# Cryptography and the Global South: Secrecy, Signals and Information Imperialism

*Robert Dover and Richard J. Aldrich*

Abstract

For decades, espionage during the Cold War was often presented as a competition between East and West. The extent to which the Global South constituted the main battleground for this conflict is now being appreciated, together with the way coups and covert regime change represented a continuation of colonialism by other means. Recent revelations about the nature of technical surveillance and signals intelligence during this period suggests an even more alarming picture. New research materials released in Germany show the ways in which Washington, London and even Moscow conspired to systematically attack the secure communications of the Global South. For almost half a century, less advanced countries were persuaded to invest significant sums in encryption machines that were adapted to perform poorly. This was a deceptive system of non-secrecy that opened up the sensitive communications of the Global South to an elite group of nations, that included former colonial rulers, and emergent neo-imperial powers. Moreover, the nature of this technical espionage, which involved commercial communications providers, is an early and instructive example of digital global information inequality.

Keywords: Cold War, colonialism, communications, information, intelligence, signals,

Almost all states in the world, large or small, can claim a substantial tradition of espionage and internal security organisations. Reflecting the growth of the study of intelligence in universities, the literature on this subject is increasingly voluminous and sophisticated.[1] There is a growing awareness that a largely Atlanticist focus has dominated the study of secret services, limiting our understanding of intelligence machinery in the Global South , as well as our understanding of diverse intelligence practices.[2] Although this work is sophisticated and can claim to have recovered the "missing intelligence dimension" of both international relations and international history,[3] there is now an active effort to diversify and globalise this subject.[4] Recently, Davies and Gustafson, in an important agenda-setting contribution entitled *Intelligence Elsewhere,* have advanced a more inclusive and comparative study of national intelligence beyond the "Anglosphere".[5] Moreover, there is a growing awareness that Cold War intelligence activity formed part of efforts to delay the retreat of empire, and to replace it with a neo-colonial world order.[6]

Cold War historians have also begun to rehistoricise this conflict.[7] In his magisterial 2005 study*, The Global Cold War*, Odd Arne Westad focused on Third World interventions, rejecting the idea of a superpower struggle "mostly centered on Europe". Instead, he suggested that the key developments during the Cold War were connected to, but not drivers of, significant in political and social development in the Third World. Most strikingly, he

argues that Cold War interventions in the Third World shaped political, economic and social relations as we know them today, thus the Cold War was "a continuation of colonialism through slightly different means".[8] To this extent Westad's work echoes the theoretical insights provided in historical materialist contributions of uneven and combined development and Gramscian readings of international politics that focus on the management of what they describe as the periphery by core states.[9] The neo-liberal world order that emerged after Bretton Woods, paved the way for the multinational enterprises that increasingly transcended the governments that had nurtured them and thus created forms of social and economic neo-colonialism in the global south.[10] Consequently, international law, governance mandates, peacekeeping missions and perhaps even the notion of the "anarchical society" itself, are part of a Eurocentric imperial overhang.[11]

Descriptions of communications intelligence practice and its contribution to the emergence of neo-colonialism are largely missing from the extant literature. Therefore, this article seeks to bridge this gap with analysis of newly revealed German and American government documentation. We demonstrate the extent to which these governments and a select group of allied countries systematically intercepted the sensitive government communications of the Global South to manage and keep supplicant a large proportion of the globe. We are able to provide clarity to the partially revealed details of this affair: writing the CIA and BND (the German secret service) into a story that was assumed to only contain the US National Security Agency (NSA). Moreover, we add important details about the numbers of countries exposed, precisely how their cypher machines were compromised and episodes in contemporary history impacted by this long-running operation. What this article is not yet able to do is to reveal the minutiae of cable intercepts and what this day-to-day activity tells us about the active management of the Global South. Despite its own anti-colonial antecedents, the US and its allies used economic warfare, propaganda, intelligence and covert intervention as part of their colonial toolbox, and this will require further research as more archives become available.

## Communications Intelligence and the Global South

Where intelligence operations in the Global South have been researched, they have only rarely included information around communications intelligence – derived from signals interception and decyphering. However, in March 2019, documentation emerged that contributes to our understanding and that highlights the complex interaction between the United States, Germany, Switzerland and Sweden as a communications core, and countries of the Global South as periphery. The documents also validate what many analysts and activists suspected about the relationship between technology corporations and western intelligence agencies.

The new material shows that during the 1950s, the owner of one of the world's largest cypher machine factories, Crypto-AG, concluded a "Gentleman's Agreement" with the famous American codebreaker William Friedman to restrict the sales and later weaken the cryptography in his devices so that Washington and a small number of technocratic allies could read them. The machines would, however, continue to produce cyphers strong enough to fool purchasers into thinking their communications were secure. This operation, eventually known by the codenames "Thesaurus" and later "Rubicon," ranks among the most audacious in intelligence history – a latter-day equivalent of the British World War Two Bletchley Park

operation that decrypted Axis communications.[12] Here, to avoid confusion, we use the codename "Rubicon" throughout. The eventual beneficiaries of Operation Rubicon, directly or indirectly, included Britain, Germany the Netherlands, France, Israel, Sweden, Switzerland, the USA and the USSR: nearly all of Operation Rubicon's victims were drawn from the Global South.

Over 120 countries bought cypher machines from Crypto-AG, trusting in Switzerland's twin reputations for neutrality and advanced technology. During the 1960s, Crypto-AG had captured more than 80% of the global market.[13] In reality, this factory was – between 1970 and 1993 - secretly owned by the CIA and the BND, using a share ownership structure that would be familiar to those who have studied the more recent Panama Papers.[14] Crypto-AG's customers paid millions of dollars to have their secrets stolen by the advanced countries of the North: a form of neo-colonial rent-seeking, exploiting the gaps in research capacity in the Global South and the consequent inability to understand the vulnerabilities in the machines.[15] Indeed, taking into account the cost of diplomatic communications infrastructures, including secure rooms in embassies and armies of clerks and stenographers, governments of the Global South invested literally billions in elaborate communications bureaucracies and spent their time patiently cyphering and decyphering messages, all of which did little other than render their most sensitive communications visible to a small club in the North. During the 1970s and 1980s, countries like the United States read approximately half of all "secret" communications traffic across the Global South with significant consequences for economic and political negotiations, and the evolution of small wars and insurgencies, together with the wider matrix of power relations in the world.[16]

A key aspect of the Operation Rubicon history, with current implications, is the participation – in terms of direct research and manufacturing support and the leveraging of contacts - of large companies like Phillips, Siemens and Motorola.[17] Here we can track the continuation of colonial methods into the neo-imperialist era. But we can also see the operation of neo-liberal economics that persists into the internet age where independent competitor manufacturers of encryption machines were discouraged, bought out or shut down. We argue here that this behaviour constitutes an important element of the information divide, more recently termed the "digital divide". In 1999, the UN Secretary General Kofi Annan argued that access to communication technologies runs in parallel to other fundamental human rights. Consequently, the digital divide is a humanitarian issue, noting that for many, "the great scientific and technical achievements of our era might as well be taking place on another planet".[18] Control over these technologies is therefore an key component of keeping the Global South in its supplicant position.[19] The current digital divide was preceded – even pioneered - by a secret American and German precursor that has a sixty year history, illuminating the weaponization of controlling technological access in order to reinforce these disparities. As such, this provides us with evidence for why the US and its intelligence allies currently feel so defensive towards Chinese technology constituting the backbone of the 5G infrastructure: they know all too well the power and control that can be achieved through advanced communications intelligence.

**Methodology and Sources**

Researching the history of intelligence presents complex methodological problems. Much of what we know about Cold War intelligence is the result of a propaganda conflict that saw secret services attempt to self-aggrandize their own achievements and denigrate their

competitors.[20] Elsewhere, some states have opened their intelligence archives, and sometimes closed them again: these materials must also be treated with caution as "laundered archives".[21] From World War Two to the present day, investigative journalists and whistleblowers have provided sensational and often partial insights into American and British intelligence activities. This created information conflicts between journalists and intelligence officers, within a broader discourse that was a component of the military, diplomatic, economic and often ideological contest between the Global North and South.[22] That some of the foundational knowledge for these activities comes from investigative journalism and limited datasets, creates methodological challenges for researchers. Even more than other branches of social science we need to proceed with caution, triangulation and additional verification, whilst being cautious with our findings.[23]

Operation Rubicon operated at such a high level of secrecy that, within the State Department, only the Secretary of State was cleared to know how it worked. Whilst many officials benefitted from the end product, the contours of the operation were tightly held. We only know about Rubicon because it was a product of intelligence collaboration or "liaison" between many advanced countries and therefore the secrecy net widened as the operation aged. Importantly, in September 1999, with Operation Rubicon in decline but still active, veterans of the American and German secret services gathered for a historical conference at Teufelsberg in Berlin. Some of the attendees, brimming with pride at the amount of intelligence their joint operation produced decided to create a final report.[24]

Five years later, a 96 page historical outline called "Minerva" had been written by the CIA, using the CIA cover codename for Crypto-AG's. Unusually, this history was not undertaken by the CIA's History Staff, which normally produces high-grade academic studies. Moreover, the 'Minerva' document was in fact a summary of a larger and highly classified three-volume study of the same subject. The 96-page summary was designed to be sent to the BND as an official history, a memorialisation, that was deliberately classified at an artificially low-level to permit exchange. Subsequently, and because of inaccuracies they perceived in the American document, the German BND responded with their own oral history made up contributions from senior intelligence officers who had either staffed the programme or served as senior managers and viewed it as important.[25]

Operation Rubicon first emerged in fragments into the public realm via books published by Ronald Clark in 1977 and James Bamford in 1983, who sensed there was a wider story in the US communications intelligence effort.[26] Rubicon can be triangulated further, for curiously, the story has been known in a fragmentary form for many years through the public information slips of politicians, from stories by investigative reporters and releases into archives. Even while Rubicon was at the height of its importance and productivity it was partially revealed - to the intense fury of its managers. The main cause of the breach in the wall of secrecy was the papers of William Friedman, which were deposited at the Marshall Library in Lexington in 1969. Friedman was proud of what he and his friend Boris Hagelin had achieved and clearly hoped the secret would eventually come out. Accordingly, among the seventy-two boxes of his papers, were copies of his lifelong correspondence with Hagelin and references to something called the "Boris Project".[27]

In the mid-1970s, inspired by the emergence of the Bletchley Park story, British journalist Ronald Clark decided to write biography of Friedman, America's leading cryptographer, and his wartime work against German and Japanese codes.[28] But Clark found more than he bargained for, including references to Friedman's visit to Europe during the 1950s and speculated about what these visits might have meant. Friedman's biographer

recounts: “Ciphering machines incorporating ingenious variants and improvements were being produced in Europe by more than one manufacturer and were being bought and adapted by more than one NATO country”. Unsurprisingly, Friedman’s subsequent destinations on his grand European tour were Sweden and Switzerland.[29]

Hard on Clark’s heels was an investigative journalist called James Bamford. In 1982, after years of patient sleuthing, and to the horror of the western security establishment, he published a history of NSA and its collaboration with Britain’s GCHQ. Much of his research was open-source and, following in Clark’s footsteps, he examined the Friedman papers, however Bamford did a better job of piecing the story together. In two breath-taking pages, buried in the middle of the book, Bamford broke the Rubicon story and pointed the finger squarely at the Crypto-AG factory in Switzerland, albeit suggesting that the agreement had turned on informing the NSA about design modifications for customers.[30] This in turn triggered a battle over the opening and closure of the Friedman papers, indeed NSA tried legal action to impede Bamford’s research.[31] It also ensured that the papers of his Swedish partner, Boris Hagelin, would be swept up and incarcerated at the CIA’s headquarters at Langley.[32] Most of the letters written between Friedman and Hagelin were declassified in 2015, with the exception of one which remains classified on national security grounds.[33]

Oddly, as we shall see, Bamford’s remarkable revelations did not dent Operation Rubicon. The Crypto-AG factory near Zug in Switzerland dismissed Bamford’s account as rumours deigned to discourage countries in the Global South from benefitting from the secrecy provided by high-grade Swiss machines. However, in 1993, one of the company sales team, Hans Bühler, was arrested in Iran. After his release, Bühler charged his former employer with selling rigged equipment. He also accused the Swiss government with complicity in the intelligence operation. Crypto-AG denied the story, but in March 1994, Swiss investigative journalist, Res Strehle, published a book called *Encrypted,* coinciding with broadcasts on Swiss and Austrian national television.[34] Immediately, Bühler’s story attracted the attention of Scott Shane, a journalist working for *The Baltimore Sun*, a paper based close to NSA’s headquarters north of Washington DC. He continued to probe retired Crypto-AG employees for further information. On 10 December 1995, he published a lengthy article adding much new detail.

In 2018, more complete German and US records finally came via the efforts of the German broadcasting company ZDF who began making a series about the BND, the German foreign intelligence service, which undertakes both human and technical espionage. During the investigation, the 96-page Minerva document emerged, together with the German oral history commentaries, triggering a new wave of research by veteran journalists Peter Müller, Ulrich Stoll and David Ridd. Nicole Vögele and Fiona Enderes from Swiss television *SRF* together with Huub Jaspers from the Dutch radio programme *Argos* also contributed Subsequently they collaborated with Greg Miller at the *Washington Post* to further probe the American side of the story. Eventually, many senior officials, including a former Director of the NSA, Bobby Ray Inman, confirmed the accuracy of the material that had been uncovered.[35]

The unravelling of Operation Rubicon offers insights into intelligence studies and the paradoxes of secrecy: piecing together intelligence history is akin to early palaeontology and its attempts to provide accurate knowledge about dinosaurs from a fragmented evidence base. Accordingly, this paper is based on multiple triangulated sources that all confirm the same basic story. The CIA and especially the BND files are self-congratulatory as we might expect from histories written to memorialise a successful joint operation, but they were written in opposition to each other, making agreement on the essential terms compelling.

The extensive German oral histories provide good levels of detail, albeit sometimes delivered with the idiosyncrasies it would be reasonable to expect from testimony provided by retired intelligence officers with the passing of time. The German files have left gaps about key international partners, such as the American NSA, and the role of neutral nations like Switzerland and Sweden. Beyond this inner circle were other (sometimes surprising) partners, including the USSR, playing roles that are still poorly understood, suggesting a further reframing of our understanding of the Cold War. Operation Rubicon was vast in scale and excavating its full extent will keep intelligence scholars busy for many years to come.

**Operation Rubicon's Origins**

During World War Two, the US Army needed a basic but compact encryption device for its forward formations. Boris Hagelin, Crypto-AG's founder, was a Russian inventor who fled to Sweden to escape the 1917 revolution and had created some of the world's best cypher machines during the 1930s. Arriving in the United States in 1940, he brought with him a design for a light and robust field encryption machine, known as the M-209. Small, durable, hand-powered and ideal for forces on the move it was licensed by the US government and produced in its thousands for wartime use by forward combat formations. By 1945, some 140,000 had been made under license by Smith-Corona, and remained in use until the 1960s.

After World War Two, Hagelin returned home to Sweden and reopened his factory. Here, in the early 1950s, he developed a new cypher machine, more akin to the wartime German Enigma, but with a new, "irregular" stepping motion that alarmed American code-breakers.[36] One of the founders of the CIA, Allen Dulles, worried that the rest of the world would soon be immune to American codebreaking activities if they bought Hagelin's new, secure machines. Dulles was important because he ran his own mini-version of the NSA within the CIA called "Division D" and even poached NSA cryptographers like Frank Rowlett. It was the buccaneering spirit of figures like Dulles and his colleague Bill Harvey, the first Head of Division D, that drove Operation Rubicon. They were not only intrigued by an operation that combined human intelligence and signals, but were also more attuned to targets in the global south.[37] Moreover, the Americans believed they enjoyed leverage over Hagelin as they could put him out of business by flooding the market with wartime surplus M-209s.[38]

Veteran American cryptographer William Friedman offered Hagelin what amounted to a "Gentleman's Agreement".[39] In doing so they hoped to use friendship instead of coercion. Friedman and Hagelin belonged to a small group of founding engineers who understood mechanical encryption, and who remained in the vanguard of talented and well-funded teams working on the development of electro-mechanical devices. Widely regarded as two of the founders of modern cryptography, they had known each other since the 1930s. Their agreement was struck over dinner at the Cosmos Club in Washington in 1951 and required Hagelin, who was re-locating his company to Switzerland, to limit the sales of his most sophisticated models to countries approved by Washington. Countries that were not on Friedman's Washington-approved list would be supplied with older, weaker systems. Meanwhile, Hagelin would be cushioned for his lost sales, as much as $700,000 up front, with further annual payments. The CIA was somewhat keener than the NSA to secure this arrangement.[40] Here, the CIA was behaving in a manner consistent with the US government and their defence industrial base: providing state sanctioned distortion of private markets

and state aid to strategically important businesses.[41] After the agreement, Friedman wrote to Hagelin that he had thought the NSA might frown on further visits to see him.[42]

In 1960s, the relationship between the CIA, BND and Crypto-AG matured and sales grew strongly. The company sold 5,089 machines around the world in 1963 alone. Working with the German BND, the CIA sourced engineers from Siemens who helped with the research element of the company.[43] The CIA and Hagelin now moved forward towards a "licensing agreement" that provided him with nearly one million dollars a year for participation, whilst Friedman retired. In 1959, the NSA visited Friedman's house and over time he became disenchanted with government. In 1962, he gave with an open lecture to the American Philosophical Society, where he mused on the problems of democracy set against the activities of secret intelligence and communications interception.[44] Cryptographic technologies were rapidly evolving and so the assistance of Siemens and US government technologists – behind the scenes - allowed Crypto-AG to maintain a competitive advantage. In 1967, Crypto-AG released a new machine, the H-460, an all-electronic machine whose inner workings were in fact designed by the NSA. Other machines in the Crypto-AG range were designed with the assistance of Motorola who joined the project at the request of the CIA.[45]

In 1970, the CIA and the BND entered into a joint purchase arrangement for Crypto-AG and so Rubicon achieved a stable platform that it would retain through to 1993. Early accounts of often speak of "back doors" or secret programmes that meant the Crypto-AG devices gave away their encryption keys.[46] Those accounts are untrue. The machines simply produced weaker cyphers, sometimes using rather shorter keys, than the purchasers expected. This made them vulnerable to plain-text attacks. The NSA and other interested governments still had to intercept the target country's communications and then decypher the messages, and it is here that the United States and its Rubicon allies had the distinct advantages of knowing how the communications would be encrypted, whilst also possessing the advanced computing to make 'brute force' decryption possible. These two advantages reinforced the divide in the information order, between those able to intercept these weakened cyphers and those who could not. Some of these included NATO members, who were using a handbook written by the NSA.[47]

In the 1960s and 1970s, the NSA invested in faster processors for their computers from companies like IBM and eventually the famous Cray Supercomputer Company.[48] At the time of manufacture the $10 million Cray 1 had a processor that was ten times quicker than its nearest known competition, which places its performance as the equivalent of Apple's first iPhone.[49] It was thought that the NSA was investing in this advanced technology to overcome the computational challenge of Chinese and Soviet communications encryption.[50] This was the case, but this vast computational power was also used to process the voluminous communications of the Global South that could be broken with relative ease because of Operation Rubicon, with chosen international partners being supplied with supercomputers to assist with this work. Neither China nor the Soviet Union bought Crypto-AG encryption devices, being correctly suspicious of the company's origins.[51]

**Fixing the Global Market for Encryption**

In intelligence terms, Operation Rubicon is unprecedented because of its global extent. For Rubicon to work there needed to be collective international action to suppress competitors

to Crypto-AG. Curiously, this even entailed the cooperation of European allies who were also variously intelligence targets. After considerable debate, the CIA and the BND had agreed that only their own countries, together with Sweden, Switzerland and their banks would be protected from Rubicon, in something that became known as the "Four Pillars Agreement". But in reality, the assistance of other cryptanalytical powers, especially Britain, was required by the USA, and hence secret services like GCHQ, the successors to Bletchley Park, were also kept informed of the operation.

This meant that GCHQ, along with other services, effectively became a "free rider" on Operation Rubicon. Any country who understood the approach and that had significant computing resources could exploit the weaknesses. There was significant annoyance expressed by Britain that they were not amongst the inner-circle and therefore we can see Rubicon as part of British decline relative to US neo-imperial power. Resisting this, an attempt was made by GCHQ in the mid-1970s to formally join Rubicon in a demarche led by Director Bill Bonsall and his assistant Dougy Nicoll. The German government was infuriated to learn that the US had privately kept GCHQ informed of Rubicon and vetoed Britain's entry.[52] In 1979, Bonsall's successor, Brian Tovey, ordered GCHQ to look more closely at Operation Rubicon, when he discovered, to his horror, that the Italians were a target country for the NSA.[53] The parallel diplomacy of intelligence liaison ensured an uneven topography of tensions, with the ultimate victim being the Global South.

During the Cold War, the United States bore much of the costs of re-equipping Western Europe's diplomatic and military communications. This was partly to improve the security of its NATO allies, as electro-mechanical cypher machines were complex and extremely expensive, in the hope of thwarting Soviet and Chinese code breakers. The additional purpose for the NSA and GCHQ was to suppress any independent efforts of European countries to make or export their own cypher machines.[54] The British and Americans did not want the continental Europeans – or anyone else - to develop their own commercial cypher machine industry, exporting unique machines around the world in competition with Crypto-AG, which would be difficult for GCHQ or the NSA to attack. They adopted a bizarre strategy of supplying British and American machines almost for free that was intended to undercut the market and to remove any financial incentive for competitor manufacturers.[55]

Therefore, the Operation Rubicon cartel anti-competitive actions manifested themselves as strange kind of political economy of secrecy. The NSA developed a "free-licensing" plan that allowed NATO countries to produce American and British designed cypher machines at no-cost. This scheme ensured that the NATO countries enjoyed greater levels of security and interoperability – reinforcing a core of communications elites – whilst simultaneously disincentivising any European country from designing rival machines.[56] Whilst GCHQ supported free-licensing, the rest of Whitehall did not, mindful of the lucrative deals that had been signed with Canada and Australia to supply the technically impressive Alvis cypher system and so in June 1962 they rejected the NSA's scheme.[57] This news 'shocked NSA' and GCHQ's liaison officers in America feared that this would impair the relations between NSA and GCHQ, two of the most important secret services in the world.[58]

Predictably perhaps, GCHQ did not give up on the NSA's "free-licensing" initiative and the internal Whitehall debate culminated in a remarkable show-down at the Treasury on 10 July 1962. Strategic fundamentals were now at stake and GCHQ worried that for the sake of relatively small sums of money being outside of the Rubicon cartel might render Britain also a US target, in addition to losing access to the global cyphers used by other countries. In the

event, GCHQ won the internal debate, thereafter equipment was supplied to NATO nations at a highly-subsidised cost and the secure communications core was reinforced.[59]

In return for free-licensing, GCHQ and NSA quietly encouraged their NATO allies to introduce legislation that brought the export of cypher machines in line with the export of military equipment. However, these measures left the loophole of neutral countries like Sweden and Switzerland, to address this the US was able to continue secretly influencing Crypto-AG. Within much of the oblivious NATO, this was referred to as the 'neutrals problem', but it does also go some way to explain the importance of Operation Rubicon. The exploitation of the neutrals issue also helps to explain why revelations about Rubicon have resulted in public anger in Switzerland with its strict neutrality laws.[60]

Where NATO countries did export machines in competition with Crypto-AG, these machines were also fixed. The Swiss company Gretag at Reensdorf posed a real threat, as did German companies like STST/Timmann. Accordingly, US and German intelligence officers placed undercover officers in or near to these companies to try to manipulate their senior leaders.[61] When those approaches did not work with Gretag, they opted for smear campaigns against its products.[62] The Netherlands boasted large electronic engineering companies likes Phillips, which manufactured a series of cypher machines called Aroflex and Beroflex during the 1970s, and it is understood that these machines were set up in a similar way. The NSA worked with the Dutch to create machines that were supplied to Turkey, in an operation that the BND was not privy to.[63] Another major exporter was Israel, so whilst the Argentine Navy purchased its machines from Crypto-AG, the Army bought many of its machines from Israeli government sources.

Much like Britain, Israel, the Netherlands and France were therefore privy to some of the secrets of Rubicon but were not within the inner circle: indeed it was suggested by an East-West defector that France was also a target.[64] Yet the CIA and BND deemed it essential for them to be involved to ensure the global control of encryption.[65] By purchasing advanced technology like the Cray supercomputer from the United States, they could all free ride on Rubicon, joining Germany and Sweden as major producers of intelligence from less advanced countries in a process that now looks like an informational equivalent of commodity extraction. By contrast, Italy, Greece and Spain were not "in the loop" at all and indeed purchased Swiss Crypto-AG machines. In the strange world of signals intelligence, the Global South began with the Alps and Pyrenees and extended westward to Ireland.[66]

**The Consequences**

Admiral Bobby Ray Inman is one of America's most distinguished intelligence officers. He served as Director of the NSA in the late 1970s and then as a Deputy Director of the CIA. Inman recently made the following observation about Rubicon: "It was a very valuable source of communications on significantly large parts of the world important to U.S. policymakers".[67] But what did this mean in practice? The NSA's eavesdropping was organized around three main geographic targets, each with its own organisation or group: "A" for the Soviets, "B" for Asia and "G" for virtually everywhere else. By the early 1980s, more than half of the intelligence gathered by G group came from Crypto-AG machines, providing key insights. The

story was much the same for K Division at GCHQ – the so-called “exotics” - which handled the Global South for Britain. In the 1980s, countries buying these machines included Algeria, Argentina, Brazil, India, Indonesia, Iran, Saudi Arabia, Iraq, Libya, Jordan, Pakistan, South Korea, and Yugoslavia.[68]

Process-tracing the impact of intelligence on decision-making is notoriously difficult. Leading policy makers are busy and rarely note how the intelligence they read influences their immediate decisions or wider policy. However, four examples were singled out by officials as especially striking, even if they pose some interesting historical counterfactuals. Firstly, the Camp David peace agreements of September 1978. A decade after the Six-Day War, President Jimmy Carter developed a Middle East peace initiative. Designed to secure a lasting settlement between Israel and Egypt, the negotiations were somewhat fraught. Carter brought Egyptian President Sadat and Israeli Prime Minister Begin to Camp David to develop a plan to stabilise the Middle East. It is now clear that the critical Egyptian communications with their allied Arab states were read in real time, allowing Jimmy Carter to understand what could be achieved and where concessions could be obtained.[69]

Secondly, the Iran hostages negotiations. In early 1979, the ruling Shah fled Iran amid growing protests and came to the United States for medical treatment. In November 1979, angry Iranian students protesting about the Shah’s presence in New York, occupied the US embassy in Tehran and took fifty-two Americans hostage. More than a year later, with Algeria acting as a neutral mediator, the hostages were released. Washington had a clear advantage during the negotiations, since it could read the encrypted communications of both Iran and Algeria, who were Crypto-AG customers. Inman, the NSA’s director at the time, said he routinely got calls from President Carter asking how the government in Tehran was thinking. “We were able to respond to his questions about 85 percent of the time,” Inman said. So important was this material than Inman developed a unique “telephone friendship” with Carter.[70]

The third example is Argentina. The unpleasant military regime from 1976 to 1983 was also a customer of Crypto-AG. The manipulated ciphering devices enabled the BND and the CIA to learn how the Argentine Junta dealt with opponents of the regime and its connections to Operation Condor, a global operation to repress the left in Latin America. The Junta clearly had American support and indeed Henry Kissinger, in his last year as Secretary of State, was not only cognisant but encouraging on these practices, telling the Argentine Foreign Minster “We want you to succeed," and adding assuring him that "we do not want to harass you”. He urged Argentina to move quickly against the left to avoid the spotlight of world opinion.[71] The Argentine Navy used Crypto-AG machines and were the leaders in this repression. In total, more than 30,000 people fell victim to the programme of persecution. Rubicon raises questions about what governments in Washington, London and Bonn knew about these activities and therefore what their arms sales to such regimes across the region represents as a political choice: were they to foster “creative tensions” without clear winners as British arms sales to both Iran and Iraq had done in the 1980s, or to lock out Soviet influence?[72]

The fourth example is Panama. In October 1989, the US invaded the country and sought to arrest Manuel Noriega for money-laundering and narcotics offences. Some 20,000 American troops took part and the fighting ended in less than a week. Noriega escaped and took refuge in the Vatican embassy. He was discovered because the Vatican was communicating with its embassy using a device purchased from Crypto-AG and the NSA was reading the traffic.[73] Blasted with endless rock music, he was eventually persuaded to give himself up and was taken to the United States to face trial.[74]

However, the importance of intelligence from Operation Rubicon was not limited to these particular episodes. Indeed, the focus on set-pieces potentially obscures the larger impact on everyday economic, political and military relations with the Global South. Rubicon also provided the United States with a side-window on the activities of the USSR, since for much of the Cold War, Soviet communications were hard to penetrate.[75]

**Exposure and Closure**

One of the curiosities of Operation Rubicon was that despite being partially exposed many times during its history, it persisted. This demonstrated – in part – the financial and practical difficulties countries of the Global South faced in replacing Crypto-AG technologies with alternatives (with no guarantees of the alternatives being more secure), and the pressure the US could bring to continue using this technology. Such asymmetries are being replicated today in the contest between the US and China, with this contest being sited in third countries, over personal and cloud computing, internet switches and the roll-out of 5G technologies.

The earliest example of these efforts, if not the precise operation being revealed, came in September 1960 with the defection of two NSA employees to the Soviet Union, William Martin and Bernon Mitchell. In a press conference in Moscow they stated one of the reasons for their defection was 'the US government's practice of intercepting and deciphering the secret communications of its own allies'.[76] William Martin also revealed that this interception was occurring against Italy, Turkey, France, Yugoslavia, the United Arab Republic (covering what we now know as Egypt, the Gaza Strip, and Syria), Indonesia and Uruguay, amongst others.[77] A similarly stark example of Operation Rubicon being publicly revealed occurred in 1986 after the bombing of La Belle Discotheque in Berlin. Intercepted communications implicated Libya and Ronald Reagan deliberately revealed this in publicly justifying his retaliatory airstrike on Tripoli. Reagan's decision vexed the CIA, NSA and allies in GCHQ and the BND, which feared extensive repercussions for Rubicon. The feared disruption from this and other exposures was surprisingly minimal and governments continued to buy the machines in the 1980s.[78]

Why did governments of the Global South ignore warnings that their communications were insecure? In the case of Argentina, Crypto-AG engineers were repeatedly summonsed about concerns that the cyphers were weak. The 'fixes' applied by Crypto-AG engineers were approved by the NSA and BND, and this would have been apparent to technically competent cryptographers in Argentina. So, we can reasonably assume that the Argentinian government were aware that their communications were perhaps being intercepted by Americans, and that in their strategic calculation this was less problematic than if the Chileans (for example) had access. This strategic equation shifted dramatically during the 1982 conflict for the Falklands Islands/Malvinas when Argentinian intercepts were passed to the British government. Such equations were replicated across the globe: Pakistani officials were more concerned about Indian interception than they were about US interception. This did not apply to the Middle East, where America's role was more contentious. For example, Egypt began an independent crypto effort with university mathematicians as early as 1975 in the hope of

protecting its communications against the United States. Yet Iran, Saudi Arabia and Jordan continued to buy large numbers of the machines without anxiety.[79]

Within the Crypto-AG workforce, the engineers often questioned the algorithms being foisted on them by unknown external actors. Only a few people in the company were "plants" and knew of the arrangement, although it would be extraordinary if others had not realised what was going on. The internal line at Crypto-AG was that the designs were provided as part of the consulting arrangement with Siemens. In 1977, Heinz Wagner, Crypto's Chief Executive abruptly dismissed a wayward engineer after he had responded to Syrian complaints about weak algorithms with too much zeal. This engineer had travelled to Damascus and genuinely fixed the vulnerabilities the Syrian authorities had identified, thus rendering Syrian traffic unreadable.[80]

Iran was remarkably late in raising suspicions about Crypto-AG, and did not pick up on Reagan's public statements about Libyan communications in 1986. However, in March 1992, Iran suddenly arrested Hans Bühler, one of the leading salesmen for Crypto-AG, who regularly visited countries in the Middle East, including Saudi Arabia. The alarming Bühler episode acquired the joint CIA/BND codename "HYDRA", presumably in honour of the multifaceted problems it generated, and this was as damaging as the agencies had feared. The charges brought against Bühler were vague and he was released nine months later, in January 1993, after a bail of US$1,000,000 had been paid via funds secured by the BND. The CIA had also tried to help with the bail money, but this was vetoed by the White House. After his release from prison, Bühler publicly campaigned against his former employer. He was convinced that Crypto-AG had not done enough to obtain his release and voiced the suspicions of some of his colleagues that the machines he had sold were fixed. Whilst the BND and CIA – correctly, as it turns out - felt he should be kept on the inside and silenced on preferential terms, Crypto-AG decided to terminate his contract in March 1993.[81]

In November 1993, Bühler accepted CHF250,000 in compensation for his dismissal, but Crypto-AG failed to include a confidentiality clause. In March 1994, Swiss investigative journalist Res Strehle published a book about the affair "Verschlüsselt, Der Fall Hans Bühler" (Encrypted, The Case of Hans Bühler) in which he provided a detailed account of Bühler's imprisonment, the interrogations, the bail money and his subsequent release. The book was accompanied by documentaries on national television. Bühler's revelations gained further impact in late September 1995, when he was interviewed by American journalist Scott Shane of *The Baltimore Sun*, leading to further stories that had wider circulation. By 1996 countries including Argentina, Italy, Saudi Arabia, Egypt and Indonesia — either cancelled or suspended their contracts with Crypto-AG, compromising the US intelligence community's ability to read their communications. This was compounded by more general developments in communications technology, including Public Key Cryptography, which gave governments a wider choice of options. By 1996, a growing number of countries across the Global South were starting to use their own home-grown cyphers.[82] There is a suggestion, from our interview evidence, that by 1996 the CIA had pressured US computer manufacturers to introduce vulnerabilities in desktop computers, effectively patching the loss of access that the decline of Operation Rubicon had caused.[83] This pattern of collaboration between US intelligence and private industry suggests Rubicon was the forerunner of a very modern way of working. The Snowden revelations demonstrated the extent to which the NSA had worked in collaboration or coerced technology companies (be they manufacturers or service providers) to secure access to large quantities of private communications, internet traffic and meta-data.[84]

The Bühler episode had prompted widespread speculation that Crypto-AG was owned by the BND and CIA, although Crypto-AG continually denied this, and as we have seen from the fallout in Switzerland in 2020, this notion remains antithetical to long-held Swiss neutrality.[85] Bühler's revelations caused the BND to review its participation in Rubicon. During 1993, Konrad Porzner, the chief of the BND, made clear to CIA Director James Woolsey that support in the German government was waning. On Sept. 9, the local CIA station reached an agreement with BND officials to purchase Germany's shares for $17 million. The fear of full public revelation triggered the BND's decision to terminate the joint venture with the CIA. Thus, from July 1994 to 2019, the Swiss company Crypto-AG was solely controlled by the American CIA.

**Conclusions**

The revelations around the long history of Operation Rubicon are also a window upon the contemporary world. Rubicon helps us to understand the transition from traditional colonial powers to neo-colonialism and neo-liberal economics. It suggests that at the end of the Cold War, Germany's strategic policy cadre were reducing the number of nations it was willing to aggressively target, whilst the United States were widening out the number of targets to include its allies as well as historical adversaries and competitors, on the basis that "in the world of intelligence, there were no friends". The fundamental problem was American exceptionalism: the feeling that, in an emerging unipolar world, everyone else was the Global South.[86]

This episode foregrounds the hitherto underexplored role of intelligence agencies and communications technology in attempts to manage the Global South. Moreover, Rubicon helps us to contextualise the revelations made by the former US intelligence contractor, Edward Snowden, that were seen at the time as paradigm shifting, but which can now be seen as a merely one chapter in a long-established story of global communications interference by the United States. Germany's withdrawal from Operation Rubicon in 1993 was regretted by the BND but was an early recognition of what the political fallout might be. Similarly, the current American policy nausea about Chinese-manufactured internet equipment in the development of 5G networks is in part a reflection of the concerns the governments of the Global North have about Chinese involvement in core infrastructure projects, including the Belt and Road initiative, and in part a reflection of what the United States knows about how capable intelligence states can use private companies to further their own strategic ambitions. It also explains why the NSA fought hard against Public Key Cryptography in the 1990s, whilst seeking to place vulnerabilities in American manufactured computer terminals.[87] There is also a strong suggestion that these operations are still on-going. In 2012, the BND observed that Operation Rubicon had shaped its approach and that its current signals intelligence operations are still to this day "based on a system of infiltration".[88]

Remarkably, it is also now clear that Russian intelligence was part of Rubicon. They enjoyed the same "free-rider" status as countries like Denmark, Israel and France. As late as 2005, the CIA did not know the Russian position on Crypto-AG.[89] But by 2012 the BND were clear that other beneficiaries of the operation included "even those with capable services from the then Soviet bloc with the Soviet Union on top".[90] More recently this was confirmed by a defector form the KGB 16th department (signals intelligence) who was located by intrepid

ZDF journalists during the making of their documentary, together with East German archival material. Typically during the Lebanon crisis in the 1980s, the KGB had agents on the ground, but its best intelligence came from reading the cables of people like the Greek ambassador, who was sending messages back to Athens over a Crypto-AG machine.[91]

The Soviet dimension in turn raises further fascinating questions. Perhaps the West prioritized its having access to the otherwise protected communications of developing nations over the possibility that the USSR could achieve similar access. Alternatively, it may have discounted the likelihood that Moscow could achieve that goal, as it did in other area such as ICBM development. The Soviet Union had advanced computing, but not at the level enjoyed by the United States or Western Europe. Clearly, more work needs to be done to unravel this complex and fascinating informational work by technocratic core states. However, what we know already is reshaping how we might think about the management of core-periphery relations, the true nature of the informational order and how it evolved over more than fifty years.

**References**


Aid, M.M. *The Secret Sentry: The untold history of the NSA*. New York: Bloomsbury, 2009.

Aldrich, R.J. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency – Centenary Edition.* London: Collins, 2019.

Andrew. C.M. and Vasili Mitrokhin. *The World Was Going Our Way: The KGB and the Battle for the Third World*. New York: Basic, 2006.

Andrew, C.M. "Secret Intelligence and British Foreign Policy, 1900-1939" in Christopher Andrew and Jeremy Noakes (eds.) *Intelligence and International Relations, 1900-1945.* Exeter: Exeter University Press, 1987.

Annan, K., Speech at the ITU Opening Ceremony. 1999. Available from: http://www.itu.int/telecom-wt99/press_service/information_for_the_press/press_kit/speeches/annan_ceremony.html

Bamford, J. *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization.* New York: Granite Hill, 1983.

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.

Bauman, Z; D. Bigo; P. Esteves; E. Guild; V. Jabri; D Lyon; R. B. J. Walker, 'After Snowden: Rethinking the Impact of Surveillance', *International Political Sociology*, 8, No.2 (2014):121-144.

Berger. M.T. "The real Cold War was hot: The global struggle for the Third World." *Intelligence and National Security.* 23, No.1 (2008):112-126.

Boone, Catherine, "Trade, taxes, and tribute: Market liberalizations and the new importers in West Africa." *World Development*. 22, No.3 (1994):453-467.

Borger, Julian. "CIA controlled global encryption company for decades", *Guardian,* 11 February 2020.

Budiansky, Stephen, *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union*, New York: Knopf, 2016.

Castells, M., *The Rise of the Networked Society.* Oxford: Blackwells, 2000.

Central Intelligence Agency, *Minerva: A History*, Langley: CIA, 2004.

Clark, Ronald, *The Man Who Broke Purple*, London: Penguin, 1977.

Cole, Ronald GH. *Operation Just Cause: Planning and Execution of Joint Operations in Panama February 1988 – January 1990*, Joint History Office, Office of the Chairman of the JCS 1995,

https://nsarchive2.gwu.edu/NSAEBB/NSAEBB443/docs/area51_22.PDF Accessed 21.05.20

Corera, Gordon. *Intercept: The secret history of computers and spies*. London: Hachette, 2015.

Cormac, Rory. *Disrupt and deny: spies special forces and the secret pursuit of British foreign policy.* Oxford: Oxford University Press, 2018.

Davies P.H.J. and K.C. Gustafson, eds. *Intelligence elsewhere: spies and espionage outside the Anglosphere*. Washington: Georgetown University Press, 2016.

Davies, P.H.J. "Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services." *Politics,* 21, No.1 (2001):73-80.

Dover, Robert, and Michael S. Goodman (eds), *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence*. New York: Columbia, 2009.

Foulkes, Imogen. "Swiss Crypto AG spying scandal shakes reputation for neutrality". *BBC News*, 16 February 2020**:** https://www.bbc.co.uk/news/world-europe-51487856 accessed 27 March 2020.

Frontal 21 reports on ZDF on February 11, 2020 at 9 p.m.

Gill, Peter and Mark Phythian. "What is intelligence studies?" *International Journal of Intelligence, Security, and Public Affairs* 18, No.1 (2016):5-19.

Goodman, M.S. *The Official History of the Joint Intelligence Committee: Vol.I*. London: Routledge, 2014.

Halliday, Fred. *Cold War, Third World: An Essay on Soviet American Relations.* London: Hutchinson, 1989.

https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/?itid=hp_hp-cards_hp-card-world%3Ahomepage%2Fcard-ans

Heuser, Angsar, Head of Division for Technical Reconnaissance, 'Operation Thesaurus/Rubicon', BND oral history.

Karabell, Zachary. *Architects of Intervention: The United States, the Third World, and the Cold War, 1946–1962.* Baton Rouge: Louisiana State University Press, 1999.

Kolko, Gabriel. *Confronting the Third World: United States Foreign Policy 1945–1980*. New York: Pantheon, 1988.

Kothari, Uma, and Rorden Wilkinson. "Colonial imaginaries and postcolonial transformations: exiles, bases, beaches." *Third World Quarterly* 31, No.8 (2010):1395-1412.

Krasner, S.D. *Structural Conflict: The Third World Against Global Liberalism*. Berkeley: University of California Press, 1985.

Herrington, Lewis. "The debatable land: spies, secrets and persistent shadows," *International Affairs* 94, No.3 (2018):645-655.

Lockhart, James. *Chile, the CIA and the Cold War: A Transatlantic Perspective*. Edinburgh: Edinburgh University Press, 2019.

Maddrell, Paul. "What we have discovered about the Cold War is what we already knew." *Cold War History* 5, No.2 (2005):235-258.

Maguire, T. *The Intelligence-Propaganda Nexus: British and American covert action in Cold War Southeast Asia*. Oxford: Oxford University Press, 2020.

Matin, Kamran. "Uneven and combined development in world history: the international relations of state-formation in premodern Iran". *European Journal of International Relations*, 13, No.3, (2007):419-447.

McGarr, P. "'Quiet Americans in India': the CIA and the politics of intelligence in Cold War South Asia." *Diplomatic History* 38, No.5 (2014):1046-1082.

Melman, Seymour, *Pentagon Capitalism: The Political Economy of War*. New York: McGraw, 1970.

Miller, Greg. "The intelligence coup of the century: For decades, the CIA read the encrypted communications of allies and adversaries." *Washington Post*, 10 February 2020.

Moran, C. *Classified: Secrecy and the state in modern Britain*. Cambridge: Cambridge University Press, 2016.

NSA "Draft Report of Visit to Crypto AG (Hagelin) by William F Friedman", Top Secret, 15th March 1955. https://nsarchive2.gwu.edu//dc.html?doc=6773844-National-Security-Archive-Doc-6-NSA-Draft-Report

Phythian, Mark. *The Politics of British Arms Sales Since 1964*. Manchester: Manchester University Press, 2000.

Rabe, Stephen G., *The Most Dangerous Area in the World: John F. Kennedy Confronts Communist Revolution in Latin America.* Chapel Hill: University of North Carolina Press, 1999.

Rezk, Dina. "Egypt's spy chiefs: servants or leaders?" in Paul Maddrell et al, eds., *Intelligence leaders in Europe, the Middle East, and Asia.* Washington: Georgetown University Press, 2018.

Richterova, Daniela & Natalia Telepnava, special issue of *International History Review,* forthcoming 2020, "Secret Struggle for the Third World".

Riek, Herbert, "Minerva", BND oral history, June 2011.

Rosenberg, Justin. "The 'philosophical premises' of uneven and combined development, *Review of International Studies,* 39, No.3 (2013):569-597.

Shane, Scott & Tom Bowan, "Rigging the Game: Spy Sting", *Baltimore Sun*, 10 December 1995.

Sherman, David. "The National Security Agency and the William F. Friedman Collection", *Cryptologia*, 41, No.3: 195-238.

Shiraz, Zakia. "Drugs and dirty wars: intelligence cooperation in the global South," *Third World Quarterly* 34, No.10, (2013):1749-1766.

SM-2721-52, Memo of the Reps. of the British COS, 'Report of the UK/US Communications Security Conference, 1952', JCS.1951-3, CCS311 (1-10-42) Sec.15, RG218, NARA.

Smidt, Wolbert, BND oral history, Operation Thesaurus, Experiences of the party responsible of BND operations 1973-80.

Smith, Michael, *The Secrets of Station X.* London: Biteback, 2011.

SRF "Crypto Spying Affair: How manipulated Swiss tech shaped world politics".

Stockton, B. *Flawed Patriot: The Rise and Fall of CIA Legend Bill Harvey*. Washington: Potomac, 2006.

T225/2074, 'Provision of On-line Cryptographic equipment for NATO', note of a meeting in Mr Trend's Room at the Treasury, 07 July 1962, 73/155/01, UKTNA.

T225/2074, Stephenson to Trend, 29 June 1962, UKTNA.

T225/2074, 'Provision of On-line cryptographic Equipment for NATO', note of mtg. 10 July 1962, TNA

T225/2074, Stannard to Stephenson, BM55/0504, 29 January 1963, UKTNA.

The "Rundschau" of the Swiss television SRF 12 February 2020.

ZDF, "Secret Operation 'Rubikon'. The BND's Biggest Coup" 18 March 2020.

Theveßen, Elmar, P.F. Müller and Ulrich Stoll. zdf.de news #Cryptoleaks: How BND and CIA Deceived Everyone heute.de logo, "Operation 'Rubikon'" 11 February 2020.

van der Pijl, Kees, *Global Rivalries from the Cold War to Iraq.* London: Pluto, 2006.

Walton, Calder. *Empire of secrets: British intelligence, the cold war, and the twilight of empire*. London: Collins, 2014.

Willmetts, Simon. "The CIA and the invention of tradition." *Journal of Intelligence History* 14, No.2 (2015):112-128.

---

The authors would like to acknowledge support from the Leverhulme Trust and the assistance of the dedicated ZDF research team P.F. Müller, David Ridd, Erich Schmidt-Eenboom and Ulrich Stoll. Also Nicole Vögele and Fiona Enderes from Swiss television *SRF* together with Huub Jaspers from the Dutch radio programme *Argos.* The authors were fortunate to serve as academic advisers on these projects.

[1] Herrington, “The debatable land”; Willmetts, “The CIA and the invention of tradition”.

[2] Richterova & Telepnava, “Secret Struggle for the Third World.”

[3] Andrew and Dilks (eds.), *The missing dimension*.

[4] Important contributions include: Shiraz, “Drugs and Dirty Wars”; McGarr, “Quiet Americans in India”; Goodman, *The Official History of the JIC*; Lockhart, *Chile, the CIA and the Cold War*; Rezk, “Egypt’s spy chiefs”; Walton, *Empire of Secrets*.

[5] Davies and Gustafson, eds. *Intelligence elsewhere*.

[6] Cormac, *Disrupt and deny;* Maguire, *Intelligence-Propaganda Nexus*.

[7] Berger, “The Real Cold War.”

[8] Westad, *Global Cold War*, 396.

[9] Rosenberg, “Uneven and Combined Development”, 569-597; Matin, “Uneven and Combined Development”; van der Pijl, *Global Rivalries;* Krasner, *Structural Conflict;* Kolko, *Confronting the Third World,* Halliday, *Cold War, Third World,* Karabell, *Architects of Intervention,* Rabe, *The Most Dangerous Area.*

[10] Girvan, *Corporate Imperialism.*

[11] Kothari and Wilkinson, “Colonial Imaginaries”.

[12] Smith, *The Secrets of Station X.*

[13] Heuser, oral history, 1.

[14] Smidt, oral history, 3.

[15] Boone, “Trade, Taxes and Tributes”, 463-467; Wolbert, oral history.

[16] Miller, “The intelligence coup of the century”.

[17] Heuser, oral history, 6.

[18] Annan, Speech at the ITU, 1999.

[19] Castells, *Networked Society*, 248.

[20] Maddrell, "What we have discovered”.

[21] Andrew, “Secret Intelligence and British Foreign Policy,” 9.

[22] Dover and Goodman (eds), *Spinning Intelligence*, 3-5.

[23] Davies, “Spies as Informants”.

[24] Riek, oral history.

[25] These were completed in 2011/12.

[26] One might also claim that the antecedents or Rubicon were quickly blown by East-West defectors as early as 1960, see Barrett, “Secrecy, Security, and Sex”.

[27] Bamford, *Puzzle Palace*, 391-425.

[28] Maquire, *Intelligence Propaganda.*

[29] Clark, *The Man Who Broke Purple*, 185-9.

[30] Bamford, *Puzzle Palace,* 408.

[31] Some of them were recently released, for an excellent analysis see Corera, *Intercept*.

[32] Bamford, *Puzzle Palace*.

[33] Sherman, “The William Friedman Collection”, 236.

[34] Strehle, *Verschlüsselt*.

[35] Miller, “The intelligence coup of the century”.
[36] Budiansky, *Code Warriors*, 251.
[37] Stockton, *Flawed Patriot*, 71-82.

[38] CIA, *Minerva*, 17-25.
[39] Personal for Freidman from Canine, July 22 1954; Personal Messages Concerning Hagelin Machines, Friedman Documents, NSAD.

[40] NSA “Draft Report of Visit to Crypto AG” March 1955.

[41] Melman, *Pentagon Capitalism.*
[42] Sherman, “The William Friedman Collection”, 216.

[43] Smidt, oral history, 10.
[44] Clark, *The Man Who Broke Purple*, 201; Sherman, ‘The William Friedman Collection’, 210.

[45] CIA, *Minerva*, 10, 46, 48.
[46] Shane & Bowman, “Rigging the Game”.
[47] Report of Visit to Crypto AG (Hagelin) by William F. Friedman, 21-28 February 1955; Memorandum of Colonel Davis, Subject: 16 June Comments of Mr Friedman, June 17, 1955.

[48] Ibid., 56.
[49] Budiansky, *Code Warriors*, 326.
[50] Ibid.

[51] Borger, “CIA controlled global encryption”.

[52] CIA, *Minerva*, 33, 42. Andre Mueller, head of the French codebreakers, was also repeatedly rebuffed.

[53] Heuser, oral history.

[54] SM-2721-52, Memo of the Reps. of the British COS.

[55] Aldrich, *GCHQ*, 207-15.

[56] T225/2074, 'Provision of On-line Cryptographic equipment for NATO'

[57] LCSB (62) 6, 22 May 1962.

[58] T225/2074, Stephenson to Trend, 29 June 1962.

[59] T225/2074, 'Provision of On-line cryptographic Equipment for NATO'.

[60] Foulkes, ‘Swiss Crypto AG’.

[61] Wolbert, oral history, 12-13

[62] Riek, oral history, 20.

[63] Heuser, oral history, 37.
[64] Audio Recording of the Press Conference, William H Martin and Bernon F Mitchell, Moscow, 6 September 1960, NSA60.

[65] Heuser, oral history, 1.

[66] CIA, *Minerva*; Heuser, oral history, 1, 11.

[67] Miller, “The intelligence coup of the century”.

[68] CIA, *Minerva,* 66-7.

[69] CIA, *Minerva*, 56.

[70] Miller, "The intelligence coup of the century". Private information.

[71] Document 02, Department of State, Memorandum of Conversation between Secretary of State Henry Kissinger and Argentine Foreign Minister Adm. Cesar Guzzetti, Secret, June 10, 1976 1976-06-10, National Security Archive, https://nsarchive.gwu.edu/briefing-book/southern-cone/2016-05-27/operation-condor-verdict-guilty

[72] Phythian, *The Politics of British Arms Sales.*

[73] CIA, *Minerva*,76
[74] Cole, *Operation Just Cause*, 59.

[75] Aid, *Secret Sentry*; Budiansky, *Code Warriors*, 59-77.
[76] Audio Recording of the Press Conference, William H Martin and Bernon F Mitchell, Moscow, 6 September 1960, NSA60.
[77] Ibid.
[78] Aid, *Secret Sentry*, 185.

[79] Private information.

[80] Heurer, oral history.
[81] CIA, *Minerva*, 83-7.

[82] CIA, *Minerva*, 88.

[83] Private information.
[84] Baumann et al, 121-144,
[85] Voegele, Crytoleaks.
[86] Miller, "The intelligence coup of the century".

[87] Heuser, oral history, 11.

[88] Ibid., 2.

[89] CIA, *Minerva*, 54.

[90] Smidt, oral history, 11-12.

[91] Theveßen, Müller and Stoll, #Cryptoleaks.