




Exploring the relationship between crypto AG and the CIA in the use of rigged encryption machines for espionage in Brazil

Vitelio Brustolin 

Harvard University and UFF

Dennison de Oliveira 

University of Parana

Alcides Eduardo dos Reis Peron 

University of São Paulo (USP)

Abstract *In this article, we explore how the United States developed an intelligence strategy that, since the Cold War, has been based on relationships with private high-tech companies. Specifically, we analyse documents that demonstrate that the Swiss company Crypto AG – a supplier of cryptographic equipment to more than 120 countries – was controlled by the CIA. We analyse the implications of this for Brazil, in a comparative perspective with the experience of these other nations. Our methodology includes: (1) analysis of documents recently declassified by the US and Brazil; (2) analysis of budget expenditure data; (3) information made available by Crypto AG on its international operations. In our conclusion, we highlight the irrefutability of the relationship established between the CIA and Crypto AG, which lasted from the 1950s to 2018. Finally, we present documents that show that Brazil continued to buy cryptographic equipment from Crypto AG for its Armed Forces until 2019.*

Introduction

On 11 February 2020, Greg Miller, a national security correspondent for the *Washington Post*, published an article created in partnership with the German public TV station *Zweites Deutsches Fernsehen*, entitled: ‘*The intelligence coup of the century: For decades, the CIA read the encrypted communications of allies and adversaries*’ (Miller 2020). The article was about the company *Crypto Aktiengesellschaft* (Crypto AG), formally a private company based in Switzerland, that dedicated itself, between 1950 to 2018, to the sale of encoding and decoding devices to more than 120 countries. However, the article also revealed that the company was secretly owned by the Central Intelligence Agency (CIA) and its German counterpart, the *Bundesnachrichtendienst* –

The authors are grateful to Sarah Block for her crucial assistance.

German Federal Intelligence Service (BND). Both intelligence agencies rigged the company's devices, so they could easily break the codes that countries used to send encrypted messages. Cryptographic machines were thus transformed into espionage equipment, becoming permanent and invaluable sources of information. Brazil, which is the focus of this study, is among the many countries that purchased equipment from Crypto AG.

The article provided data on how possession of the secrets revealed by rigged cryptographic machines helped the American government for many decades. This is because, on several occasions, access to secret communications from other countries gave the United States a substantial advantage.¹ Examples of this advantage would be: (1) information to respond to the Cold War (1947-1991) crises; (2) eventual disclosure of the identity of dual agents; (3) production of an extensive source of information that helped shape the United States' foreign policy (Dover and Aldrich 2020).

The revelations from the joint reporting of the *Washington Post* and the *Zweites Deutsches Fernsehen* have the potential to dramatically change the way in which the Cold War history is understood and interpreted. The fact that the American authorities knew in advance what the governments of other countries would do, can lead to extensive reviews on how several episodes of the Cold War were decided.²

What can also be highlighted from the article is that the impact of secrets and data leaked by Crypto AG's rigged machines in different countries needs to be examined taking into account the relationship that each of these countries had with the company. In addition, it is important to investigate what types of machines were purchased, what they were used for, and for how long they were in operation.³ In order to better delimit these issues, a brief examination of the company's history is necessary. Then, problems and research topics related to the company's relationship with different institutions in Brazil will be presented.

Crypto AG began to establish its links with the US government during World War II. The company was founded by Boris Hagelin, a Russian immigrant based in Sweden who, with the German occupation of almost all of Europe, emigrated to the United States. Once in the US, Hagelin founded Crypto AG, a company dedicated to producing cryptographic machines for US troops. The company quickly gained a worldwide reputation for manufacturing such equipment (Miller 2020). With the end of the war, the company and its founder returned to Sweden, without losing his commercial, personal and institutional ties with the US government.

¹ 'It was revealed that, through Crypto AG machines, the BND and CIA had profound knowledge of South American human rights abuses in the late 1970s. Operation Condor was the collective effort of six South American military dictatorships Chile, Argentina, Bolivia, Paraguay, Uruguay and Brazil to defend their territories and rule against purported challengers, predominantly through extreme violence. Evidence confirms a number of disturbing violations against their own population. This included the imprisonment of nuns and priests, as well as the murder of those who opposed their rule by throwing them out of airplanes without parachutes. To coordinate atrocities and maintain secure communications, the Condor countries relied on manipulated Crypto AG encryption devices (Miller and Mueller 2020). American and German inaction in the face of these human rights violations indicates that there were other (as yet unknown) factors in play during this time' (Dobson 2020).

² Dymydiuk (2020), Miller (2020), and Jacobs (2020), for example, discuss the US quandary over the Malvinas/Falklands War.

³ This information is presented in Section 4.

Negotiations started in 1955 – as shown in the National Security Agency (NSA) report that will soon be presented⁴ – and in 1958 an agreement between the company and the CIA began to produce equipment that generated messages that would be easily read by American spies. The agreement ‘secretly allowed NSA to design and insert backdoors in the cryptographic equipment supplied at least through 1992 to some [of] Hagelin’s customers, intelligence agencies of governments whose policies were decidedly hostile to the United States’ (Konheim 2015, 310). In the early 1950s, Hagelin moved the factory from Sweden to Switzerland, which had the effect of reinforcing the company’s image as being ‘neutral’, gaining credibility and leveraging sales of its products worldwide.

In the 1960s, the CIA’s control over the company increased, with the transfer of technology developed by the United States to machines that were destined to leak secrets from its future buyers. The United States also provided generous financial subsidies to Crypto AG (Miller 2020).

In 1970, the company was transferred from the Hagelin family to the control of CIA and BND agents, expanding its business, the number of employees and the scale of production. The management of the company’s activities was shared by the CIA with another American agency, the National Security Agency.⁵ These agencies controlled Crypto AG. They imposed themselves on their German partners, developing the technology of cryptographic machines, sabotaging the algorithms to make them easily decipherable, and choosing the countries and institutions as targets for sales. Both countries, the United States and Germany, identified which companies were to serve as subcontractors of Crypto AG at different stages of the production process. The Germans chose Siemens for commercial and technical advice, while the Americans chose Motorola to repair problematic equipment. The partnership with Siemens served as a cover story for the origin of the systems that Crypto AG workers installed on the machines, which were actually developed by the NSA (Miller 2020).

The relationship between the CIA and the NSA was often tense, marked by inter-bureaucratic rivalry. The NSA, created in 1952, managed to obtain a monopoly on intelligence operations based on the collection of information by intercepting communication signals. The agency grew significantly, with a billion dollar budget and more than 100,000 employees in the late 1960s. Half of the agency’s operations were dedicated to the interception, decryption and interpretation of messages from the Soviet Union. The information obtained by the NSA supported all levels of the US government (Bauer 2013, 346).

On the other hand, the CIA, despite having been created before, in 1947, was charged with intelligence operations based on the collection of information by agents.⁶ The CIA was also dedicated to executing and directing clandestine actions abroad, under the authority of the President. The CIA was responsible

⁴ United States of America, National Security Agency (1955b) ‘Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February’ [second draft] <https://www.nsa.gov/Portals/70/documents/news-features/decclassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf> accessed 20 July 2020.

⁵ The NSA was created in 1952 for studies, research, and intelligence operations. The NSA is also responsible for the interception, cryptographic analysis and protection of American communications.

⁶ United States of America, Central Intelligence Agency (2007) ‘History of the CIA’ <www.cia.gov/about-cia/history-of-the-cia/index.html> accessed 24 July 2020.

for providing information and intelligence reports to the president and his cabinet.

The fact that both agencies have conducted Crypto AG's operations for decades without raising suspicion suggests that, at least in this case, collaboration has supplanted competition. It is possible that there was a permanent agreement between the two agencies that made the operations of Crypto AG coherent and effective. This is a rare case in the trajectory of the two organisations. Little has been published on the subject, but it is known that the history of the NSA is marked by tensions and disputes with the CIA (Mainwaring 2020). Disputes continued despite efforts starting in 1977 to force the NSA and CIA to reach an agreement to resolve the interagency conflicts.⁷

It was an ongoing challenge to maintain the secrecy behind Crypto AG's true control including the features and purposes of the equipment sold. Not only its existing and potential customers but also from its employees, developers, partners and representatives who had no knowledge of the real purpose of the company's operations despite sporadic press reports which over the years exposed the company and its clandestine operations. For example, in 1995, the *Baltimore Sun* revealed connections between Crypto AG and the NSA (Murakami Wood and Wright 2015, 134–135).⁸

On other occasions, company representatives were publicly embarrassed or even arrested, as in the 1992 incident in Tehran, when the Iranian government arrested Crypto AG's top salesman, Hans Buehler (Bauer 2013, 355). With each new episode, Crypto AG lost customers and failed to attract new business. The company was finally liquidated and sold in 2018 to Crypto International Group.⁹

The authors of this article found a report classified as 'Top Secret' by the NSA, which was declassified on 20 June 2014. The NSA released two versions of the report entitled '*Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, National Security Agency, 21–28 February, 1955*', a first¹⁰ and a second draft.¹¹ Both versions of the report were redacted by the NSA prior to being declassified, however a comparison of the two versions released reveals that the redacted information did not always coincide and, therefore, it is possible to read, in the first draft, information that is hidden in the second. Additionally, the first draft was released by the NSA, but on a different date: 22 July 2014.

⁷ United States of America, National Security Agency (1998) 'American Cryptology During the Cold War, 1945-1989' <www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/cold_war_iii.pdf> accessed 23 July 2020.

⁸ In 1975, former CIA agent Philip Agee wrote that Swiss-made Hagelin machines had vulnerabilities that the NSA used to exploit to decipher messages from the United Arab Republic. Johnson, TR (1995) 'American Cryptology During the Cold War, 1945-1989', Center for Cryptologic History, National Security Agency, Ft. George G. Mead, MD, p. 83.

⁹ Crypto International Group's Official Website: <<https://crypto.ch/en>> accessed 4 May 2020.

¹⁰ United States of America, National Security Agency (1955a) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February' [first draft] <<https://cryptome.org/2015/07/nsa-crypto-ag.pdf>> accessed 20 July 2020.

¹¹ United States of America, National Security Agency (1955b) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February' [second draft] <https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf> accessed 20 July 2020.

Exploring the relationship between crypto AG and the CIA 5

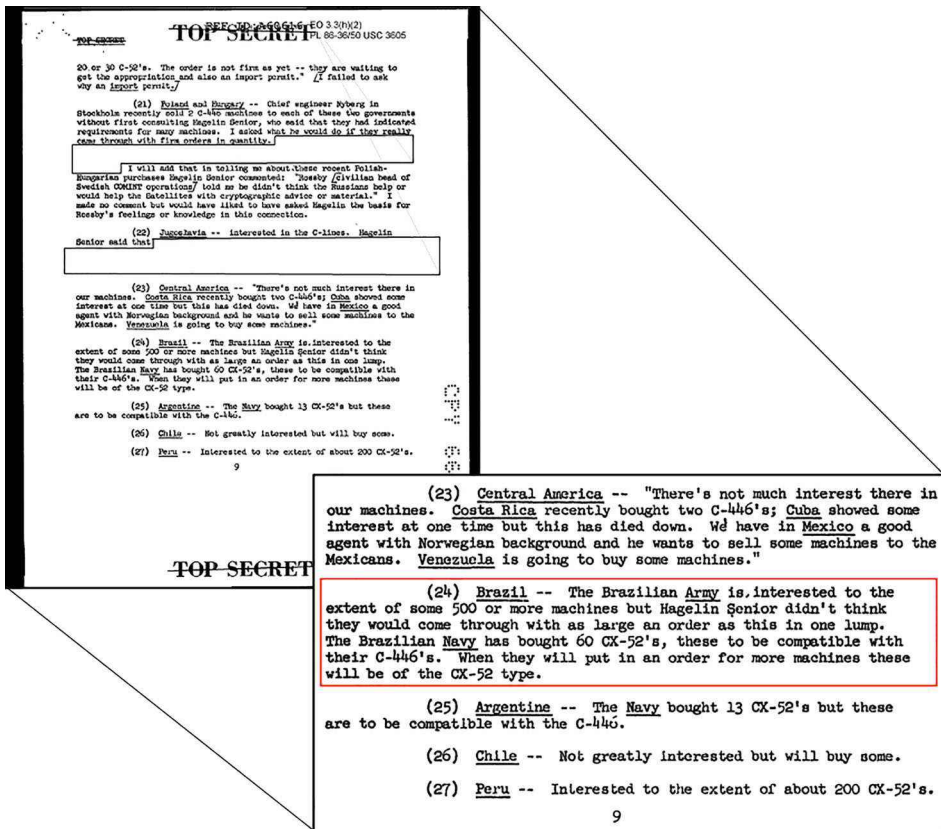


Figure 1. First Mention of Brazil in the NSA Report (1955).

Source: United States of America, National Security Agency (1955a) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February', p. 9 [second draft of the document].

The NSA report mentions several countries that, at the time, had acquired or were negotiating the acquisition of cryptographic machines produced by the Swiss company Crypto AG. Brazil stands out among these countries, with the following mention (Figure 1).

According to the NSA report, 'the Brazilian Army is interested to the extent of some 500 or more machines but Hagelin Senior didn't think they would come through with as large an order as this in one lump.' On the other hand, '... the Brazilian Navy has bought 60 CX-52's, these to be compatible with their C-446's. When they will put in an order for more machines these will be of the CX-52 type.'

Brazil is mentioned a second time, on page 12 of the second draft of the report (Figure 2).

At this point in the NSA report, a contract for teleciphering machines with the company Siemens is mentioned, adding that this company had divided the market with Crypto AG. Brazil emerges as a client only of the latter.

The NSA report potentially allows the reinterpretation of historical facts from the second half of the 20th century. This is because, as emphasized above, the company Crypto AG was in fact formally acquired by the CIA in 1970, configuring what was called, in 2020, 'the intelligence coup of the

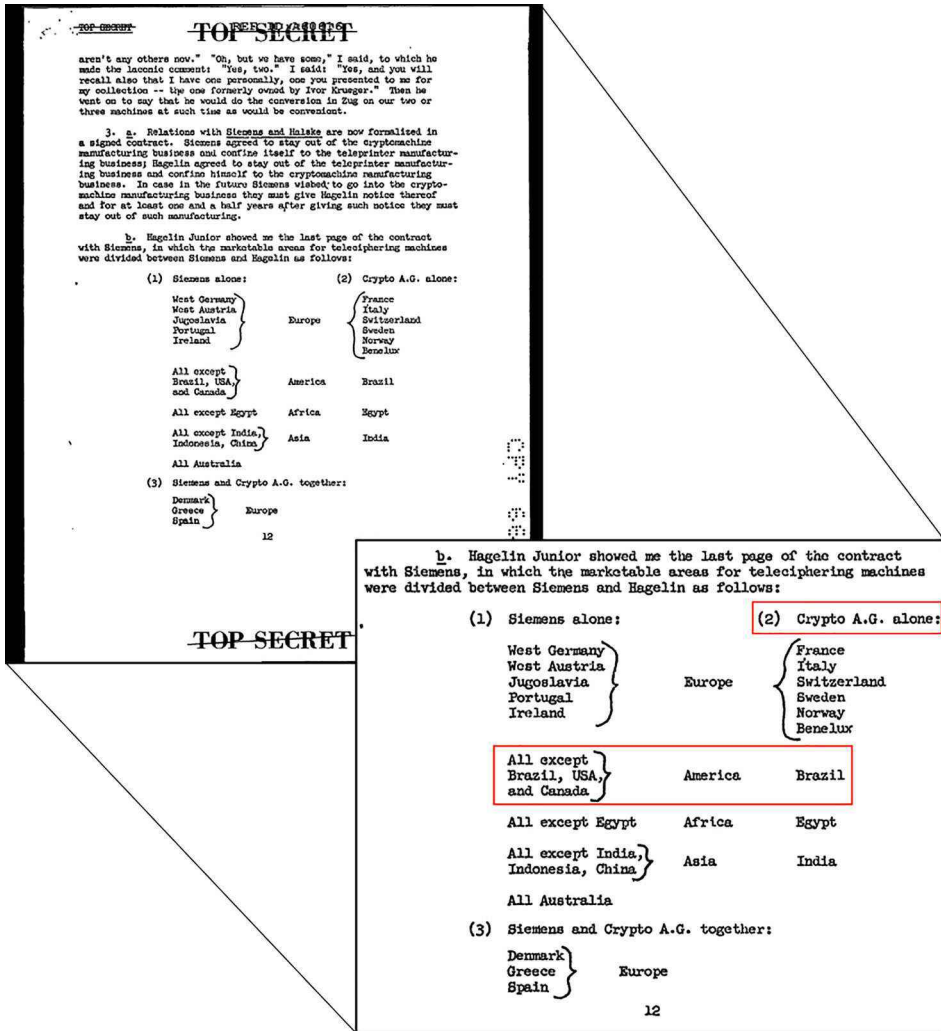


Figure 2. Second Mention of Brazil in the NSA Report (1955).

Source: United States of America, National Security Agency (1955b) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February', p. 12 [second draft of the document].

century' (Miller 2020), and its products were sold to many countries as encryption and secure communications solutions. In addition, the report is evidence that disinformation (counterintelligence), interception and information control underpinned the technological and strategic basis of the USA power in the 20th century.

In light of this, an in-depth analysis demonstrates the way in which the United States used an intelligence strategy that, since the Cold War, has been sustained by public-private partnerships. Thereby the US considerably expanded its capacity for information control and bestowed countries like Brazil a position of dependence and subservience to these technologies. In addition, the report reveals evidence that the United States has potentially

intercepted and read secret communications from Brazil and other nations since the end of World War II.¹²

For methodological purposes, we accessed the aforementioned NSA report, in addition to historical documents, recently declassified by the Brazilian Government, reporting the acquisition of equipment for use by the Armed Forces, as well as the role of the Ministry of Foreign Affairs of Brazil in these acquisitions. We also analysed budget expenditure information, obtained through the Transparency Portal of Brazil.¹³ A considerable part of our comparative analysis employed discussions contained in scientific and investigative articles, as well as books that report the relationship between Crypto AG and the NSA. We also analysed information publicly provided by Crypto AG, about its equipment and its international operations. The theoretical and methodological assumptions of this article are related to some of the key discussions on intelligence, surveillance and encryption in the formation of the US global power.

That said, this article is divided as follows: initially we discuss the relationship between surveillance, intelligence and power. Next, we analyse the extent of the partnership between Crypto AG and the CIA – with the NSA as a technical partner – in the ‘global surveillance and intelligence network’. Finally, we analyse how Crypto AG has been operating in Brazil, which equipment has been purchased and implemented and which actors have participated in this process.

Surveillance and intelligence: knowledge production and power organization

The control and management of information conducted by the State, which characterizes intelligence activity, is considered fundamental for the guarantee of strategic advantage and for maintaining and amassing power. In this sense, intelligence capability is an immense range of activities that encompasses the surveillance and monitoring of individuals, data and signals, and the processing and analysis of this information, and in turn developing relevant material for decision makers.

In general, the maintenance of intelligence capabilities allows the State to anticipate the movements of other actors, to refine its action strategies in both the military and diplomatic fields. In a broad sense, intelligence activity is a grey zone between diplomacy and war, and can be defined as the collection and processing of information in a discrete or secret manner about actors, threats and other states (Herman 1996). The objective of a State’s intelligence agency is the preservation of national security, the stability of its foreign policy and the protection of its people, processes and products related to these processes (Warner 2007; Gill and Phythian 2018). The gathering of information can also be defined in strategic terms, such as knowledge and foreknowledge of

¹² The literature review reveals that the interception of communications could have been happening since the First World War (Yardley 1981, 222). Prior to the use of cipher machines in the 1930s, manual methods of encryption had to be used for diplomatic and secret correspondence. Yardley describes some of the codes in use and the methods he used to decipher those codes, while working for the US State Department.

¹³ An official accountability tool of the Brazilian Government.

the world and supporting decision making. In addition, it can be defined in tactical terms, such as events and conditions on specific battlefields and providing 'situational awareness' (Johnson 2007, 1).

Therefore, intelligence is an activity that encompasses a cycle of procedures, that includes but is not limited to (1) Targeting – identification of objectives, which can range from individuals, military installations, and population contingents. (2) Collection – the survey of elements and sources. (3) Analysis – apprehension, adding value and exploring the implications of the material obtained. (4) Dissemination and analysis – in which the intelligence material reaches decision makers (Gill and Phythian 2018; Hedley 2007).¹⁴

The intelligence cycle can occur in different ways, from different inputs, as described below. Human (Humint), when civilian or military agents, linked to embassies or other agencies, are responsible for obtaining information and its dissemination. Technological (Techint), telemetric signals, from satellites or radar, in addition to image intelligences, different signal metrics, become central to obtaining and intercepting materials (Richelson 2007; Hedley 2007; Harris 2016). According to Herman (1996, 40), in the 1970's, the American intelligence effort for data collection was 87% directed at technological intelligence agencies.

In all cases, the intelligence activity empowers the State through the accumulation of knowledge about the actors and processes via surveillance and monitoring. The knowledge extracted from the surveillance activities serves as raw material that, when properly worked, constitutes an apparatus to anticipate threats and movements from other actors and consequently, to manage these movements.

In this sense, the studies on surveillance – perhaps the main stage of the information activity cycle – enhances our perspectives on how Intelligence becomes a coercive and modulating defence capability that is essential to maintaining the power of states. Surveillance has been, for a long time, a key determinant for both the design of political-military strategies and for the establishment of population control and management (Marx 2015; Lyon 2018).

The practice of surveillance encompasses constant observation of subjects, their pattern of relationships and communications, but thanks to new big data techniques, the analysis of metadata gathered from smartphones, web and other *dispositifs*¹⁵ widened the scope of subjects and the type of information acquired. Its purpose is not solely to identify individuals, but primarily to assemble knowledge about the individual or entities observed and their patterns and movements. Big data techniques allow a series of automated (machine learning) systems to collect and process unstructured data, which means raw data produced by users on the web, individuals in their phones, or interacting in social networks which are not related to a communication process. For instance, the access to a website, the patterns of visualization of certain contents, the pattern of circulation of an individual through the GPS data analysis on his phone, are examples of metadata analysis, or data produced

¹⁴ Herman (1996) adds more intelligence activities to those listed above. He includes counterintelligence, for example.

¹⁵ *Dispositif* or *dispositive* is a term used by Foucault, generally to refer to the mechanisms and knowledge structures which enhance and maintain the exercise of power within the social body (Foucault 2014).

over unstructured data. In this case, when a pattern is identified, the method of surveillance evolves to identify the changes and irregularities in the individual or entities targeted.

It requires the collection of specific information – criminal practices, health, and/or political-strategic knowledge – about those monitored. As Michel Foucault (2014) discusses in ‘Discipline and Punish’, disciplinary power is based on the control and administration of individuals through examination of schools, factories, hospitals, prisons, etc. For Foucault, there is also biopower, a technology of power for managing humans in large groups. Biopower could allow control of entire populations.

So, both disciplinary power and biopower are exercised by ‘hierarchical surveillance’, where the State – as a higher institution or via its omnipresent data collection – performs constant surveillance. This practice is designed to produce both information about and as a means of coercion of those monitored, forcing them to submit to norms and other accepted forms of behaviour (Foucault 2014, 169). Thus, the primary role of surveillance is to help to control individuals and organizations without requiring the use of force or violence, therefore, the use of surveillance by the State constitutes a fundamental component that forms the modern bases of sovereignty which is employed to maintain governmental control and power (Gill and Phythian 2018, 68).

Although surveillance activities can be practiced by other institutions (corporations for example), regardless of whether it is an official State activity, there is a fundamental need for intelligence. The production of useful and actionable information underlies both surveillance and intelligence. It is a way of sustaining and increasing power, whether in its micro dimension, or in the configuration of a State and its social security apparatus. In this sense, there is a profound connection between the activities of surveillance and intelligence, not only by the way these increase power via knowledge acquired from frequent monitoring, but fundamentally, by the way these activities influence and change the individuals and activities monitored (Gill and Phythian 2018).

Both surveillance practices and intelligence activities seek to produce information, constraints and control on those observed. That is, when the representatives of surveillance studies explore this practice, they describe it not as a passive way of collecting data and monitoring individuals, but as a process that acts on their bodies, altering their behaviour, ending-up taming it. Similarly, intelligence activity deploys the acquired knowledge as a way of influencing the reality observed, producing coercion effects in the military environment, or conducting interests in diplomatic contexts. In this case, the monitoring of groups, data, or individuals, may serve to subsidize diverse covert operations, produce deception in opponents (to mislead them), in general, intelligent activity is configured as an apparatus that modulates the reality on which it acts.

Recalling our definition of surveillance, which includes both the monitoring of behaviour and attempts to discipline it (or, the development of knowledge in order to deploy power), then we must acknowledge that, in practice, the two may be indistinguishable. For example, while the use of informers may be intended primarily to acquire information about their target, they may also (knowingly or unknowingly) have some impact on the activities of the target. Technical surveillance may be used overtly so that it

simultaneously gathers information and acts as a ‘scarecrow’ to deviant behaviours (Gill and Phythian 2018, 197).

Thus, as the coercive capacity of disciplinary institutions stems from their capacity to surveil and modulate individuals, the exercise of State power is developed through the deployment of a wide socio-technical network of intelligence. Instead of deploying violent and destructive methods, States build their intelligence capacities to operate both through formal and informal channels, and to use the knowledge acquired – or the interception and dissemination of information – to embarrass adversaries, to prevent access to sensitive information, and to minimize the harms of violent actions.¹⁶

This dynamic is clear when we analyse the restraint and control exercised by nations during the Cold War, when both the collection of information about the movements of opponents and the production of disinformation by the US were central as a deterrent.¹⁷ Many of the US intelligence operations were conducted at that time by the CIA and the Pentagon, with the NSA being one of the agencies responsible for refining information and producing intelligence. In the same period, a number of other agencies, organizations and technologies began to be developed to support these activities in the US – such as satellite and imagery agencies like the *Photographic Intelligence Center* (Bamford 1983, 245–246). Because of this, much of the US military spending during the years after the Second World War were linked to the capabilities of its intelligence. Spending was also directed to the development of further capacity to control information and intelligence, contributing to the goal of its use as a deterrent.¹⁸

Technint, private companies, and new entanglements for intelligence practices

In the same period, the US began to produce new communication technologies, which would be able to further its goal to stand out internationally (Morales 2005, 349). Thus, several technological initiatives were created in the so-called ‘Big Science’ (Weinberg 1961, 161–164). Among these programs, conducted by the Advanced Research Projects Agency (DARPA) and the Department of Defense (DoD), some stand out: (1) the Strategic Computing Program, whose objective was to develop new military technologies in artificial intelligence and computers, which would allow the creation of products, such as unmanned vehicles, conflict management systems, and other military systems. (2) Very High Speed Integrated Circuits, whose development of new military technologies in microelectronics would enable the production of microprocessors for armaments and control systems. (3) ARPANET, a first step in what would become the Internet, which allowed greater communication between research

¹⁶ Historically, the collection of information involves the chancelleries established in other countries and the collection of daily information (Herman 1996, 10).

¹⁷ In which, as stated by Buzan (1987), the information needs to be accurate in order to avoid mistakes and inappropriate expectations in addition to the ability to demobilize and frustrate opponents’ strategies. An example of this would be the military coups in South America during the Cold War, supported by the United States, through its intelligence network.

¹⁸ Mainwaring and Aldrich (2019) analysing the case of United Kingdom’s dominance over its colonial territories, pose that several technological developments in the period were determinant to sustain fast, economic and agile communication and signals interception.

agencies and the military in the US, in addition to increasing the capacity for the circulation of information (Pianta 1988, Medeiros 2005). Some of the aerospace programs developed in that period were not only related to the composition of military power and intelligence in the United States, but also to the establishment of a communication network via satellites. Satellites quickly became a fundamental component of communication infrastructure, and as a result earth orbit became a topic of dispute between countries competing for its use to enhance their technological communication network. Satellite communication and surveillance, in turn, would increase global capacity and control of the interception and collection of information. As a result, the National Reconnaissance Office (NRO) was founded in 1960, in Chantilly, Virginia (US), and the NRO was given responsibility for the design, construction and launch of spy satellites. In addition, the use of these satellites and photograph systems contributed enormously to the advancement of signals intelligence, electronics intelligence, and foreign instrumentation signals intelligence (Aid and Wiebes 2001, 3–4).

In parallel to the aforementioned agencies, several other agencies were founded, composing the collection of US Intelligence agencies. One of them is the Defense Intelligence Agency (DIA), also founded in 1961, whose objective, in addition to providing intelligence advice to other agencies, was to produce intelligence about the military capabilities of other countries, using all available means to do so. Public-private partnerships were of great importance in this context.

The configuration of a wide network of surveillance and intelligence strategies, marked by the growing role of socio-technical apparatus (*Technint*) in the strategic management of information at the expense of human performance (*Humint*) (Harris 2016). In this sense, the activities of collecting material and adding value during the analysis phase, have increasingly involved technicians specialized in identifying signals obtained via massive data collection algorithms, and who are able to react to threats (Harris 2016, 28).

For instance, throughout the period from the 1950s to the 1990s, most secret communications of countries around the world continued to be transmitted via teleciphering machines, and the largest supplier of this equipment in the world was Crypto AG. In the following decades, information technologies and Big Data techniques became the centre of the accumulation processes, in which 'Big Techs' and several other private companies began to organize and practice surveillance as a business, in some cases, aligning and providing intelligence infrastructures for States (Zuboff 2019).

In this context, in which public-private relations were of great importance in the organization of intelligence apparatus, we found that Crypto AG's involvement with the NSA was previously mentioned in a few academic papers, but Brazil was rarely cited. Before the 11 September 2001 attack, some reports made the connection between Crypto AG and the NSA, and some of them are described in the article by Murakami Wood and Wright:

Prior to 9/11, perhaps the single most in-depth account was a series of articles called 'No Such Agency' (Shane and Bowman 1995) published by the Baltimore Sun, the 'local

paper' of the NSA. Over a decade after *The Puzzle Palace*, the pieces summarised most of the Bamford and Campbell material and provided histories of the NSA, including some newer allegations particularly over the NSA's subversion of the leading international cryptographic equipment supplier Crypto AG and world-leading software provider, Microsoft. These allegations were expanded upon by the whistle-blower who, prior to the 2000s, was the most vociferous critic of the NSA, Wayne Madsen. (Murakami Wood and Wright 2015, 134-135).¹⁹

In 2004, Rudner summarizes the number of countries that had their communications compromised, as well as the possible speed at which the crypto breach could be made:

Countries that still relied for their communications security on Hagelin-type encryption machines manufactured by the Swiss firm, Crypto AG, were especially vulnerable. These machines were similar in design to the German Enigma, which had already been overcome by British cryptanalysts during World War II. In order to shield its ongoing cryptographic efforts, British intelligence kept secret its Ultra success for decades afterwards. From the 1970s onwards, a covert arrangement between the NSA and Crypto AG effectively compromised the communications security of successive models of their encryption machines. As a result, the ostensibly secure diplomatic and military communications of some 130 countries relying on Crypto AG encryption machines were effectively accessible to the NSA and therefore to other UK USA partners. NSA and GCHQ supposedly could read the coded messages as fast or faster than the intended recipients. (Rudner 2004).

It should be noted that although Rudner estimated that around 130 countries had their secure diplomatic and military communications accessible to the NSA, most authors estimate that this number is closer to 120, as shown below.

In 2009, evidence about the cryptographic breach of Crypto AG equipment appears most clearly in the work of Jan Bury, who presents documents that 'suggests that messages encrypted with Hagelin CX-52 machines were read by the Poles during the 1960s' (Bury 2009). Allegations of impropriety became public in the late 2010s and the statements by former NSA technical director Brian Snow were quite clear:

He suspects in some cases cloud providers will be companies influenced by government spy agencies, similar to the way Crypto AG security gear gave the NSA backdoor access to encrypted messages sent by foreign governments that had bought the gear. 'Please don't use Cloud AG,' he said. (Greene 2010).

In 2013, Craig Bauer points out in his work 'Secret History: The Story of Cryptology', that the NSA and Crypto AG signed an agreement as early as 1958. Additionally, the first public suspicions about the involvement between the NSA and Crypto AG date back to 1983:

As the story goes, the deal was not made in a single trip. Friedman had to return, and in 1958 Hagelin agreed. Crypto AG machines were eventually adopted for use by 120

¹⁹ Scott Shane is an American journalist. Tom Bowman is National Public Radio's Pentagon reporter. James Bamford is an American journalist and documentary film producer. Duncan Campbell is a British freelance investigative journalist. Wayne Madsen is an American writer specializing in propaganda and international affairs.

nations, but it seems unlikely that they were all rigged. According to some accounts the security levels provided depended on the country in which the machine was to be used. In any case, there doesn't appear to have been any suspicion of rigging until 1983. Twenty-five years is a tremendous time to keep such a large-scale project secret. If true, this would be one of the greatest success stories of all time in the intelligence community. Since the 25-year time period includes the switch from electro-mechanical machines to computerized digital encryption, the back doors would have to have remained in place through this transition. (Bauer 2013, 355).

Bauer also points out that the reports available up to that point about the association of Crypto AG with the NSA were 'not nearly as detailed as we would desire' (Bauer 2013, 356). Moreover, he adds: 'it should be noted that Crypto AG executives have consistently denied the existence of back doors in any of their machines, as one would expect whether the tale is true or not' (Bauer 2013, 357).

In 2015, Konheim reiterated that the agreement between NSA and Crypto AG was signed in 1958. In addition, he points out that the cryptographic equipment would have been provided until at least 1992 'to some Hagelin's customers, intelligence agencies of governments whose policies were decidedly hostile to the United States':

The alleged agreement in 1958 negotiated by the retired American cryptographer William Friedman and Boris Hagelin, the founder and CEO of the Swiss company *Crypto AG*. It secretly allowed NSA to design and insert backdoors in the cryptographic equipment supplied at least through 1992 to some of Hagelin's customers, intelligence agencies of governments whose policies were decidedly hostile to the United States. (Konheim 2015, 310).

After the publication of Miller's article, Dymydiuk also published an article on the topic:

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. (...) 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 (...) 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' (Dymydiuk 2020, 1-2).

Further work on the Crypto AG case was published after Miller's article: Aldrich (2020), Dobson (2020), Dover (2020), Jacobs (2020), Mainwaring (2020). Studies on the topic are likely to continue to be published over the years, helping to rewrite history.

This literature review demonstrates that suspicions about the connection between NSA and Crypto AG have grown over the past two decades. Despite

this, the publications presented little documentary evidence and any evidence regarding Brazil is practically non-existent.

It should be noted that access to strategic information from more than 120 countries around the world is certainly a true ‘knowledge-power’, centred on the production of intelligence for subsidizing interventions.²⁰ Currently, several companies that provide services and communication solutions – just like Crypto AG – are part of this intelligence information network. It is common for system users to provide information voluntarily. This is a practice that reveals the persistent nature of public-private interaction that is characteristic of US intelligence and counterintelligence policies (Dobson 2020, 4).

Moreover, supported by sophisticated socio technical devices, intelligence activity increases the power of states. In addition, intelligence can also frustrate opponents’ expectations, as it has a disciplinary function.

In the following sections, we will analyse the relationship between Crypto AG and the NSA. In addition, we will describe how Brazil may have been affected by these interceptions and espionage procedures.

Crypto AG and the global surveillance and intelligence network

The information made available by Greg Miller in the Washington Post, although succinct, may potentially rewrite several chapters of recent history, as well as indicate relevant historical issues. The number of intercepted messages from the CIA’s rigged machines is considerable. It was through the rigged encryption machines of Crypto AG that the US collected most of the information about several countries, including some of those allied to the Soviet Union and communist China.

All the information available refers to a few sources, with emphasis on the official history of the operation written by the CIA in 2004 and another written by the BND in 2008, interviews with former intelligence officials in both countries and former Crypto AG employees, in addition to a few other documents. These sources show that countries from all over the Middle East, Latin America, India, Pakistan, and the Vatican bought encryption machines rigged by the CIA.

By secretly using encryption machines rigged by the CIA, the US followed the conversations between different Iranian authorities, during the hostage crisis after the invasion of the US Embassy in that country in 1979. It also enabled the US to provide information to the British about conversations between Argentine authorities during the Malvinas/Falklands War (1982). This last episode served to arouse the suspicions of the Argentine authorities about the reliability of the cryptographic equipment, concerns that were at the time

²⁰ ‘The post-Second World War signals intelligence (SIGINT) cooperation between five Anglo-Saxon countries – Australia, Canada, the United Kingdom, New Zealand, and the United States – is well-documented. This alliance is often called Five Eyes and is based on the 1946 UKUSA Agreement. What is not publicly known so far is that there is a second, parallel, western signals intelligence alliance, namely in north-western Europe, also with five members. It has existed since 1976 and is called Maximator. It comprises Denmark, France, Germany, Sweden, and the Netherlands and is still active today. The Maximator alliance deepens our understanding of the recently-revealed operation Thesaurus/Rubicon: the joint CIA-BND ownership and control of the Swiss manufacturer of cryptographic equipment Crypto AG, from 1970 to 1993.’ (Jacobs 2020, 1).

dispelled by one of the employees of Crypto AG, who was in reality fully aware of the real purpose and surveillance capabilities of the machines. The Argentines continued to buy and use equipment from Crypto AG (Miller 2020).

Other episodes demonstrate the power and usefulness of these machines in intelligence gathering, such as: (1) the revelation of the authors of the bombing in a Berlin nightclub in 1986 – Libyans of the Gaddafi regime, (2) The discovery of the whereabouts and subsequent arrest of the former Panama dictator Manuel Noriega – obtained from Vatican communications, (3) The revelation that Billy Carter, brother of the President of the US, Jimmy Carter, received money from Libyan leader Muammar Gaddafi to defend his interests in Washington (Youssef 1981). The NSA also used Crypto AG machines purchased by Egypt to secretly monitor President Anwar Sadat's communications in 1978, during the peace negotiations between Egypt and Israel.

It is possible to conclude that there is abundant evidence to infer that the espionage operation conducted by the CIA/BND through Crypto AG had a considerable (although not explicit) impact on a series of events and contexts. Uncovering this previously undisclosed connection between the CIA/BND through Crypto AG may lead to new areas of research, in order to explore a highly relevant factor which was largely ignored until recently: the use of Crypto AG machines by nations and organizations that had no suspicion of the real objective of this equipment.²¹

As previously mentioned, in the decades that followed the end of the Cold War, information technologies and techniques of Big Data and Machine Learning gained traction. The use of personal computers, smartphones, and other forms of communication focused on data processing became popular (Zuboff 2019; Lyon 2018).

The continued development of these technologies (Big Data and Machine Learning) has become known worldwide through the revelations of Wikileaks and former NSA contractor Edward Snowden, that pointed that not only private companies would be interested in collecting this data, but also states. Snowden revealed that the United States had updated its form of data collection and interception, using sophisticated systems in partnership and with the support of private companies (Bauman et al 2015, 10). In other words, a similar arrangement to what the NSA had been conducting with Crypto AG, since the 1950s.

In general, the Internet and the massive collection of data, in the decades after the end of the Cold War, became the new instruments for interception and production of intelligence information. As Bauman demonstrates, not only the USA or European states have resorted to this practice, but mainly collisions

²¹ '...because of an American-led scheme that began in the 1950s to weaken the Swiss cypher machines bought by countries across the Global South, signals intelligence was much more effective in places like the Middle East, Africa and Asia than in Europe. The West struggled to read Soviet codes and vice versa, but across much of the rest of the world, communications were largely an open book. Organisations like GCHQ and its American equivalent, the National Security Agency (NSA) read more than half the communications they collected. While most of this material is as yet unavailable, in years to come we will be able to see everything sent by Colonel Gaddafi and transcripts of all the phone calls made by Yasser Arafat – this will change international history significantly.' (Mainwaring and Aldrich 2019, 3).

between private companies and states have started to act more exposed in the production of information and intelligence.

Balance of power between agencies

One difficulty in the operation of Crypto AG was maintaining consensus between the CIA and the BND regarding the scope and purposes of sales of the machines. The available information shows that at least four countries were aware of the nature of Crypto AG's operations (or received information collected by the company through the United States or Germany): Israel, Sweden, Switzerland and the United Kingdom. Initially, the NSA resisted the idea of controlling Crypto AG, adhering to the CIA's initiative just to prevent the company from coming under French control (Mainwaring 2020, 7). Although the British had access to much information provided by Operation Rubicon, they never had any control over Crypto AG, thanks to the veto of their participation by the BND (Dover and Richard 2020, 8). In addition to the operational problems listed above, American managers apparently had less qualms about selling Crypto AG encryption machines to allies. This practice was in direct contrast to the German guidelines of the partners. The Germans were resistant to such practices and were more inclined to use the sale of Crypto AG's equipment as a source of profit that would enable the financing of other classified operations rather than for gathering intelligence from allies.

These tensions eventually led the BND to abandon Crypto AG in 1993. The risk of the operation being discovered appears to have weighed heavily on this decision. There was fear on the part of the Germans that, sooner or later, the clandestine activities and espionage policies practiced by their country would be exposed. After the Germans ended the partnership, the CIA went on independently to run the company, which, over the years, ended up becoming even larger than it was. In 2004, Crypto AG acquired one of its main competitors in the cryptographic machine business – the Swiss company Gretag AG. Finally, in 2018 the CIA dismantled the company, which was then, 'liquidated by shareholders whose identities have been permanently shielded by the byzantine laws of Liechtenstein, a tiny European nation with a Cayman Islands-like reputation for financial secrecy' (Miller 2020).

It is difficult to find evidence to explain why the partnership between the NSA and the CIA in managing Crypto AG lasted so long. One hypothesis to explain this is that the BND played a relevant role in this partnership. The BND exercised control over strategic companies like Siemens. Thanks to Siemens' operational support, the NSA continued to invest in technology to maintain the strategic advantages of machines manufactured by Crypto AG (Dobson 2020, 6). It is known that the CIA was primarily responsible for organizing the structure of the partnership. Both the CIA and the BND promoted the advertising, distribution and sale of Crypto AG machines. At the same time, both benefited from information obtained from countries that purchased the rigged encryption machines.

The NSA, on the other hand, had to develop and implement the mechanisms used to infiltrate in the machines that would be sold to the target countries. Neither the CIA nor the BND could replace the NSA in these tasks. In fact, the NSA has managed to build a true monopoly on knowledge in

cryptography, which has been maintained with increasing difficulty, due to the creation of new university courses dedicated to the subject (Dymydiuk 2020, 5). One of our hypotheses is that the nature of the division of tasks between these three agencies was a crucial factor in the stability of the agreement with Crypto AG. Only additional research or the publication of new discoveries on the subject can clarify the issue.

Relations between Brazil and Crypto AG

During the Cold War, relations between Brazil and the United States were marked by moments of tension and rapprochement. Among the moments of tension, we highlight the episode in which the Brazilian President, Jânio Quadros, gave a *Medal of the National Order of Cruzeiro do Sul* to the Argentine/Cuban revolutionary leader Che Guevara (1961). President Quadros also initiated a rapprochement with the Chinese government. These events represented a brief rapprochement between Brazil and communist regimes. On the other hand, during almost the entire military dictatorial period in Brazil (which began in 1964 and lasted until the re-democratization in 1985), there was a strong relationship between Brazil and the United States.

During the period of military dictatorship, Brazilian foreign policy was unconditionally aligned with the US. The only exception occurred during the presidency of General Ernesto Geisel (1974-1979). Geisel broke the military agreement with the United States, practiced independent foreign policy and repudiated the safeguards imposed by Westinghouse Electric Corporation for the nuclear agreement. This 'friendly relationship' between Brazil and the United States during almost the entire military dictatorship in Brazil, however, did not prevent the US from conducting espionage and surveillance on Brazil.

A first evidence of the relationship between Brazil and Crypto AG can be found in an NSA list of 13 January 1954, in the folder 'Friedman Documents'. The list is currently posted in William Friedman's folder on the NSA website, it includes a list of countries, including Brazil, that used Hagelin machines.²² As previously presented, Friedman was a special assistant to the director of the NSA, who in 1955 would visit Crypto AG.

It is highly likely that Brazil has continued to buy cryptographic machines exclusively from Crypto AG. Brazil even considered the US as a potential supplier of cryptographic equipment. The US, however, refused, as it did not want to set a precedent for other South American countries:

There is no way in which provision of such aid to one country could be kept a lasting secret from others. Requests for aid from Brazil, say, *favorably* considered, would lead to similar requests from Chile, and there would be no way of denying the same aid to Chile.²³

²² United States of America, National Security Agency (1954a) 'List' <www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_517/41789209082821.pdf> accessed 23 July 2020.

²³ United States of America, National Security Agency (1954b) 'Memorandum for the Members of the United States Communications Intelligence Board and the Members of the United States Communications Security Board: Implications of a Policy Which Would Permit Cryptographic Aid to Friendly Foreign Governments for their National Purposes' <www.nsa.gov/

Therefore, most likely, Crypto AG remained the only supplier of cryptographic equipment to Brazil.

A second and much more important evidence of Brazil's relationship with Crypto AG emerges in the report of the visit of William Friedman to Crypto AG, in 1955, as presented in the Introduction of this article.²⁴

In the document, the author notes Brazil's interest in buying 500 or more cryptographic machines, although in Hagelin's opinion, the actual order would not be so great. It is noteworthy that the Brazilian Navy had already purchased 60 units of the CX-52 encryption machine, compatible with those already acquired, the C-446 machines.

Here it is necessary to differentiate the equipment: C-52 and CX-52 machines were developed by Boris Hagelin and started to be manufactured by his company, Crypto AG, around 1952.²⁵ They are mechanical, but when combined with an electric keyboard accessory, the B-52, form a larger system, called BC-52, or BCX-52 (Bury 2009). There are other keyboard models, such as the B-62 and the B-621.²⁶ They all make encryption faster, since without the use of keyboards, the text needs to be encrypted letter by letter.²⁷ In turn, the C-446 machines, although also created by Boris Hagelin, are older, dating from 1946.²⁸ They were manufactured by AB Cryptoteknik, from Stockholm, Sweden, which was succeeded by Crypto AG itself.²⁹

According to the NSA report, the Brazilian Army was interested in the purchase of some 500 or more machines but Hagelin Senior didn't think they could produce such a large order as this in one shipment. On the other hand, the Brazilian Navy purchased 60 CX-52's.³⁰ Shortly thereafter, the machines in possession of the Navy could have been assigned in whole or in part to the Ministry of Foreign Affairs

Portals/70/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_373/41754969079412.pdf> accessed 23 July 2020.

²⁴ It should be noted that some authors claim that the partnership between Crypto AG and NSA would have been formalized in 1958 (Bauer 2013, 355).

²⁵ Crypto AG produced three different versions of each of its machines. The highest category was Best Security. These machines were the best that Crypto AG could produce, aimed at friendly countries, including NATO members. The instruction manuals were intended to ensure maximum safety for its users. Just below came the Medium Security machines, destined for neutral and friendly countries, liable to be infiltrated. Finally, there were Low Security machines, low quality equipment and with a simpler switching mechanism. The instruction manuals and guidelines for use were also different for each category.' See: Crypto Museum (2020d) 'The gentleman's agreement' <www.cryptomuseum.com/manuf/crypto/friedman.htm> accessed 14 September 2020.

²⁶ Some countries changed their machine versions to meet the strategic interests of the United States. Hagelin 'managed to persuade Brazil – who had purchased CX-52/RT machines – to swap them for the exploitable (readable) CX-52-M-27.' *In*: Crypto Museum (2020e) 'Operation RUBICON – THESAURUS' <www.cryptomuseum.com/intel/cia/rubicon.htm> accessed 14 September 2020.

²⁷ Crypto Museum (2020c) 'Hagelin CX-52: Advanced Pin-and-lug Cipher Machine, Keyboard B-52, B-62, B-621' <www.cryptomuseum.com/crypto/hagelin/cx52/index.htm#keyboard> accessed 4 May 2020.

²⁸ Crypto Museum (2020b) 'Hagelin C-446: Pin-and-lug Cipher Machine' <www.cryptomuseum.com/crypto/hagelin/c446/index.htm> accessed 4 May 2020.

²⁹ Crypto Museum (2020a) 'Crypto AG: Hagelin Cipher Machines' <www.cryptomuseum.com/crypto/hagelin/index.htm> accessed 4 May 2020.

³⁰ United States of America, National Security Agency (1955b) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February' [second draft] <https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf> accessed 20 July 2020, p. 9.

(MRE),³¹ as shown by the evidence presented below. This evidence was found in the 'Itamaraty Reports', official historical documents of Brazil, made available in the Archive of the Ministry of Foreign Affairs of the country.

In 1958, in the Annual Report sent to the Brazilian President, Juscelino Kubitschek, the Minister of Foreign Affairs, Francisco Negrão de Lima, communicated the merger of the Communications and Archive Divisions. The new arrangement gave space to a sector hitherto not mentioned in the reports: the Cryptography Sector (Federative Republic of Brazil 1958, 247).³²

The 1960 Report is probably the first document of the Brazilian Ministry of Foreign Affairs (already under the management of Horácio Lafer) to mention the mechanization of cryptographic practices:

(...) several and valuable modifications were made to the cryptography service. The first of these concerns mechanization (...) In order to replace the normal, slow system that is gradually becoming incompatible with the great increase in service, machines were installed in our Diplomatic Missions of greater importance and activity. Furthermore, studies were carried out aiming at the installation, in the near future, of similar devices in the various Diplomatic Missions and Consular Departments of Brazil abroad. These Missions and Departments would employ, according to their degree of importance and volume of work, cryptographic machines of different types and of greater or lesser complexity. The advantages of the system mentioned above over the manual are obvious. Initially, they represent a huge saving of time and consequently of money, since it allows the encryption and decryption of telegrams in a tenth of the time used by the classic method. Furthermore, what is even more important, is that the use of encryption devices brings greater security to the transmission of messages.³³ (Federative Republic of Brazil 1960, 232–233).³⁴

Another mention of cryptography in the Brazilian Ministry of Foreign Affairs appears in the 1965 Report, during the administration of Juracy Magalhães. Extremely vague and succinct, the text reveals that 'various activities of the Communications and Archive Division, especially of the Telegram Section of the Communications Service, cannot be in an ostensible report, and it would be better to be in a classified, secret and confidential report.' In that

³¹ Ministry of Foreign Affairs: 'Ministério das Relações Exteriores' (MRE), in Portuguese.

³² Brazil, Federative Republic of (1958) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/Relatoriosdoltamaraty/Relato%CC%81rio%201958#page/n267/mode/2up>> accessed 4 May 2020, 247.

³³ N.A.: Translated from the original, in Portuguese: '(...) foram introduzidas várias e valiosas modificações no serviço de criptografia. A primeira delas diz respeito à mecanização (...) Com o fim de substituir o sistema normal, lento e que vai se tornando aos poucos incompatível com o grande aumento do serviço, foram instaladas máquinas em nossas Missões Diplomáticas de maior importância e atividade. Outrossim, estudos foram realizados visando a instalação, em futuro próximo, de aparelhos semelhantes nas várias Missões Diplomáticas e Repartições Consulares do Brasil no exterior. Essas Missões e Repartições empregariam, segundo seu grau de importância e volume de trabalho, máquinas criptográficas de diferentes tipos e de maior ou menor complexidade. As vantagens do sistema acima referido sobre o manual são óbvias. De início, representam uma economia enorme de tempo e conseqüentemente de dinheiro, pois permite a cifração e decifração de telegramas em uma décima parte do tempo empregado pelo método clássico. Acresce também, o que é ainda mais importante, que a utilização dos aparelhos cifradores traz maior segurança à transmissão das mensagens.'

³⁴ Brazil, Federative Republic of (1960) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/Relatoriosdoltamaraty/Relato%CC%81rio%201960#page/n251/mode/2up>> accessed 4 May 2020, 232–233.

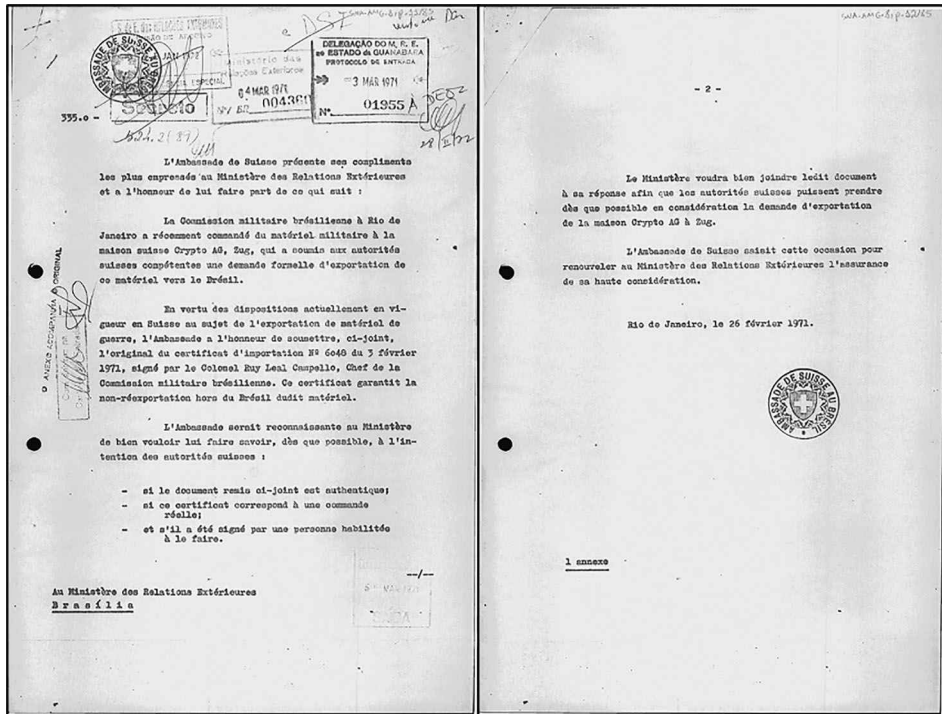


Figure 3. Correspondence from the Swiss Embassy to the Ministry of Foreign Affairs of Brazil about Crypto AG (1971).

Source: National Archives of Brazil.

year, the MRE promoted a public contest to hire cryptologists (Federative Republic of Brazil 1965a, 315).³⁵

The Head of the Communication and Archives Division (DCA)³⁶ of the MRE was intensely involved in initiatives in the area of cryptography. He taught cryptography courses himself. He also travelled, accompanied by a cryptologist, visiting a dozen countries in Latin America, 'in order to provide them with modern means of encryption, allowing for the first time, an on-site verification of the needs of Diplomatic Missions, visited in terms of communications and in terms of security of archives' (Federative Republic of Brazil 1965b, 316).³⁷

To complement the information obtained in the aforementioned reports from the Brazilian Ministry of Foreign Affairs, as well as the extent of the commercial relationship between Brazil and Crypto AG, the authors resorted to documentary research in the National Archives of Brazil. The documents show that the acquisition of cryptographic equipment took place in negotiations

³⁵ Brazil, Federative Republic of (1965) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/RelatoriosdoItamaraty/Relato%CC%81rio%201965#page/n291/mode/2up>> accessed 4 May 2020, 315.

³⁶ Communication and Archives Division: 'Divisão de Comunicação e Arquivos' (DCA), in Portuguese.

³⁷ Brazil, Federative Republic of (1965) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/RelatoriosdoItamaraty/Relato%CC%81rio%201965#page/n293/mode/2up>> accessed 4 May 2020, 316.

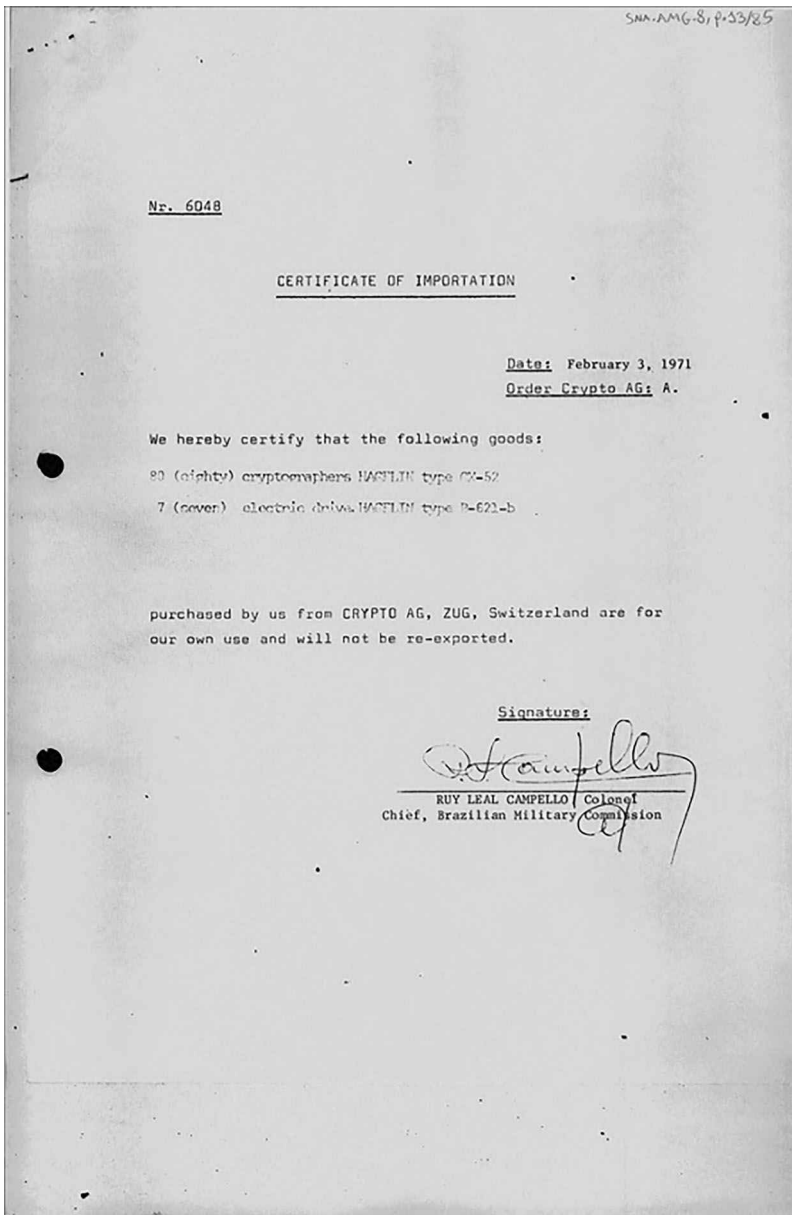


Figure 4. Certificate of Importation of Equipment from Crypto AG to Brazil (1971).
Source: National Archives of Brazil.

between national states, and not directly with Crypto AG. The negotiation passed through the Swiss Embassy in Brazil, as can be seen in the secret correspondence sent by that one to the Ministry of Foreign Affairs of Brazil, on 26 February 1971 (Figure 3).

The aforementioned correspondence, written in French and issued by the Swiss Embassy in Brazil, has an attachment, written in English. This is the

Certificate of Importation for 80 CX-52 encryption machines and another seven 'electric drive' type Hagelin B-621-b (as previously described, it is an electric keyboard). The Certificate dates from 3 February 1971 and is signed by the Chief of the Brazilian Military Commission, Colonel Ruy Leal Campello (Figure 4).

The references and documents presented above demonstrate that, in fact, Brazil acquired cryptographic equipment from Crypto AG between the 1950s and 1970s. Considering that the messages potentially began to be decrypted by the CIA in 1970,³⁸ when Crypto AG was acquired, it is likely that Brazil's secret communications may have been read by the United States for a long time.³⁹

Several countries in South America started using machines from Crypto AG in the second half of the 1970s. There is evidence that Brazil acted as a supplier of this cryptographic equipment to the other South American dictatorships involved in Operation Condor.⁴⁰ ⁴¹ Subsequently, Argentina also played the role of supplier of this equipment. The machines had been tampered with by the NSA.⁴² Thus, this proves the fact that American government officials

³⁸ As mentioned earlier in Section 2 and in another footnote, some authors claim that the partnership between Crypto AG and NSA would have been formalized in 1958 (Bauer 2013, 355).

³⁹ The National Archives and Records Administration II (Maryland, USA), has the records of the National Security Agency. There are 4,410,170 textual pages estimated in this Registration Group, of which only 132 digitised documents are available online. Among the various collections recently released for consultation, several concern Brazil. Of these, the most important are: 'Cryptographic Codes And Ciphers: Brazil Encode And Decode', 'Evaluation of Cryptographic and Cryptanalysis Work in Brazil'; 'Codes and Ciphers: Brazil', 'Brazil/General Communications Data', 'Correspondence to and from German Embassies Brazil', 'Portuguese-Brazilian Material in Files of MI-8'. Future research dedicated to these collections will certainly expand our knowledge about the American espionage of Brazilian communications. See: The National Archives and Records Administration (2020) 'Record Group 457 – Records of the National Security Agency/Central Security Service' <www.archives.gov/findingaid/stat/discovery/457> accessed 14 September 2020.

⁴⁰ National Security Archive (2020) "CIA cable, 'Communications System Employed by the Condor Organization,' Secret, February 1, 1977" <<https://nsarchive.gwu.edu/dc.html?doc=6773841-National-Security-Archive-Doc-3-CIA-cable>> accessed 23 July 2020. ["This CIA cable summarizes that 'All countries belonging to the Condor organization maintain communications (...) the cipher system employed by Condor is a manual machine system of Swiss origin given to all Condor countries by the Brazilians and bearing the designation CX52. The machine is similar in appearance to an old cash register which has numbers, slide handles, and a manually operated dial on the side which is turned after each entry.' According to William Friedman's tour report [see Document 6 below], Boris Hagelin sent machines similar to the CX52 to the NSA for testing. The CX52 is one of Swiss company Crypto A.G.'s flagship machines".

⁴¹ National Security Archive (2020) "CIA report, 'Counterterrorism in the Southern Cone,' Secret, May 9, 1977" <<https://nsarchive.gwu.edu/dc.html?doc=6773840-National-Security-Archive-Doc-2-CIA-report>> accessed 23 July 2020. ["A CIA summary of Operation Condor to the Carter Administration's NSC states that in 1976, 'Brazil agreed to provide gear for 'Condortel' – the group's communication network.' 'The Condor communications system uses both voice and teletype'"].

⁴² National Security Archive (2020) "DIA Intelligence Appraisal, 'Latin America: Counterterrorism and Trends in Terrorism,' August 11, 1978" <<https://nsarchive.gwu.edu/dc.html?doc=6773842-National-Security-Archive-Doc-4-DIA-Intelligence>> accessed 23 July 2020. ["[I]n late 1977, Argentina provided Hagelin Crypto H-4605 equipment to Condortel to enhance the security of its teletype nets.' 'Communications for operations in Latin America are to be provided by Condortel facilities. Operations conducted elsewhere are to rely upon coded messages transmitted by public cable or telephone facilities...' The Condor machines provided by Argentina (H-4605) are similar, if not a variant of, the Crypto H-460 which according to the Washington Post is "an all-electronic machine whose inner workings were designed by the NSA".

were aware of the kidnapping, torture and murder carried out by the dictatorships participating in Operation Condor.⁴³

There is no precise information on when the use of CX-52 type encryption machines ceased in Brazil. There are data, however, about the presence of the company Crypto AG in Brazilian territory. A 2014 publication, produced by the company itself, provides evidence about its office in Brazil, based in Rio de Janeiro, as a representative to all of Latin America (Figure 5).

Another edition of the magazine, from 2015, displays a map of the company's international offices. Brazil stands out in the Americas (Figure 6).

A search under the name Crypto AG on the Brazilian Transparency Portal (an official accountability tool of the Brazilian Government, which started in 2004)⁴⁴ shows that despite having a Center that produces encryption technologies inside the Brazilian Intelligence Agency, Brazil has continued to do business with Crypto AG until recently.⁴⁵ Twenty-Five records were found, all in recent years (2014-2019). All celebrated by the Ministry of Defence of Brazil and, in its entirety, for the Naval Command. A 2014 record stands out. This involves the acquisition of encryption technology for radio communication for the Brazilian Navy (Figure 7).

The document above, available only in Portuguese, shows that there was a financial transaction in the amount of US\$275,014 in the acquisition of the 'MultiCom Radio Encryption HC-2650' for the Brazilian Navy. In addition, similar expenses were repeated in 2015, when Brazil spent another US\$355,460 on this equipment.⁴⁶ In that same year, a new record emerged, adding US\$37,147 to expenses.⁴⁷ All of these money transfers went to Crypto AG.

This is the information provided by Crypto AG about the MultiCom Radio Encryption HC-2650:

From now on, all you need is a single encryption platform. The flexible MultiCom Radio Encryption HC-2650 meets all requirements regarding frequency ranges (HF, VHF, UHF, SatCom) and operating modes (narrowband/broadband, digital voice encryption, data encryption, secure messaging, IP VPN). With appropriate software updates, the system can also accommodate future additions and technical advances with ease, which eliminates the need for expensive and time-consuming new purchases. MultiCom Radio Encryption HC-2650 is suitable for connection to all military IP networks and for rendering all radio networks secure. Its superb diversity with respect to applications and

⁴³ As mentioned earlier, new document releases from The National Archives and Records Administration will certainly expand our knowledge about American espionage. See: The National Archives and Records Administration (2020) 'Record Group 457 – Records of the National Security Agency/Central Security Service' <www.archives.gov/findingaid/stat/discovery/457> accessed 14 September 2020.

⁴⁴ Transparency Portal of Brazil (2020a) '*O que é e como funciona*' [What it is and how it works]: 'the Federal Government's Transparency Portal is a free access site, where citizens can find information on how public money is used, in addition to information on matters related to public management in Brazil', <www.portaltransparencia.gov.br/sobre/o-que-e-e-como-funciona> accessed 4 May 2020. N.A.: Translated from the original, in Portuguese.

⁴⁵ Transparency Portal of Brazil (2020d) <www.portaltransparencia.gov.br/url/96d7ade6> accessed 4 May 2020.

⁴⁶ Transparency Portal of Brazil (2020e) <www.portaltransparencia.gov.br/url/70b16c8d> accessed 4 May 2020.

⁴⁷ Transparency Portal of Brazil (2020f) <www.portaltransparencia.gov.br/url/4b9ed865> accessed 4 May 2020.

Crypto AG strengthens its presence in Latin America

Bem-vindo and bienvenidos! Crypto AG has had a regional office in Brazil since the summer of 2014. Now it is even closer to its customers throughout Latin America and can talk with them personally to help them more effectively handle their information security challenges.

Tanja Dahinden | PR & Corporate Communications Manager

Rio de Janeiro – “January River” in Portuguese – is the former capital of Brazil and, with a population of over six million, its second largest city after São Paulo. It is also one of the most significant centres of trade and finance in the country and has been home to the new regional office of Crypto AG for several months.

Crypto AG stepped up its geographic market coverage in July of this year by opening its new branch. This step was taken to address the increasing demand in Latin America for maximum information security. With this central base on the east coast of Latin America, Crypto AG has laid ideal groundwork for its Swiss corporate headquarters to be available to customers throughout Latin America at any time despite the time difference.

Jörg Baumgartner, Head of Sales Latin America, has taken over at the helm of the new regional office. He is an experienced employee of Crypto AG who has already worked for many years in Latin America. One of his central objectives is to enter into a personal dialogue with local customers and devise top-quality information security solutions for them that are tailored to their needs. He will benefit in these efforts from the extensive international experience of Crypto AG. The company has developed and implemented customised security solutions for clients in the areas of defence, state governance, diplomacy and internal security in over 130 countries.

Below are the contact details for the regional office of Crypto AG in Rio de Janeiro, Brazil:

Crypto AG
Avenida das Américas, 500
Bloco 4 – Sala 317
Barra da Tijuca
Rio de Janeiro, RJ
22640-100
Brazil

T +55 21 3648 3500
crypto@crypto.ch
www.crypto.ch

Jörg Baumgartner, Head of Sales Latin America, has taken over at the helm of the regional office in Rio de Janeiro, Brazil.

In addition to Jörg Baumgartner, the customers in Latin America are also served by Carlo Cosentieri, Head of Sales Latin America at the headquarters of Crypto AG in Switzerland.

CryptoMagazine 3/14 | 15

Figure 5. Crypto AG Official Publication About its Office in Rio de Janeiro (2014).
Source: Crypto Magazine (2014) ‘Crypto AG Strengthens its Presence in Latin America’, *Crypto AG: Zug, Switzerland*, n. 3, p. 15.

interfaces allow the system to be used in both current and future communication systems. The system is mechanically and electrically so robust that it can be used in regular vehicles, armoured vehicles, coastal and ocean-going vessels, aeroplanes and helicopters. This solution, too, is based on the unique security architecture from Crypto International AG.⁴⁸

⁴⁸ Crypto AG (2020) ‘MultiCom Radio Encryption HC-2650’ <www.crypto.ch/en/products-and-services/products/multicom-radio-encryption-hc-2650> accessed 4 May 2020.



Figure 6. Map Published by Crypto AG about its Offices Around the World (2015).
Source: Crypto Magazine (2015) '# Crypto', Crypto AG: Zug, Switzerland, n. 2, p. 24.

In other words, technically the HC-2650 that the Brazilian Navy acquired in 2015 appears to be the replacement – and a 'unique encryption platform', as the company calls it – of the old CX-52 encryption machines, which Brazil acquired in the past.

Most of the other data about Crypto AG on the Brazilian Transparency Portal do not reveal which product was purchased. Despite this, expenses with this company have been frequent since 2014. In 2016, a new purchase of encryption technology is recorded registered for the Brazilian Navy (Figure 8).


Nº do documento 2014NE400221	Data 31/03/2014	Descrição NOTA DE EMPENHO (NE)		
Fase EMPENHO	Espécie/tipo de documento ORIGINAL	Valor do documento R\$ 580.279,54		
Valor original USD 275.014,00	Valor convertido R\$ 580.279,54 - CONVERSÃO REALIZADA COM O VALOR DA MOEDA DOLAR NORTE AMERICANO NO DIA DA EMISSÃO DO DOCUMENTO: R\$ 1,00 = USD 0,4739. VALOR EM MOEDA ESTRANGEIRA CONVERTIDO PARA REAL (R\$).			
Observação do documento APROPRIAÇÃO DE PAGAMENTO EFETUADO PELA OP 2013001282 FATURAS: 421547A, 421547B DO(A) CRYPTO AG				
DADOS DO FAVORECIDO				
CPF/CNPJ/Outros EX9300367	Nome CRYPTO AG			
DADOS DO ÓRGÃO EMITENTE				
Órgão Superior 52000 MINISTÉRIO DA DEFESA	Órgão / Entidade Vinculada 52131 COMANDO DA MARINHA	Unidade Gestora 770100 COMISSÃO NAVAL BRASILEIRA NA EUROPA - LONDRES	Gestão 00001 TESOURO NACIONAL	
DETALHES LICITAÇÃO/CONTRATO				
Modalidade da Licitação DISPENSA DE LICITAÇÃO	Inciso 02	Amparo LEI 8666		
Referência da Dispensa ou Inexigibilidade ART24º02 LEI 8666/93	Nº convênio/ outro acordo			
DETALHE DA DESPESA				
Categoria da Despesa 4 - DESPESA DE CAPITAL	Grupo de Despesa 4 - INVESTIMENTOS			
Modalidade de Aplicação 90 - RESERVA DE CONTINGÊNCIA	Elemento de Despesa 52 - EQUIPAMENTOS E MATERIAL PERMANENTE			
Detalhamento do Gasto				
 BAIXAR				
SUBITEM	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL	DESCRIÇÃO
APARELHOS E EQUIPAMENTOS DE COMUNICAÇÃO	1	275.014,00	275.014,00	CONTRACT 7010002013-016/0000 DUE AS PER CONTRACT REFERENCED ABOVE AFTER DELIVERY OF MULTICOM RADIO ENCRYPTION HC-2650

Figure 7. Acquisition of Crypto AG Encryption Equipment by Brazil (2014).

Source: Transparency Portal of Brazil (2020h) <www.portaltransparencia.gov.br/url/cf9fe719> accessed 4 May 2020.

The expense is for an encryption software license for the HC-2650, in the amount of US\$26,950. In 2017, the information is more accurate and indicates even where some equipment could be used (Figure 9).

The information revealed by Figure 9 is relatively clear. The Brazilian Navy paid US\$53,780 to Crypto AG for the 'D7665 software license for MultiCom Radio Encryption System HC-2650, which will compose the S-BR.' In the case of the Brazilian Navy, and taking into account the Submarine Development Program (Prosub),⁴⁹ one of the possible deductions is that 'S-BR' are 'Brazilian submarines'.

⁴⁹ Submarine Development Program: 'Programa de Desenvolvimento de Submarinos' (Prosub), in Portuguese.

Nº do documento 2016NE001001	Data 18/07/2016	Descrição NOTA DE EMPENHO (NE)		
Fase EMPENHO	Espécie/tipo de documento ORIGINAL	Valor do documento R\$ 89.571,02		
Valor original USD 26.950,00	Valor convertido R\$ 89.571,02 - CONVERSÃO REALIZADA COM O VALOR DA MOEDA DOLAR NORTE AMERICANO NO DIA DA EMISSÃO DO DOCUMENTO: R\$ 1,00 = USD 0,3009. VALOR EM MOEDA ESTRANGEIRA CONVERTIDO PARA REAL (R\$).			
Observação do documento PV 49000-2016-5000054266				
DADOS DO FAVORECIDO				
CPF/CNPJ/Outros EX9300367	Nome CRYPTO AG			
DADOS DO ÓRGÃO EMITENTE				
Órgão Superior 52000 MINISTÉRIO DA DEFESA	Órgão / Entidade Vinculada 52131 COMANDO DA MARINHA	Unidade Gestora 770100 COMISSAO NAVAL BRASILEIRA NA EUROPA - LONDRES	Gestão 00001 TESOURO NACIONAL	
DETALHES LICITAÇÃO/CONTRATO				
Modalidade da Licitação DISPENSA DE LICITAÇÃO	Inciso 02	Amparo LEI 8666		
Referência da Dispensa ou Inexigibilidade ART2402 LEI 8666/93	Nº convênio/ outro acordo			
DETALHE DA DESPESA				
Categoria da Despesa 4 - DESPESAS DE CAPITAL	Grupo de Despesa 4 - INVESTIMENTOS			
Modalidade de Aplicação 90 - RESERVA DE CONTINGÊNCIA	Elemento de Despesa 39 - OUTROS SERVIÇOS DE TERCEIROS - PESSOA JURÍDICA			
Detalhamento do Gasto				
BAIXAR				
SUBITEM	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL	DESCRIÇÃO
ACQUISICAO DE SOFTWARE	1	26.950,00	26.950,00	LICENSE SOFTWARE 07665 FOR MULTICOM RADIO ENCRYPTION SYSTEM HC-2650/PV-49000-2016-500003

Figure 8. Acquisition of Crypto AG Encryption Software by Brazil (2016).
 Source: Transparency Portal of Brazil (2020c) <<http://www.portaltransparencia.gov.br/url/a6207081>>
 accessed 4 May 2020.

The last transfer of funds from Brazil to Crypto AG registered so far is on 3 December 2019. It says that the amount of US\$113,337.58 was intended for the ‘acquisition of custom or customized software’.⁵⁰

On 12 February 2020, the day after it became public that ‘for decades, the CIA has read the encrypted communications of allies and opponents’ (Miller 2020), the company Crypto published a statement on its official website (Figure 10).

⁵⁰ Transparency Portal of Brazil (2020b) <<http://portaltransparencia.gov.br/url/6a5671c6>>
 accessed 4 May 2020.


Nº do documento 2017NE003347	Data 17/11/2017	Descrição NOTA DE EMPENHO (NE)		
Fase EMPENHO	Espécie/tipo de documento ORIGINAL	Valor do documento R\$ 174.833,40		
Valor original USD 53.780,00	Valor convertido R\$ 174.833,40 - CONVERSÃO REALIZADA COM O VALOR DA MOEDA DOLAR NORTE AMERICANO NO DIA DA EMISSÃO DO DOCUMENTO: R\$ 1,00 = USD 0,3076. VALOR EM MOEDA ESTRANGEIRA CONVERTIDO PARA REAL (R\$).			
Observação do documento 54266 - CRYPTO AGLICENCA DE SOFTWARE D7665 FOR MULTICOM RADIO ENCRYPTION SYSTEM HC-2650, QUE COMPORAO OS 5 BR,(SE PV49000-2017-500002017NC002314)				
DADOS DO FAVORECIDO				
CPF/CNPJ/Outros EX9300367	Nome CRYPTO AG			
DADOS DO ÓRGÃO EMITENTE				
Órgão Superior 52000 MINISTÉRIO DA DEFESA	Órgão / Entidade Vinculada 52131 COMANDO DA MARINHA	Unidade Gestora 770100 COMISSÃO NAVAL BRASILEIRA NA EUROPA - LONDRES	Gestão 00001 TESOURO NACIONAL	
DETALHES LICITAÇÃO/CONTRATO				
Modalidade da Licitação DISPENSA DE LICITAÇÃO	Inciso 02	Amparo LEI 8666		
Referência da Dispensa ou Inexigibilidade ART 24º/02 LEI 8666/93	Nº convênio/ outro acordo			
DETALHE DA DESPESA				
Categoria da Despesa 4 - DESPESAS DE CAPITAL	Grupo de Despesa 4 - INVESTIMENTOS			
Modalidade de Aplicação 90 - RESERVA DE CONTINGÊNCIA	Elemento de Despesa 39 - OUTROS SERVIÇOS DE TERCEIROS - PESSOA JURÍDICA			
Detalhamento do Gasto				
				
SUBITEM	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL	DESCRIÇÃO
AQUISIÇÃO DE SOFTWARE(S)	1	53.780,00	53.780,00	LICENÇA DE SOFTWARE D7665 FOR MULTICOM RADIO ENCRYPTION SYSTEM HC-2650, QUE COMPORAO OS 5 BR, (SE PV49000-2017-50000-2017-500002017NC002314)

Figure 9. Payment from Brazil to Crypto AG for Software License (2017).

Source: Transparency Portal of Brazil (2020g) <www.portaltransparencia.gov.br/url/53612914> accessed 4 May 2020.

According to the statement, Crypto International Group (Crypto CH), a Swedish company, acquired in 2018 the brand and other assets of Crypto AG. The Swedish company denies having a connection to the CIA or the BND.

5. Conclusion

The controversy, hitherto recurrent, about the involvement of US and German intelligence agencies with Crypto AG can be considered closed. It is irrefutable that the company, which has remained the world leader in the manufacture of cryptographic equipment, had been secretly operated for several decades by the CIA, NSA and BND. With regard to the Brazilian case, we demonstrate

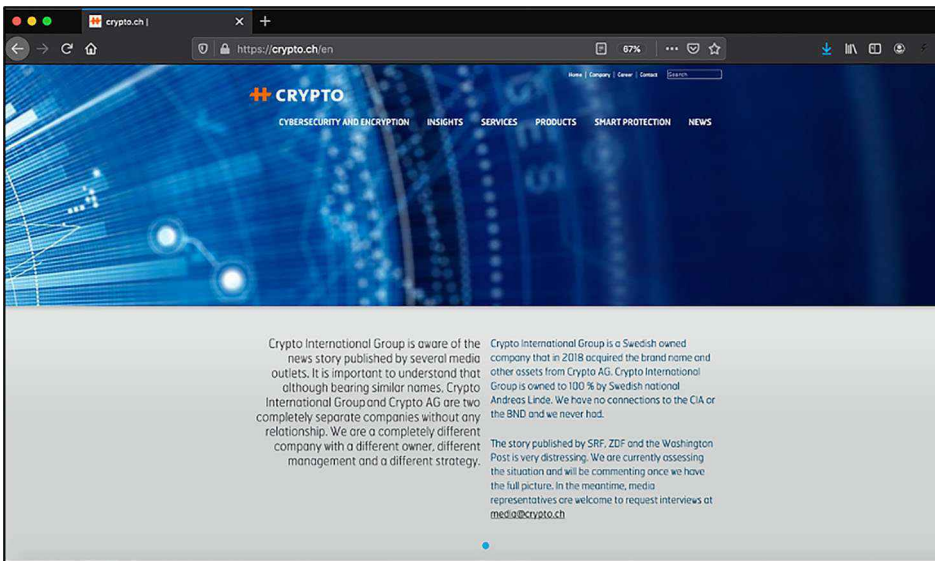


Figure 10. Crypto International Group Statement on the Acquisition of Crypto AG.
Source: Crypto International Group's Official Website: <<https://crypto.ch/en>> accessed 12 February 2020.

that the country was a client of Crypto AG since at least 1955, at the time when the company had already started negotiations with the CIA. We also demonstrate that Brazil continued to buy equipment from this company until as late as 2019.

The confidential nature of almost all the historical sources available on the subject poses a serious challenge. The main issue for a researcher interested in the subject, is to find sources that allow estimating or measuring what the Americans knew, as well as the subsequent impact of the information thus obtained on the decision-making process in the area of international relations.

The Wikileaks and Snowden revelations provide additional evidence that communications from national authorities, as well as government agencies, have been monitored by US intelligence agencies for a long time, dating back at least to World War II (Bauman et al 2015, 10). Greg Miller's findings about Crypto AG repeats this pattern (Miller 2020). It is worth asking whether these revelations will impact the interpretation of recent history between Brazil and the USA, or whether they will merely reiterate what can be considered 'normal' in the relations of these two countries. This is because, as the literature review demonstrates, for more than a century, US agencies have been secretly breaking the Brazilian government's message transmission codes (Yardley 1981, 222). Further investigation will be needed to clarify how exactly the past practice of espionage has affected relations between these countries.

In addition to the possible 'normalization' of global US intelligence practices, it should be noted that the interception and decryption of such messages is only part of intelligence operations. These operations also include the analysis of data and its dissemination to decision-making centres (this seems to have been increasingly processed through data surveillance practices). Although the interception and decryption of messages from rival powers is an important

advantage, it may not be decisive in understanding the outcome of events. Breaking the codes used by other countries is only a part – although relevant – of the complex operations of obtaining, analysing and interpreting information. Its relevance can only be assessed by taking into account the way it will be deployed.

Other questions that can be raised from the research relates to the possibility that other nations may have also taken advantage of the dissemination of the Swiss company's equipment, and also break the codes of its end users.

Bury (2009) published a document in which a former Polish intelligence agent describes the interception and decryption of communications from all diplomatic missions in Western countries, beginning in the early 1960s. These Western countries were using Hagelin CX-52 machines. This is further evidence that it is extremely difficult to build unbreakable communication systems (Bury 2009, 350).

It is also important to highlight the impasses and conflicts resulting from technological dependence to obtain encoding and decoding equipment. In the case of Polish agents under Communist rule, such technological dependence was much more dramatic than that of Crypto AG's regular customers. Those in charge of operating foreign machinery, whose trade is restricted or even prohibited, depend on precarious and uncertain supply channels, which can compromise the progress of intelligence operations (Bury 2009, 351).

In view of these findings, it is difficult to determine the impact that the revelations exposing the links between Crypto AG and the American intelligence agencies will have on historical studies. We may be on the threshold of a new era of radical revisions to the recent history of US relations with other countries, including Brazil. Or, conversely, we can only witness the mere confirmation of a pattern of subordinate and asymmetric relations that usually condition Brazil-United States relations.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Vitelio Brustolin Research Scientist at Harvard Law School, Visiting Professor in the Harvard Department of the History of Science, Adjunct Professor at Columbia University in the School of International and Public Affairs, and University Professor at the Institute of Strategic Studies and International Relations (INEST) of the Fluminense Federal University (UFF). PhD and MSc in Public Policy, Strategy, and Development (UFRJ and Harvard). Bachelor of Legal Sciences (JD) and Social Sciences (BA) from URI. Email: viteliobrustolin@id.uff.br

Academic websites:

<https://scholar.harvard.edu/brustolin>

<http://www.professores.uff.br/brustolin>

Dennison de Oliveira Postdoctoral Researcher at the Department of History of the Federal University of Parana. He received his PhD in Social Sciences and his Master's degree in Political Science from Unicamp. He received his Bachelor's Degree in History from Federal University of Parana.

Google Scholar: <http://www.prppg.ufpr.br/site/ppghis/pb/corpo-docente>

Alcides Eduardo dos Reis Peron Postdoctoral Researcher at the Department of Sociology of the University of São Paulo (USP). He received his PhD and his Master's Degree in Technological and Scientific Policy from Unicamp. He received his Bachelor's Degree in International Affairs, and in Economics from Facamp. Peron is, also, a Member of the Latin American Network for Studies of Surveillance, Technology and Society (Lavits), of the Centre for Studies and International Analysis (NEAI - Unicamp, PUC, Unesp).

Academic website: <https://bv.fapesp.br/pt/pesquisador/695669/alcides-eduardo-dos-reis-peron/>

ORCID

Vitelio Brustolin  <http://orcid.org/0000-0002-6737-570X>

Dennison de Oliveira  <http://orcid.org/0000-0002-9120-5938>

Alcides Eduardo dos Reis Peron  <http://orcid.org/0000-0003-4537-2775>

References

- Aid, Matthew M and Cees Wiebes (2001) 'Introduction: the importance of signals intelligence in the Cold War' in Matthew Aid and Cees Wiebes (eds) *Secrets of signals intelligence during the cold war and Beyond* (London: Frank Cass)
- Aldrich, Richard J, Peter F Müller, David Ridd, and Erich Schmidt-Eenboom (2020) 'Operation Rubicon: sixty years of German-American success in signals intelligence', *Intelligence and National Security*, 35:5, 603–607
- Bamford, James (1983) *The puzzle palace* (Boston: Houghton Mifflin Company)
- Bauer, Craig (2013) *Secret history: the story of cryptology* (Boca Raton: CRC Press, Taylor and Francys Group)
- Bauman, Zygmunt, et al (2015) 'Após Snowden: Repensando o Impacto da Vigilância', *Eco-pós*, 18:2, 7–35
- Bury, Jan (2009) 'From the archives: CX-52 messages read by red poles?', *Cryptologia*, 33:4, 347–352
- Buzan, Barry (1987) *An introduction to strategic studies* (London: Macmillan)
- Crypto AG (2020) 'MultiCom Radio Encryption HC-2650' <www.crypto.ch/en/products-and-services/products/multicom-radio-encryption-hc-2650>, accessed 4 May 2020
- Crypto International Group's Official Website <<https://crypto.ch/en>>, accessed 4 May 2020
- Crypto Magazine (2014) 'Crypto AG strengthens its presence in Latin America', *Crypto AG*, Zug, Switzerland, n. 3
- Crypto Magazine (2015) '# Crypto', *Crypto AG*: Zug, Switzerland, n. 2
- Crypto Museum (2020a) 'Crypto AG: Hagelin cipher machines' www.cryptomuseum.com/crypto/hagelin/index.htm>, accessed 4 May 2020
- Crypto Museum (2020b) 'Hagelin C-446: pin-and-lug cipher machine' <www.cryptomuseum.com/crypto/hagelin/c446/index.htm>, accessed 4 May 2020
- Crypto Museum (2020c) 'Hagelin CX-52: advanced pin-and-lug cipher machine, Keyboard B-52, B-62, B-621' <www.cryptomuseum.com/crypto/hagelin/cx52/index.htm#keyboard>, accessed 4 May 2020

- Crypto Museum (2020d) 'The gentleman's agreement' <www.cryptomuseum.com/manuf/crypto/friedman.htm>, accessed 14 September 2020
- Crypto Museum (2020e) 'Operation RUBICON – THESAURUS' <www.cryptomuseum.com/intel/cia/rubicon.htm>, accessed 14 September 2020
- Dobson, Melina (2020) 'Operation Rubicon: Germany as an intelligence 'Great Power?''', *Intelligence and National Security*, 35:5, 608–622
- Dover, Robert and Aldrich Richard (2020) 'Cryptography and the Global South: secrecy, signals and information imperialism', *Third World Quarterly* 41:11, 1900–1917
- Dymydiuk, Jason (2020) 'RUBICON and revelation: the curious robustness of the 'secret' CIA-BND operation with Crypto AG, Intelligence and National Security', *Intelligence and National Security*, 35:5, 641–658
- Federative Republic of Brazil (1958) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/RelatoriosdoItamaraty/Relato%CC%81rio%201958#page/n267/mode/2up>> accessed 4 May 2020, 247
- Federative Republic of Brazil (1960) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/RelatoriosdoItamaraty/Relato%CC%81rio%201960#page/n251/mode/2up>> accessed 4 May 2020, 232–233
- Federative Republic of Brazil (1965a) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/RelatoriosdoItamaraty/Relato%CC%81rio%201965#page/n291/mode/2up>> accessed 4 May 2020, 315
- Federative Republic of Brazil (1965b) 'Report by the Ministry of Foreign Affairs' <<https://archive.org/stream/RelatoriosdoItamaraty/Relato%CC%81rio%201965#page/n293/mode/2up>> accessed 4 May 2020, 316
- Foucault, Michel (2014) *Vigiar e punir: Nascimento da prisão* (Petrópolis: Editora Vozes)
- Gill Peter and Mark Phythian (2018) *Intelligence in an insecure world* (Cambridge Press: Polity Press)
- Greene, Tim (2010) 'Former NSA tech chief: I don't trust the cloud', *Network World*, 4 March <www.networkworld.com/article/2203619/former-nsa-tech-chief-i-don-t-trust-the-cloud.html>, accessed 4 May 2020
- Harris, Matthew (2016) 'The limits of intelligence gathering: Gianni Vattimo and the need to monitor 'violent' thinkers' in Jai Galliot and Warren Reed (eds) *Ethics and the future of spying: technology, national security and intelligence collection* (New York: Routledge), 27–38
- Hedley, John H (2007) 'Analysis for strategic intelligence' in Loch K Johnson (ed) *Handbook of intelligence studies* (New York: Routledge), 211–226
- Herman, M (1996) *Intelligence power in peace and war* (Cambridge: Cambridge University Press)
- Jacobs, Bart (2020) 'Maximator: European signals intelligence cooperation, from a Dutch perspective', *Intelligence and National Security*, 35:5, 659–668
- Johnson, Loch K (2007) 'Introduction' in Loch K Johnson (ed) *Handbook of intelligence studies* (New York: Routledge), 01–16
- Johnson, Thomas R (1995) *American cryptology during the cold war, 1945–1989* (Ft. George G. Mead, MD: Center for Cryptologic History, National Security Agency)
- Konheim, Alan (2015) 'The impetus to creativity in technology', *Cryptologia*, 39:4, 291–314
- Lyon, David (2018) *The culture of surveillance* (Cambridge: Polity Press)
- Mainwaring, Sarah (2020) 'Division D: operation Rubicon and the CIA's secret SIGINT empire', *Intelligence and National Security*, 35:5, 623–640
- Mainwaring, Sarah and Richard Aldrich (2019) 'The secret empire of signals intelligence: GCHQ and the persistence of the colonial presence', *The International History Review*
- Marx, Gary T. (2015) 'Surveillance Studies' in James D. Wright (ed.) *International Encyclopedia of the Social & Behavioral Sciences*, Second Edition (Elsevier)
- Medeiros, Carlos A (2005) 'O desenvolvimento tecnológico americano no pós guerra como um empreendimento militar' in JL Fiori (org) *O poder americano* (Petrópolis: Vozes)
- Miller, Greg (2020) 'The intelligence coup of the century', *The Washington Post*, 11 February <<https://wapo.st/crypto>>, accessed 4 May 2020

- Miller, Greg, and Peter Mueller (2020) 'Compromised encryption machines gave CIA window into major human rights abuses in South America', *The Washington Post*, 17 February <www.washingtonpost.com/national-security/compromised-encryption-machines-gave-cia-window-into-major-human-rights-abuses-in-south-america/2020/02/15/bbfa5e56-4f63-11ea-b721-9f4cdc90bc1c_story.html>, accessed 9 September 2020
- Moraes, Glória (2005) 'Telecomunicações e o Poder Global dos Estados Unidos' in J.L. Fiori (org) *O poder americano* (Petrópolis: Vozes)
- Murakami Wood, David and Steve Wright (2015) 'Before and after Snowden', *Surveillance & Society*, 13:2, 132–138
- National Security Archive (2020a) 'CIA report, 'Counterterrorism in the Southern Cone,' Secret, May 9, 1977' <<https://nsarchive.gwu.edu/dc.html?doc=6773840-National-Security-Archive-Doc-2-CIA-report>>, accessed 23 July 2020
- National Security Archive (2020b) 'DIA intelligence appraisal, 'Latin America: counterterrorism and trends in terrorism,' August 11, 1978' <<https://nsarchive.gwu.edu/dc.html?doc=6773842-National-Security-Archive-Doc-4-DIA-Intelligence>>, accessed 23 July 2020
- Pianta, Mario (1988) *New technologies across the atlantics: US leadership or european autonomy?* (Worcester: Billing & Sons)
- Richelson, Jeffrey T (2007) 'The technical collection of Intelligence' in Loch K Johnson (ed) *Handbook of intelligence studies* (New York: Routledge), 105–117
- Rudner, Martin (2004) 'Hunters and gatherers: the intelligence coalition against Islamic terrorism', *International Journal of Intelligence and Counterintelligence*, 17:2, 193–230
- Shane, S and Bowman T. (1995) "No Such Agency", series of 6 articles, Baltimore Sun, part 4 reprinted at: accessed 4 May 2020
- The National Archives and Records Administration (2020) 'Record Group 457 – Records of the National Security Agency/Central Security Service' <www.archives.gov/findingaid/stat/discovery/457>, accessed 14 September 2020
- Transparency Portal of Brazil (2020a) 'O que é e como funciona [What it is and how it works]' <www.portaltransparencia.gov.br/sobre/o-que-e-e-como-funciona>, accessed 4 May 2020
- Transparency Portal of Brazil (2020b) <<http://portaltransparencia.gov.br/url/6a5671c6>>, accessed 4 May 2020
- Transparency Portal of Brazil (2020c) <<http://www.portaltransparencia.gov.br/url/a6207081>>, accessed 4 May 2020
- Transparency Portal of Brazil (2020d) <www.portaltransparencia.gov.br/url/96d7ade6>, accessed 4 May 2020
- Transparency Portal of Brazil (2020e) <www.portaltransparencia.gov.br/url/70b16c8d>, accessed 4 May 2020
- Transparency Portal of Brazil (2020f) <www.portaltransparencia.gov.br/url/4b9ed865>, accessed 4 May 2020
- Transparency Portal of Brazil (2020g) <www.portaltransparencia.gov.br/url/53612914>, accessed 4 May 2020
- Transparency Portal of Brazil (2020h) <www.portaltransparencia.gov.br/url/cf9fe719>, accessed 4 May 2020
- United States of America, National Security Agency (1954a) 'List' <www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_517/41789209082821.pdf>, accessed 23 July 2020
- United States of America, National Security Agency (1954b) 'Memorandum for the Members of the United States Communications Intelligence Board and the Members of the United States Communications Security Board: Implications of a Policy Which Would Permit Cryptographic Aid to Friendly Foreign Governments for their National Purposes' <www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/panel-committee-board/FOLDER_373/41754969079412.pdf>, accessed 23 July 2020
- United States of America, National Security Agency (1955a) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February' [first draft] <<https://cryptome.org/2015/07/nsa-crypto-ag.pdf>>, accessed 20 July 2020

- United States of America, National Security Agency (1955b) 'Report of visit to Crypto AG (Hagelin) by William F. Friedman, Special Assistant to the Director, NSA, 21-28 February' [second draft] <https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf>, accessed 20 July 2020
- United States of America, National Security Agency (1998) 'American cryptology during the Cold War, 1945-1989' <www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/cold_war_iii.pdf>, accessed 23 July 2020
- United States of America, Central Intelligence Agency (2007) 'History of the CIA' <www.cia.gov/about-cia/history-of-the-cia/index.html>, accessed 24 July 2020
- Warner, Michael (2007) 'Sources and methods for the study of intelligence' in Loch K Johnson (ed) *Handbook of intelligence studies* (New York: Routledge), 17-27
- Weinberg, Alvin M (1961) 'Impact of large-scale science on the United States', *Science*, 134:3473, 161-164
- Yardley, Herbert (1981) *The American black chamber* (New York: Ballantine Books)
- Youssef, Ibrahim (1981) 'Qaddafi terms the \$220,000 given Billy Carter a loan tied to business', *The New York Times*, 27 June <<https://nyti.ms/29RgLvq>>, accessed 4 May 2020
- Zuboff, Shoshana (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (London: Profile Books)