to exploit Crypto AG machines owned by countries like Greece with relative ease,[14] and by the 1990s we might be – who amongst the more advanced countries was not aware of the relationship or security issues at Crypto AG?

The key episodes of evolving revelation can be grouped into four themes. First, because sigint operations are often of long-duration, governments need to police the past and control historical archives. For a quarter of a century the UK government fought to protect the Bletchley Park secret from probing historians.[15] Therefore, the personal papers and correspondence of the primary actors William Friedman and Boris Hagelin created a stir at NSA as they had limited control on their release. Historical research into these papers led to two books that posed a threat to Rubicon, *The Man Who Broke Purple* published in 1977 and *The Puzzle Palace* in 1982.[16] NSAs reaction drew further attention to the revelations, but at least further releases of compromising papers were avoided.

The second theme is what we might call an expanding crowd of cryptographic experts. By the 1990s, a growing number of people in the encryption industry in Europe knew something about the rigged nature of the market. An increasing number of American officials, including staffers on Capitol Hill, also seemed to know the secret. Clearly a variety of technicians in the Global South also had their suspicions about their machines. Engineers in Argentina, Syria, Egypt, and other countries repeated at Crypto AG to "fix" problems with machines that seemed to be generating weak encryption. Some of these clearly entertained wider suspicions, but do not seem to have voiced them to their superiors as a systematic problem, instead addressing only specific errors to be "patched". This is perhaps a function of technicians being relegated to the back room in the bureaucracies of foreign policy. Would anyone working in Shah of Iran's government, for example, want to risk asking a senior manager to provide millions to re-equip the embassies of Iran, citing only a vague hunch about weak encryption?

The third theme revolves around the deliberate disclosure of exploitation by loose-lipped politicians. Two infamous scenarios are focused on here: the fallout from the 1982 speech by the British Member of Parliament Ted Rowlands concerning the reading of Argentinian communications and Ronald Reagan's declaration that he had irrefutable proof that Libya had ordered the 1986 terrorist attack in West Berlin. These examples underline the inability of countries in the Global South to think about communications as a general system. Argentina was more worried about Chile reading its cables than Germany. Iran failed

to learn the lessons of the Libyan episodes and did not ask questions of its own ciphers. Both probably knew that improved secrecy required high costs and a great deal of determination.

The fourth theme is dissident employees as whistleblowers. In 1993, the "Hydra" affair posed the sternest challenge to the longevity of Rubicon. Hans Bühler, a disgruntled employee, exerted pressure on Crypto AG after being interned and interrogated in Iran, before being dismissed by the company. The security debate about the company's products reached the Swiss courtrooms. Then *Baltimore Sun* investigative journalists followed the reports from the Swiss media and gained documentary evidence of American intelligence influence at Crypto AG. They insisted that US cryptologists had been present at design meetings.[17] Considering the past revelations and accusations, there was now enough information to raise significant suspicions on the security of the products. Once more the operation continued. What was known as the "Hydra affair" followed by *The Baltimore Sun* publication did some damage, but also demonstrated the resilience of the operation on global south targets.

It is likely to be decades before the value of the sigint product from Rubicon can be fully assessed by historians. Only with fully opened files can we begin to assess the impact of the various kinds of revelations, meanwhile valuable witnesses are already slipping away. Accordingly, now might be an auspicious time to at least begin to examine the resilience and longevity of Rubicon and the intelligence it afforded on the global south, employing material unearthed by *ZDF* and *The Washington Post* in their joint investigations.

## The Friedman and Hagelin Papers

Rubicon's first major security concern occurred because of a controversy over history.[18] Toward the end of this career William Friedman deposited his papers in the privately run George C. Marshall Library. Friedman was annoyed by NSAs disregard for his academic work and its desire to classify many of his findings, lectures, and publications.[19] Furthermore, he felt as though he had been marginalised in Rubicon discussions with Hagelin, despite the fact that his personal drive helped to overcome NSA's inertia.[20] Constituting part of the old guard and not relevant in the new computerised NSA, in later years he was moved to the periphery and worked from home on an annually renewable contract.[21] Yet when relations with Hagelin soured, it was Friedman who smoothed tensions by repeatedly visiting Europe.[22] Friedman had been the lynchpin in the relationship, but didn't feel appreciated by

NSA. He hankered after his place in history and the tensions grew so much that he wrote to one friend confiding that: "the NSA considers me their greatest security risk".[23]

Ultimately, Friedman and his wife Elizabeth – a fellow expert in cryptography – decided that their work and papers would be left in a private library for scholarly enlightenment.[24] In December 1970, the collection arrived at the Marshall Library. Nevertheless, over the next five years, NSA emissaries searched the collection for sensitive material. Vince Wilson of NSA was part of all three visits in January 1971, November 1971, and July 1975.[25] What concerned NSA was the correspondence between Friedman and Hagelin. They feared that the letters contained enough details about the origins of Rubicon to compromise the operation if publicly disclosed. But the NSA officers were short of time and could not unpack all the boxes, instead relying on index cards. Moreover, they could not access the special collections kept in a safe since Elizabeth Friedman refused to give the archivist the combination. As the index cards suggested that there was nothing of concern, the collection was shelved and opened, nevertheless the NSA visited twice more, unable to find the Friedman-Hagelin file they desired. Interestingly, they declassified other material that was deemed over-classified.[26]

The NSA was informed by archivist Tony Crawford that British investigative journalist Ronald Clark was due to see the files for his biography of Friedman.[27] NSA were especially worried about Clark's discovery of the trips that Friedman made to Europe over 1957-8. Two officials who were involved in the ongoing Rubicon operation visited him.[28] But the journalist had mis-interpreted the visits as part of NSAs reconciliation efforts after the Suez Crisis. According to Clark, GCHQ believed that the US had been spying on British and French communications prior to the intervention by these countries in collusion with Israel.[29] Clark noted that Friedman also visited Sweden and Switzerland on one visit. Then travelled to Frankfurt on another journey as well as back to Cheltenham. Each time, quite wrongly, Clark perceived the most important common denominator was Cheltenham. Therefore, Clark wrote that it was all about the US reading of allied NATO communications.[30] NSA were unnerved but for whatever reason, Clark failed to join the final dots concerning Crypto AG and American influence.[31]

Clark's success at the Marshall Library prompted a return by NSA to withdraw more files from public view. Clark's research had confirmed the existence of the potentially damaging Hagelin-Friedman correspondence. Within weeks of Clark's research visit, NSA had succeeded in convincing the archive to lock the correspondence among other files in its vault away from public view, since the agency could not take personal care of them. Crawford

complied initially.[32] Clark's biography, published in 1977, revealed the Friedman-Hagelin friendship but did not spotlight Crypto AG. It was not the last time the correspondence caused concern, for an inquisitive journalist named James Bamford now followed the winding trail to Friedman's collection.

In 1979, after a year of research, Bamford was contracted by Houghton Mifflin to write *The Puzzle Palace* - a detailed history of the NSA starting with its origins as the American Black Chamber.[33] Unfortunately for Bamford, the NSA had convinced the Marshall Library to close some of files that Clark had accessed.[34] Knowing full well why Friedman had chosen the Marshall Library to deposit his papers, Bamford approached the archivist Crawford to release them from the vault. Crawford was reluctant at first, but Bamford sensed that he sympathized with the author and with the spirit of Friedman's requests. Crawford, who had now been trusted with the vault combination, finally allowed the files to be read against the wishes of NSA.[35]

Bamford saw there was rather more to the Friedman's European trips than Clark had realised. The detailed correspondence with Hagelin, as well as the trips to Sweden and Switzerland where Hagelin, his company, and factory were based pointed to a more exciting story. In the *Puzzle Palace* Bamford suggested that the real reason for the trips were to meet with Hagelin. The purpose of these visits "probably were directed at reasserting the need for close cooperation between GCHQ and NSA and at establishing some sort of agreement with Europe's largest manufacturer of cryptographic devices, Crypto AG".[36] This conclusion had been surmised from the extent of correspondence between Friedman and Hagelin and strengthened by a letter written by a frustrated Friedman to Howard Engstrom, days before ended his term as Deputy Director of NSA. In the letter Friedman indicated his dissatisfaction of being removed from the "Boris project".[37] It was not irrefutable proof, but added to Stuart Hedden's comments as the representative of Crypto AG in the US and a former CIA Inspector General that hinted at approaches from US agencies, it was enough for Bamford to deduce the truth.[38] Though it appeared to NSA that Bamford made an educated guess at the potential relationship – he had pretty much hit the nail on the head.[39]

The NSA then tried and failed to prevent the publication of Bamford's work. It was not for the want of effort.[40] Subsequent NSA directors Admiral Bobby Ray Inman and General Lincoln Faurer attempted to regain control of information released to Bamford through Freedom of Information – the latter even threatened prosecution.[41] Initially, they had to initially settle for the closure of some of Friedman's documents used in the book. Under Faurer, the agency now wanted the complete closure of the Friedman collection.

They did not want to risk any more information being inferred from the correspondence either by journalists, academics, or foreign agents. Accordingly, in 1983, the Friedman-Hagelin papers were closed after court action. The case appeared rather odd to many journalists and even to the proceeding appeals judge.[42] According to Justice Green, the papers had been viewed and copied by at least five persons in the time they were open – the information was to an extent now public knowledge through copies made and publications. Yet a new Executive Order gave the NSA the right to close the papers retrospectively. [43] A new National Security Decision Directive allowed the NSA to review all documentation before release into the public domain and that all personnel inform senior officers of media contact before cooperating.[44] This brought international press attention to both *The Puzzle Palace* and to the Friedman papers.[45]

There were now similar fears over Hagelin's papers. In 1982, Hagelin was living in Switzerland and about to turn 90. To celebrate, he visited Sweden where he became ill. His family feared that the hospitalized Hagelin would die in Sweden – where the enterprising Swedes might try to impose back tax and uncover the details of his estate. It was unlikely that details of his relations with US and German intelligence would have been disclosed by the Swedes, since Swedish intelligence were active recipients of Rubicon successes. Nonetheless, he was moved back to the sanctuary of Switzerland at the first possibility. Hagelin had long retired at this point, but with the recent release of Bamford's *Puzzle Palace* nothing could be left to chance. Hagelin had a number of documents as well as photos demonstrating the length of the relationship since his retirement.[46] Facilitated by his second wife, the CIA was able to weed out any incriminating files before inquisitive researchers accessed them and confirmed the conclusions made from the Friedman collection. The relating documents to the history of Rubicon and the partnership were packed up and shipped to Langley for storage.[47]

## Public Key Cryptography and the Growth of Consumer Knowledge

The 1970s experienced a growth in the amount of people researching cryptography. Alongside a general explosion of work on computing, academics across universities in many countries, including some of the advancing states across the Global South were designing new forms of both offensive and defensive measures. Where a few governments had once held the monopoly over such research – and had actively discouraged others - they were now challenged.[48]

The most important driver were path-breaking American scientists. Chief among them were Whitfield Diffie, Martin Hellman, and Ralph Merkle – remarkable American mathematicians – who were teaching their techniques publicly. Their work on Public Key Cryptography ignited a wave of open university research on subject that the NSA would have preferred to remain closed. These three were nothing less than the "l'enfant terrible of the cryptologic world".[49] There was now a general tendency to ask awkward questions and it was at this point Joerg Spoerndli and Mengia Caflisch, both engineers and designers at Crypto AG, independently tested the company's machines. Spoerndli later informed *The Washington Post* journalist Greg Miller that they displayed remarkably low security considering what the company promised, but added that this was not unusual in commercial machines.[50] Much as Crypto AG engineers discovered the vulnerability, at broadly the same time, customers were beginning to recognise the weaknesses for themselves.

In 1978-9, Egypt presented Rubicon with a stern test. Egypt had been one of Crypto AG's best customers and was also a major intelligence target for the United States. America had failed to anticipate the war with Israel in 1973 and with heightened tensions in the region, sigint was seen as invaluable.[51] The episode coincided with Jimmy Carter's famous Camp David accords and the post-summit negotiations. Crypto AG's new head of the Research and Design department, nicknamed "Mickie", was on a routine trip to Cairo when the Egyptians surprised him with difficult questions about the security of the T-450 machine that Crypto AG had sold them. In his panic, Mickie did the one thing he was warned not to do; he mentioned the existence of the newer CRT-320 machine as an alternative – a device NSA believed to be invulnerable. The questioning startled NSA officers that handled the Rubicon intercepts. Puzzlingly, the Egyptians had been using the old machine for their diplomatic communications at the Camp David summit – "[w]hy would they use it at Camp David if they didn't trust it?" they asked.[52]

Subsequently, NSA demanded that Mickie retract the offer of the CRT-320, substituting an "improved" and NSA modified T-450 that was exploitable. Within Crypto AG controversy erupted over the decision to modify the T-450. The CRT-320 was deemed the superior of the two. Furthermore, Spoerndli had his own secure improvement to the T-450. This left Mickie isolated and to fight alone for the NSA's modified machine, hopefully without confirming suspicions from staff that it was rigged. Against the wishes of his engineers, Mickie took the modified T-450 to Egypt in order to replace the old machines. He contended that it was he who personally built the machine and that it was secure. Moreover, Mickie convinced the Egyptians to buy the modification. Cairo now had a

stronger machine, but it was still exploitable.[53] The US delegation had already figured out Anwar Sadat's bottom line in the negotiations through their personal relationship with the leader.[54] Nevertheless, the detailed intelligence gathered thanks to Rubicon proved "priceless" in the negotiations of the Camp David accords between 1978-9.[55]

The controversy continued at Crypto AG after the purchase by Egypt was finalised. Employees in the design team pressed for greater clarity behind the executive decision not to sell Egypt the new CRT-320. The revolt required the CEO of Crypto AG, Heinz Wagner, to intervene. Rather obliquely, he finally admitted to the design team that Crypto AG's hands were tied behind their backs on the Egyptian crisis. What did this mean? Many concluded that it was a German-imposed solution to the problem, but still the design team were ignorant of the full scale of the operation. They understood there was influence higher up, but were not clear if it was German intelligence or Western intelligence more generally.

Furthermore, the Egypt controversy spilled over into a wider CIA-BND controversy. German intelligence did not see Egypt as a major intelligence target, but a good customer not worth jeopardizing the Crypto AG reputation for. In short, they wanted to sell the new invulnerable machines to Cairo.[56] But Egypt was a top target for the NSA in the Middle East. They were a major part of potential superpower negotiations and were crucial to wider peace in the region.[57] Therefore the BND were told that intelligence from Rubicon was a priority. Although Mickie had initially stoked the controversy in Zug, the CEO Wagner had carried the day. Unwitting staff remained puzzled by the decisions that weakened security the security of their customers. The Egyptians were perhaps less than convinced and began their own independent cryptographic effort by seconding their best mathematicians from Cairo University.[58]

## Insecure Politicians

The growing threat from greater cryptographic knowledge was now partnered by Western politicians who blabbed. In 1979, there was another crisis, this time in Argentina, that posed a risk to the operation. This episode demonstrated how individual agent ability in Crypto AG lent important resilience to the operation. In June, the Argentinian Navy had discovered a plain text attack against their machines. Subsequently, they requested that Heinz Wagner as CEO visit the country to discuss the vulnerability. Wagner feared for his life on this business trip, since the ruling Junta was fighting the "Dirty War" and its atrocities included throwing

protesters from the back of planes.[59] According to Human Rights Watch "[t]he overwhelming majority of those who entered the system of 'disappearances' were never seen again".[60]

Fearful of what awaited him, Wagner instead received a remarkable lesson in local geopolitics during his trip to South America. The Argentinian Navy had discovered the vulnerability, but whether they understood that the US and German intelligence were involved was not clear to Wagner at the time. Once in Buenos Aires, their communications experts demonstrated a successful plain text attack on the Navy's machines and demanded an explanation for the vulnerability. By 1979, plain text attacks were common knowledge – in the cryptologic world. Admittedly, it required 100 characters of known plain text to succeed, but this did not stop it being a serious vulnerability of the machines. Wagner promised a remedy similar to the previous fix offered to Egypt. Yet, what the Argentinian government really wanted from Wagner was his assurance that regional rivals like Chile would not be informed of the vulnerability. Indeed, the Argentinian government wanted to exploit Chilean communications and attempted to secure Wagner's word that their own sigint efforts would not be compromised.[61] Wider questions around why such vulnerability was permitted on a Crypto AG machine had been overlooked. These questions would be revisited in 1982, but it would take the conflict over the Falkland Islands for the issues to be raised with Crypto AG.

With Egypt, Argentina, Yugoslavia and South Africa, it was the same story. Increased customer capability meant that the machines required strengthening. Countries were finding the vulnerabilities too easily. Local geopolitics and the individual charisma of figures like Wagner only sustained the operation so far. The NSA now designed new algorithms for the machines that were still readable, but far stronger that previously designed. Thanks to the investment in Cray supercomputers, the US continued to be able to exploit the vulnerabilities – even though the cost of doing so increased both financially and in terms of the time consumed by processing. [62]

In 1982, Argentina invaded the Falkland Islands. They trusted their upgraded machines throughout the conflict. Puzzlingly, Britain had already broken some of the communications cyphers used by Argentina, yet had not predicted the military assault on the islands. As a result, Ted Rowlands, who had been Minister of State at the Foreign Office until 1979, was furious and let slip in Parliament that the UK had long been scooping Argentinian communications. Rowlands shouted: "as well as trying to read the mind of our enemy, we have been reading its telegrams for many years".[63] (In fact, the Junta had launched its attack at short notice and with little preparation, thus providing GCHQ with few

warning signs.) But by venting his misplaced frustration, Rowlands had not only destroyed Britain's ability to read Argentina's messages, but also the messages of some of those countries that used similar machines, who now took the hint.[64] According to Lawrence Freeman and Virginia Gamba-Stonehouse, the darkness lasted only weeks if not days before American intelligence most likely helped to refill the gap.[65] GCHQ were fully aware that US and German intelligence had rigged the machines.[66] Yet recent investigations published by Bart Jacobs and Crypto Museum have suggested that the UK-US special relationship might not have been strong enough for US intelligence to risk compromising Rubicon and instead GCHQ received help from Europe.[67]

Subsequently, the Dutch Navy came to the rescue and shared its ability to read not only Crypto AG machines, but also Datotek machines used by Argentina. This allowed GCHQ to break the communications themselves.[68] This episode raises wider questions on the extent of the US-UK special relationship and where the lines of intelligence sharing were drawn on agreements, especially on diplomatic material. This was different to the BND, who had reacted quite badly when GCHQ first approached them to become a full partner in Rubicon.[69] Jacobs, in this issue, suggests that GCHQ likely asked both the US and Maximator nations for support, just the Dutch were the first to respond. Meanwhile, the Reagan administration agonised over a conflict between two of its important Cold War allies.[70]

In the wake of the conflict, Argentina demanded an explanation. On this occasion a new employee at Crypto AG was sent to try and remedy the problem. Kjell-Ove Widman "Henry" - codenamed "Athena" by US intelligence – was despatched. Henry was both an excellent cryptologist and a great diplomat. Indeed the CIA considered him to be "the irreplaceable man" at the centre of Rubicon's continued success.[71] Henry visited Argentina and demonstrated how the brilliance in individual relations could smooth over the fact that security flaws had been discovered. Henry explained that there had been a break in security of the voice communications, adding that the analog systems used in these communications were notoriously weak. Fortunately, he added, Crypto AG had now designed an "invulnerable" machine for voice. Or so the smooth Henry allowed the Argentinian's to believe. The bluff worked and Argentina – begrudgingly – bought updated systems from Crypto AG.[72] Henry's poker-face allowed the operation to continue and faced down customer accusations that the machines were rigged.

Yet Rowlands' calamitous comments in the Commons were soon overtaken by even more outrageous White House decisions. In 1986, Ronald Reagan deliberately disclosed that he had irrefutable proof of Libyan government involvement in the La Belle Discotheque

terrorist bombing in West Berlin. Determined to retaliate with military force, he wished to make the strongest case and politics now trumped state secrecy. America's ability to read certain Crypto AG machines was effectively disclosed by President Ronald Reagan in a live media address.

On 5 April 1986, the Berlin nightclub was bombed killing two US service personnel and a Turkish woman. The NSA had decoded orders from Tripoli to East Berlin confirming Libyan involvement. The Reagan administration wanted the world to know who was responsible for the attack and so Reagan disclosed in his presidential address that he had irrefutable proof of the Libyan link. He attempted to suggest vague sources had leaked the messages and orders. It failed to fool the Libyans as they followed strict operational security. Moreover, Reagan had referred to three communications between Tripoli and East Berlin. The first requested that an attack take place on US personnel in Berlin. The second and third messages between them bookended the attack. The day before the attack, Tripoli was informed that it would be carried out the following day. Then after the attack the Libyan People's Bureau confirmed its success. Reagan had disclosed the main points of each communication.[73]

Both the US press and Tripoli understood that Libyan communications had been exploited.[74] The Libyan government used what they believed to be their most secure devices and very few people were aware of the orders. The Libyan's now knew their Crypto AG machines were vulnerable and adapted their communications accordingly. General Bill Odom, as NSA director, was said to have "raised holy hell" at the loss of the Libyan communications.[75] His Daily Log note for 15 April 1986 stressed the loss of traffic and the NSA's inability to answer questions with up to date information on Tripoli.[76] The following month, the President's National Security Adviser, Admiral Poindexter, apologized personally to the British Home Secretary, Douglas Hurd, saying: "after the air raid on Libya, it had been necessary to disclose publicly the broad nature of the intelligence available to the US Government. Admiral Poindexter understood that this had been unwelcome to the agencies concerned, particularly he believed GCHQ. But in his view, it was a price that had to be paid in the circumstances".[77]

Libya was an important customer for Crypto AG. Moreover, they were a remarkably consistent customer as well as a major intelligence target. Other than the loss of Egypt and Iraq in this period, Rubicon continued with success against various Middle East and North African customers who were eventually convinced the security breach was patched up or waited to act on their suspicions. Saudi Arabia, one of the most important targets, did not

even need to be re-assured, but were insistent on cryptographic training.[78] Even so, Reagan's pronouncements caused damage because they were too high profile to be ignored. The President had risked the uncovering of US influence on Crypto AG, hence the high-level apologies to allies. Once more the partners managed to avoid serious damage to the overall Rubicon operation due to the limited evidence of how NSA had exploited the communications.

Henry's determination and individual brilliance was not enough to keep the Egyptians on board. Increasingly confident with the technology, they piled questions upon the Crypto AG team surrounding the design of the machines. In January 1986 Egypt wanted 3000 devices but demanded more information on the encryption.[79] They constantly found problems, which fortunately were superficial to the security of the machine. Henry continuously reassured the Egyptian representatives but to no avail and by the late-1980s the Egyptian government moved supplier.[80] Though a personal loss for Henry, the move supposedly "provided them no more security than did [Crypto AG] equipment" and has raised questions of BND influence once more.[81] Unfortunately, there was the potential for countries that discovered flaws to notify other nations. More than likely, the revelations published in the public domain amplified this distrust.

Reagan's pronouncements about reading Libyan communications were not only dangerous but ironic. They were broadly contemporaneous with a veritable war that had been launched by Bill Odom, together with the Director of the CIA, Bill Casey, against the press on the subject of sigint. The pair significantly advanced the stance taken by Faurer to prevent media attention.[82] Although sigint enjoyed stronger legal protection in terms of its secrecy than other activities, the specific statute - 18USC#798 - was rarely employed. Faurer had approached the Attorney General in order to use USC#798 over Bamford's receipt of Justice Department documents about NSA to no avail.[83] However the discussion of this legal protection held up the publication of Gordon Welchman's *Hut Six Story* from 1975 until 1980 after a tumultuous tussle with GCHQ and NSA.[84]

Initially the Odom-Casey offensive against the press attempted a push-back against specialist intelligence investigation teams within in the media, led by legendary figures like Bob Woodward.[85] Suddenly, during the mid-1980s, editors like Ben Bradlee found themselves directly threatened with the courts for mentioning sigint. Over the winter of 1985, Bradlee agreed to hold publications in *The Washington Post* because the editor was unsure exactly what the Soviet spy Ronald Pelton had revealed to the USSR, in turn earning Bradlee a thank you call from Deputy Secretary of Defense William Howard Taft IV.[86] Odom,

Casey, and Bradlee tussled over publication for months before the intelligence chiefs secured permission to hold USC#798 over the *Post* editor who was duly informed by the DIRNSA.[87] Bradlee was not slow to fire back, identifying other instances where senior members of the Reagan government, including Richard Perle, had blabbed about sigint.[88] In the event, the pressure failed as NBC scooped the *Post* and sidelined the agencies on the Pelton coverage. Casey's targeting sights then shifted towards NBC with President Reagan in ironic support after his garrulous Libya episode only a month before. It was all in vain, for fears of a Pentagon Papers 2.0 and enhanced First Amendment rights melted away and Odom and Casey's war footing proved an over-reaction.[89]

## Hydra – Crypto AG's Whistleblower

On 3 December 1995, American journalists Scott Shane and Tom Bowman published the first in their remarkable series on the NSA: "No Such Agency" in *The Baltimore Sun.* The series of stories was named after the running joke in the community about what NSA really stood for.[90] The programme was the first major investigative work into the intelligence activities of the NSA since the publication of James Bamford's groundbreaking book *The Puzzle Palace* more than a decade before. On 10 December 1995, their story "Rigging the Game" was published as part of the series. Within the pages of *The Baltimore Sun*, Shane and Bowman had demonstrated that the likely collaboration Bamford uncovered for *Puzzle Palace* had become an official NSA operation – and they had evidence. *The Baltimore Sun* published an abstract from a document that provided evidence that NSA's Nora Mackabee had been present at design meetings for Crypto AG alongside other operatives and advisers from Motorola. Collaboration and proof of attempted US influence was now in ink, yet, quite remarkably, Rubicon continued to succeed for years afterwards.[91] Interestingly, in 2016, historian Craig Bauer argued that the document Shane provided as evidence of the NSA's work with Crypto AG was difficult to explain away and was one for which "Crypto AG has not provided any alternative explanation".[92]

The revelations in *The Baltimore Sun* formed the pinnacle of what was codenamed the "Hydra-affair". Though CIA influence at Crypto AG continued – indeed intensified - it spurred the end of an illustrious partnership between US and German intelligence when the US bought the German share of the company.[93] Hydra was the greatest threat to the security of Rubicon because it presented legal action and therefore drew concerted

attention from Swiss and American press. Hydra revolved around the unfortunate arrest of Crypto AG salesman Hans Bühler on a routine sales trip to Iran. In the same year French authorities were looking to extradite Iranian Zayal Sarhadi who was accused of the assassination of Shapour Baktiar, a former Iranian Prime Minister, in France. According to the CIA assessment, Iran required a Swiss citizen in order to spur a prisoner exchange and Bühler simply fitted the bill. Because of his sales of cryptographic machinery, it was easy to accuse him of trying to work contacts as a spy, but it is likely that Teheran was still oblivious to Crypto AG as a CIA proxy. Sales of cryptographic machinery meant liaison with leading military officials in Iran to convince and conduct the purchases.[94] Furthermore, Crypto AG offered training on the machinery and therefore paid expenses for some Iranian citizens to visit Switzerland – so he could easily be accused of bribing officials.[95] Once arrested, Iranian intelligence accused him of rigging the machines that he was selling – and it was an accusation that started to take hold in his mind. Bühler had been unwitting of the influence, but now he had his suspicions.[96]

Released in 1993 after the BND paid his bail, Bühler started reaching out to Swiss press. An unknown "journalist" caught his attention and informed him that there was something going on at Crypto AG and to get in touch. The mystery man was no journalist, but former employee Peter Frutiger who was fired from Crypto AG for ensuring additional and effective security of products he designed for Syria – against company policy. Disaffected and having always been suspicious of German and US interference at Crypto AG, Frutiger became a risk to Rubicon.[97] Swiss Military Intelligence knew that Frutiger's charges were correct, but decided to look the other way. It was no wonder that during the Hydra affair, the Swiss Ministry of Justice were not surprised and ready to aid the firm.[98]

In the press, Bühler accused Crypto AG of not supporting him sufficiently and of demanding he repay his bail. At Crypto AG, Michael Grupe, the CEO, handled the affair poorly; he believed shock therapy was the way forward and fired Bühler - to the amazement and fury of the other partners. They believed that something had to be done, but it was safer he remained an employee of Crypto AG first, partly because he could be bound to confidentiality as an employee. Bühler was now on the attack. Initially, Bühler demanded a payment of Sfr 2.5 million to settle his subsequent dismissal lawsuit out of court. Though Grupe wanted a quick settlement, he offered only Sfr 250,000 – a tenth of the original demand. The security problem was inching its way towards the courts where increased attention and the requirement to provide evidence to dispute the damaging claims that he made.

Tensions rose at Crypto AG and between the partners. With no evidence found by Swiss intelligence or Federal Police to take the matter to court, Bühler relented and decided to settle. On 15 November 1993, Bühler called Grupe to inform him he would settle for the original Crypto AG offer of Sfr 250,000. But foolishly, Grupe failed to include a standard confidentiality clause and now had a whistleblower on his hands. Crypto AG had to navigate a book by investigative journalist Res Strehle on the Bühler affair, a subsequent documentary, and then a court case raised against Bühler to restrain his accusations.

To their horror, the CIA learned that Bühler was to star in a TV documentary around the time the book would be released. It was feared that this simultaneous exposure would cause too much damage without some push back from Crypto AG. Therefore, Grupe, without notifying the partners, accepted an interview invitation for the TV documentary. The documentary played on Swiss and Austrian Television and allowed Grupe to meet the accusations head on. On 23 March 1994, Bühler appeared on television to make his claims against the interference of Crypto AG products. A spooky masked-out Peter Frutiger joined him. They pressed their case for the long-standing German BND ownership in Crypto AG. The programme also asserted that new technology was coming from a US Government Electronics Division in Arizona – without directly mentioning the witting involvement of Motorola.

Amazingly, Grupe responded confidently by dismissing them as disgruntled former employees. He then moved on to state that the claims of German interference were insane, pointing out that the company sold in Germany – as well as Switzerland. The latter, he added, had cleared the machines through their investigations. Moreover, the accusations inferring visits from other intelligence agencies were clearly exaggerated "nonsense". Grupe's interview was a masterpiece of gentle skepticism and had done enough to cast doubts on the accusations made by former employees and had provided substantial reasoning for the evidence provided in the accusations. The CIA were stunned and concluded that his "performance was credible, and may have saved the program[me]".[99]

But Bühler did not relent. He continued to publicise his accusations. A German magazine, *Focus,* picked up the story and published the claims. Employees started to leave or openly complained at work. On several occasions Grupe intervened and denied the accusations to the workforce directly.[100] Worse for the company, their customers soon picked up on a number of allegations and the fact that people were leaving the company.[101] The Argentine Navy threatened to buy their products elsewhere unless they were convinced otherwise, putting their next order under government review. Egypt's renewed faith was

shaken. Even the hitherto credulous Saudi Arabia briefly halted all orders pending clarification.[102] Yet the Iranian government continued with their order of Crypto AG machines almost immediately after the accusation with little fuss.[103]

On the 15 July 1994, the company had enough and again went on the offensive. Lawyers at Crypto AG filed papers to halt Bühler's accusations. A restraining order was created, but it was a temporary fix.[104] The company would be required to take the measures to court if they wanted it to become permanent. The outcome depended on the police findings. If they uncovered interference or foreign intelligence ownership – it would be the end of the company. If the police found nothing incriminating then the company might be able to silence the critics and restore confidence in their products from suspicious customers. It was a risk to take the matter to court, but one that allowed the company to succeed.

Bühler's main corroborator for his accusations was Frutiger. Fortunately for Crypto AG his testimony unraveled before it went to court. Frutiger's suspicion allowed him to correctly name and link members of the NSA to Crypto AG. Furthermore, he stated that the company refused to use his algorithms, instead preferring those supplied by German and American intelligence. Yet, when he was asked to provide proof of the external influence, all he offered was an innocuous letter dated in 1976 from an NSA cryptanalyst to Boris Hagelin. It proved only that someone in NSA knew Hagelin well enough to correspond with him – the passage of time had meant it was impossible to discern anything from the letter about the relationship.[105] Bühler now broke the regulations of the temporary restraining order and spoke to Scott Shane from *The Baltimore Sun* and settled days before proceedings were set to start.[106]

Forensically, Shane gathered enough information and evidence to publish the story in the *Sun*. On 10 December 1995 the Crypto AG story was released. The article included several testimonies from former employees that talked about suspicious circumstances in the design room. Some engineers, including Spoerndli, recalled being mysteriously ordered to change the algorithms for no apparent reason. Others including contractors from Motorola recalled working with Nora Mackabee on the design team at Crypto AG.[107]

Publicly, both NSA and Crypto AG remained quiet.[108] Privately, DIRNSA Vice Admiral John M. "Mike" McConnell issued an all staff memo that reminded his staff that they "can neither confirm nor deny" any questions that are related to supposed revelations by the media. This included conversations in passing with friends, family, and neighbours who might be aware of their association to Fort Meade. Moreover, it reminded them of the

secrecy oath they took when they enlisted – military or civilian – into the NSA.[109] It was not proof of the story, but demonstrated that the series had struck a chord on the Seventh Floor.[110] Hydra, from Bühler's arrest in Iran through to the aftermath of Shane's publication, was the most serious security threat that Rubicon experienced. The aftershocks of the affair continued to be felt by the partners and in the company long after the breach had been remedied. Yet even after the security issues raised by the affair the company continued to sell its commercial crypto products to target states of the US and German intelligence agencies. Remarkably, Iran as well as other nations, continued to buy Crypto AG products after the affair had receded.

## Conclusion

Each of these four episodes threatened the success of Operation Rubicon. The individual CIA-BND brilliance of those involved initially allowed the wool to be pulled over the eyes of both customers and employees of the firm, who clearly suspected outside interference in the engineering of the cryptologic devices. A small number of eloquent and convincing personnel encouraged the continued purchase of equipment from priority states during the Cold War such as Libya, Iran, Argentina, and Egypt. Rubicon often hung by a knife-edge, requiring a remarkable fusion of humint and sigint capabilities, together with remarkably close liaison between the CIA and BND of a kind that only a few partner services were capable of. As a reward it allowed great insight into the operations and strategy of target states across the Global South at a time of mounting concern about terrorism. There were also traditional diplomatic triumphs, it was likely that through the use of these machines the US secured the Camp David talks, uncovered Koreagate, and identified the culprits of the La Belle discotheque bombing in 1986. Furthermore, it offered deep insights into the Falklands and the Iran-Iraq war, respectively.

Yet as diplomatic historians have increasingly argued, the Cold War was a complex conflict. Accordingly, many of the targets of Operation Rubicon had other priorities than the outcome of the "global" Cold War and were not especially concerned about the predations of the NSA upon their traffic. While often serving as proxies in this conflict, and while the battles might have been fought in Africa, Asia, and Latin America – what American or German intelligence might be able to read were not always of the greatest concern of these nations. It was regional considerations that were priorities, such as Argentina's territorial disputes with Chile, or India's frictions with Pakistan. It was not necessarily a concern if the NSA or the BND could read diplomatic and military communications with their multi-billion-

dollar sigint budget, so long as their local geopolitical rivals could not exploit them. With their smaller budgets, indigenous cryptology was rarely possible or affordable and to the most part "secure" equipment that Crypto AG provided was enticing despite periodic security lapses. Oddly then, Crypto AG provided many states across the Global South with comprehensive communications security "of a kind", which was not unimportant. Meanwhile there are still many gaps in the history of Rubicon. They require much time and many FOIA requests before a rigorous assessment of Rubicon can be made, but for now we can conclude that this was an operation of some significance.


## Acknowledgements

The author would like to extend particular thanks to Richard J. Aldrich, Sarah Mainwaring and Melina Dobson for their comments and advice on earlier drafts of this article. Particular thanks also go to the editors of the Intelligence and National Security involved with this special section. This paper is a result of an Institute of Advanced Studies Early Career Fellowship at the University of Warwick. It would not have been possible without the dedicated team of journalists who worked to bring the knowledge of Operation Rubicon to the public. This includes Peter F. Müller, David Ridd and the ZDF team for its pioneering research. Also Nicole Vögele and Fiona Endres at SRF in Switzerland and Greg Miller in Washington. Thank you to colleagues, friends, and family for their comments on drafts and to Richard Aldrich for bringing this special section together.

**Disclosure**

No conflict of interest was reported by the author


## Notes on contributor


Jason Dymydiuk is currently an Early Career Fellow at the Institute of Advanced Studies, University of Warwick. He has recently completed his ESRC funded PhD in collaboration the International Spy Museum focused on GCHQ, NSA, and investigative journalism.

## Bibliography:


Aid, Mathew M. “All Glory is Fleeting: Sigint and the Fight Against International Terrorism.” *Intelligence and National Security* 18, no.4 (2003): 72-120.

Aid, Mathew M. *Secret Sentry: The Untold History of the National Security Agency*. London: Bloomsbury, 2010.

Aldrich, Richard. *GCHQ* 2nd edition. London: William Collins, 2019.

Andrew, Christopher. "British Intelligence and the Breach with Russia in 1927." *The Historical Journal* 25, no.4 (1982): 957-964.

Ball, Desmond, and Robert Windrem. “Soviet Signals Intelligence (Sigint): Organization and management.” *Intelligence and National Security* 4, no.4 (1989): 621-659.

Bamford, James. *The Puzzle Palace: A Report on America’s Most Secret Agency.* New York: Houghton Mifflin Company, 2009.

Bamford, James. “The NSA and Me”, *The Intercept* [Online], October 2, 2014, URL: https://theintercept.com/2014/10/02/the-nsa-and-me/ Accessed: 12/09/16.

Barrett, David M. “Secrecy, Security, and Sex: The NSA, Congress, and the Martin–Mitchell Defections.” *International Journal of Intelligence and Counter Intelligence* 22, no.4 (2009): 699-729.

Black, Ian. “CIA Spills Camp David Secrets on 1978 Egyptian-Israeli agreement”, *The Guardian* [Online], URL https://www.theguardian.com/world/on-the-middle-east/2013/nov/15/egypt-israel-carter-cia Accessed: 20/03/2020.

Bradlee, Ben. *A Good Life: Newspapering and Other Adventures*. New York: Simon and Shuster, 1995.

BBC, “Grim Account of Argentine Deaths”, *BBC News Online*, January 20, 2005, URL: http://news.bbc.co.uk/1/hi/world/americas/4193341.stm Accessed: 01/05/2020.

Bauer, Craig. *Secret History: The Story of Cryptology.* Boca Raton: CRC Press, 2013.

Central Intelligence Agency. Aaron Epstein, “Reagan moves war on in war against leaks”, *Miami Herald*, 25 May 1986’, General CIA Records, CREST, NARA.

Central Intelligence Agency. “He Wrote about the Puzzle Palace and the US would rather he Hadn’t, *Boston Globe*” 15 March 1982, General CIA Records, CREST, NARA.

Central Intelligence Agency. “Letter: Admiral B. R. Inman to Attorney General Benjamin R. Civiletti”, August 20, 1979, General CIA Records, CREST, NARA.

Central Intelligence Agency. “Letter: General Lincoln Faurer to Attorney General William French Smith”, April 3, 1981, General CIA Records, CREST, NARA.

Central Intelligence Agency, “Memorandum for the record: Staff meeting minutes of 7 September 1983”, September 7, 1982, General CIA Records, CREST, NARA.

Central Intelligence Agency. *MINERVA: A History*, Internal CIA document, 2004.

Central Intelligence Agency. "NSA Chief takes aim at leakers", September 3, 1987, General CIA Records, CREST, NARA.

Central Intelligence Agency. "President Carter and the Role of Intelligence I the Camp David Accords", *CREST*, November 2013, URL: https://www.cia.gov/library/readingroom/collection/carter-camp-david-accords Accessed: 20/03/2020

Central Intelligence Agency. "The Puzzle Palace: Archives and National Security", July 1983, General CIA Records, CREST, NARA.

Clark, Ronald. *The Man Who Broke Purple: The Life of the Worlds Greatest Cryptologist Colonel William F. Friedman.* London: Weidenfeld and Nicolson, 1977.

Crypto Museum. "Operation RUBICON (THESAURUS): The secret purchase of Crypto AG by BND and CIA", *Crypto Museum* [oniline], April 25, 2020, URL: https://www.cryptomuseum.com/intel/cia/rubicon.htm#ref_9 Accessed: 30/04/2020.

Freedman, Lawrence and Virginia Gamba-Stonehouse. *Signals of War: The Falklands Conflict of 1982.* London: Faber and Faber, 1990.

Green, June L. (Judge) "Opinion", *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL: https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

Harper, Lauren. "Unredacted: President Carter Reflects on the Camp David Accords", *National Security Archive*, November 15, 2013, URL: https://unredacted.com/2013/11/15/president-carter-reflects-on-the-camp-david-accords/ Accessed: 20/03/2020.

Hayden, Michael. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.

Horowitz, David. "US Electronic Espionage: A Memoir." *Ramparts*, 11, no 2, (1927): 35-50.

Human Rights Watch. *Truth and Partial Justice in Argentina: an update*, April 1991, URL: https://www.hrw.org/sites/default/files/reports/argen914full.pdf Accessed: 01/05/2020.

Jacobs, Bart. "Maximator: European signals intelligence cooperation, from a Dutch perspective." *Intelligence and National* Security, April 7, 2020, 1-10.

Kahn, David. "Cryptology Goes Public." *Foreign Affairs* 58, no.1 (1979): 141-159.

Kalugin, Oleg. *Spymaster*, London: Smyth Gryphon, 2009.

Keefe, Patrick Radden. *Chatter: Dispatches from the secret world of global eavesdropping.* New York: Random House, 2005.

Los Angeles Times. “A Distrust of Freedom”, *LA Times*, May 9, 1983, 6.

Miller, Greg. “Intelligence Coup of the Century”, *Washington Post* [online], February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
Accessed: 11/02/2020.

Miller, Greg. “Uncovering The CIA’s Audacious Operation that Gave Them Access to State Secrets: Interviewed by Dave Davis “, *National Public Radio*, March 5, 2020, Accessed: 05/03/2020.

Miller, Judith. “Agency Demand Documents Back.” *New York Times*, 14 March 1982, 19.

Moran, Christopher. *Classified: Secrecy and the State in Modern Britain*. Cambridge: Cambridge University press, 2013.

New York Times. “Transcript of Address by Reagan on Libya.” *New York Times*, 15 April 1986, 10.

Norton Taylor, Richard and Dominic Rusche, “Ex-MI6 deputy chief plays down damage caused by Snowden leaks”, *Guardian* [online], September 12, 2013, URL: https://www.theguardian.com/world/2013/sep/12/mi6-plays-down-damage-edward-snowden-leaks Accessed: 30/04/2020.

Odom Papers. Folder: Daily Activity Log 1985 September-December, Box 25, Library of Congress.

Odom Papers. Folder: Daily Activity Log January-June 1986, Box 25, Library of Congress.

Odom Papers. Folder: Daily Activity Log July-December 1986, Box 25, Library of Congress.

Pozen, David E. “Deep secrecy.” *Stanford Law Review*, 62, no 1 (2009): 257-339.

Priess, David. *The President’s Book of Secrets: The Untold Story of Intelligence Briefings to America’s Presidents from Kennedy to Obama*. New York: Public Affairs, 2016.

Reynolds, David. *Summits: Six Meetings that Shaped the Twentieth Century*. London: Allen Lane, 2007.

Ronald Reagan Presidential Library. “Letter from William J. Casey (Director CIA) to David A. Stockman”, February 19th 1982, Folder: ND006(Intelligence)[2of5], Box ND006(028182-069838), WHORM Files, RRPL.

Ronald Reagan Presidential Library. “William H. Taft IV to David A. Stockman”, March 8, 1982, Folder: ND006 (Intelligence)[2of5], Box ND006(028182-069838), WHORM Files, RRPL.

Rowlands, Ted. “Falkland Islands”, April 3, 1982, Volume 21, Column 650, URL: https://api.parliament.uk/historic-hansard/commons/1982/apr/03/falkland-islands Accessed: 09/08/2019.

Schumacher, Edward. “The United States and Libya.” *Foreign Affairs*, 65, no.2 (1986): 329-348.

Shane, Scott. “No Such Agency”, in Frederic B. Hill and Stephens Broening (eds), *The Life Of Kings: The Baltimore Sun and The Golden Age of the American Newspaper*. Lanham: Rowman and Littlefield, 2016.

Shane, Scott and Tom Bowman. “Rigging The Game”, *Baltimore Sun*, December 10, 1995.

Shane, Scott, and Tom Bowman. ““No Such Agency”; Secretive NSA: Obscure, global eavesdropper at Fort Meade is largest state employer”, *Baltimore Sun,* 3 December 1995, 1.

Shane, Scott and Tom Bowman. “Busy Signals at NSA: Agency of spies keeps code of silence with few clear lines”, *Baltimore Sun*, 24 December 1995, 1.

Simcox, Robin. *Surveillance after Snowden: Effective Espionage in an Age of Transparency.* London: Henry Jackson Society, 2015.

Sims, Calvin. “Argentine Tells of Dumping “Dirty War” Captives Into Sea”, *New York Times*, 13 March 1995, 1.

Stocker, Ed. “Top-secret files shed new light on Argentina’s “Dirty War”, *Independent [Online]*, URL: https://www.independent.co.uk/news/world/americas/top-secret-files-shed-new-light-on-argentina-s-dirty-war-8923307.html Accessed: 05/04/2020.

Taubman, Philip. “Security Agency Bars Access to Nonsecret Material, library records show”, *New York Times*, April 28, 1983, 18.

Taubman, Philip. “Sons of the Black Chamber”, *New York Times: Book Review*, September 19, 1982, 9.

Welchman, Gordon. “How I came to write *The Hut Six* story.” *Intelligence and National Security*, 33, no.1 (2018): 139-144.

Whitehead, Tom. ‘GCHQ leaks have “gifted” terrorists ability to “attack at will”, warns spy chief’, *Telegraph* [Online], October 9, 2013, URL: https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10365026/GCHQ-leaks-have-gifted-terrorists-ability-to-attack-at-will-warns-spy-chief.html Accessed: 30/04/2020.

Woodward, Bob and Patrick Tyler, “Libyan Cables Intercepted and Decoded”, *Washington Post*, April 15, 1986, p. 1.

Woodward, Bob. *Veil: The Secret Wars of the CIA 1981-1987.* New York: Simon and Schuster, 2005.

[1] Entry for 6 Nov 1986, Folder: Daily Activity Log January-June 1986, Box 25, Odom Papers, Library of Congress.
[2] Scott Shane & Tom Bowman, ‘Rigging The Game’, *Baltimore Sun*, 10 December 1995, p. 1.
[3] CIA ‘MINERVA: A History’, 2004: 41; Greg Miller, ‘Intelligence Coup of the Century’, *Washington Post* [online], 11 February 2020, URL:

https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
Accessed: 11/02/2020.

[4] According to the Crytologic Museum, recently revealed BND documents have confirmed that Mils Electronic was also under the influence of the BND in a similar fashion to Crypto AG and Datotek had its machines ciphers broken by the Dutch Navy at least for 1982. See: Crypto Museum, 'Operation RUBICON (THESAURUS): The secret purchase of Crypto AG by BND and CIA', *Crypto Museum* [online], April 25, 2020, URL: https://www.cryptomuseum.com/intel/cia/rubicon.htm#ref_9 Accessed: 30/04/2020.

[5] CIA, MINERVA, 95.

[6] Kahn, 'Cryptology Goes Public', 141-3; Aid, 'All Glory is Fleeting', 103-4.

[7] Andrew, 'British Intelligence and the Breach with Russia in 1927', 957-964.

[8] Dymydiuk, 'Filling the Information Void', PhD. Warwick 2020.

[9] Tom Whitehead, 'GCHQ leaks have "gifted" terrorists ability to "attack at will", warns spy chief', *Telegraph* [Online], October 9, 2013, URL: https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10365026/GCHQ-leaks-have-gifted-terrorists-ability-to-attack-at-will-warns-spy-chief.html Accessed: 30/04/2020; Richard Norton Taylor and Dominic Rusche, 'Ex-MI6 deputy chief plays down damage caused by Snowden leaks', *Guardian* [online], September 12, 2013, URL: https://www.theguardian.com/world/2013/sep/12/mi6-plays-down-damage-edward-snowden-leaks Accessed: 30/04/2020; Simcox, *Surveillance after Snowden*, 55-60

[10] Kahn, 'Crytology Goes Public', 143.

[11] Pozen, 'Deep secrecy', 257. Furthermore, the Soviet Union likely had significant knowledge of US success in breaking the communications of Global South countries prior to Rubicon thanks to Martin and Mitchell, see: Bamford, *Puzzle Palace*, 190. It was likely reinforced by Kalugin's unnamed mole in the mid-1960s, See: Kalugin, *Spymaster*, 90, and the overstated revelations of Perry Fellwock in 1971, see: Horowitz, 'US Electronic Espionage: A memoir', 35-50.

[12] Bamford, *Puzzle Palace*, 190; Kalugin, *Spymaster*, 90; Horowitz, 'Electronic Espionage: A Memoir', 35-50; Aid, *Secret Sentry*, 184.

[13] Ball and Windrem, 'Soviet Signals Intelligence', 621.

[14] Private information.

[15] Moran, *Classified*, 4.

[16] Clark, *The Man Who Broke Purple,* x; Bamford, *Puzzle Palace*.

[17] Shane and Bowman, 'Rigging the Game', 1.

[18] The defection of Martin and Mitchell in 1960 in might also be considered, but they do not seem to have referred to this operation specifically, see Barrett, 'Secrecy, Security, and Sex'

[19] Clark, *The Man Who Broke Purple*, 193 & 196.

[20] CIA, MINERVA, 15-16.

[21] Clark, *The Man Who Broke Purple*, 186.

[22] CIA, MINERVA, 26-31; Bamford, *The Puzzle Palace*, 408-10.

[23] Clark, *The Man Who Broke Purple,* 198.

[24] Clark, *The Man Who Broke Purple,* 204.

[25] June L. Green (Judge) 'Opinion', *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL: https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

[26] CIA, MINERVA, 64; June L. Green (Judge) 'Opinion', *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL:

https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

[27] CIA, MINERVA, 64.

[28] Clark, *The Man Who Broke Purple,* x; Bamford, *Puzzle Palace*, 408-10; MINERVA, 64-65.

[29] In fact, US intelligence was focused on a simultaneous event in Hungary and failed to spot the massive pre-Suez mobilisation, Aldrich, *GCHQ*, 2nd edition, 149.

[30] Clark, *The Man Who Broke Purple,* 188-90

[31] CIA, MINERVA, 65; Clark, *The Man Who Broke Purple,* x.

[32] Author Interview: James Bamford, May 17, 2017, Washington DC; Judge June Green, 'Opinion', *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL: https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

[33] Bamford, *The Puzzle Palace*; Bamford, 'The NSA and Me', *The Intercept* [Online], October 2, 2014, URL: https://theintercept.com/2014/10/02/the-nsa-and-me/ Accessed: 12/09/16

[34] 'The Puzzle Palace: Archives and National Security', July 1983, General CIA Records, CREST, NARA; June L. Green (Judge), 'Opinion', *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL: https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

[35] Author Interview: James Bamford, May 17, 2017, Washington DC; 'The NSA and Me', *The Intercept* [Online], October 2, 2014, URL: https://theintercept.com/2014/10/02/the-nsa-and-me/ Accessed: 12/09/16; MINERVA.

[36] Bamford, *Puzzle Palace*, 406.

[37] Bamford, *Puzzle Palace*, 409.

[38] Bamford, *Puzzle Palace*, 410.

[39] CIA, MINERVA, 65-66.

[40] Author Interview: James Bamford, May 17, 2017, Washington DC; 'The NSA and Me', *The Intercept* [Online], October 2, 2014, URL: https://theintercept.com/2014/10/02/the-nsa-and-me/ Accessed: 12/09/16.

[41] 'Letter: Admiral B. R. Inman to Attorney General Benjamin R. Civiletti', August 20, 1979, General CIA Records, CREST; 'Letter: General Lincoln Faurer to Attorney General William French Smith', April 3, 1981, General CIA Records, CREST.

[42] June L. Green (Judge), 'Opinion', *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL: https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

[43] June L. Green (Judge), 'Opinion', *American Library Association et al V Lincoln Faurer, Director, National Security Agency*, March 27, 1986, URL: https://www.courtlistener.com/opinion/1958973/american-library-assn-v-faurer/ Accessed: 29/8/2019.

[44] 'Letter from William J. Casey (Director CIA) to David A. Stockman', February 19th 1982, Folder: ND006(Intelligence)[2of5], Box ND006(028182-069838), WHORM Files, RRPL; 'William H. Taft IV to David A. Stockman', March 8, 1982, Folder: ND006(Intelligence)[2of5], Box ND006(028182-069838), WHORM Files, RRPL.

[45] Philip Taubman, 'Security Agency Bars Access to Nonsecret Material, library records show', *New York Times*, April 28, 1983, 18; Philip Taubman, 'Sons of the Black Chamber', *New York Times: Book Review*, September 19, 1982, 9; 'The Puzzle Palace: Archives and national Security', July 1983, General CIA Records, CREST; 'He Wrote about the Puzzle Palace and the US would rather he Hadn't, *Boston Globe*' March 15, 1982, General CIA Records, CREST;

Judith Miller, 'Agency Demand Documents Back', *New York Times*, March 14, 1982, 19; Los Angeles Times, 'A Distrust of Freedom', *LA Times*, May 9, 1983, 6.
[46] CIA, MINERVA, 70.
[47] CIA< MINERVA, 71.
[48] Kahn, 'Cryptology Goes Public', 143; Bauer, *Secret History: The Story of Cryptology*, 414-421. Bauer includes documentation between the Institute of Electrical and Electronics Engineers and the NSA regarding academic work and the export controls on cryptographic research.
[49] Bauer, *Secret History: The Story of Cryptology,* 404; MINERVA, 60.
[50] Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.
[51] Greg Miller, 'Uncovering The CIA's Audacious Operation that Gave Them Access to State Secrets: Interviewed by Dave Davis ', *National Public Radio*, March 5, 2020, Accessed: 05/03/2020; Priess, *The President's Book of Secrets: The Untold Story of Intelligence Briefings to America's Presidents from Kennedy to Obama*, 81-3. & 107.
[52] CIA, MINERVA, 54.
[53] CIA, MINERVA, 54.
[54] Reynolds, *Summits*, 315.
[55] CIA, MINERVA, 57.
[56] CIA, MINERVA, 54.
[57] See: CIA, 'President Carter and the Role of Intelligence I the Camp David Accords', *CREST*, November 2013, URL: https://www.cia.gov/library/readingroom/collection/carter-camp-david-accords Accessed: 20/03/2020; Lauren Harper, 'Unredacted: President Carter Reflects on the Camp David Accords', *National Security Archive*, November 15, 2013, URL: https://unredacted.com/2013/11/15/president-carter-reflects-on-the-camp-david-accords/ Accessed: 20/03/2020; Ian Black, 'CIA Spills Camp David Secrets on 1978 Egytian-Israeli agreement', *The Guardian* [Online], URL https://www.theguardian.com/world/on-the-middle-east/2013/nov/15/egypt-israel-carter-cia Accessed: 20/03/2020.
[58] Private information.
[59] Ed Stocker, 'Top-secret files shed new light on Argentina's "Dirty War", *Independent [Online]*, URL: https://www.independent.co.uk/news/world/americas/top-secret-files-shed-new-light-on-argentina-s-dirty-war-8923307.html Accessed: 05/04/2020.
[60] Human Rights Watch, *Truth and Partial Justice in Argentina: an update*, April 1991, URL: https://www.hrw.org/sites/default/files/reports/argen914full.pdf Accessed: 01/05/2020 p. 6; BBC, 'Grim Account of Argentine Deaths', *BBC News Online*, January 20, 2005, URL: http://news.bbc.co.uk/1/hi/world/americas/4193341.stm Accessed: 01/05/2020; Calvin Sims, 'Argentine Tells of Dumping "Dirty War" Captives Into Sea', *New York Times*, March 13, 1995, 1.
[61] CIA, MINERVA, 61.
[62] Bamford, *Puzzle Palace*, 137-9; MINERVA, 55.
[63] Ted Rowlands, 'Falkland Islands', April 3, 1982, Volume 21, Column 650, URL: https://api.parliament.uk/historic-hansard/commons/1982/apr/03/falkland-islands Accessed: 09/08/2019.
[64] Freedman and Gamba-Stonehouse, *Signals of War*, 131.
[65] Ibid. 131.
[66] CIA, MINERVA, 43.
[67] Jacobs, 'Maximator', 5; Crypto Museum, 'Operation RUBICON (THESAURUS): The secret purchase of Crypto AG by BND and CIA', *Crypto Museum* [oniline], April 25, 2020, URL: https://www.cryptomuseum.com/intel/cia/rubicon.htm#ref_9 Accessed: 30/04/2020.

[68] Jacobs, 5.
[69] CIA, MINERVA, 43.
[70] Jacobs, 8; Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.
[71] Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.
[72] CIA, MINERVA, 69.
[73] New York Times, 'Transcript of Address by Reagan on Libya', *New York Times*, April 15, 1986, p. 10.
[74] Bob Woodward and Patrick Tyler, 'Libyan Cables Intercepted and Decoded', *Washington Post*, April 15, 1986, p. 1.
[75] Keefe, *Chatter,* 211.
[76] '15 April 1986', Folder: Daily Activity Log January-June 1986, Box 25, Odom Papers, Library of Congress.
[77] Douglas Hurd, meeting with Admiral Poindexter, 28 May 1986, HO HO325/757, UK TNA.
[78] CIA, MINERVA, 62, 69, 75; Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.
[79] Entry for 28 January 1986, Folder: Daily Activity Log 1986 January-June, Box 25, Odom Papers, Library of Congress
[80] CIA, MINERVA, 69.
[81] Crypto Museum, 'RUBICON (THESAURUS)'.
[82] Dymydiuk, 'Filling the Information Void', PhD, Warwick, 2020.
[83] 'Letter: General Lincoln Faurer to Attorney General William French Smith', April 3, 1981, General CIA Records, CREST, NARA.
[84] Welchman, 'How I came to write *The Hut Six* story', 139-144.
[85] 'Memorandum for the record: Staff meeting minutes of 7 September 1983', September 7, 1982, General CIA Records, CREST, NARA.
[86] Entry for 5 December 1985, Folder: Daily Activity Log 1985 September-December, Box 25, Odom Papers, Library of Congress; Woodward, *Veil*, 253.
[87] Entry for 6 May 1986, Folder: Daily Activity Log 1986 January-June, Box 25, Odom Papers, Library of Congress.
[88] Bradlee, *A Good Life*, 273.
[89] 'NSA Chief takes aim at leakers', September 3, 1987, General CIA Records, CREST, NARA; 'Aaron Epstein, "Reagan moves war on in war against leaks", *Miami Herald*, 25 May 1986', General CIA Records, CREST, NARA; Woodward, *Veil*, 469.
[90] Scott Shane, and Tom Bowman, '"No Such Agency"; Secretive NSA: Obscure, global eavesdropper at Fort Meade is largest state employer', *Baltimore Sun,* December 3, 1995, 1.
[91] Shane and Bowman, 'Rigging the Game'.
[92] Bauer, *Secret History*, 356.
[93] CIA, MINERVA, 93; for more information on the divorce see M. Dobson in this issue.
[94] CIA, MINERVA, 80.
[95] Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.
[96] Shane and Bowman, 'Rigging the Game'.

[97] Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.; MINERVA.
[98] CIA, MINERVA, 84.
[99] CIA, MINERVA, 84-85.
[100] CIA, MINERVA, 85.
[101] Shane and Bowman, 'Rigging the Game'.
[102] CIA, MINERVA, 85.
[103] Shane and Bowman, 'Rigging the Game'; Greg Miller, 'The Intelligence Coup of the Century', *Washington Post*, February 11, 2020, URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ Accessed: 11/02/2020.
[104] Shane and Bowman, 'Rigging the Game'.
[105] CIA, MINERVA, 87.
[106] CIA, MINERVA, 89; Shane and Bowman, 'Rigging the Game'.
[107] Shane and Bowman, 'Rigging the Game'.
[108] Bauer, *Secret History*, 356.
[109] Scott Shane and Tom Bowman, 'Busy Signals at NSA: Agency of spies keeps code of silence with few clear lines', *Baltimore Sun*, December 24, 1995, 1.
[110] Shane, 'No Such Agency', in Hill and Broening (eds), *The Life Of Kings*, 236.