1

History and Repertoire of Communication Interception Practices

The interception of correspondence has been ongoing for centuries. However, we will not attempt to date its origin. By focusing on the period closest to the present, it is possible to identify its multiple contexts of use, as well as its civil, military, political, economic and diplomatic applications. On the one hand, the emergence of new modes of communication in the 19th century led to a considerable increase in the volume and distribution speed of correspondence, and to changes in the geographical dimension, on the other hand. It became much easier to correspond with the other side of the world, thanks to the speed of messages reaching their destination and the reduction in communication costs. Communication also diversified its methods: there was a gradual shift from writing to voice transmission with telephony and radio communications.

The principle of the optical telegraph, then called the aerial telegraph so as to differentiate it from the electric telegraph, has been known since antiquity. As early as the second century BC, the Greek general, statesman and historian Polybius described, in Book X, Chapter VII "Fire Signals" of his *General History*, a system "by means of which anyone who cares to do so even though he is at a distance of three, four, or even more days' journey, can be informed"[1]. He describes the process in the following terms:

> Divide the alphabet into five groups of five letters each […] the signaling party raises first torches on the left to indicate which of the tablets he means. […] He next raises torches on the right showing in a

1 Polybius, Book X, Chapter VII [Online]. Available at: www.remacle.org/bloodwolf/historiens/polybe/dix1.htm. In English: http://www.perseus.tufts.edu/hopper/text?doc=Perseus:abo:tlg,0543,001:10.

similar manner by their number which of the letters in the tablet he wishes to indicate to the recipient.

As early as the 18th century, many inventors proposed and experimented with optical devices for remote communication:

– in 1672, the Englishman Robert Hooke (1635–1703) imagined an assembly of three masts equipped with a horizontal girder for encoding cut-out symbols;

– in 1690, the Frenchman Guillaume Amotons (1663–1705) improved the mechanism to transmit alphabetic symbols;

– in 1786, while in the presence of the Prince of Hesse-Cassel, the German Johan Andreas Benignus Bergsträsser (1732–1812), rector of the University of Hanau, experimented with a mast equipped with two pivoting arms, in order to transmit a message made up of numbers;

– in 1788, Charles-François Dupuis, future deputy to the Convention for Seine-et-Oise, carried out a communication between Ménilmontant and Bagneux using an alphabetical telegraph.

But the telegraph would only experience real growth after 1791 with the invention of the optical communication method by Claude Chappe (1763–1805), which bears his name. After numerous demonstrations and improvements, including a rapid transmission experiment on July 12, 1793 covering a 40 km distance, the Convention decided to nationalize the invention on July 26 of the same year and to entrust its administration to Chappe, under the aegis of the Ministry of War. From this followed a considerable development of the invention, which Chappe and his brothers exploited on a large scale.

Its actual construction at the end of the 18th century did not respond to technical innovations, but to a particular need in the context of the French Revolution and its centralized state administration, for which the speed of communication was crucial.

A Chappe telegraph station is a small stone building furnished with a mast carrying three articulated arms, painted black: the central arm is called the regulator and the two side arms are the indicators. Information is conveyed by the relative position of the regulator and the indicators.

A first Paris–Lille line completed in 1795 included 16 stations and made it possible to transmit a 25-word message within an average of 15 minutes, compared to a whole day required by traditional postal services. This first line was followed by others, forming a network which covered not only metropolitan France, but also Algeria and Tunisia.

In 1844, the French territory had 534 towers for connections over more than 5,000 km between the main cities. The telegraph was initially reserved for government communications. In 1824, the network expanded to commerce, and was made available to the general public in 1851, when it began to decline.

As the position of the articulated arms carrying the transmitted information is visible to all, it is necessary to use a confidential code. The code's secrecy is based on a hierarchical organization with pseudo-military discipline. In 1823, the Central Administration was at the top of the structure, with three administrators, a chief and two assistants for four bureaus: dispatches, staff, equipment and accountability. Then there were the directors in charge of a department, who were responsible for coding, decoding and sending dispatches, using a codebook which was kept secret. From 1795 onwards, 92 arms positions were retained, each being identified by a two-digit number. This number referred to the codebook pages and the lines on each page containing a word or a group of words, which resulted in a total of 8,464 meanings. After the code was revised in 1830, increasing the number of arm positions to 184, 33,856 meanings could be conveyed.

The message could only be understood by the directors at the lines' ends, but remained incomprehensible for all the intermediaries.

The directors supervised the activity of the inspectors assigned to a department who were responsible for a line section comprising around 10 stations.

At the bottom of the hierarchy, stationary workers represented 90% of the staff. Each station was staffed by two operators: one was in charge of the telescope observation, while the other manipulated the controls. The stationaries were poorly paid, as much as 1.25 francs per day until 1826, the salary of a daily laborer. This was considered as a side work, since most of the stations were located in rural areas. Due to budgetary reasons, the stationary position was soon to be occupied by only one person.

Its last use was a light, transportable model on the back of a mule, at the service of military operations during the Crimean war (1853–1856), allowing stations to be moved according to military operations.

Having been the first organized telecommunications system, the Chappe telegraph gradually disappeared from 1847 and was definitively replaced by the electric telegraph in 1855. The latter had the advantage of also operating at night and in foggy weather, while its undersea cables made it possible to cross the seas.

As early as 1820, the French mathematician, physicist, chemist and philosopher André-Marie Ampère (1775–1836), known for his works on electromagnetism, proposed to apply these phenomena to a remote communication system. The electric telegraph was later designed by several inventors, including Pavel Schilling (1786–1837), a German-origin diplomat at the service of Russia. Experiments with electric telegraphs began in England in 1832 under the initiative of William Fothergill Cooke (1806–1879) and later in France, Spain and Italy.

In 1838, the physicist and inventor Charles Wheatstone (1802–1875) installed the first electric telegraph line in England between London and Birmingham. This was a private business.

In 1844, the American inventor Samuel Morse (1791–1872) created the code that bears his name, establishing a telegraphic connection between Baltimore and Washington. Originally sensitive to transmission errors, this code was improved by the German author, journalist and musician Friedrich-Clemens Gerke (1801–1888), who was a pioneer of telegraphy and gave it its final shape in 1850.

In 1845, a first electric telegraph line was set up in France between Paris and Rouen, triggering the decline of the Chappe telegraph. In 1851, a first undersea cable was built between England and France. In 1855, the Anglo-American inventor David Edward Hughes (1831–1900) designed the teleprinter, a printing telegraph with a transmission capacity of approximately 1,000 words per hour. In 1866, the first transatlantic cable (whose installation required about 10 years of work), was put into service. Many cables would follow, making up a world-scale telegraphic network at the beginning of the 20th century.

In 1874, Hughes' teleprinter was improved by Émile Baudot (1845–1903), who invented the code that currently bears his name. It is a device for printing text with a typewriter mechanism which accelerates transmissions by means of an electromechanical process, surpassing the capacities of human operators. Baudot's device, capable of transmitting up to 4,000 words per hour, was adopted by the French telegraph administration in 1875. Each character of the alphabet was coded by five binary units. This would result in the passage (or the absence) of an electric current, directly stemming from the typist operator's keystroke on the keyboard. This coding was written onto a perforated paper tape. It was represented by a mark, or a mark's absence, along five positions. The marks were materialized by a hole on the paper tape.

The holes' layout could represent a letter or a number as a function of a code developed by Baudot, and then modified by Donald Murray (1865–1945) in 1901, to acknowledge typewriter writing. A special encoding activated the number mode, while another activated the letter mode.

These teleprinters were widely used until 1980 for communicating the news to press organizations and newspapers. The baud is a signal transmission speed unit still in use today, in homage to Baudot.

In 1879, the Ministry of Posts and Telegraphs was created in France.

The Frenchman Charles Bourseul (1829–1912), agent of the Telegraphs administration, laid the foundations for the telephone in 1854. He published an article entitled "Electrical transmission of speech" in a journal called *L'Illustration*. As it had occurred with the electric telegraph, many inventors were involved in the invention and improvement of the telephone:

– the German Philipp Ress (1834–1874) performed a good quality speech transmission, but of weak intensity in 1863;

– the Italian-American Antonio Meucci (1808–1889) is said to have manufactured several telephone devices between 1849 and 1870, for which he filed a patent in 1870;

– the Americans Graham Bell (1847–1922) and Elisha Gray (1835–1901) filed a similar patent within two hours in 1876, which led to controversy over inventorship. The Bell Laboratories, a private research institute, was founded in 1925.

The telephone began being commercially exploited in the United States in 1877, and in France in 1879.

Wireless telegraphy was inspired in the works of James-Clerk Maxwell (1832–1819). In his 1872 treatise on electricity and magnetism, Maxwell established that magnetic and electric fields can propagate through space under the shape of an electromagnetic wave carrying energy. He laid the theoretical foundations that Herfich Rudolf Hertz (1857–1894) relied on to discover the waves that bear his name. Hertz was able to produce them using an oscillator.

Édouard Branly (1844–1940) became interested in Hertz's works and noted that the conductivity of a metallic powder varies under the influence of electromagnetic radiation, a discovery which was at the origin of the iron filing field detector. This device could be used as a receiver for the Hertz oscillator, paving the way for the transmission of information over a distance.

On May 7, 1875, the Russian Alexandre Popov (1858–1905) performed one of the first radioelectric transmissions from a distance of 2,400 m in front of the Russian society of physics and chemistry. In 1896, he succeeded a wave transmission among various buildings of the University of Saint Petersburg, with

vertical antennas to improve reception, as well as the recording of messages on a Morse device.

Other names are associated with the development of radiocommunications: Guglielmo Marconi (1874–1937) in Italy, Eugène Ducretet (1844–1915) in France. General Ferrié (1868–1932) performed a radio broadcast from the Eiffel Tower in 1904 in France.

Amateurs also played an important role in the discovery of shortwave propagation modes. On November 28, 1923, the first bilateral transatlantic medium-wave communication (110 m) took place between the American radio amateur Fred Schnell, callsign 1MO, in Hardford, Connecticut and the French radio amateur Léon Deloy (1894–1969), callsign 8AB, in Nice. This performance, which was previously unthought-of due to the rectilinear propagation of electromagnetic waves, evidenced their reflection on the ionosphere (the upper layer of the Earth's atmosphere), paving the way for transcontinental communications and triggering their use for global communications.

The development of FST could only be achieved thanks to electronics that strongly shaped scientific and technical advances and had a strong impact on society, encouraging the development of radio, television, computers and telecommunications. In 1904, John Fleming (1849–1945) invented the vacuum diode in England, a device enabling the unidirectional flow of an electric current. This invention was followed in 1906 by the triode vacuum tube, by Lee de Forest (1873–1961), which paved the way for the creation and amplification of electric signals. As early as 1902, a patent was filed in the United States by the Indian botanist physicist Jagadish Chandra Bose (1858–1937) on the semiconducting properties of galena (lead sulfide). In 1906, Geeleaf Wittier Pickard (1877–1956) filed a similar patent on silicon for a silicon crystal detector, permitting the demodulation of radio waves. It was not until the invention of the transistor in 1947 that a semiconductor amplification device appeared.

The second half of the 20th century was undoubtedly marked by the Internet. This period gave rise to a variety of technologies and a new impetus to the progress made in the field of telecommunications in the 19th century and during the first half of the 20th century with radio and telephony. Progress was then reflected in terms of increased transmission speed, distance, increase in correspondence volumes and information flows circulating around the world.

The interception of correspondence has adapted to all these developments, accompanying each of the new technological generations.

1.1. Military interceptions during the war

Communication has always played a strategic role in the war. Intercepting communications, either to gain further information or to interrupt its route, is an act as old as war itself. Reading the minds of enemies, knowing their intentions, contributes to the construction of an advantage or a superiority based on the mastery of information, which partially contributes to lifting the fog of war. "The endeavor to learn what is in the opponent's mind and to draw advantage from it has always been very important in the history of mankind in peacetime and particularly in wartime. During thousands of years only the methods have changed" [FLI 53].

In *The Gallic Wars* [RAT 64], Julius Caesar mentions the interception of letters sent by the warlords and which must escape the enemy: "Then he persuaded one of the Gallic troopers with great rewards to deliver a letter to Cicero. The letter he sent written in Greek characters, lest by intercepting it the enemy might get to know of our designs".

1.1.1. *The interception of telegraphic communications*

Strictly speaking, the 19th century marked the entry into the era of modern communications. The optical telegraph, born during the revolutionary period in France, and in many European countries over the same period, quickly spread to other continents, establishing networks across societies. It has settled in diverse landscapes and in the daily lives of societies, offering the possibility of modern, fast communications over long distances. Before being commercial, the first uses of the Chappe telegraph were warfare-related. In the middle of the 19th century, the optical telegraph was succeeded by the electric telegraph, with its thousands of kilometers of cables deployed on land and across the oceans, which would only increase global networking, accelerating communications over ever greater distances, contribute to the development of economies, to the construction of colonial empires, state powers, as well as to the emergence of new private companies which quickly made their fortunes by producing network infrastructure and offering communication services. As will be frequently stressed here, these networks have often played an essential role in wars, not only in tactical, but also in strategic terms. All these new means of communication impacted the way in which the states conceived and practiced the interception of correspondence until that moment.

On every occasion, technological developments gave new life to interceptions, with new capabilities, authorizing new modes of attacks against communications (interceptions are considered an offensive action): "In the middle of the nineteenth century, when the Morse telegraph came into use, soon followed by the telephone,

new technical possibilities of attack resulted by switching-in and listening this quickly produced a new situation" [FLI 53].

The development of the state's capabilities to intercept these new modes of communication seems related to the intelligence-gathering culture or history specific to each state:

> There were two countries in Europe in which the espionage service had been especially cultivated for centuries: France and Austria-Hungary. Consequently, these were the two countries which first recognized the importance of technical means of intercepting communications and took corresponding action [FRI 53].

1.1.1.1. *The American Civil War*

The intensive use of the telegraph was essential during the American Civil War (1861–1865).

The technical characteristics of the electric telegraph exposed unencrypted correspondence to any indiscreet ear. Wiretapping possibilities were multiple and few resources had to be mobilized for this. Network architecture and the characteristics of their components made it relatively easy to intercept signals:

> I then discovered, by sheer necessity, that I could read the messages coming, by watching the movement of the armature of the magnet. The vibrations of a telegraph armature are so slight as to be scarcely perceptible to the naked eye, yet a break, or the separating of the points of contact, are necessary to make the proper signals. Further experiences developed the phenomena that when sound and sight failed I could read still by the sense of feeling, by holding my finger-tips gently against the armature and noting its pulsations. I thus became by practice not only proficient, but expert in telegraphy. Telegraphers know, though the general public may not, that messages can be sent by touching together the ends of a cut telegraph wire, and can be received by holding the ends to the tongue [KER 89].

In addition to these interception "attacks", the telegraph infrastructure suffered direct attacks (cutting of cables, destruction of poles, etc.). The network was particularly exposed and vulnerable:

> As soon as the deed had been accomplished in Baltimore, the news was to be telegraphed along the line of the road, and immediately upon the reception of this intelligence the telegraph wires were to be cut, the railroad bridges destroyed and the tracks torn up, in order to

> prevent for some time any information being conveyed to the cities of the North, or the passage of any Northern men towards the capital [PIN 84].

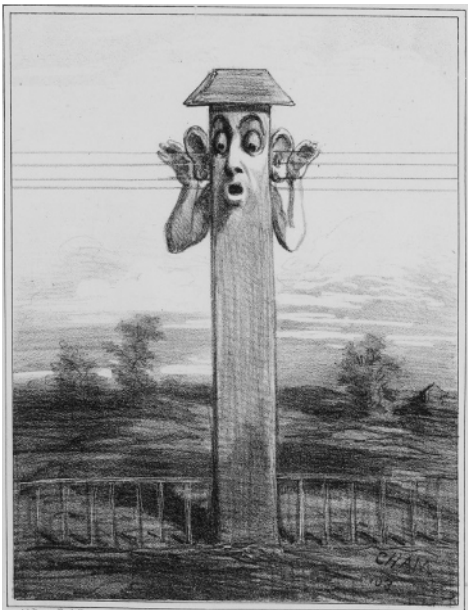

Figure 1.1. *"The electric telegraph shocked by the news it was entrusted to transmit for some time", Cham (Amédée Charles de Noé), 1867, CC0 Paris Museums/Carnavalet Museum*[2]

Telegraph workers were one of the essential links in the intelligence-gathering chain. The quality of the results obtained from the collection of telegraphic information depended as much on cleverness and inventiveness, as on technological vulnerabilities. While telegraph spies had access to information that often ended up being without interest, it sometimes occurred that it had a strategic value. Some of these employees could be tempted to keep a copy of this information for themselves and divert it from its primary purpose:

> I had thought, while in possession of the official dispatch, what a pleasant gratification it would be to my old friend Covode to be able to show him an intercepted dispatch from Richmond to the commander of the Rebel armies in the field; and as the thought of this

2 See: www.parismuseescollections.paris.fr/sites/default/files/styles/pm_notice/public/atoms/images/CAR/aze_carg021974-49_rec_001.jpg?itok=sGZbwTrI.

> performance dwelt in my brain as I walked along, I formed a hasty plan, which I believed I could mature and carry into effect – of securing from the files or papers in the telegraph office a number of copies of the most important dispatches, either in the handwriting of Generals Joseph E. Johnston or Beauregard, addressed to Richmond, or at least signed by them officially [KER 89].

The American Civil War intensified the exploitation of the telegraph and electronic warfare operations. The encryption and interception of messages passing through the telegraph are among the key actions of war.

Many stories abound regarding these practices. In the second chapter of his work dedicated to the role of telegraphy in the American Civil War, William R. Plum [PLU 82] describes the many encryption systems used by the belligerents during the conflict. The balance of power was strongly influenced by the quality of encryption and the ability to ensure the secrecy of telegraphic messages. The Confederates seem to have failed to master the encryption of their messages (telegraph, couriers, signals), which earned them many defeats:

> Lincoln took a personal interest in our translation of the enemy's cipher-despatches, intercepted and brought to the War Department for translation, and whenever he saw the three of us with our heads together he knew that we had something on hand of special interest […] At various other times our troops intercepted despatches, sent from one Confederate general to another, containing important information in cipher. As a rule, we were able to translate these ciphers after more or less labor. They were generally ordinary letter ciphers, the letters of the alphabet being transposed in various ways [BAT 07].

During this war, encryption was a critical element for superiority. George Washington also used deception methods, intentionally transmitting messages containing false information, to be intercepted by the enemy.

Interceptions were only one of the many bricks of this information war, among others: encryption, deception, the physical control of the telegraphic infrastructure, the attacks against the telegraphic communication network, the engagement of individuals (telegraph agents) in correspondence surveillance.

Let us recall to what extent A. Lincoln was attached to this informational dimension of the war, spending whole days near the telegraph post to scrutinize the arrival of new dispatches. We could also mention the role played by these

telegraphic communication networks on the disclosure of information to the American and international press during the war.

1.1.1.2. *The civil war in Chile*

From January to September 1891, Chile engaged in a civil war. President Balmaceda's communications (described as a "dictator" in the following quotation) were intercepted. Note the way in which the belligerents exploit communications: they take into account the existing network infrastructure, they position their means of interception at the best places, they decipher the intercepted messages by taking advantage of the weakness of the encryption method used and they finally communicate their own information to several foreign countries thanks to international cable networks. While intercepts cannot probably be considered the only key to the success of the president's opponents, they certainly played a major role. By combining the interception of communications and the use of network communication tools to organize the opposition, the stakeholders in this conflict were already immersed in the modern era of information warfare:

> Given the fact that the Dictator's communications with his agents outside Chile were hindered by means of the Pacific submarine cable, they could only be verified *via* the trans-Andean route. We were thus able to organize a service for intercepting the Dictator's telegraphic correspondence in the Argentine Republic, becoming fully aware of its contents. All the messages in secret ciphers were easily translated, thanks to the bad choice of keywords used by the Ministry of Foreign Affairs. The information thus acquired was immediately communicated to Iquique or to the Revolution agents in Paris, and proved being crucial to prepare the final result. On an illustrative basis, it will suffice to point out that from February 28 to July 28 we sent 12 telegrams to Iquique, 13 to Antofagasta, 1 to Tupiza, 10 to Pulacayo, 60 to Paris, 2 to London, 1 to Bordeaux, 1 to Hamburg, 1 to New York, 3 to Rio Janeiro, 9 to Petrópolis, 14 to Montevideo; apart from an indeterminate number within the Argentine Republic ([BIA 92], translation from Spanish).

1.1.1.3. *The Spanish American war of 1898*

During this brief war, telegraph cables between Spain and its South American colonies (particularly Puerto Rico, Cuba and the Philippines) [WIN 15] were the target of destruction operations by the American army. The choice was in favor of a systematic destruction instead of maintaining networks. The Americans preferred to deprive themselves of the information that interceptions could have delivered. The strategy was to isolate the armed forces and the enemy authorities, depriving them of their long-distance communication means. The two strategies are opposed: on the

one hand, the informational isolation of the enemy via the destruction of its communication means; on the other hand, the collection of enemy information by intercepting (and thus preserving) their communications.

1.1.1.4. *Telegraph interception at the beginning of the 20th century*

At the beginning of the 20th century, the level of organization and integration of interception activities within the military intelligence-gathering services was uneven, depending on the country. Austria seemed to be ahead of Germany on these questions at the beginning of World War I. It would take almost a year for the systematic interceptions of foreign communications to be implemented on the German side. Other nations, like Russia, were rather slow to take stock of the challenges associated with these new methods of communication. Russian transmissions were unencrypted during the war, or poorly encrypted: "The intercepted Russian telegrams constitute a very trustworthy source of information. Of course, the orders were enciphered, but the cipher system was very simple and was rarely changed; consequently it was easy to read the radiograms" [FLI 53].

During World War I, multiple new communication technologies could be used: the radio, the telegraph, the telephone, electronic tubes, etc. The telegraph was by then a mature technology, which had already been used for several decades, especially in other conflicts. But these techniques were often vulnerable, dependent on electricity lines which could be cut, subjected to the terrain's configuration, to climatic conditions, to distance. During the conflict, however, the belligerents maintained their lines of communication far from the theater of war, in order to preserve them. In the war, wired networks such as the telegraph or the telephone were highly vulnerable. While radio communications made it possible to send messages to several recipients at the same time and enabled the mobility of men and vehicles, they were still vulnerable because they could be easily intercepted by enemies, without the need to physically connect to cables. Radio communications appeared at the end of the 19th century and found immediate applications in the military field (getting rid of cables' physical constraints, extending communication distances, reaching several points, disseminating orders more quickly, etc.). Modern communication means were vulnerable in terms of security, jeopardizing the infrastructure, equipment and data when these could not be encrypted, or were imperfectly encrypted (although their communications were regularly decrypted throughout the war, the Germans were convinced of the resistance of their encryption). As they entered the war in 1914, the British cut several undersea cables connecting Germany and the United States. The Germans favored radio communications which the enemies could easily intercept. In order to divert North American forces to other conflicts and dissuade them from entering the war in Europe, the Germans contemplated inciting Mexico to attack the United States. It is

in this context that a senior German official, Arthur Zimmerman, transmitted a message to the German ambassador in Mexico City.

From these few insights into World War I, it will be noted that interceptions have a variable importance. The interception of Zimmerman's telegram can be presented as one of the triggers for the United States' decision to enter the war. But that was not the only element. The maritime war launched by the Germans at the same time, deciding to systematically sink all merchant ships – especially American ones – was just as decisive. Throughout the war, German messages were intercepted and decrypted in large volumes. Despite the fact that interceptions provided often strategic information regarding the various battles conducted, we cannot state that the interceptions provided one belligerent or the other with such mastery over the informational space that the war was shortened in time, or made less lethal. While mastering the information from the opposing camp is essential, it is not necessarily a guarantee of victory. The multiple communication techniques acted more as a complement than as competition against each other. The appearance of the radio did not signal the end of wired communications, nor did satellite communications dethrone cable transmissions years later.

1.1.2. *The interception of radio communications*

Wireless communications appeared at the very beginning of the 20th century and were adopted by the armies during World War I.

The appearance of wireless telegraphy opened up new possibilities for interception. Communications were particularly vulnerable during the war, in particular, telegraphy:

> The problem of secrecy does not appear in similar conditions for these two kinds of communications: while the transmission of military telegrams will always risk being disturbed by the enemy, the security of long-distance communications encounter no other difficulties other than those resulting from the nature of things […] High-speed telegraphy […] contributes to secrecy by reducing the time during which interception is possible [PER 11].

The protection of wireless communications caused deep concern at the beginning of the 20th century. No solution seemed to suffice for protecting radiotelegraphic communications in times of war:

> M. Edouard Branly, who is general credited in Paris with having been the real inventor of wireless telegraphy, has just patented an important

> improvement by which interception of messages will be rendered impossible, except by a special apparatus. At present, M. Branly states, it is a popular delusion to imagine that wireless telegraphy could render any service in time of war across country or seas held by an enemy. The latter can, with the greatest ease, either intercept messages, or so disturb their transmission as to render them incomprehensible. M. Branly claims that his new apparatus ensures for a given set of electric waves complete immunity from accidental interference of other waves. But at the same time, it will always be possible in time of war to disturb messages willfully, even when sent off by his new appliance. He says that no wireless telegraph system known is a proof against interferences if a special mechanism giving out waves uninterruptedly by used to that end. His conclusion is that for war purposes on land or at sea "the usefulness of wireless telegraphy would be illusory" [THE 06].

Austrian capabilities for intercepting radio communications enabled them to monitor the Italian army operations on a daily basis during the war against Turkey in 1911. On the eve of World War I, France had also developed military capabilities for the interception and cryptanalysis of telegraphic and radio communications, which enabled it to steadily surveil Germany.

Communication technologies multiplied on the eve of World War I. The French and British forces preparing the defense of the Suez Canal in 1914–1915 deployed several infrastructures around centralized networks, as well as the means to defend them: "A comprehensive system of telegraphic, telephonic and wireless telegraphy communications links the various posts with the headquarters. Defenses have been erected to protect the railway, the telegraphic lines and the freshwater canal" [DOU 22].

For Wilhelm F. Flicke [FLI 53], the battle of Tannenberg (August 26–30, 1914) would be one of the first battles, if not the first, during which radio communication interceptions played a key role in the confrontation's outcome. During this battle, marked by the victory of the German army over the Russian army, the Russian generals exchanged detailed operational orders by radio (unencrypted messages), which were intercepted by the Germans. Strengthened by the information that had been gathered for making strategic decisions, the Germans quickly gained advantage. They accessed information about the enemy's intentions, troop movements, organization, battle plan, points of attack. Since this information was transmitted unencrypted by the Russians, the task was relatively easy for the Germans who – once the data were intercepted – only had to translate them and transfer them from the interception stations to the headquarters. However, it would seem that the German military did not give interceptions a major strategic role in

this battle, which would eventually be won despite all odds, according to them. The flaws in the organization of the Russian information system were significant: insufficient cables to establish wired communications, no encryption means between the headquarters and the troops for radio communications, which involved unencrypted transmissions.

On the other hand, unencrypted messages were not harmless for those who intercepted them and took them at face value. Armies could deliberately send unencrypted messages so that the enemy intercepted them and read them without any difficulty. Sending unencrypted messages could be a deception maneuver. The Germans used this maneuver against the Russians: "In the forenoon of 7 September, the radio station at Konigsberg sent a radiogram in plain text […] The radiogram was intercepted by the Russians and the strategy succeeded. This is the first known case of purposely misleading radio traffic during World War I" [FLI 53].

At the beginning of World War I, there was still no real doctrine for the interception of these new modes of communication (radio). The military doctrine had not yet integrated the transformations that the use of radio interceptions implied:

> People were astounded at the technical progress which made possible wireless transmission of information over rather great distances, but they did not yet understand how to make sensible use of this technical advance in order to gain information […] On the German side the idea was utterly foreign in lower and medium commands that one might be in a position to shape or alter one's own plans on the basis of intercepted traffic. Military thinking tended to consider one's own operation on the basis of the orders issued to be a fixed factor which could in no wise be influenced by any messages which might be intercepted [FLI 53].

The resources allocated to intelligence-gathering and in particular to wiretapping and the interception of communications are unevenly deployed from state to state. Regarding the Japanese abilities during the war against China, an American report observed that, strengthened by its superiority, the Japanese army neglected intelligence-gathering because it did not deem it essential [STR 46]:

> Since the Manchurian incident, a bad habit of neglecting the intelligence service was created among the Japanese forces in North China as they had always fought against weaker enemy forces. The Japanese forces always were confident of winning worth enemy. The Chinese forces were weaker in quality and equipment. Information obtained regarding the Chinese forces was not the deciding factor for the victory of the Japanese forces.

The relative disinterest of the Japanese headquarters for the intelligence gathered from radio interceptions partly explained the deterioration of the Japanese condition during the war against the Chinese Communists: “Here may be traced one of the causes which lead Japanese forces gradually to an unfavorable war situation”.

In certain regions of China, the Japanese forces made significant efforts for intercepting enemy communications:

> Value of Information Obtained: Headquarters of the Japanese North China Army achieved quite satisfactory results intercepting radio communications transmitted by Chungking forces as the latter’s supervision and control of radio communication was poor. During actual operations the Japanese forces could relatively accurately perceive in advance attempts and movements to be carried out by Chungking forces.

However, the results were not up to par, and the intelligence gathered was of poor quality. Among the various reasons, let us mention the cautious communication mode of the Chinese forces: “Strict supervision and control of the Chinese Communist forces over their radio communication as well as the poor facilities of the Japanese forces for intercepting the enemy radio communication”.

Insufficient intelligence-gathering from the multiple fronts seemingly contributed to the loss of Japan in China:

> Japanese forces had no facilities for intercepting radio communications transmitted by the Soviet-Mongolian forces in the Outer Mongolian area, and also it was almost impossible for the Japanese forces to dispatch their secret agents to that area. It is not too much to say, therefore, that no information was obtained regarding the Soviet-Mongolian forces.

1.1.3. *Telephone interception*

The electric telegraph showed its great sensitivity to interception during the American Civil War (see section 1.1.1.1). Shortly after the American Civil War appeared the telephone, which was equally vulnerable to interceptions.

The Engineer’s Handbook published in 1931 describes the duties of wartime communication interception:

The organization of transmissions in the defensive differs from what is suitable for an offensive situation, having the following particularities: […] The fixedness of command posts facilitates the organization of transmissions […] The telephone becomes the capital process; it is set to function even when the struggle reaches its maximum intensity. This implies the construction of layers as numerous, dense and less vulnerable as possible. In particular, the telephone is connected until it reaches the battalion, the battery, even the company command posts, and the front line observatories (all precautions being taken to avoid wiretapping by the enemy). […] Part of the transmission processes enable the surveillance and capture of enemy transmissions, thus enabling useful intelligence-gathering for the command. The processes offering the broadest coverage for surveillance purposes are wireless telegraphy (and telephony), only requiring to tune the earphone station with the emission characteristics of the opposing station, with ground telegraphy and wired telephony. One same station cannot normally assure the emission and reception of our own messages and the listening to the enemy transmissions. It is therefore essential to particularly reserve certain stations for listening to the enemy stations. The organization of surveillance is done at the armed forces level, following the general guidelines of the intelligence-gathering plan. It includes listening to (interception of messages) telegraphy and wireless telephony, ground telegraphy, wired telephony; and radiogoniometry (determining the location of transmitters) for wireless telegraphy (and telephony). Depending on the case, it is either performed by the listening sections of the telegraph sapper battalions (wired telephony, ground telegraphy), or by the radiogoniometry and listening sections of the army's radiotelegraphic companies (other processes). Although discharged from the special listening mission, any station which (without deviating from its own mission), overhears a message from the enemy has the duty to record it and to immediately report it. This rule applies to the ground telegraphy stations of the forward units. In view of the small range of action of the ground telegraphy, the organization of listening by the army cannot include a continuous chain of special stations. Listening relates not only to the text itself, but to all the emission's technical particularities. The staff engaged in optical transmissions, and all the qualified staff, in particular those at the observatories, must record the optical signals which can be observed in the enemy zone (nature, points of emission, and, if it corresponds, the text on the telegram) [COL 31].

During World War II, the Nazis had established telephone lines between all the occupied territories and Germany. To make sure there was no wiretapping, they monitored the voltage level on the lines, as any suspicious change could signal an attempted interception. Frenchman Robert Keller ("source K") is said to have managed to achieve a connection without drawing any attention on himself.

1.1.4. *The use of SIGINT capabilities*

SIGINT (Signal Intelligence) designates electromagnetic intelligence-gathering from signal interception. It comprises the following three components:

– ELINT (Electronic INTelligence) is the intelligence-gathering technique based on electromagnetic signals, except for voice and text. For example, it includes the radar;

– the FISINT (Foreign Instrumentation Signal INTelligence) designates the interception of electromagnetic emissions associated with the testing and outdoor operational deployment of aerospace, surface and undersea systems;

– COMINT (COMmunications INTelligence) includes voice and text: "The interception and analysis of the radio communications is the main application of COMINT systems"[3].

> COMINT is intelligence and technical information derived from collecting and processing intercepted foreign communications passed by radio, wire, or other electromagnetic means. COMINT also may include imagery, when pictures or diagrams are encoded by a computer network/radio frequency method for storage and/or transmission. The imagery can be static or streaming [JOI 13].

COMINT can itself be segmented into five domains or fields[4]:

– the interception of HF radio communications (0.5 MHz to 30 MHz);

– the interception of communications in the V/UHF band (20 MHz to 3 or 6 GHz);

– GSM COMINT;

– satellite communications;

– Internet communications.

---

3 See: www.emsopedia.org/entries/communication-intelligence-comint/ [Accessed April 21, 2021].

4 Here, following the segmentation proposed on the site www.emsopedia.org/entries/communication-intelligence-comint/ [Accessed April 21, 2021].

The importance of COMINT lies in "its ability to reveal the intercepted source's posture, activity and intent, thanks to the access of data and voice content"[5].

When it entered the war in 1939, Germany had already acquired experience in interceptions during the interwar period and deployed international listening capabilities integrated into intelligence services combining human intelligence and SIGINT. Some countries were prone to systematic interception, using large-scale infrastructures deployed with allied countries: "All cable lines leading out of Czechoslovakia which touched German, Austrian, or Hungarian territory were monitored. For this purpose there was close cooperation between the German, Australian, and Hungarian espionage and cryptanalytic services" [FLI 53].

At the beginning of World War II, the United States was also in possession of advanced COMINT capabilities. For example, in 1930, the US Army created its own SIGINT intelligence service, the SIS (Signal Intelligence Service) (for a thoroughly documented history of SIGINT within the US Army during World War II, see the important work of James L. Gilbert and John P. Finnegan, published in 1993 [GIL 93]). Even though the military intelligence services had developed significant means of interception and decryption, the Pearl Harbor attack came as a shock, which prompted the Americans to adopt a more systematic approach to diplomatic interceptions [GIL 93]. Unsurprisingly, the development of SIGINT capabilities brings to light the competition between the different forces, in this case, the US Army[6] and the US Navy who competed on these goals[7].

At the end of World War II, intelligence-gathering activities continued to be pursued, and the entry into the Cold War provided a new theater of intelligence operations to legitimize the construction of a SIGINT architecture at a global scale. The goal was to detect any offensive maneuver on the part of the USSR as soon as possible, preventing a nuclear attack and protecting the airspace of the United States. The enemy was communism. China was also under the sight of the United States. SIGINT capabilities were deployed to monitor China, Taiwan (then Formosa) and the region as a whole.

---

5 See: www.emsopedia.org/entries/communication-intelligence-comint/ [Accessed April 21, 2021].

6 The United States Army Signal Corps (USASC) was created as a branch of the US Army in June 1860. It then included only one man, Doctor Albert James Meyer, who was also its initiator. The purpose of this service was to provide the army with a communication system by means of visual signals (flags, light signals, etc.). In 1867, the military exploitation of the electric telegraph became one of the responsibilities of the Signal Corps [KAT 94].

7 See: www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/SIGINT_Goes_to_War.pdf.

At the end of the two great world wars, the benefits of SIGINT seemed unquestionable:

> The value to the Allies of our Signal Intelligence effort during World War II can scarcely be overestimated. Through the reading of high-grade German and Japanese ciphers, we were able to penetrate the enemy lines and enter the headquarters of High Commands, Army Groups, and Armies. On a strategic level, "Special Intelligence" was the unique source of advance knowledge to the enemy's plans for both offensive and defensive operations. It was the timeliest, most complete, and most reliable source of intelligence in his Order of Battle, intentions, and capabilities [NSA 53].

The expression "special intelligence" (in the original text)[8] denotes the intelligence gathered from cryptanalysis, and its successes, against the enemy's encryption systems. This dimension of technology in war was essential for the effectiveness of SIGINT.

The superiority acquired by SIGINT was reflected at all levels, both strategic, tactical and operational:

> On the tactical level, reading the medium and low-grade ciphers, traffic analysis, and direction-finding provided a rapid flow of operational intelligence in the field. The value of operational intelligence from those sources was proved again during the conflict in Korea, and the vital part which COMINT will play in the event of a third world war of reasonably conventional duration cannot now be in any serious doubt [NSA 53].
>
> COMINT here includes: both the Special Intelligence of World War II and all other intelligence which may be derived from the radio communications activities of a foreign government medium and low-grade cipher messages, plain language transmissions, radio telephone conversations, traffic analysis and direction-finding [NSA 53].

It is in a war context that the states built their SIGINT capabilities. Australia, for example, began its SIGINT activities in 1942 as part of cooperation between its armies and the American defense forces[9].

8 "'Special Intelligence' is COMINT derived from decryption of high level cryptographic systems. Potentially, it is the most important and the most reliable source of indicators of hostile intention" [NSA 54].

The SIGINT agencies created at that moment had the mission of intercepting Japanese military communications. At the end of the conflict, the Australian authorities perpetuated these SIGINT activities within the army.

During World War II, COMINT supported a variety of pursuits in multiple theaters of operations. The literature and archives provide abundant illustrations of these uses:

– in the Pacific theater, the United States deployed capabilities to intercept the communications from the Japanese enemy: for example, it was thanks to the COMINT's interceptions of the Japanese command that the warship Yamato was spotted, tracked and sunk in 1945[10];

– in particular, the reader may refer to the following publications: a history of American COMINT during World War II by Robert Louis Benson [BEN 97]; a reflection on the impact of technology on organization in general, and more particularly, of COMINT technologies on the American military organization during World War II [BER 18].

1.1.5. *Wartime interceptions in cyberspace*

The use of cyberspace by armies and intelligence agencies was accompanied by the introduction of new concepts, including those of CYBINT (Cyber Network Intelligence) or DNINT (Digital Network Intelligence), which refer to network intelligence operations. Cyberspace interceptions are one of three forms of offensive actions undertaken in this dimension:

> In general, attacks in cyberspace fall into one of three categories – the interception, modification, or denial of information [WOO 06].
>
> CYBINT is the process of explicitly gaining intelligence from available resources on the Internet. CYBINT can be considered as a subset of OSINT [SOO 14].
>
> Cyberintelligence thus makes it possible to have an almost total vision of the cyber structure of a society, an organization or an individual [LEG 16].

9 See: www.naa.gov.au/explore-collection/intelligence-and-security/history-australian-intelligence-and-security.

10 Schulz LR, Comint and the Sinking of the Battleship Yamato, NSA Online Archives, [Online]. Available at: www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/comint_and_the_sinking.pdf.

> Under the premise that SIGINT is gathered from signals and HUMINT is gathered from humans, an emergent simple definition of CYBINT is intelligence gathered from cyberspace. […] The lack of consensus of what comprises cyberspace makes the definition of cyber intelligence equally pervasive […] with a lack of consensus on the cyberspace definition, information that would commonly be considered a component of other intelligence-gathering disciplines can easily be defined as a CYBINT component. For example, intercepting signaling channels of digital-communications links to capture information in establishing links between systems is traditionally a practice of SIGINT. Using the "interconnected technology" cyberspace definition and the fact that this intelligence was gathered from connecting two (or more) technological systems brings this intelligence into the realm of CYBINT, as it was arguably gathered from cyberspace. Hence, any information gathered from any technical interconnection could now become CYBINT [SEE 18].

The US Department of Defense [JOI 18] considers cyberspace as a "terrain", analogous to the conventional physical realm. The expression used is "key terrain in cyberspace". In this "cyber" territory, the army can isolate spaces, some of which are vulnerable to interceptions:

> The military aspects of terrain (obstacles, avenues of approach, cover and concealment, observation and fields of fire, and key terrain) provide a way to visualize and describe a network map. Obstacles in cyberspace may include firewalls and port blocks. Avenues of approach can be analyzed by identifying nodes and links, which connect endpoints to specific sites. Cover and concealment may refer to hidden IP addresses or password protected access. Cyberspace observation and fields of fire refer to areas where network traffic can be monitored, intercepted, or recorded. Examples of potential key terrain in cyberspace include access points to major lines of communications (LOCs), key waypoints for observing incoming threats, launch points for cyberspace attacks, and mission-relevant cyberspace terrain related to critical assets connected to the DODIN [JOI 18].

The notion of MOE (Measure of Effectiveness) is also available there. Adversary systems must be observed in order to detect any changes in enemy practices and to

seize the opportunity to conduct interceptions: "MOEs are used to assess changes in targeted system behavior or in the OE[11] […] For example, a MOE for a cyberspace attack action might be a meaningful reduction in the throughput of enemy data traffic or their shift to a more interceptable means of communication" [JOI 18].

1.1.6. *Drones and interceptions*

Drones can act as interception tools or as interception targets, especially in a military context:

– as part of a call for projects published in 2020, the French army planned to use drones equipped with sensors to intercept radio communications at diverse theaters of operations [SEE 20];

– drones could be used to conduct not only physical attacks, but also software attacks: deploying fake Wi-Fi networks in order to intercept smartphone traffic; attacking other drones equipped with communication tools programmed to intercept other drones' communications, etc. [YAA 20];

– in 2009, Iraqi insurgents intercepted live video feeds from US Predator drones using a $26 program available on the Internet [GOR 09].

1.2. The interception of international communications: espionage, surveillance, war

> The combination of speed and volume of Internet traffic means most states have limited capability to intercept and monitor cyberspace communications. This limited ability to intercept and monitor traffic through cyberspace is important to maintaining the neutrality of states that are mere intermediaries in information warfare, as in our opening scenario, because the transited state is unlikely to be aware of the transmission [BAR 01].

1.2.1. *The interception of telegrams*

The economic and commercial field has always been a suitable arena for fraudulent practices and espionage. with its extensive and dense communication networks as never before, the 20th century offered a privileged framework for such practices.

11 OE: operational environment.

Fraudulent transactions are mentioned in the international press. The daily *The Straits Times* (Singapore) thus evoked on July 21, 1909[12] the complaints of traders who in Calcutta suspect the interception of their telegrams:

> For the past eighteen months complaints have been reaching the Calcutta telegraph office from local merchants of the interception of their market cables from London relating to the prevailing rates of gold, silver, rice, wheat, jute, etc. The Calcutta police arrested three men in the 10th inst. which clear up the mystery. These men were a telegraph peon named Gunga Saran Roy and Durgahi Lal. The two last named opened a small office near Dalhousie Square in a narrow lane where Dwarks and other peons used to take telegrams. These used to be carefully opened by Gunga and copied by Durgahi; and their contents telephoned to various firms and the particular goods mentioned in the cables bought up. Dwarka will be prosecuted for criminal breach of trust, and Gunga and Durgahi for aiding and abetting him, as well as on charges under the Telegraph Act.

1.2.2. *Espionage during the Cold War: satellite, radio, telephone interceptions*

The Cold War was one of the major periods in the history of intelligence-gathering. Spying on, gauging, confronting one another and sometimes clashing in peripheral wars, the great powers deployed considerable means to spy on each other throughout this period (1947–1991).

All along, operations were planned to intercept the enemy's communications. While certain communications, as, for example, those by satellite, could be subject to interception at great distance in function of the geographical location of the facilities, others required approaching the sources as close as possible. Among the latter, we can mention the following operations:

– Silver: conducted by British intelligence services between 1949 and 1955, and whose goal was to tap into landline communications of the Soviet army headquarters in Vienna.

– Gold (Berlin Tunnel Operation Gold for the United States; Operation Stopwatch for the UK), code name PBJOINTLY, or REGAL[13]: conducted jointly by

12 See: www.eresources.nlb.gov.sg/newspapers/Digitised/Article/straitstimes19090721-1.2.75?ST=1&AT=search&k=interception%20of%20telegraph&QT=interception,of,telegraph&oref=article.

13 See: www.coldwar.org/articles/50s/berlin_tunnel.asp.

the Americans (CIA) and the British SIS (Secret Intelligence Services), it exploited a tunnel dug in 1954 into the Soviet-occupied zone of Berlin in order to tap into Soviet communications. This was practiced for nearly a year in 1955–1956 and enabled the recording of hundreds of thousands of conversations and millions of telexes, which then had to be translated, requiring the mobilization of colossal resources by the intelligence agencies.

– These two operations to intercept Soviet strategic communications provided Westerners (American and British) with key information regarding the USSR's intentions.

– Technological developments forced intelligence services to get as close as possible to their sources in order to listen to them. Although low-frequency radio broadcasts could be listened to at great distances, the transmission of communications in large volumes and at high frequencies raised new practical problems. The CIA sought to exploit messages transmitted over landlines. The discovery of a vulnerability in an encryption system from the Bell System company paved the way for the interception of unencrypted signals, without the need for decryption (echoes of the unencrypted message were transmitted on the cables at the same time as the encrypted message). The hypothesis was that this flaw in the Bell system could be shared by other communication systems. The choice of Berlin for the tunnel interceptions can also be explained by the position of the city in the architecture of the communication systems from Eastern Europe. Berlin acted as a hub. Every communication from a point in Eastern Europe passed through Berlin [NSA 88].

1.2.3. *The interception of international communications: the Echelon program*

The Echelon[14] network was established by the United States, the United Kingdom, Canada, Australia and New Zealand to intercept communications from commercial satellites. Its origins lie in the 1943 agreement between the United Kingdom and the United States, amidst World War II. It then developed and extended to other partners during the Cold War with the goal of bulk interception and whose existence was disclosed to the public after the 1990s [FOR 05]. It contributed to economic intelligence actions which gave a competitive advantage to American companies. The loss by Thomson-CSF of the call for tenders for a radar system in Brazil to the American Raytheon is attributable to Echelon interceptions.

14 See: www.fr.wikipedia.org/wiki/Echelon.

In 1988, Duncan Campbell[15] published an article in the journal *New Statesman*, which brought the Echelon program to the fore. At the end of the 1990s, the European Parliament published reports on the subject: the 1997 STOA (Science and Technology Options Assessment) report, the "Interception Capabilities 2000" report which addresses commercial satellite espionage systems, and especially the Schmid report which is an uncompromising document, presented to the European Parliament [SCH 01]. From the report "Interception Capabilities 2000" written by Duncan Campbell, let us retain the following points:

– Dozens of Silicon Valley companies supply SIGINT technologies to the NSA (companies such as Lockheed Martin, TRW, Raytheon, etc.).

– Some of the companies that provide SIGINT and COMINT capabilities are run by former senior NSA officers.

– International communications from the United Kingdom and the United States and those directed to these same countries have been intercepted since the early 1920s. In the United Kingdom, a law passed in 1920 on official secrets provides access to all types of communication. Other laws followed, such as the Interception of Communications Act 1984 (also in the United Kingdom). The other countries taking part in the Echelon project have adopted laws creating obligations for telecommunication operators.

– Pre-1970 was the era of analog technologies. Post-1990 is essentially digital.

– The access to data/messages is done either "with the complicity of the network operators", or "without their knowledge" [CAM 00].

– International communications are systematically intercepted, including messages sent by or to American citizens.

– Internet interception: "Since the early 1990s, fast and sophisticated COMINT systems have been developed to collect, filter and analyze the types of fast digital communication used by the Internet" [CAM 00]. "Access to communications systems is likely to be remain clandestine, whereas access to Internet exchanges might be more detectable but provides easier access to more data and simpler sorting methods" [CAM 00].

– In the 2000s, the task of interception became more complicated by the shift from telecoms to fiber optic networks. "Physical access to the cable is necessary for interception" [CAM 00].

15 Duncan Campbell is a British investigative journalist, who in 1988 revealed the existence of the Echelon network to the general public, in an article entitled "Somebody's Listening". The article is available at: www.new.duncan.gn.apc.org/menu/journalism/newstatesman/Somebody's_Listening.pdf.

During the Cold War, the NSA, whose primary function was the analysis of signals (SIGINT), focused on the passive interception of (over-the-air) wireless transmissions, such as satellite communications. enshrining the analog–digital transition, the Internet changed the game. Conventional interception became ineffective on optical cables, and the expansion of computer networks required an in-depth review of interception methods. They had to be practiced as close as possible to the source, with physical access to the transmission equipment. The considerable increase in the volume of communications has induced a change in scale which has jointly called for the development of surveillance capabilities. As the United States are at the heart of global Internet networks, the NSA has a considerable advantage from this point of view [CLE 14]:

> On August 14, 1962 [REU 62], the Australian newspaper *The Age* published a news brief relating to the interception of communications between Moscow and a soviet space station: "The Japanese Government radio station N.H.K. in Chiba, east of Tokyo, reported that it had intercepted Soviet radio instructions to Vostok IV, ordering it to prepare to return to Earth".

1.2.4. *Bulk cyber surveillance*

The September 11, 2001 attacks seem to have been a breaking point in the NSA culture:

> Ex-NSA analyst J. Kirk Wiebe recalls: "everything changed at the NSA after the attacks on September 11. The prior approach focused on complying with the Foreign Intelligence Surveillance Act ("FISA"). The post-September 11 approach was that NSA could circumvent federal statutes and the Constitution as long as there was some visceral connection to looking for terrorists". While another ex-NSA analyst also remembers: "The individual liberties preserved in the US Constitution were no longer a consideration [at the NSA]"[16].

This analysis can be called into question. The NSA had already extended surveillance to American citizens before the September 11 attacks, as evidenced by the great United States public intelligence crisis throughout 1975 which had resulted in an unprecedented conflict between the Congress, the White House and the agencies, following the revelations about the CIA and the FBI activities by the press [LAU 14].

16 Quoted in "Timeline of NSA Domestic Spying" [Online]. Available at: www.eff.org/fr/nsa-spying/timeline.

In 2001, William Binney and J. Kirk Wiebe resigned from the NSA and denounced the excesses of the activities carried out there, especially via the *Thin Thread* program, which they had contributed to develop within the agency. *Afterward, Binney and Wiebe denounced the existence of the Stellar Wind program, which intercepted communications within the country (telephone, email messages)*[17].

The disclosure of classified documents by E. Snowden brought to light the existence of NSA cyber surveillance practices and capabilities on a massive scale. At present, practices are part of the long term and affect all citizens, unlike the programs for the interception of satellite communications denounced in the 1990s, which mostly concerned states and businesses.

At that moment, the issues mainly concerned economic espionage, unfair competition, political espionage, etc. Echelon reflected the state's quest for power. The practices denounced by Snowden mark America's power strategy, but they are part of a security policy in the war against terrorism. At the same time, according to Snowden, they create risks for citizens.

Internet and the various applications having developed since the early 1990s worldwide have offered intelligence agencies new opportunities for collecting and accessing data.

The "Interception Capabilities 2014" report[18] highlights the difference between old and new interception methods. Old methods are characterized by the legal and targeted interception model, the proportionality of the means and the European security exception. New methods, on the other hand, are characterized by scale, depth level, the multiplicity of methods, secret partnerships, illicit attacks and compromised hardware.

1.2.5. *Foreign companies in national telecommunication infrastructures*

Recently, international relations have brought to the fore the question of technological sovereignty, due to the risks posed to states by the level of control/penetration of foreign companies into sensitive and critical infrastructures, including communication systems. International tensions have particularly crystallized around 5G technology.

17 "The National Security Agency (NSA) Controversy: Timeline" [Online]. Available at: www.discoverthenetworks.org/viewSubCategory.asp?id=1933. [Accessed March 1, 2017].

18 See: www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf.

Chinese telecommunication companies are under the sight of Western countries, because they provide telephone operators with the means to deploy their vast networks (formerly 3G, then 4G and finally 5G). However, these companies are accused of acting as Trojan horses, of opening backdoors in national networks, of authorizing foreign powers (in this case, China), to capture feeds for espionage purposes. They allegedly even have the capacity to take control of the networks, something which, in a conflict scenario, could represent a major vulnerability for the countries dependent on such technologies. The Chinese operator Huawei has thus been accused, among others by the Netherlands, of having accessed the data of millions of customers from the KPN operator and to have had the possibility of listening to all their communications for years [BAY 21].

1.2.6. *Actions over undersea Internet cables*

In the 1960s, the United States secretly operated in international undersea spaces. As part of the Holystone program, the US Navy carried out espionage tasks using submarines. The practice was debated in the United States in the 1970s [HER 75] due to the confrontation risks posed by intrusions into the Soviet maritime space, on the one hand, and the interception of submarines themselves by the Soviet Defense Forces, on the other. More generally, the debates focused on intelligence-gathering and the control of government initiatives in this area. While the whole challenge for the Americans was to remain undetectable, it seems that the USSR was informed about the program's existence. The submarines were able to tap into Soviet undersea communication cables and to intercept high-level military messages which were not transmitted via other channels such as the radio, due to the vulnerability of other modes of communication. The submarines used for these operations were Sturgeon or 637 Class attack submarines to which specific electronic equipment was added.

When, in the early 1970s, the Americans became aware of the existence of undersea cables near the Kuril Islands, they launched Ivy Bell Operation, which lasted until 1981, placing sensors on these cables, regularly collecting data which were then processed by NSA services [KHA 13].

According to the Corpwatch website, the Californian company Glimmerglass offered government agencies the CyberSweep software that can intercept undersea cable signals [CHA 13] and analyze Gmail, Yahoo! and social media feeds such as Facebook or Twitter:

> With the introduction of fibre-optic cables and the ensuing dependence of businesses and governments on trans-ocean communications, the world's oceans have become a target-rich environment that provides

> adversaries with incentives to develop undersea operational competence and strike these difficult-to-defend systems [ZIO 13].

The disclosures by E. Snowden reported the existence of multiple communication interception programs installed in undersea infrastructures. To accomplish this, the states benefited from the contribution of private companies (the British agency GCHQ is said to have used technologies from the Vodafone company[19]).

Internet undersea cables, fiber optic cables, are no less vulnerable to interception attacks than other communication technologies:

> There is a prevailing, misguided belief that fibre networks are more secure than other media, such as copper and wireless technologies. Fiber networks are vulnerable to tapping through the use of well-known techniques such as man-in-the-middle, re-routing and exploiting protocol vulnerabilities and software vulnerabilities in network devices. There is also a perception that fibre networks are much better protected against physical interference and the installation of tapping equipment. This is a misunderstanding: fiber networks are at least as vulnerable to physical tapping as traditional copper [DEL 17].

1.2.7. *Interceptions in planes and airports*

Aircraft on board GSM services were introduced on March 20, 2008. The number of its users rapidly grew. NSA SIGINT systems, as well as GCHQ British services, were mobilized to intercept these communications [FOL 16].

Intelligence-gathering agencies or the police monitor and intercept communications at the airports. In 2017, a Canadian journalist detected the presence of IMSI-catchers in Trudeau airport (Montreal)[20].

1.2.8. *International interceptions as a product of secret alliances*

Companies in charge of securing communications can act as intelligence providers for the states, according to the findings of an investigation published by the *Washington Post* in February 2020, which affirms that the German company

19 See: www.securityaffairs.co/wordpress/30438/intelligence/gchq-wiretapping-undersea-cables.html.

20 See: www.cbc.ca/news/canada/montreal/trudeau-airport-spying-1.4055803.

Crypto AG (providing encryption solutions to a hundred countries) was allegedly bought by the CIA in 1970, thus enabling the American agency to intercept encrypted communications. The systems are said to have been rigged with backdoors so that intelligence services could access the contents. The operation was supposedly called "Thesaurus", then "Rubicon", and according to a former German intelligence official, it made it possible to make the world a bit safer [AGE 20].

1.3. Interception of diplomatic correspondence

Intelligence gathered from the interception of communications in all their forms plays a central role in the political and diplomatic life. Interceptions are organized methodically:

> All the dispatches from the Prince of Kaunitz, all those from imperial ministers in foreign courts, all those from foreign courts and ministers which are intercepted, pass through what we here call the cabinet. This is where the decipherers' offices are established. The Baron de Pichler is its director; he discusses directly with the Empress and reports only to her. This director always gives the princess five copies of each dispatch, either imperial or intercepted. From these five copies, the Empress gives one to the Emperor, sends one to Florence, to the Grand Duke of Tuscany, as the eventual successor of the Austrian monarchy, if the Emperor has no children; one to Brussels to the Prince of Starhemberg, as appointed to replace the Prince of Kaunitz; and one to the Count of Rosemberg, as confidant, whose advice is believed to be useful […] Another singular and very true anecdote is that the Empress sometimes adds or removes information from the intercepted dispatches.

The author of these lines continues the description, referring to the extensive interception of the private correspondence from the King of Prussia to his minister in Vienna:

> Through this channel, we have real and very interesting notions about the politics of the two currently befriended courts, their hidden designs, the nuances of their liaisons with the court of Petersburg, and the monarch's language and maneuvers […] We have been able to know the full weight of this interception by the successive sending of the sequence of these Prussian dispatches, which already form a voluminous series […] I would like to finish this presentation of my discoveries by announcing an infallible key that I myself carry to the king to get to know the most secret details of the correspondence of

> the king of Prussia with his minister in Paris. It is the decryption of their cipher […] Vienna, July 4, 1774 [FAV 93].

This document sheds light on the various facets of the profession of diplomat and spy, the place occupied by postal interception, and the various tactics and subterfuges deployed by the actors to take full advantage of it.

The encryption and decryption of couriers are two integrated functions within the French Ministry of Foreign Affairs, as depicted by Jean-Baptiste-René Robinet in his Universal dictionary of moral, economic and political and diplomatic sciences (*Dictionnaire universel des sciences morale, économique, politique et diplomatique*) at the end of the 18th century [ROB 77]:

> The Department also maintains two sorts of decipherers: the first are responsible for ciphering the dispatches the Court sends to its Ministers residing in foreign Courts, and for deciphering the reports they receive from them. This is a laborious and confidence-requiring work, which deserves to be rewarded with a good salary […] The other decipherers have applied themselves to deciphering without a key the ciphered dispatches the foreign Courts address to their Ministers residing with us, or that the latter send to their Masters. This art is not as infallible as many people claim, and we will show instead that a well-sealed letter, properly ciphered with a solid key, is absolutely indecipherable. However, as not all the Courts have ciphers so difficult to guess, and not all Chancelleries are so accurate in ciphering well, nor in closing their letters with sufficient precaution, the Department sometimes avails itself of their negligence, and, by employing the know-how of these kinds of decipherers, manages to discover very dangerous projects, or matters of the greatest importance.

Powers operate outside their territories: “We have certainly not forgotten the declarations of Mr. Clemenceau, who promised to put an end to the zeal of the Russian secret police, which, in the heart of Paris, openly ‘stole’ the correspondence received by the political escapees from the Tsar’s Empire” [MAH 13].

The construction of the electric telegraph vast cable networks in the 19th century quickly raised questions about the risk of exposure to indiscreet ears, of the messages conveyed by these infrastructures extending over thousands of kilometers:

> We are sure of the approval of every intelligent man when we say that the most perfect and most exclusive control is absolutely necessary to ensure the regular reception of our political and commercial

> dispatches from India without any interception or indiscretion. It is not enough to have our employees or our stations, when the wires belong to another government and are maintained by foreigners [DES 58].

1.4. Political surveillance: targeted and bulk interceptions

1.4.1. *Interception of correspondence*

King Louis XI of France (1423–1483) was, it is said, one of the first to organize a royal courier service, which afterwards enabled the transport of private correspondence. But in return for the transport of private correspondence, the royal services had to be aware of the messages' contents:

> The ancient legislation teaches us that the postal administration has always made it its business to unseal letters. It was forbidden for all post offices, post clerks and postmen, to open any letters or packages entrusted to them, under penalty of death, so odious was considered such a crime. A sovereign judgment issued by the Police Lieutenant-General of Paris on May 3, 1741, condemned Louis Leprince, an office clerk from the Paris post office, to death by hanging for prevaricate in his functions, having intercepted, unsealed and opened two letters coming from Caen. The following year, positive law stated that any postal employee convicted of having fraudulently unsealed letters and diverted its contents to make profit, would be condemned to death; this proves that the practice was quite common. For the case of suppression or simple interception, and depending on the gravity of the facts, the penalty was the galleys in perpetuity or for a period of time, banishment or a reprimand [ATH 28].

But this right of scrutiny would continue to arouse reservations and criticism. The inviolability of the secrecy of letters was well enshrined in law, and its violations severely punished: "Nothing is more fatal and more prejudicial to society's order than the power to violate, under any pretext whatsoever, the inviolability of postal secrecy" [ATH 28].

But the practice of interceptions made the 19th century the object of a dispute opposing citizens and those who supported this form of espionage.

Let us recall the order given by the English Minister of the Interior, Graham in 1844, to intercept the letters from Mazzini, who at this moment was a refugee in London (he would later become a statesman in Italy). Mazzini protested, the British people were indignant, Graham resigned. In the popular slang of the time,

to grahamise meant to intercept communications. The surveillance Graham wished to bring against Mazzini did not limit the information exploited to the benefit of his own government. He communicated the contents to partner governments on the continent. This sharing of information between powers echoes more contemporary practices.

For a long time, politicians and statesmen have succumbed to the temptation to intercept mail, messages, communications, intrigued by the contents passing within their reach. But the victims of these practices are not easily fooled. Interceptions are more or less discreet, leaving more or less traces. One of the major challenges of those in charge of interception is to ensure that their intervention is invisible. The other challenge concerns the decryption of messages the most cautious senders have thus tried to protect. It is also remarkable that since the 19th century the civil society, the population, turned out to be an actor of resistance, of opposition. This practice was denounced by the press in several European countries in particular (Spain, England, for example). This meant that state actors were forced to be even more discreet, on the one hand, and to enshrine in law the principles consecrating the inviolability of secrecy: "Following too flagrant abuses in 1826, a paragraph was inserted in the Constitutional Act in Portugal instituting the absolute inviolability of the secrecy of correspondence" [MAH 13].

Notwithstanding these resistances, denunciations and principles enshrined in law, 19th-century states intensively practiced interceptions. The situation was so critical that the number of letters never arriving at their destination have reached considerable proportions [MAH 13].

1.4.1.1. *The cabinet noir*

The term "cabinet noir" (black room or dark chamber) refers to secret premises, placed under the control of states during the *Ancien Régime*, which existed in most European countries. These services were in charge of intercepting postal mail and cryptography in order to "identify and censor political opponents, and to inquire about diplomatic or military couriers"[21]:

> In the month of December 1880, during the somewhat resounding fall of the Ristics ministry in Belgrade, one could read in numerous Serbian newspapers that in the ex-Premier's bureau over two thousand letters had been suppressed and opened by the "cabinet noir", and among them many insured letters. This was a revelation, and its repetition should be carefully avoided. Nevertheless, the practice

21 See: www.fr.wikipedia.org/wiki/Cabinet_noir.

> persisted. For the adversaries of successive governments, in all the Balkan states without exception, the secrecy of letters was violated without the least scruple. Since hostilities broke out in the Balkans, many facts (and foreigners' testimonies) have proven that the interception of correspondence is practiced on a vast scale, both on the side of the Allies and in Turkish circles [MAH 13].

In France, these cabinets have existed since the appearance of the postal service. The edict signed by Louis XI on June 19, 1464 specifies in its Articles 13 and 14: "Couriers and messengers will be reviewed by the clerks of the Grand Master, to whom letters will have to be shown in order to find out whether there is anything detrimental to the service of the King, or which many contravene his edicts and ordinances"[22].

These "cabinets noirs" were particularly developed under Louis XV. There even existed a secret cabinet for the postal service, where the superintendent instructed opening certain packages. These services unsealed the letters, recomposed the stamps and sent the copies to the Police Lieutenant-General and the Minister of Foreign Affairs.

In 1789, many registers of grievances demanded the abolition of dark chambers [LAU 15]. The Constituent Assembly and the Convention proclaimed the inviolability of correspondence. Despite this, the dark chamber was restored by the French Directory, limiting surveillance to foreign letters. It was maintained under the Empire, the Restoration and would last until the Second Empire [LAU 09].

Aware of the fact that they were being observed, listened to, spied on, that their official and private correspondence could be intercepted, statesmen, politicians and diplomats ended up writing mere trivialities on their letters, a sign of self-censorship on the part of those concerned, as well as a clever way to deceive actors who were too indiscreet. Furthermore, the banalities could sometimes conceal hidden messages. Ordinary language became a code, a mask. The awareness that correspondence – regardless of its form or method – could be opened, read, seen or intercepted by third parties modified the behavior of correspondents. Humans never stopped imagining countermeasures, circumvention methods, aimed at protecting the messages from undesirable eyes. The history of interceptions, the history of interception methods, techniques and technologies is closely related to that of countermeasures, of all the ways invented to prevent interceptions. "Unencrypted", unprotected communication can sometimes be part of a broader tactical or strategic choice.

22 See: www.cosmovisions.com/Cabinet-Noir.htm.

1.4.1.2. *The Nazi state and the interception of telegrams and telephony*

In 1933, the activity of the National Socialists in the Saar was a major concern. The pressure exerted by the Nazi party against the population and the political leaders resorted to the interception of communications among other instruments, thus contributing to the construction of an authoritarian government:

> Rivaling the government of Society, a secret Nazi government seeks to exercise authority […] Police officers, even the highest and senior ones, are secretly at its orders […] The public services: the posts and telegraphs, taxation offices, municipal authorities, mayors, many bishops and prelates, even the judges and magistrates, obey, to a large extent, to this Nazi state within the state. Strictly speaking there is a reign of terror – including intimidation and espionage, anonymous denunciations, abductions of individuals, transported across Germany's frontiers, internments in concentration camps in Germany, threats of dismissal and withdrawal of pensions addressed to civil servants who do not obey the orders of the unofficial government, the interception of letters, telegrams, and telephone conversations… [SLO 33].

1.4.2. *Bulk domestic surveillance in East Germany*

The surveillance operated by the security services in the German Democratic Republic was part of bulk surveillance practices.

The practices of the Stasi in the former East Germany undoubtedly made the greatest impact. It is hard to think about a "political police" without bearing in mind the Stasi's name. On the eve of the fall of the Berlin Wall, the Stasi had over 100,000 employees. This potential was based on systematic recourse to informants, ruling the East-German society with an iron fist. The organization was completed by recourse to systematic tapping and interception of correspondence, tasks performed by approximately 2,000–3,000 members of the Stasi. The statistics seem to show a very strong correlation between the number of individual arrests and the density level of surveillance [CHE 16].

1.4.3. *Cyber surveillance in Russia: the SORM system*

The Russian SORM (*System of Operative Search Methods*) makes it possible to monitor the traffic of radio, telegraph, telephone and electronic networks (Internet) [GAÜ 16]. This system was implemented by the Soviet KGB to wiretap telephone communications. The next generation, also known by the acronym SORM-2,

enables the interception of telecommunications in Russia, capabilities which now include Internet flows. The latest generation SORM-3 incorporates all telecommunications. The law authorizes intelligence-gathering services (FSB) to collect and analyze metadata and contents, to store the data for three years and compels access providers to install surveillance equipment on their networks, with a direct access to traffic [LAW 14].

1.4.4. *Fixed and mobile telephone tapping*

1.4.4.1. *Wiretapping in American politics*

From October 1963 to June 1966, the FBI wiretapped activist Martin Luther King under the COINTELPRO program (*COunter INTelligence PROgram*), operated by the agency between 1956 and 1971. The targets of this program were the political organizations or movements representing a destabilization risk in the eyes of the government. It was not limited to the electronic surveillance of leaders and members of radical groups, but also implemented denigration or influence operations. The agency was also suspected of assassinations [WOL 01]. An investigation on assassinations, carried out by the Congress in 1979[23], concluded that the FBI had exceeded its surveillance prerogatives. The purpose of wiretaps was to identify contacts between Martin Luther King and the Communists, but targeted all private communications as well as exchanges government members without any discernment[24].

Lyndon Baines Johnson, a Democrat who unwillingly became President of the United States in November 1963 following the assassination of J.F. Kennedy, and who was later elected in 1964, was in office until January 1969. In 1964, he had to address the issue of racial riots in several cities across the country.

At the time of the 1964 Democratic Convention, L.B. Johnson wished to make sure that the protesters would not disrupt debates, which is why he required being kept informed about the opposition's negotiations. For this, he summoned the FBI services, who tapped the telephones of his opponents [MAY 01].

Between 1969 and 1971, Henry Kissinger was involved in telephone tapping ordered by the White House due to national security reasons, targeting several members of the *National Security Council* (NSC) as well as journalists. Wiretapping

23 *Select Committee on Assassinations, US House of Representatives, 95th Congress, 2 session*, 1979.

24 See: www.archives.gov/research/jfk/select-committee-report/part-2e.html.

was intended to find out who was behind media leaks of secret bombings in Cambodia[25]:

> Former President Richard M. Nixon said his efforts to undermine the presidency of the late Salvador Allende in Chile were prompted by the 'same national security interests' which led Presidents Kennedy and Johnson to intervene secretly in that country […] The former President's responses covered a range of questions touching on the Chile intervention as well as his authorization of domestic operations by the CIA and FBI such as break-ins, wiretapping and interception of cable traffic. In dealing with the Chilean intervention as well as the controversial surveillance programs targeted against American citizens, Nixon repeatedly argued that he has followed the lead of his predecessors in the White House […] In the arena of surveillance activities within the United States, Nixon said: "I remember learning on various occasions that during administrations prior to mine, agencies or employees of the United States Government, acting presumably without a warrant, conducted wiretaps, surreptitious or unauthorized entries, and intercepts of voice and non-voice communications". In a sharp response to the former President's answers, chairman Franck Church of the Senate Intelligence committee criticized Nixon's advocacy of a doctrine of "the sovereign presidency" as a "pernicious and dangerous doctrine" [STE 76].

In a testimony released on March 10, 1976 by his attorneys, Nixon confirmed that he had ordered a wiretap program in 1969. But he tried to disavow himself by placing the responsibility on the shoulders of his national security adviser, H. Kissinger, for choosing the targets [HOR 76].

1.4.4.2. *The Élysée wiretapping affair*

This scandalous affair took place during the first term of President François Mitterrand, between 1983 and 1986. The Élysée's anti-terrorist unit, headed by a GIGN (*Groupe d'intervention de la Gendarmerie nationale*) officer, wiretapped numerous personalities (media, entertainment, politics, etc.) on the orders of the President of the Republic. These wiretaps diverted the means of the state to private ends, because they only served the personal interests of Mitterrand. A judicial procedure was opened in 1993 and a trial took place in 2005. The unit used part of

25 "Kissinger Telephone Conversation Transcripts" [Online]. Available at: www. nixonlibrary. gov/index.php/finding-aids/kissinger-telephone-conversation-transcripts.

the GIC (*Groupement interministériel de contrôle*) means, dedicated to administrative interceptions.

1.4.4.3. *Argentina wiretapping scandal*

A scandal broke out in Argentina in 2009, relating to espionage practices not only aimed at the victims (and relatives) of the AMIA (Spanish for Argentine Israelite Mutual Association) headquarters 1994 attack in Buenos Aires (causing 85 deaths and 200 injuries), but also targeting politicians and journalists. The case took a new turn when it was discovered that President Cristina Fernández and her husband Nestor Kirchner could also have been the object of wiretaps. Personal data relating to numerous political personalities, civil servants, trade unionists and businessmen were found on the computers of the agency who performed the interceptions. In November 2009, the justice ordered the detention of the former police head of the city of Buenos Aires. This scandal motivated several interventions from the Supreme Court, who still insisted in 2019 on the need to strictly limit interceptions to investigations conducted by the judge[26]. The Court was concerned about the systematic use of interceptions, a practice erroneously considered as an ordinary means of investigation, despite the fact that it should only be used as a last resort for the most serious crimes. This warning was issued in 2019, after wiretapping records were leaked. These cases raised the question as to the limits of the actions pursued by the intelligence services and their connections with the justice, the police and politics.

1.4.4.4. *The case of Chile: "W" and Topógrafo operations*

"W" (in 2016) and Topógrafo (in 2017) operations designate surveillance actions conducted by the military intelligence. This was the first time a journalist was targeted, and the second time it happened to four soldiers, who denounced embezzlement within the institution. According to military intelligence officials, these operations involving telephone tapping were completely legal and were carried out with the judge's authorization. These practices raised the question as to the judge's role and the authorization procedure in general. The responsibilities weighing on judges are important. Are they still able to perform their role without any pressure, in total autonomy? Are authorizations always in accordance with what is provided for by the law? Do any spurious arrangements exist "among friends"? The question was posed by the media: who were the judges who had granted the authorizations [VED 19]? In any case, the fact that an interception has been authorized does not necessarily make it lawful.

26 See: www.mundo.sputniknews.com/america-latina/201906191087698866-corte-suprema-argentina-restringe-escuchas-telefonicas-judiciales/.

1.4.4.5. *Scandals in Peru*

In 1997, a scandal broke out after it was revealed that the government had wiretapped political opponents and journalists. Wiretaps are carried out by the military intelligence services (SIN, Spanish for *Servicio de Inteligencia Nacional*).

In 2018, legal wiretaps as part of an investigation against drug trafficking led to the revelation of a vast network of corruption at the top of the justice.

1.4.5. *The interception of electronic communications in the political sphere*

1.4.5.1. *The scandal of fierce interceptions in Colombia*

Political interceptions arouse strong reactions in the societies which experience such phenomenon, because they are considered as a severe attack on the principles of democracy.

In Colombia, many scandals related to the interception of communications in the political arena have been grabbing the headlines for years. Interceptions are often associated with corruption cases.

A case of illegal wiretapping, known as the "Chuzadas", tarnished President Uribe's second term (2006–2010). Among other scandals, let us mention: Parapolitica, Yidispolitica, Falsos Positivos [DUB 11]. The government was called into question in 2007 by revelations concerning fierce wiretapping. The Colombian President Alvaro Uribe was accused of transforming the intelligence services (the DAS, Spanish for Administrative Department of Security, who acted as frontier police, intelligence and counter-intelligence police)[27] into a force working for his sole political interest. The fight against all forms of opposition resulted in the surveillance of journalists, politicians, trade unionists, human rights defenders and magistrates, to mention only a few. These extrajudicial interceptions (telephone tapping, email and written correspondence interception, etc.) made it possible to surveil political opponents for several years. The information collected during the wiretaps made it possible to surveil individuals, their relationships and networks, their activities and ideological positions. These practices allegedly took place between 2004 and 2008.

In 2007, a dozen generals were dismissed. But the practice persisted. In February 2009, the magazine *Semana 13* published revelations regarding the extent of DAS's

27 During President Uribe's first term, the DAS had already suffered a scandal, accused of having bonds with the paramilitary forces.

illegal activities. In 2010, the justice took up the case and several officials were indicted, including officials from the intelligence services and the Secretary General of the Presidency of the Republic. In their defense, the defendants claimed that the activities were aimed at finding out the relationship between organized crime and the Supreme Court judges. Agents working in these intelligence services also reported using surveillance technologies provided by Washington [FOR 11].

These interceptions were only one of the bricks of the political surveillance strategy implemented within the country to ensure that the power in place could keep a grip on anti-establishment speeches. Wiretapping and the interception of electronic communications were only a supplement to stalking, threats and the violation of private homes.

The government dissolved the DAS and replaced it with the ANIC (Spanish for National Intelligence Agency). The purpose was to break with a past of corruption and criminal practices. In September 2017, the former director of the DAS was sentenced to seven years and 10 months in prison for the interception of private communications and surveillance without any orders from the judicial authority.

But new revelations at the end of 2019 seemed to bring to life those moments in Colombian history. New illegal wiretaps were carried out, this time targeting magistrates, opposition politicians and journalists. But this time wiretapping was due to the workings of the military [PAN 20] and targeted all those who had denounced corrupt practices within the army. Wiretapping had been carried out at two military garrisons, in an attempt to evade justice. The press published the disclosures of a Colombian cyber defense junior officer at the end of 2019. Armed with cyber education capabilities, the military intercepted WhatsApp and Telegram exchanges, the content of mobile phone communications and accessed computer contents.

1.4.5.2. *Espionage in Togo*

In August 2020, the Togolese authorities were accused[28] by the newspapers *Le Monde* [TIL 20] and the *Guardian* of having spied on members of the opposition, clerics (playing a role in the efforts to establish a dialogue between the power and the opposition) and civil society actors, by intercepting mobile telephone communications (geolocation, reading emails and messages, taking control of the camera and the microphone), with Pegasus[29] software provided by the Israeli

28 "Togo: Media reveal acts of espionage from the authorities", RFI, August 4, 2020 [Online]. Available at: www.rfi.fr/fr/afrique/20200804-togo-médias-révèlent-actes-despionnages-la-part-authorities.

29 See: https://en.wikipedia.org/wiki/Pegasus_(spyware).

company NSO[30] Group. When they were informed of being the targets of such practices, the victims were hardly surprised because "in Togo[31], it is common knowledge that everyone can be wiretapped".

1.5. Criminal interceptions

As soon as new communication technologies emerge, they can be used fraudulently. Without it technically being an interception, let us recall the misappropriation of the Chappe optical telegraph in France between 1834 and 1836 by clever crooks gambling on the stock market. Their goal was to get to know the stock values in Paris before the arrival of the information by mail, and to sell or buy depending on the trend.

Two bankers from Bordeaux, Louis and François Blanc, had the idea of exploiting the speed of the telegraph to transmit the information subliminally. This is how the issue No. 3506 of the *Gazette des tribunaux* from December 10, 1836 described the operation:

> An agent from Paris transmitted to Tours, *poste restante*, certain items, such as gloves, etc., whose color conveyed a rise or fall in stocks. Upon seeing these objects, the telegraph employee gave an agreed signal […] The Tours employee sent out an *error* signal, which was repeated all along the line, and consequently did not figure in the official dispatches.

Informed via a third agent, our two accomplices were certain of winning and could handsomely remunerate their accomplices. The affair was revealed following numerous errors made on purpose, detected by the Telegraphs' administration.

During the 19th century, interceptions became quite common, to the point that the states felt obliged to pass law on the question: "Shortly after the telegraph came into existence and wires were strung from pole to pole, wiretappers were busy intercepting the coded communications […] As early as 1862, California found it necessary to enact legislation prohibiting the interception of telegraph messages [DAS 59].

30 A Wikipedia entry indicates that this Israeli company is majority controlled by the British company Novalpina Capital: https://en.wikipedia.org/wiki/Pegasus_(spyware).

31 "Togo: Media reveal espionage actions from the authorities", RFI, August 4, 2020 [Online]. Available at: www.rfi.fr/fr/afrique/20200804-togo-médias-révèlent-actes-despionnages-la-part-autorités.

In the United States, the same skills, which had been acquired in the army during the revolution war, were recycled into the criminal field:

> After the Civil War, a number of former telegraph operators engaged in wiretapping for private gain […] As early as 1893, "past posters" were busy at work. They employed former linemen and operators for the Western Union Company to flash race news to gang members, so that bets could be placed with bookies before official race results had arrived [DAS 59].

Companies also engaged in these practices, particularly in the media:

> Equally active wiretapping practices existed at the same time among newspaper rivals. Telephone calls by reporters of one newspaper were being intercepted by reporters of a rival newspaper for the purpose of picking up "scoops." This practice existed across the country. It was reported in Boston, New York, Chicago, and San Francisco. In 1895, Illinois enacted legislation prohibiting wiretapping for the purpose of intercepting news dispatches [DAS 59].

The 19th-century "hackers" proved that they could cleverly exploit vulnerabilities in wired communications:

> A fraudulent interception of cable telegrams from Marseilles. We borrow from *Anales de la Electricidad* the following account of a real attack against the secrecy of telegraphic correspondence, committed in Barcelona by intercepting underground cables and whose authors have not yet been discovered. For a year and a half, over the section of the Marseilles cable, (between the Company's office in Barcelona and the landing gate), current diversions had been observed, increasing on a daily basis […] The technical observations made by the cable's offices (measurement of resistances), indicated that the fault should be found in the vicinity of the Promenade of San Juan […] We immediately proceeded to the opening of the channel on this short route and Mr. Brown was shocked to discover four conductor branches at the corner of the Rond de San Pedro and the Promenade de San Juan, which, starting from the four cables, went towards house No. 47 […] The thieves, who had to perfectly distinguish Marseilles' cables from those of the government […] had preferably made a connection over those from Marseilles, since the information from the Paris Stock Exchange was the only correspondence they could intercept. These telegrams

> were transmitted by Morse apparatus, whereas those from Madrid were transmitted by the Hughes system, whose signals cannot be received by sound"[32].

1.6. Police, justice: the fight against crime, lawful interceptions

The introduction of tools for the interception of electronic communications in the police sphere remarkably varied from state to state (done at different moments and paces). They sometimes even took place too late, after relatively isolated initiatives. Australia, for example, only became interested in these practices near the end of the 1960s according to the findings established in a report by the Royal Commission of Inquiry into alleged telephone interceptions, published in 1986[33]:

> In approximately 1967 Sergeant D.R. Williams was attached to the Communication Branch of the NSW Police as a senior technician. In that year, according to Williams, the Commissioner of Police, Mr. N.T.W. Allen, asked Williams to attend Police Headquarters in order to discuss new electronic means of obtaining criminal information […] Williams' recollection of the conversation is that the Commissioner requested him to explore the possibility of utilizing both listening devices and devices for the interception of telephone conversations […] Williams said he was joined in the task by Constable G.P. Smith early in 1968. Smith had been attached to the Radio Technical Unit of the Police Communications Branch since 1966. His recollection was that during the period 1966 to 1967 he developed, on a part time basis, several small transistorized transmitter devices. These devices were used as listening devices and were not at that stage used for the interception of telephone conversations" […] Smith began to experiment with the notion of using the transistorized transmitter devices on telephone lines. Williams said that the first device suitable for the interception of telephone conversations was constructed by himself and Smith in 1968. […] In 1969 Williams visited the United States to study the progress and development of radar speed detection equipment.

---

32 *Le Journal télégraphique*, July 25, 1889, p. 155–156 [Online]. Available at: www.gallica.bnf.fr/ark:/12148/bpt6k5575657j/f15.image.r=interception?rk=42918;4.

33 *Report of the Royal Commission of Inquiry into alleged telephone interceptions*, volume 1, April 30, 1986, Melbourne [Online]. Available at: www.parliament.vic.gov. at/papers/govpub/VPARL1985-87No96.pdf.

Williams then tried to look further into the development of interception technologies in the United States, but "he obtained very little information relating to such devices".

The interceptions implemented by the police forces have nourished the images of multiple works of fiction, novels or cinema. Policemen are portrayed as stationed in vehicles, earphones on their heads, recorders on and after hours of often fruitless waiting, capturing a few snatches of conversation which provide the keys to the case in progress. However, these taps result from microphones placed inside the buildings, not from the interception of communications between a transmitter and a receiver. This practice is illustrated by the images of police placing "contact clips" on telephone cables, and then listening to communications from a distant exchange. An audible, rasping, parasitic noise would signal to correspondents the presence of these indiscreet devices.

Today, the police practice "legal interceptions", contemplated by the law (few countries do not have such legislation), technically relying on legal interception systems or platforms. However, marginal practices persist, as evidenced by the recent confessions from the Israeli police services who admitted to illegally using the Pegasus application, although at first, they had strongly denied using this software.

In prison, the use of the telephone is not forbidden, but strictly limited. On the contrary, the introduction of mobile phones and any form of electronic communication tool is prohibited. This ban should allow the institution to monitor the prisoners' activities and to prevent criminal pursuits outside the prison. This prohibition does not always prevent the introduction of mobile phones, which surprisingly manage to enter the prison through various means. To counter this risk, prisons can equip themselves with detection tools which locate phones as soon as they are activated. Prisoners' telephone communications may be monitored, their exchanges intercepted and recorded[34]. These taps are not secret, the prisoners are informed.

1.7. On the usefulness and effectiveness of interceptions

During a cybersecurity conference held in France in 2018, the technical director of the DGSE spoke about the difficulties of the intelligence-gathering profession, and more particularly its technological challenges:

34 See: www.le.alcoda.org/publications/point_of_view/files/IPC.pdf.

> […] The first challenges for an intelligence service like mine, a technical service, is to keep up with technological developments. It may sound trivial, but in fact we completely suffer from technological developments, we can anticipate absolutely nothing […] We suffer from crypto labs attacks who are trying to crack crypto. We have people who make the interceptions […] Historically […] we developed these different capacities: crypto, interception […] As a technique, it no longer works. Crypto on its own, in broad terms, we no longer break. Interceptions, if you just intercept, as it is encrypted, it is useless since the crypto won't be able to break it. Despite all, computing is still required, there are vulnerabilities, there are pieces of keys in circulation […] So very often when, we have a problem to solve, we articulate our capacities"[35].

Interceptions alone would be of limited use if the contents could not be accessed. And to achieve this, intelligence actors have to mobilize techniques, methods, different capacities, expertise called upon to work together.

It is difficult to dispute the usefulness of interceptions because they are at the heart of intelligence practices, whether in times of peace, crisis or armed conflict. Intelligence based on interceptions enriches the knowledge acquired by other techniques (HUMINT or OSINT, for example). However, they do not provide an absolute mastery of reality. While interceptions provide information of unequal quality, their real usefulness is assessed by the use we make of them. Quality interceptions could not prevent strategic-surprise attacks (such as the Pearl Harbor attack) or tactical ones (the attack on British law enforcement agents on Easter Monday 1916 by Irish revolutionaries, although the authorities had been informed of imminent activity on the basis of intercepted secret Irish messages) [BER 16].

In 1973, in their report made on behalf of the Control Committee of the administrative services involved in telephone tapping [MAR 73], Pierre Marcilhacy and René Monory critically scrutinized past interception practices and called into question their usefulness in terms of security:

> If we try to make an assessment of two centuries of systematic espionage, we can see that its contribution to the internal and external security of the state was rather negligible, even when the interception of private messengers supplemented the opening of postal "packets": the spies' arrests at the end of the 16th century, the discovery, at the same time, of the transport routes for forbidden books from Holland, a

35 Conference by DT Patrick Pailloux, SSTIC 2018 [Online]. Available at: www. youtube.com/watch?v=eGi1vuwHQFQ [Accessed October 25, 2021].

> few "conspiracies" under the Restoration, diplomatic intrigues, the interception of political pamphlets under the Second Empire, none of this justifies a general and permanent inquisition, nor can it make us forget the excesses and intrigues bolstered by the "cabinet noir" system [MAR 73].

Although of limited utility, interceptions have long been an instrument of political power. "All regimes have resorted to the violation of private correspondence", carefully arrogating to themselves the monopoly on practices strictly prohibited to ordinary citizens ("a Royal Declaration of 1742 equated [*interception*] to the embezzlement of public funds and this could be even punished by the death penalty") [MAR 73]. Political powers have been able to use and abuse their prerogatives, disregarding the rights of individuals: "[…] It is striking, on the other hand, to note that in this matter the most vibrant affirmations of principles, the most formal assurances of respect for the rights of nations have only ever served to conceal the worst abuses […]" [MAR 73].

And when the Republic practices fewer interceptions – by continuing the two rapporteurs – it is not so much the result of political will than a technical incapacity. This might have been the case during the French Third Republic, a period during which the significant increase in the volume of communications made it more complex to carry out interceptions.

A few years before the publication of this French report, American judges had also deemed the interception of electronic communications to have only relative utility in terms of national security. Most importantly, they considered that the element justice needs can be obtained by means other than electronic surveillance [CON 67]:

> The Task Force believes that the Congress must act – and act quickly – to preserve the privacy of all Americans. New and sophisticated electronic bugging devices are used today with few restrictions and little restraint. The Federal statutory law is silent on electronic bugging. All who have examined the existing law on wiretapping agree that it is inadequate, confused and often self-defeating. The Federal wiretapping statute – enacted in 1934 – neither protects privacy nor promotes effective law enforcement. Privacy, appropriately described by Justice Brandeis as "the most comprehensive of the rights and the right most valued by civilized men", is nothing less than the foundation of freedom. […] The Attorney General […] on March 16, 1967 […] declared […] that "the legitimate needs of law enforcement can be met without the use of such abhorrent devices (i.e. electronic surveillance devices)" and concluded:

> All of my experience indicated that (electronic surveillance) is not necessary for the public safety, it is not a desirable or effective police investigative technique, and that it should only be used in the national security field, where there is a direct threat to the welfare of the country.

However, the actors in the field of security have a different opinion on the matter: "The great majority of law enforcement officials believe that the evidence necessary to bring criminal sanctions to bear consistently on the higher echelons of organized crime will not be obtained without the aid of electronic surveillance techniques. They maintain these techniques are indispensable […]" [COR 67].

Today, the usefulness of interceptions is hardly questioned by those who practice them. For security stakeholders, interceptions are not only useful, but essential, in order to fight against crime on equal terms This pursuit elicits an ever-increasing intensive use of telecommunication means:

> Electronic intercepts are essential in helping law enforcement battle against criminal elements. Criminal entities, including drug trafficking organizations (DTO's), criminal street gangs, and dangerous individuals, frequently rely on telecommunications to advance their criminal enterprises (California Department of Justice)[36].

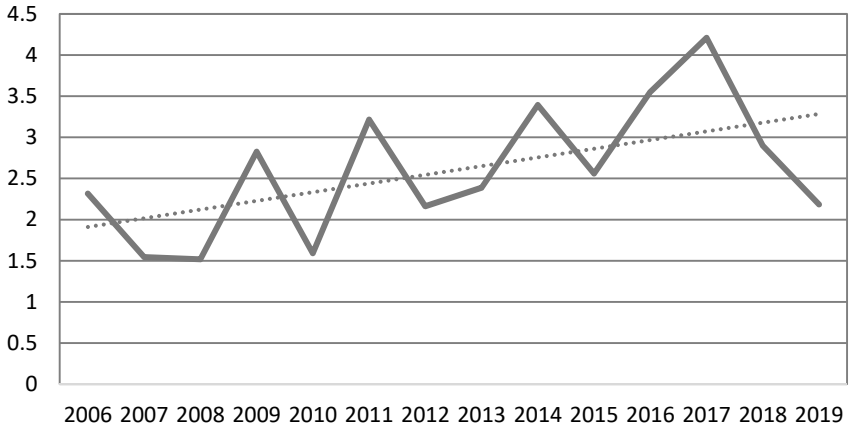

Figure 1.2. *Average number of people arrested due to interception practices in Hong Kong, between 2006 and 2019*

36 California Department of Justice, Office of the Attorney General, California Electronic Interceptions Report, Annual Report to the Legislature 2018, California [Online]. Available at: www.oag.ca.gov/sites/all/files/agweb/pdfs/publications/annual-rept-legislature-2018.pdf.

The effectiveness or usefulness of interceptions can be appreciated by means of a few figures.

For mass interceptions practiced by intelligence agencies, the side effects are important: “90 percent of messages intercepted by the NSA were not foreign targets but ordinary users, like you and me, from the United States and abroad” [KHA 14].

Let us recall that these amounts of data are not systematically subject to anonymization or secure storage and access, nor methodical erasure [GEL 14].

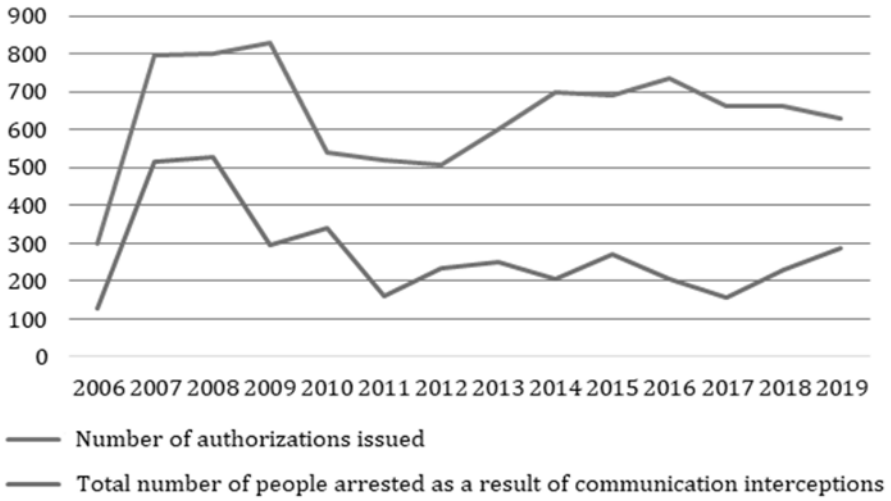

Figure 1.3. *Number of interception authorizations issued, and total number of people arrested as a result of interceptions (annual data) in Hong Kong, between 2006 and 2019. For a color version of this figure, see www.iste.co.uk/ventre/electronic.zip*

In the battle against crime, the effectiveness or usefulness of interceptions is generally assessed in terms of the number of arrests directly or indirectly resulting from them:

> Interception has not always proved an effective means of detection or deterrence. The interception of letters did not greatly reduce the traffic in lottery tickets, and this was one reason for the abandonment of this use of interception in 1953. But, with regard to the present day uses of interception, we received conclusive evidence of their effectiveness.

> We were told of many major wrong-doers who had been brought to justice, and of the frustration of espionage. We give here only a few examples of results directly achieved by methods of interception […] Between 1953 and 1956 the number of arrests made by the Metropolitan Police of important and dangerous criminals as the result of direct interception was 57 per cent of the number of telephone lines tapped. The effectiveness of interception by the Police has been getting steadily greater, especially in the last few years. So far in 1957 every interception but one has led to an arrest[37].

The annual reports from the supervising authorities in matters of intelligence have published quantified data on this.

In Hong Kong, the average number of arrests resulting from interception practices fluctuated between 1.5 and 4, over the period of 2006–2019[38].

The number of people arrested was proportional to the number of interceptions made. In the case of Hong Kong, the curves move at the same rate. Although these figures may seem low, in no way do they diminish the importance given by the law enforcement authorities to interception practices:

> It is and continues to be the common view of the LEAs that interception is a very effective and valuable investigation tool in the prevention and detection of serious crime and the protection of public security […] The intelligence gathered from interception very often leads to a fruitful and successful conclusion of an investigation. During the report period, a total of 120 persons, who were subjects of prescribed authorizations, were arrested as a result of or further to interception operations. In addition, 169 non-subjects were also arrested consequent upon the interception operations[39].

37 Report of the Committee of Privy Councilors appointed to inquire into the interception of communications, presented to Parliament by the Prime Minister by Command of Her Majesty, October 1957, London [Online]. Available at: https://www.fipr.org/rip/Birkett.htm.

38 Annual Reports to the Chief Executive by the Commissioner on Interception of Communications and Surveillance [Online]. Available at: https://www.sciocs.gov.hk/en/reports.htm.

39 Office of the Commissioner on Interception of Communications and Surveillance, Annual Report for 2019, June 29, 2020, Hong Kong [Online]. Available at: www.sciocs.gov.hk/en/pdf/Annual_Report_2019.pdf.

In the United States, the statistics from the *Wiretap Report* also show that the number of arrests is globally increasing at the same rate as interceptions[40].

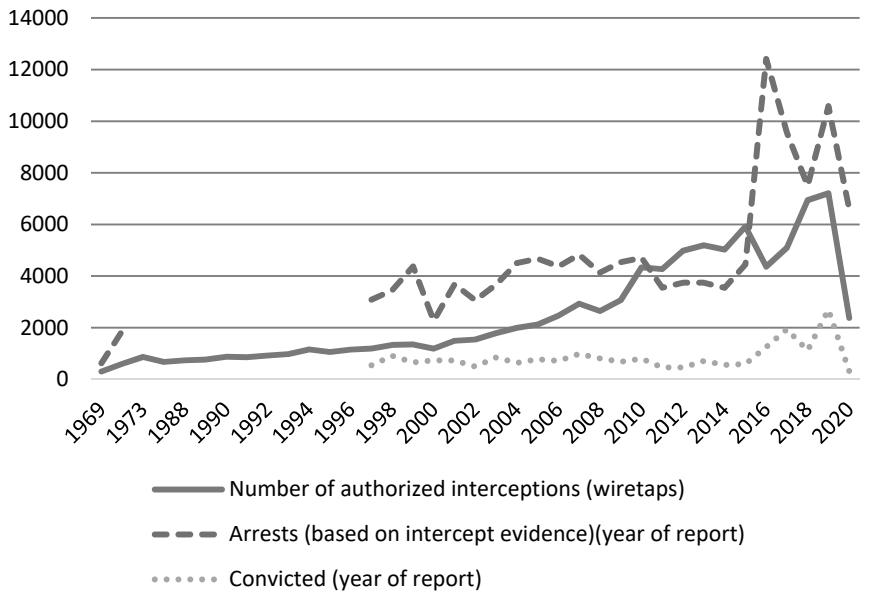

Figure 1.4. *Statistics produced from the American Wiretap Report[41] annual data. For a color version of this figure, see www.iste.co.uk/ventre/electronic.zip*

Here again, the average number of arrests made on the basis of interception fluctuates between one and three.

American reports also provide information on the barrier encryption represents in the context of interceptions: the number of interceptions involving encrypted communications and the number of communications which were successfully decrypted (or not).

40 This data set only takes into account national interception requests. The FISA (Foreign Intelligence Surveillance Act) requests from 1978 are not included in these data.

41 Wiretap Report, Administrative Office of the United States Courts [Online]. Available at: www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

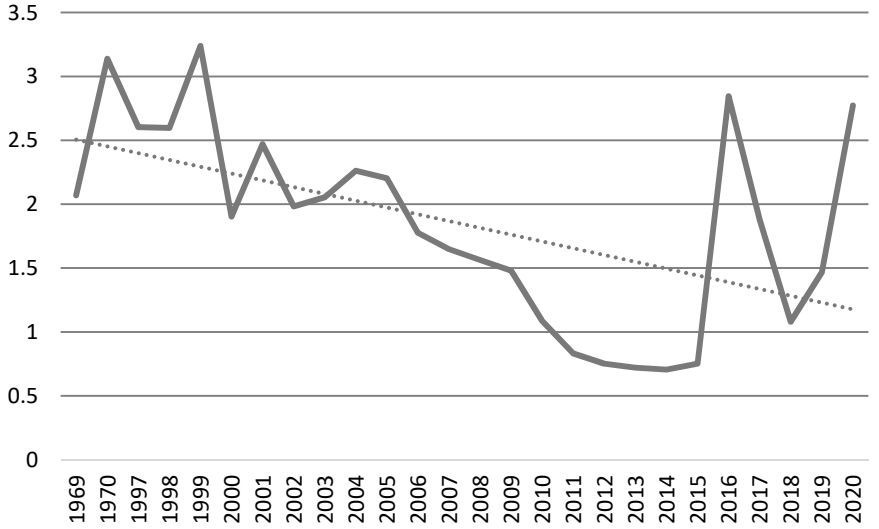

Figure 1.5. *Average number of arrests made based on interceptions, in the United States (Wiretap Report)*

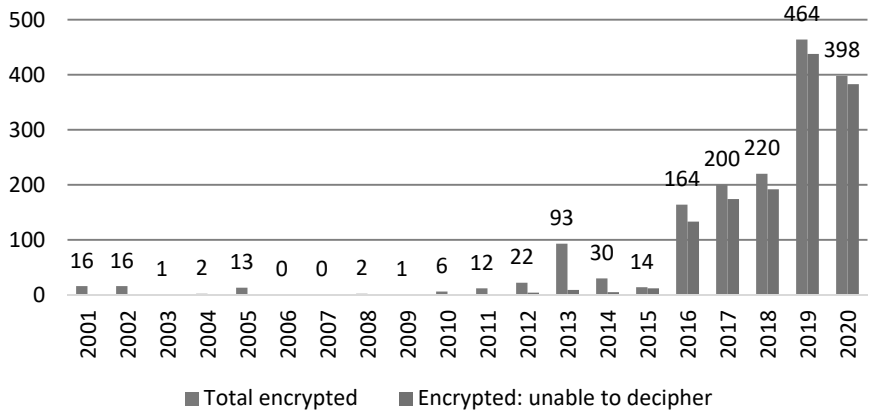

Figure 1.6. *Number of interceptions where the communications requiring processing were encrypted, and number of communications which could not be decrypted (United States, Wiretap Report). For a color version of this figure, see www.iste.co.uk/ventre/electronic.zip*

According to a study published on the Mercatus Center website (George Mason University), over the period of 2001–2014, only 147 interception operations (*wiretap*) were hindered by encryption techniques (i.e. 0.45% over a total of 32,392)[42]: 132 could be decrypted and only 15 remained inaccessible (0.046% of a total of 32,392, about 10% of 147). Those data are based on figures published in the *Wiretap annual report – United States Courts*. For the said period, we can deduce that: "The charts show that, contrary to popular assumption, encryption technologies have only complicated a minuscule percentage of reported wiretap investigations in recent years" [OSU 16].

But by reconsidering these statistics and extending them to 2020, we observe a significant change in the trend.

In 2001, 16 interceptions out of 1,491 concerned encrypted communications. In 2019, this represented 464 out of 7,210 interceptions. The proportion is quite low: 1% in 2001 and 6% in 2019. On the other hand, encryption has been increasingly resistant since in 2019, in 94% of cases, the authorities were unable to decipher communications.

> The 2012 annual report was the first to mention decryption impossibilities (even if this still represented only about four impossibility situations out of 22). The share of interceptions hindered by encryption continued growing, reaching almost 100%. Despite this trend, the number of interceptions hindered by encryption was still limited compared to the total number of interceptions carried out (398 encrypted, out of a total of 2,377 in 2020; or 464 encrypted out of a total of 7,210 in 2019). In the 2020 report on "wiretaps" the American justice system mentions a few hundred encrypted[43] messages: "The number of state wiretaps reported in which encryption was encountered decreased from 343 in 2019 to 184 in 2020. In 183 of these wiretaps, officials were unable to decipher the plain text of the messages. A total of 214 federal wiretaps were reported as being encrypted in 2020, of which 200 could not be decrypted".

42 Data compiled from the annual reports, published on the site https://www.mercatus. org/publications/technology-and-innovation/going-dark-federal-wiretap-data-show-scant-encryption.

43 Drawn from: "Public Law 106-197 amended 18 U.S.C. section 2519(2) (b) in 2001 to require that reporting should reflect the number of wiretap applications granted in which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of the communications intercepted pursuant to the court orders". Wiretap Report (2010), United States.

Encryption was encountered more frequently, but its proportion remained relatively low compared to all the interceptions made. This first observation seems to contradict the main argument of the "Going Dark" debate. In relation to these figures, it does not appear that the actions of investigators are globally paralyzed due to a generalization of encryption. Furthermore, in a significant number of cases, it is clearly indicated that investigators were able to access the desired information despite encryption. The use of encrypted communications is therefore not as frequent as it has been generally asserted.