Acta Polytechnica **64**(3):246–259, 2024
https://doi.org/10.14311/AP.2024.64.0246

Published by the Czech Technical University in Prague

CZECHOSLOVAK AND POLISH INTELLIGENCE (CRYPTOLOGIC) SERVICES AT THE TIME OF THE INSTITUTIONALISATION OF BOTH STATES AND THEIR ARMIES AFTER 1918

Daniel Kyselka*, Marcela Efmertová

Czech Technical University in Prague, Faculty of Electrical Engineering, Historical Laboratory of (Electro)Technology, Technická 2, 166 27 Prague, Czech Republic

* corresponding author: kyselda2@fel.cvut.cz

Abstract. In the course of historical development, the intelligence or cryptologic departments of individual states, usually associated with military structures, have influenced the outcomes of (military) conflicts (especially during the 19th century, World War I and II, and the Cold War), as well as political events. For this reason, it is important to examine not only their political and historical impact, but also the technologies (codes and ciphers, production of cipher machines etc.) used in their operations. To find out the form and extent of the education of intelligence (cryptologic) personnel, which takes place at different types of higher (technical, military) schools in theoretical and practical fields, and their results applied in the activities of most of the state-controlled power apparatuses (foreign, interior, army-defense, National Security Bureau etc.), as well as in the communication (secure) channels of the state.

Later, especially in the 1990s in Europe, these practices have been used outside the state apparatus in the commercial sphere. There was a demand for encryption devices and for programs for data protection (ensuring computer security, e.g. in banks, mobile operators, in the ICT industry, in the fight against international terrorism and organised crime, in ensuring the protection of individual rights, etc.), and for activities in applied cryptology. In the last five years, several cryptology conferences have been held each year to exchange knowledge in the field and to characterise and understand the constant struggle between the creators and the crackers of ciphers, as this connection has in the past led to many scientific discoveries applicable to the everyday life of individual societies. The paper focuses on the analysis of the creation and organisation of intelligence services within the Czechoslovak and Polish armies after 1918.

Keywords: History of science and technology, Czechoslovakia, Poland, 1918–1938, intelligence (cryptologic) service, French military mission, army of Czechoslovakia, army of Poland, World War I, Versailles system.

1. Research background to the constitution of intelligence services

A number of key issues can be identified. In this determination, how can we characterise the position of the newly independent Central European countries after 1918, especially Czechoslovakia and Poland, in tracing the development of their armies and intelligence services? What was the organisation of these new armies and their tasks, and how did these relate to diplomatic developments in central Europe after the Versailles negotiations? How did the intelligence (cryptologic) network take shape in the two selected countries, Czechoslovakia and Poland, after 1918? Can we characterise the ideological patterns in the Czechoslovak and Polish intelligence (cryptology) services and examine what, if any, were the differences in approach to the tasks? How was the cracking of ciphers (e.g. the complicated Enigma) approached? What, if any, was the link between the man and cipher machine? The characterisation may be aided by the recent emergence of cybernetics and computer science in various systems, and by the current ability of artificial intelligence to communicate its feelings or write poetry, for example. The 1997 chess match between Garry Kasparov and a computer called Deep Blue (IBM) may be an example of this human-machine bond. The match ended with the machine – Deep Blue – winning 2-1 against the then world chess champion [1]. At the time, it was a sensational result for the use of computers in direct human-machine interaction. Today, chess programs are much more powerful than the best players. However, these phenomena had to be achieved technically, organisationally and opinionally (by programming the machines, coding them, etc.). Therefore, by analogy, I am interested in what were the concrete results of the work of the intelligence services in the previous period – between the wars – which is also related to the topic of my dissertation.

The starting point for my work was mainly the available archival material of the *Military Historical Institute – Military Historical* ***Archive*** (VHÚ-

VHA), which I used to characterise the emerging army structure, the work of the French military mission in Czechoslovakia and the development of the Czechoslovak military intelligence, as well as the necessary biographical information, especially in relation to the person of Josef Růžek. In particular, I studied the archive of the Ministry of National Defence (MNO) – archival material relating to the Main Staff and the 2nd Intelligence Department for the period 1919–1939.[1] Of the Polish archival sources, I have mainly used the Polish Ministry of Defence's internet resources. For further research, the *Archives of the Security Forces and the National Archives or the Archives of the Ministry of Foreign Affairs* can also be used.

Furthermore, I worked with historical literature from many points of view i.e. historical-political works for the Czechoslovak and Polish environment after 1918 (VHA, e.g. [2–6]), texts on education and science (VHA, e.g. [7–11]), the development of the Czechoslovak and Polish military structures and their intelligence services (VHA, e.g. [12–17]) after 1918, biographies of important **officers** (VHA, e.g. [12–17]) and technical describing encryption machines, especially Enigma, the preparation of codes, the production of these encryption machines, etc. (VHA, e.g. [18–20]). I also used internet sources to document, for example, the work of cryptographers and the characteristics of their code-breaking, information transmission, etc., as well as some diploma theses (especially VHA, e.g. [21]), which focused, for example, on the links between the Czechoslovak and Polish military environment or described the diplomatic ties between the two countries. A selection of literature on the topic of the seminar paper is listed in the inventory at the end of the article.

2. Comparison of the political and diplomatic possibilities of Czechoslovakia and Poland for the establishment of independent armies and their intelligence networks after World War I

From a historical point of view, it is possible to consider that the First World War was a war of chemists due to the use of chlorine and mustard gas, the Second World War in relation to the use of the atomic bomb could be called a war of physicists, and the current military clashes could be called wars of mathematicians due to their control of one of the most important weapons – information (informatics) [22].

[1]Here I have read mainly the Guidelines for Cryptology Courses and the book materials, which were prepared by J. Růžek. Furthermore, the archival materials provide an overview of the individual military schools, the French Military Mission (1919–1939) and the Education and Training Department.

Poland and Czechoslovakia were two Central European states founded after the end of World War I under the Versailles system, but their historical origins and development were different. If we start from the 19th century, then at the end of the first decade of the 20th century, Poland was a rather agrarian country with an underdeveloped industry. Czechoslovakia (Czech and Austrian countries), on the other hand, formed the industrial base of the former Austro-Hungarian monarchy and was described as an agrarian-industrial state[2] at the beginning of its independent development.

Both Polish and Czechoslovak (Czech and Slovak) nations were influenced by the form of long-lasting foreign domination and different previous political, economic, and, to some extent, cultural development. The Tsar's brutal occupation of Poland[3] forced active resistance and affected the character of the people. In the period before the First World War, independent Poland did not exist. The territory of the former Polish state was divided between three European powers. These were Germany, Russia and Austria-Hungary. In the territories controlled by the German Empire, the Polish population was Germanised. This process began already in the general schools. The city of Poznań was a place where Germanisation reached a considerable intensity. The German state also economically favoured the German-speaking population at the expense of the Polish population. The territories where the Polish-speaking population lived under Russian rule faced severe Russification after 1905. This process was provoked by the defeat of the Russian fleet at the Battle of Tsushima. The debacle of the Russian naval forces caused a rise in nationalism and national resentment within the Russian Empire. One of the victims of this resentment was the Polish-speaking population.

The territories where the Polish-speaking population lived under Russian rule faced severe Russification after 1905. This process was provoked by the defeat of the Russian fleet at the Battle of Tsushima. The debacle of the Russian naval forces caused a rise in nationalism and national resentment within the Russian Empire. One of the victims of this resentment was the Polish-speaking population [23, p. 242–244].

[2]The extensive three-part historical work by Zdeněk Kárník [2].

[3]The Great Powers took advantage of the protracted crisis of Poland and carried out the partition of Poland, which was manifested in the period 1771–1795, confirmed by the Congress of Vienna in 1815, when the partition was of the following character: Austria occupied Halych, Prussia got West Prussia and Poznan, and the remaining part of the original Poland (80 % of the territory and 60 % of the population) fell into Russian hands. In 1867, the Emperor granted a degree of cultural and linguistic autonomy to the whole of Galicia, making Austria-Hungary an attractive model for all Poles (especially those under Russian rule). In 1916, an independent Polish state – a hereditary monarchy – was to be established on the original Polish territories controlled by Russia.

The Habsburg order, which, especially in the last third of the 19th century, was not so invasive, led to a rather cultural Bohemian upsurge and to the solution of problems in an intellectual way, for which the mainly Bohemian society of the previous period was already prepared. Masaryk was a broadly diplomatic negotiator, whereas Piłsudski, with the experience of the defeated Polish uprising of January 1863 against the Russian occupiers, solved problems militarily. **Interwar** Czechoslovakia was able to build on its legions that had crossed the whole of Russia, rather than on legionary generals who did not make it into high politics, although they were highly regarded by the state. The Czechoslovak legions did not interfere much in their patronage during the border protection period just after 1918, unlike the Polish legions, which had an elite status in their country. Already in the first half of 1919, the transfer of legionnaires from the French and Italian fronts to the newly established Czechoslovak state was completed. These units were particularly useful because their members were familiar with the Western way of conducting the war. French and Italian legionnaires took part in battles against the Polish and Hungarian armies [24, p. 156] to protect the Czechoslovak territory, later confirmed by the Versailles system in the 1920s.

Masaryk and Piłsudski were equally aware of the dangers of Bolshevism. Yet Masaryk had a special relationship with Poland without the offer of mutual military assistance and even without the two politicians knowing each other personally. Nor was there a linking of joint action in this matter in the case of the advancing Kun Nationalists of the Hungarian Radical Republic into foreign territory. If the Bolshevik forces, Soviet and Hungarian, had then joined forces, Central Europe would have been threatened just after the First World War. Equally, the interest in protecting their own territories, resulting from the Versailles negotiations [25], [26, p. 40], [27, pp. 3–5], [28, p. 352]. Edvard Beneš, who attended the Versailles Peace Conference, called on leading Czech politicians to try to occupy the territories that had previously been part of the Czech lands. Alternatively, those territories, which were important for the development of the Czechoslovak state and which the strength of the Czechoslovak army was sufficient to conquer, should also be conquered. It was the territory of Těšín that was important to Czechoslovakia for both political and economic reasons. As a result, the Czechoslovak army was preparing for an invasion of Těšín. This invasion was successful [29, p. 47]. In the autumn of 1919, Edvard Beneš returned to Czechoslovakia. However, disputes over the border between Czechoslovakia and Poland continued to persist. The whole problem came under the jurisdiction of the Conference of Ambassadors at the Versailles Conference. The Conference of Ambassadors decided in favour of Czechoslovakia by assigning the town of Karviná and its surroundings to the Czechoslovak state. However, this decision outraged the Polish government and damaged relations between Poland and Czechoslovakia for the entire interwar period [30, p. 111].

Both leading politicians wished to build a strong state, protected by the treaty system they sought. Masaryk oriented his political representation towards a republican, in those days after the Versailles negotiations, strong France with a parliamentary system. Piłsudski did not hide the strong-arm government, did not have good ties with the Chamber of Deputies (the constitution limited his powers) and did not run for president. Both Poland and Czechoslovakia became parliamentary republics.

The two states were also initially different in their reception in Europe. Czechoslovakia had a ready-made policy, government, and gained international recognition, while Poland, however, had no clearly established borders, no government (Piłsudski was chief until 1922, and de facto ruler of the country from 1926 after the fighting), no constitution, instability and corruption within, and lacked international recognition. On 22 November 1922, Jozef Pilsudski became the representative of the executive power in the state. Pilsudski held the temporary position of the leader of the Polish state (nation). In Polish, this title was called Tymczasowy Naczelnik Panstwa. Thanks to this title, Jozef Pilsudski could appoint the Prime Minister and ministers. Pilsudski's executive powers were also extensive. Several factors contributed to this development of Pilsudski's power and influence. The first was the fact that Poland did not yet have a constitution in force that limited the power of politicians (including Pilsudski). The second was the poor material conditions of the Polish economy. The third was the threat to Poland from abroad, particularly from Russia. Pilsudski was also favoured due to his popularity with the Polish people [31, p. 428].

Both states, however, sought political and military protection and support for their interestsfrom France,[4] the representative of the Versailles system and of a certain invincibility on which the new Europe had counted, but in which it later miscalculated. **Still, with generals like** Ferdinad Jean Marie Foch (1851–1929), Henri Philippe Benoni Omer Joseph Pétain (1856–1951), Joseph Jacques Césaire Joffre (1852–1931, commander-in-chief of the French army from 1911), Maurice César Joseph Pellé (1863–1924, first chief of the French military mission in Czechoslovakia), Eugène Desiré Antoine Mittelhausser (1873–1949), Louis-Eugène Faucher (1874–1964), etc [6, p. 52], [34, pp. 35–39], [35, p. 96], [36, p. 14]. it was possible to train and build separate armies, both Czechoslovak and Polish. Moreover, France was interested in both countries, seeing them as a kind of barrier in relation to Germany and as a possible "second" front in a possible conflict [37].

[4] Based on the work of [32], especially [33].

Both Poland and Czechoslovakia had to defend national unity and deal with national issues immediately after their creation. The Czechoslovaks in relation to Germany and the German minority in the borderlands, Poland sought an agreement with the Belarusians and Ukrainians, who, however, did not specifically seek Polish domination, and tried to limit the influence of the German minority.[5] Yet both Czechs and Poles were later expelled from the Czech borderlands and Polish Pomerania.[6]

3. Development of the Czechoslovak Army and the French Military Mission in Prague

The French military mission (led by Generals Foch, Pellé, Mittelhauser, Faucher) had a fundamental role in founding the Czechoslovak army. All of the generals mentioned had the highest possible military and technical education, in particular, they presented themselves as graduates of the so-called Grande École – École polytechnique (established in 1794) and many had previously studied at other military cadets or universities.[7]

The period between 1919–1920 was the most important stage of the mission's activities in Czechoslovakia. With the merger of the Mission with the departments of the Ministry of National Defence, the General Staff began its work from July 1919 at the latest. General Pellé had an extraordinary personal involvement in the final form of the draft conscription law adopted by the government in March 1920. This basic military law established the proper basis for the existence of the army. Pellé minimised the negative influences of the time (e.g. anti-militarism). The choice of a suitable conscription system was significantly influenced by the integration of the new state into the international coalition system.

Czechoslovakia was as an ally of France and an important member of its alliance system from the very beginning. After World War I, it was shaped by the states of central and south-eastern Europe. In French strategic thinking, they have to some extent replaced Russia, France's former powerful eastern ally. Czechoslovakia's exceptional strategic position could be used effectively in the coalition, provided that the new republic was also of military value. The Czechoslovak army was being built from scratch. It intended to draw on the experience of the former Austro-Hungarian army only to a very limited extent. It therefore had to look to the Allies for a suitable model.

The French military mission[8] had a direct influence on the command of the Czechoslovak army until the end of 1925, as its chiefs were also the chiefs of the Czechoslovak Main Staff. By 1938, the mission had been headed by three chiefs. General Pellé [41] was succeeded by General Mittelhausser. In 1924, he created the post of Vice-Chief of the Main Staff, in which General Jan Syrový of the Czechoslovak Army prepared for the post of Chief of the Main Staff under his direction. He assumed the Chief of the Main Staff in early 1926, when General Mittelhausser also left his post as Chief of the French Military Mission. At the same time, the nature of this mission changed. The commanding body became an advisory body to the Minister of National Defence. After General Mittelhausser, the mission was headed by General Faucher [34, p. 132] until the end of its operation in Czechoslovakia, i.e. until 1938. The mission was quite large, initially having up to 150 expert soldiers.[9]

Thanks to their personal ties to the Czechoslovak environment (General Pellé was the husband of Jara Braunerová, a cousin of the painter Zdeňka Braunerová), the generals also influenced the development of Czechoslovak education, The founding of the Institut français de Prague (1920, founded by the Slavist Ernest Denis), the establishment of lyceums in France for Czechoslovak students (in Dijon, Nîmes,

[5] Poles made up 69 % of the population in Poland, with significant numbers of Ukrainians (14 %), Jews (8 %) and Germans (4 %), etc. The national composition of Czechoslovakia according to the 1921 census was as follows: 64.37 % Czechoslovaks (of whom 16 % were Slovaks), 22.95 % Germans 5.47 % Hungarians, 3.39 % Ruthenians 1.33 % Jews, 0.56 % Poles, 0.17 % others, 1.75 % foreigners.

[6] Józef Piłsudski aspired to create a federation of Central and Eastern European states, the so-called Intermarium (Międzymorze, Intermarrum), which would have meant the interconnection of states in the area between the Adriatic, Baltic and Black Seas, i.e. treaties between the states of Poland, Lithuania, Latvia, Estonia, Belarus, Ukraine, Czechoslovakia, Hungary, Romania, Yugoslavia. This strategy was based on historical experience, and was intended to emulate the Republic of the Two Nations, spanning the Baltic and Black Seas from the late 16th century to the late 18th century. With these territories, the federation would be in a better position to resist domination by Germany or Russia. Within the proposed grouping, Piłsudski insisted on a leading role for Poland; the plan was opposed in particular by the Lithuanians and Ukrainians, who saw it as a threat to their independence. Therefore, Piłsudski signed ten-year non-aggression treaties with the USSR on 25 January 1932 and with Germany on 26 January 1934. In fact, Piłsudski died a year later (12 May 1935). The fourth partition of Poland began on 1 September 1939 with the start of World War II. Processed mainly according to [3, 38].

[7] These schools included the École militaire spéciale (Pétain), the École d'application de l'artillerie et du génie (Pellé), the École spéciale militaire de Saint Cyr (Mittelhausser), and Faucher taught at the École de l'artillerie in Mety in 1901–1905 and then at the École Militaire in Paris. See e.g. [39].

[8] See e.g. [40].

[9] The mission included senior and junior officers, a staff administrative officer, radio station commander, code officer, translator officer, five operations officers, five transportation officers, an automobile officer, two artillery adjutants and one senior officer, two engineer officers and a telegraph officer, two medical officers, two subintendents, two administrative officers, and two aviation officers. The above-mentioned organisational structure did not only serve the mission itself; the individual units included all the basic functions of the General Staff and the military management units of the Ministry of National Defence, making the organisation of the French military mission the prototype of the future top bodies of the Czechoslovak military organisation. See [42, p. 58], [43].

Sait-Germain near Paris), and Slavic studies (1920) at the Sorbonne in Paris [44, p. 238], [45, p. 174]. All this also contributed to the good education of Czechoslovak military leaders and ordinary soldiers, as military education had been a tradition in the Czech lands since the establishment of the Stavovská inženýrská (military) school in Prague in 1705/1707/1717 [46], [11, p. 233 and other reference bibliographic information listed here]. The structure of the Czechoslovak army in 1920 consisted of main units (infantry, artillery, cavalry, and air force) and auxiliary units (engineer, telegraph, railway, automobile, and carriage troops).[10]

Within this composition of the Czechoslovak army, it was necessary to train officers and prepare the educational structure for lower military cadres and ordinary soldiers. This activity was coordinated by Maurice Pellé. The aim was to meet the immediate need for staff officers for the new Home Army formations. Junior officers of the Home Army or the Legions who had held an officer rank for at least eighteen months, including six months of war service in the field, and who could speak French could apply. Completion of this course paved the way to a future War College. Later, the conditions for admission to the course were extended and two committees were set up: an Evaluation Committee, which was responsible for selecting candidates for the entrance examinations, and an Examination Committee, which conducted the examinations themselves. The first War School was established in Czechoslovakia in 1921, initially, it was a two-year course, from 1924 it was a three-year course. A 1926 law granted the War School university status (the Higher War School in Prague). The model for this school was the War College in Paris (École Militaire). During the years of the First Republic, 577 officers[11] graduated from the Prague War College.

Military education[12] then had to be built from scratch, as the schools of the Austro-Hungarian army, stationed until then on the territory of the newly formed Czechoslovakia, gradually disappeared. For a short time, until 8 February 1919, only the military higher school in Hranice was functioned. The beginnings of the formation of the military education system were characterised by its liveliness and fragmentation into a series of courses and short-term schools, which were set up to meet immediate needs. Czechoslovakia made use of the experience of officers and soldiers from the legions to build up the army and its education system. These units were essentially part of the Czechoslovak foreign army in the early 1920s and were originally integrated into the allied armies in whose countries they were formed, and their specialised training and education for command staff took place there. It was the schools in Zhitomir, Irkutsk, Tomsk, Barlet, and especially the French schools [47] that provided the best education. Military education was under the jurisdiction of the Commander-in-Chief and for a long time, was governed only by the regulations of the MNO.

It was only by order of the President of the Republic in 1934 [48] that a major modification took place. This order distinguished military schools, which provided comprehensive education for service, from military courses, which served to supplement and deepen the basic education acquired in military schools and practical service. He divided military schools into higher, secondary, and lower and distinguished between types of military courses. He reserved the establishment of higher and secondary military schools to the President of the Republic. Other schools and courses were established by the Minister of National Defence. As a result of the new regulations, the names of military schools were clarified. A number of existing schools were renamed to reflect the nature of their courses. As a rule, secondary and junior schools and courses were set up in or outside the classrooms of military bodies, but also in colleges and universities. Military higher education was represented by two schools. The first was the War College in Prague (VŠV), as I mentioned above, designed for the education of general staff officers. It was formed from the courses for the education of general staff officers (General Staff School), which started on 15 September 1919. The name of the War College took effect on 1 October 1934 [48]. The College of Intendancy (VIŠ), which had its origins in the School for the Education of Officers of the Supply Corps and was founded on 1 January 1920, prepared officers for the intendancy service. In 1922, the name was changed to the Intendancy School and on 1 October 1934 it was given the definitive name mentioned above. A number of schools (courses) for the education of officers of the economic and administrative services, both professional and reserve, operated at the VIŠ.

From October 1924 onwards, officers-engineers were trained for weapons and technical services at the Military Engineering College in Prague. However, this school was closed on 1 April 1934. The Military Academy in Hranice became the higher military school, which trained professional officers of arms. It started its activity on 15 January 1920, first as the Officers' School and from 10 February 1920 as the Military Academy. Other secondary military education included schools for officers of arms and reserve services, established in the training schools of the various types of arms. The State Military Reform Real Gymnasium in Moravská Třebová, operating from 1 October 1935, was a selective secondary school which, in addition to the general education required for study at civilian universities, was intended to provide pupils with a course of military education before entering the schools for reserve officers. In October 1938, this high school was moved to Hranice.

Among the lower military schools were schools for weapons and service sergeants by profession. These

[10] Adapted from [21, p. 23].

[11] This paragraph was prepared by [21, pp. 24–25].

[12] The overview characteristics of military schools and apprenticeships are based on aggregated information from [47].

were the Air Cadet School, the Air Defence School and, from 1927, the Military Medical School, which was converted into a course for the education of professional medical officers in 1934. From the courses for training physical education instructors, the Military Gymnasium School was created, the purpose of which was to train officers and staff sergeants to become teachers of gymnastics and fencing. From 1 October 1923, the Military Music School operated independently in Prague. The military apprenticeships were established mostly in 1922, always separately for each weapon. Various schools and courses operated within them, often based in Milovice. These were training schools with specific names from 1928 onwards, namely the Infantry Training School, the Artillery Training School, the Air Force Training School, the Cavalry Training School, the Charioteer Training School, the Engineer Training School, the Telegraph Training School, and the Automobile Training School. The Central Telegraph School was established in Kutná Hora, and in 1922 it became a military telegraph school, later located in Turnov. The chemical apprenticeship was established on 1 August 1937 in Olomouc.

4. The development of the Polish army and the influence of France on it

In today's Poland, for the first time since the 18th century, the generation that was born in a free state has now come of age. For them, Poland's existence is not a brief interlude between other catastrophes, as it was for nearly 20 previous generations, but a certainty. However, Polish society had to come to terms with this reality, and the after 1918 period was the stepping stone [49].

During World War I, an autonomous Polish army was established in France, but Polish units were also created in Russia with the support of the Provisional Government there and in Austria-Hungary. The most prominent Polish fighting group was a paramilitary organisation – the Strzelcy – under the leadership of Józef Piłsudski from 30 July 1914. In August 1914, the Austro-Hungarian High Command agreed to the creation of the so-called Polish Legion in western and eastern Galicia, with Polish-speaking troops once again under the command of Piłsudski. Later, the 1st Regiment of Polish Riflemen was formed and in November 1914 the Polish Riflemen Brigade was created. At the same time, the 2nd Polish Riflemen Brigade was formed from the Poles of East Galicia. In 1915, the 3rd Brigade was added. All three brigades were deployed to stop the Russian Brusilov offensive and in August 1916 they were merged into the Polish Auxiliary Corps (Polniches Hilfskorps). In 1917, Vienna and Berlin's attempt to restore the Polish kingdom failed, also due to the Russian February Revolution, and Piłsudski called on the legionaries to refuse to swear an oath to the Germans, as the Polish army must serve the independent Polish state. At that time, the Polish volunteer units were disbanded. Only the 2nd Brigade, which was loyal to Austria-Hungary until 1918, remained [50]. Another legionary group was formed in June 1917 in France, where the so-called Blue Army (named after the blue colour of the uniforms) was formed under the leadership of General Joseph Haller de Hallenburg (1873–1960) [51], who fought on the side of the Triple Entente. The Blue Army was made up of Poles who were in France or who had originally fought in the French army, Polish prisoners of war (about 35 000 men), Polish volunteers from the USA and Canada (22 000 men), and descendants of Polish immigrants from Brazil (300 men) [52].

According to the peace plan of T. W. Wilson, the US President, an independent Polish state was to be established after World War I, with territories inhabited by Polish population and with free and safe access to the sea. Piłsudski established a strong (and military) authority during World War I, with which he supported the creation of an independent Poland under the Versailles Treaties. Even after the establishment of an independent state in 1918, Poland was still unstable for a long time, having disputes with its neighbours over territory,[13] but developing as a sovereign state.

After the establishment of independent Poland in 1918, the building of the Polish army began under the strong influence of Chief of Staff Józef Klemens Piłsudski (1867–1935) [53], [54]. Soldiers and officers of the new state were trained in several foreign armies, namely in Germany, Russia, and France, while senior officers followed the traditions of the legions and riflemen and also had training from the Austro-Hungarian army. After the independence, the borders of the new state and their protection were an important issue, and therefore the Polish army had an important position in society.

5. A look at the development of the intelligence service of the Czechoslovak Army

The assistance of France in the organisation of the Czechoslovak army was advantageous, as it established a clear and functional organisation of the Czechoslovak armed forces. From 1922, the Czechoslovak Main Staff was divided into four parts. The first part dealt with the organisation of the army, the second (the

[13] Poland had border problems with Germany, Czechoslovakia (the Seven-Day War), had disputes with Lithuania and the Ukrainians, and the Poles fought the Russian Bolsheviks (the Red Army invaded the Baltic, Belarus, Ukraine and also reentered Polish territory). In 1920, Poland's existence was threatened when General Tukhachevsky, with 120 000 Russian soldiers, reached Warsaw. Piłsudski solved the problem by retreating his main forces, but the secondary units unexpectedly attacked the rear of the Russian army. The result was the crushing defeat of the Red Army, referred to as the Miracle on the Vistula. On 18 March, 1921, the Peace of Riga was signed with the Soviet power and the borders were established.

division was taken from the French Military Mission) with intelligence activities, and the third with executive and administrative activities. The fourth part was responsible for the possible mobilisation of the Czechoslovak population. The second department of the Main Staff focused on intelligence activities, which included the collection and analysis of intelligence information and the analysis of the international and domestic political and military situation. The Second Department also included a cryptologic section. It was responsible not only for cracking enemy ciphers (mainly from Germany and Hungary), but also for creating its own ciphers, as well as the duty of familiarising other parts of the Czechoslovak army with the use of ciphers [55]. The aim of the department's activities was to obtain information on military threats to the Republic, information of a military nature on armies that could threaten the Republic, to prevent the penetration of foreign intelligence services into the military structures of the Czechoslovak Republic, and the leakage of information of a strategic nature from the Republic. Information was obtained by the Second Department mostly from intelligence officers of divisions, provincial commands, and military attachés.

The Intelligence Service at the Czechoslovak Army Headquarters initially had only 20 employees. The first head of this department was Major General Čeněk Haužvic, former head of the intelligence department of the Austrian military government in Lublin. His deputy (and later the head of the search group) was a major of the Italian Legion, Mojmír Soukup. The head of the counter-intelligence department became Vladimír Vaněk in February 1920. Jan Ropek took charge of the cryptologic department. From 1928 onwards, this section was headed by Josef Růžek [13, p. 160 et seq]. In Figure 1 we can see the personal statement of Josef Růžek. The Personal statement allowed the military authorities to monitor the career of a given officer. On 27 May 1936, a joint Czechoslovak-Soviet intelligence headquarters was established in Prague against Germany. It was called VONAPO 20 (Vojennyj nabljudatělnyj post) and its chief was Staff Captain Karel Paleček. Intelligence was divided into four parts: search, study, cipher and military attachés [56, pp. 31–34]. The search party was responsible for gathering intelligence from its agents [57]. It was engaged in the search for important persons related to espionage and also found out information about these persons. This group also dealt with military espionage abroad. The study group was devoted to the analysis of information obtained by the Czechoslovak intelligence. It also worked on improving the rights of Czechoslovak intelligence officers. The cipher group created ciphers for the needs of the army and also tried to break the ciphers of the enemy. The cryptologic department was part of this group until May 1937, where new cryptologists were trained. After that year, the cryptologic department was moved to the second – study – group, which was headed by Officer Josef Růžek in 1928. The last group prepared and sent military attaches to Czechoslovak embassies abroad and was in charge of administrative and technical matters.

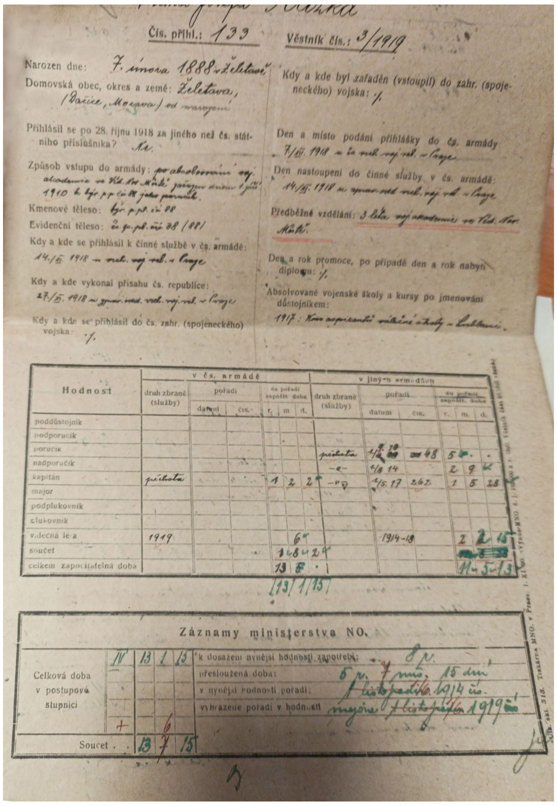
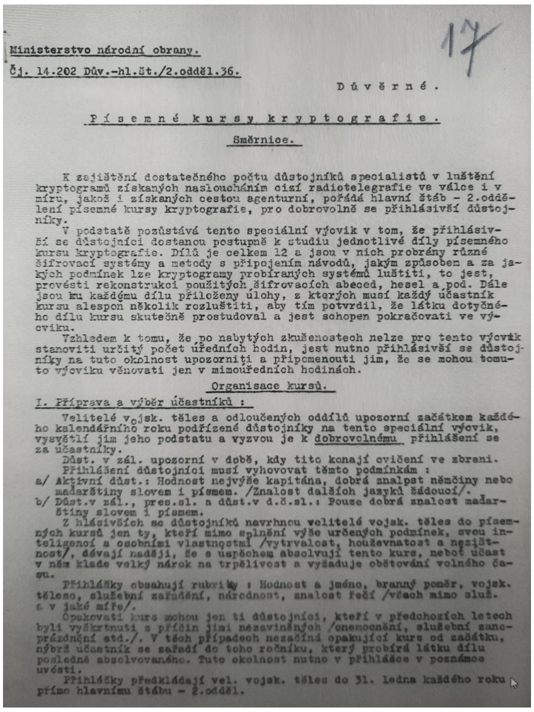


Figure 1. Personal statement of Josef Růžek [58].

Since the French army was at the birth of the institutional Czechoslovak army, the cryptologic service worked from its beginning under the influence of French cryptology and the French cryptologist assigned to Prague. This fact changed in 1937, when Czechoslovak cryptologists began to make more use of British methods and to cooperate with British intelligence (e.g. the departure of the spy Paul Thümmel, agent A-54, to England) [17, pp. 1–2] The cooperation between Paul Thümmel and Czechoslovak intelligence began on 8 February 1936. On that day, the Czechoslovak intelligence received a letter from an unknown author, in which he informed them that he would supply them with information available to the German Abwehr in return for financial payment. Czechoslovak intelligence decided to accept Thümmel's offer [59, pp. 7–9]. The arrest of Paul Thümmel took place on 22 March 1942 in Prague. Paul Thümmel had already become an agent of Czechoslovak intelligence before the Second World War. The Gestapo proved to Thümmel that he had received 40 000 marks from the Czechoslovak security authorities for his services. Paul Thümmel passed on to Czechoslovak intelligence not only the information that he had learned himself, but also information that he had received from his friends and colleagues in the German Abwehr [59, pp. 295–298]. Paul Thümmel himself eventually ended



Ministerstvo národní obrany.

Čj. 14.202 Dův.-hl.št./2.odděl.36.

Důvěrné.

Písemné kursy kryptografie.

Směrnice.

K zajištění dostatečného počtu důstojníků specialistů v luštění kryptogramů získaných nasloucháním cizí radiotelegrafie ve válce i v míru, jakož i získaných cestou agenturní, pořádá hlavní štáb - 2.oddělení písemné kursy kryptografie, pro dobrovolně se přihlásivší důstojníky.

V podstatě pozůstává tento speciální výcvik v tom, že přihlásivší se důstojníci dostanou postupně k studiu jednotlivé díly písemného kursu kryptografie. Dílů je celkem 12 a jsou v nich probrány různé šifrovací systémy a metody s připojením návodů, jakým způsobem a za jakých podmínek lze kryptogramy probíraných systémů luštiti, to jest, provésti rekonstrukci použitých šifrovacích abeced, hesel a pod. Dále jsou ku každému dílu přiloženy úlohy, z kterých musí každý účastník kursu alespoň několik rozluštiti, aby tím potvrdil, že látku dotyčného dílu kursu skutečně prostudoval a jest schopen pokračovati ve výcviku.

Vzhledem k tomu, že po nabytých zkušenostech nelze pro tento výcvik stanoviti určitý počet úředních hodin, jest nutno přihlásivší se důstojníky na tuto okolnost upozorniti a připomenouti jim, že se mohou tomuto výcviku věnovati jen v mimoúředních hodinách.

Organisace kursů.

I. Příprava a výběr účastníků :

Velitelé vojsk. těles a odloučených oddílů upozorní začátkem každého kalendářního roku podřízené důstojníky na tento speciální výcvik, vysvětlí jim jeho podstatu a vyzvou je k dobrovolnému přihlášení se za účastníky.

Důst. v zál. upozorní v době, kdy tito konají cvičení ve zbrani.

Přihlášení důstojníci musí vyhovovat těmto podmínkám :

a/ Aktivní důst.: Hodnost nejvýše kapitána, dobrá znalost němčiny nebo maďarštiny slovem i písmem. /Znalost dalších jazyků žádoucí/.

b/ Důst.v zál., pres.sl. a důst.v d.č.sl.: Pouze dobrá znalost maďarštiny slovem i písmem.

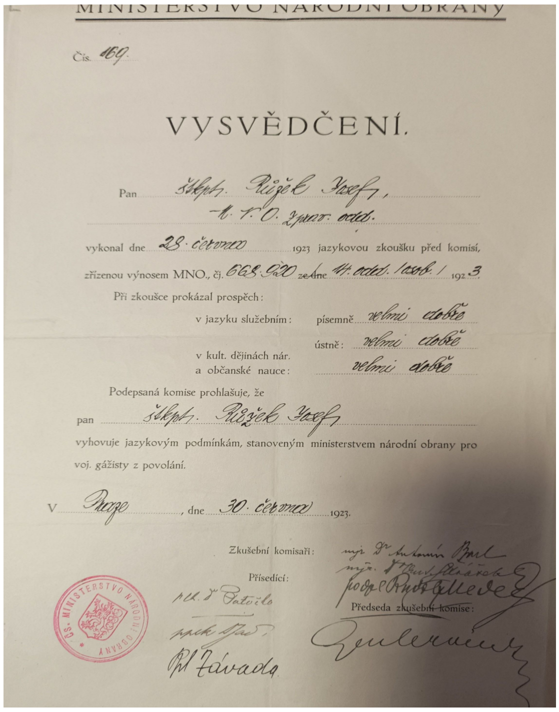
Z hlásivších se důstojníků navrhnou velitelé vojsk. těles do písemných kursů jen ty, kteří mimo splnění výše určených podmínek, svou inteligencí a osobními vlastnostmi /vytrvalost, houževnatost a nezištnost/, dávají naději, že s úspěchem absolvují tento kurs, neboť účast v něm klade velký nárok na trpělivost a vyžaduje obětování volného času.

Přihlášky obsahují rubriky : Hodnost a jméno, branný poměr, vojsk. těleso, služební zařadění, národnost, znalost řečí /všech mimo služ. a v jaké míře/.

Opakovati kurs mohou jen ti důstojníci, kteří v předchozích letech byli vyškrtnuti z příčin jimi nezaviněných /onemocnění, služební zaneprázdnění atd./. V těch případech nezačíná opakující kurs od začátku, nýbrž účastník se zařadí do toho ročníku, který probírá látku dílu posledně absolvovaného. Tuto okolnost nutno v přihlášce v poznámce uvésti.

Přihlášky předkládají vel. vojsk. těles do 31. ledna každého roku přímo hlavnímu štábu - 2.odděl.

FIGURE 2. Guidelines for written cryptography courses [60].



MINISTERSTVO NÁRODNÍ OBRANY

Čís. 169.

VYSVĚDČENÍ.

Pan škpt. Růžek Josef,
... 2. zprav. odd.

vykonal dne 28. července 1923 jazykovou zkoušku před komisí, zřízenou výnosem MNO., čj. 668.920 ze dne 14. odd. /osob./ 1923.

Při zkoušce prokázal prospěch:

v jazyku služebním: písemně velmi dobře
ústně: velmi dobře

v kult. dějinách nár. a občanské nauce: velmi dobře

Podepsaná komise prohlašuje, že pan škpt. Růžek Josef vyhovuje jazykovým podmínkám, stanoveným ministerstvem národní obrany pro voj. gážisty z povolání.

V Praze, dne 30. července 1923.

Zkušební komisaři:

Přísedící:

Předseda zkušební komise:

ČS. MINISTERSTVO NÁRODNÍ OBRANY

FIGURE 3. Josef Růžek's language exam certificate [58].

up on the scaffold, dying in the Terezín concentration camp on 20 April 1945 [59, p. 310].

The Czechoslovak army had been struggling with a shortage of cryptologists since the early 1920s. Therefore, the 2nd Department of the Main Staff organised cryptologist courses to select potential new cryptologists from the course participants. Course participants worked with 12-part written cryptographic courses. Figure 2 shows the first page of the Guidelines for written cryptography courses. These were developed by Josef Růžek and the participants were asked to study them one by one. In addition to the information and theoretical part, the courses also included a practical part. There were several encrypted texts which the candidate had to decrypt. The candidates did not have to decipher all the texts, they just had to show by their performance that they knew the subject matter and could use the relevant keys in practice. Potential Army cryptologists were selected from among professional soldiers, reservists, and citizens undergoing military training. In addition to mathematical and combinational skills, foreign language skills were also a prerequisite. For professional soldiers, this was either a good knowledge of German or Hungarian. Figure 3 shows Josef Růžek's certificate of language examination from 1923. Cryptology courses were voluntary. If a participant was unable to complete the entire course due to work obligations or health problems, they could take the course again. However, if they were unable to complete the course due to the lack of knowledge, they were not given another opportunity to join the course [60, p. 1–4]. Although the activities of the course participants were voluntary, the best cryptographers for the past calendar year were evaluated before the Christmas holidays. They subsequently received a monetary reward. The number of ciphers that the course participants were able to crack in a given year played a role in the ranking and reward. If more participants had the same score, the time it took them to crack the code was the deciding factor in the ranking of the cipher.

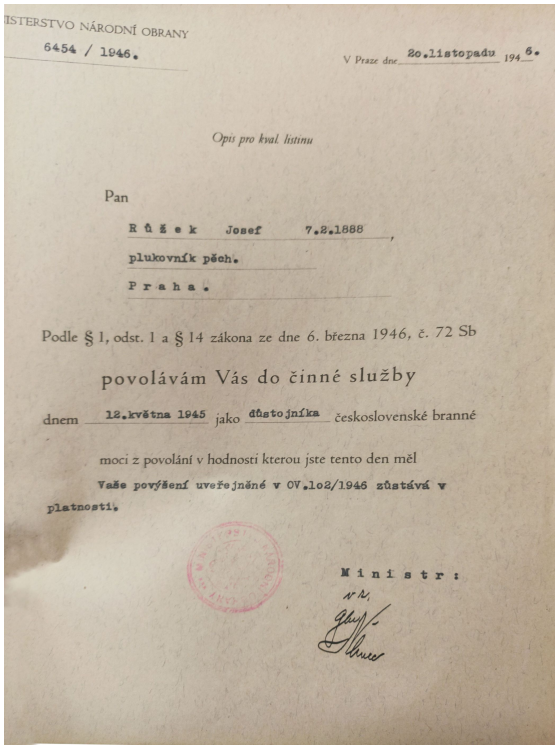
Cryptologists were assisted in cracking particularly difficult ciphers by the department to which they were assigned. Certain concessions in regular service work were justified by the importance of cryptologists for the Czechoslovak army. Those who had completed at least six parts of the course were considered trained participants. Not all graduates of the courses could become members of the 2nd Department of the Main Staff, but they could work as cryptographers in various military units [60, p. 2–4].

The information related to cryptology courses was classified. Course participants were not allowed to discuss it with anyone outside the military environment. In this respect, the 2nd Department of the Main Staff relied primarily on the headquarters of the individual military units, since the commanders of these units also selected suitable candidates for the cryptology courses. More than a hundred candidates applied for the courses each year, but in the first year more than 66 % of them dropped out [60, p. 4]. On average, 3 % of the participants reached the end of the course [60, p. 4]. For each annual course, the 2nd Department of the Main Staff developed new tasks and examples.

Officer of the Main Staff of the Czechoslovak Army Josef Růžek (7 February 1888–10 January 1975) [61] was a gifted cryptologist, completely dedicated to his

work, trained by the Austrian cryptologist General Andreas Figl. In 1924–1925, he managed to push through the publication of the G1 regulation on encryption and the organisation of written courses for the education of crackers (the group of crackers was called SIFRA[14]). From 1928, he was the head of the military crackers group (1928–1949). His professional competence was highly appreciated abroad. He wrote a ten-volume work for emerging cryptologists, Cryptographic Systems and Instructions for Cracking Cryptograms [62]. In 1936, Colonel Josef Růžek established cryptological cooperation with the French, the Poles, and the USSR. After the creation of the Protectorate of Bohemia and Moravia, the German cryptologist Wilhelm Siegwart Fenner (1891–1961)[15] visited Prague and offered Josef Růžek a job in the German cipher service. Josef Růžek refused this offer on principle. Fenner was also interested in whether the Czechoslovak cryptologists were able to decipher the Enigma.[16] Růžek and his subordinates told Fenner that they were not. The Czechoslovak cryptologists were trying to keep the German intelligence officers convinced that the Enigma could not be broken, also because of the activities of Polish cryptologists and their deciphering of the Enigma codes in the early 1930s. Josef Růžek was able to crack both the German double transposition cipher and the commercial version of Enigma in the interwar period. Some documents also prove that Czechoslovak cryptologists were able to read some of the German messages between the two world wars.

After the end of the Second World War, on 15 May 1945, Colonel Josef Růžek was appointed Chief of the 9th Department of the Main Staff of the Czechoslovak People's Army (CSLA), which was the supreme body of the cipher service. Figure 4 shows Josef Růžek's draft order from 1946. He remained in this position until 1949, when he and his colleague Václav Štolba retired. Josef Růžek also left a written testimony about how he broke German and Polish ciphers in the interwar period. He was replaced by Staff Captain Karol Cigáň, who had excellent results in the field of cryptanalysis. Experience with the failure of the Czechoslovak ciphers during World War II led to the approval to expand the cipher-cracking group to


MINISTERSTVO NÁRODNÍ OBRANY
6454 / 1946.
V Praze dne 20.listopadu 194 6.

Opis pro kval. listinu

Pan
Růžek Josef 7.2.1888,
plukovník pěch.
Praha.

Podle § 1, odst. 1 a § 14 zákona ze dne 6. března 1946, č. 72 Sb

povolávám Vás do činné služby

dnem 12.května 1945 jako důstojníka československé branné moci z povolání v hodnosti kterou jste tento den měl

Vaše povýšení uveřejněné v OV.ll02/1946 zůstává v platnosti.

Ministr:

Figure 4. Josef Růžek's draft order [58].

20 personnel in the 1950s. Therefore, in 1951–1956, 4 courses were organised on the basis of Růžek's materials, in which approximately 120 new workers were trained. Not only did many of them leave due to the difficult conditions, but the totalitarian purges ensured a substantial loss of cryptanalysts. During one of them, one of the best Czechoslovak cryptanalysts, Colonel Karol Cigáň, had to leave the service.

6. A look at the development of the news industry in Poland

The Polish army in the interwar period was shaped similarly to the Czechoslovak army, with the state wedged between two long-standing enemies, Germany and Russia/USSR. Therefore, the Poles needed to establish an army intelligence service. The skeleton of the Second Department of the Polish General Staff consisted of three departments: organisational, records and studies, and intelligence. The Polish Cryptologic Department was under the Organisational Department [5, pp. 13–22]. Within it, a cipher department called Biuro Szyfrow was created, headed by Major Gwido Langer, and they found that in their case, the threat to the state became the mother of Polish cryptanalysis. An example of the skill of the Biuro Szyfrow is the success of this department during the Russian-Polish war of 1919–1920. In August 1920 alone, when Soviet troops stood in front of Warsaw, the Bureau decrypted 400 enemy dispatches. The Poles were equally successful in monitoring German communications until 1926, when they also first encountered the Enigma.

[14] A cipher using two substitutions and one transposition, hence the name SST.

[15] He was a central figure in the German military cipher centre OKW/Chi (1922–1939). In 1937, he introduced the Hollerith punch-hole cipher for cipher analysis. See [63].

[16] The Enigma was a portable encryption machine (mechanism) used to encrypt and decrypt secret data. The Enigma was used from the early 1920s onwards, first for encrypting civilian messages, and later by armies and governments of some countries such as Germany in World War II. After some hesitation, the German army purchased a modernised version of the original machine for its ground troops and air force on 15 July 1928. One machine cost DM 600 at the time. In the first half of the 1930s, the Enigma was further improved. Several versions of the improved Enigma cipher machine (3 rotary interchangeable disks, fixed reversible disk and plugs, QWERTZ typewriter keyboard) were used by the Germans throughout World War II.

Captain Maksymilian Ciezki, who was nationalistically oriented, was responsible for deciphering German communications. Ciezki had a commercial version of the Enigma, which showed all the principles of Scheirbi's 1918 invention. Unfortunately, the commercial version differed significantly from the military version in the internal wiring of the scramblers. Without the knowledge of the military version's wiring, Ciezki had no hope of deciphering the German army's messages. Surprisingly, a disloyal German, Hans-Thilo Schmidt, an employee of the German Chiffrierstelle, helped with the first steps towards breaking the Enigma in 1931. He made it possible to obtain two documents: the *Gebrauchsanweisungfiir die Chiffriermaschine Enigma* and the *Schlusselanleitung für die Chiffriermascbine Enigma*, which were sent to France for 10 000 marks [64]. These were manuals for the use of Enigma, and although they did not contain any explicit information about the internal wiring of the scramblers, it was possible to deduce this wiring from their information. Based on the documents, it was possible to build a replica of the German military Enigma. The strength of the cipher lay not in the secrecy of the device, but in the secrecy of its initial setup. The French Bureau du chiffre did not have the personnel to work with the materials it had obtained, so under a mid-1920s agreement with Poland, it handed the documents over to Polish cryptographers. The documents showed not only the internal wiring of the scramblers, but also a description of what the German codebooks looked like. The German Enigma operators received a new codebook every month that gave the key for a particular day, which made cracking and breaking the codes in Poland all the more difficult.

For a long time, Poles, like the rest of the world, believed that the best cryptanalysts were experts in the structure of languages. Enigma, however, forced the Poles to rethink their view of cracking, since Enigma was a mechanical cipher. Biuro Szyfrow concluded that scientifically oriented experts might have a better chance. The Biuro organised a course in cryptography, inviting twenty mathematicians who were bound to strict confidentiality in advance. The mathematicians invited were from the University of Poznan. It was not one of the best in Poland at the time, but it had an advantage for the purposes of cracking. Poznan was situated in the west of Poland and this area belonged to Germany until 1918. All the mathematicians involved were, therefore, fluent in German. Three of the twenty courseworkers showed a talent for cracking ciphers, and the Bureau kept them busy.[17]

This was the beginning of the battle between man and machine in the early 1930s. At the head of the small group was Marian Adam Rejewski (1905 Bydgoszcz–1990 Warsaw) [66]. The cryptographers subjected the device to a careful cryptanalysis. Rejewski successfully applied a theorem from algebraic group theory. The result of this effort was an electromagnetic model of the Enigma, called the bomb, which allowed messages to be decoded under certain conditions. At the same time, the English were also developing methods of cracking the Enigma, with the help of the Poles, with a device that was considered to be the forerunner of self-powered computers. It was later named AGNES and its creators, mathematician Alan Mathison Turing (1912–1954) and his fellow cryptologist Alfred Dilwyn Knox, also based their construction on the Polish bomb.

Rejewski thus continued to try to solve the tasks associated with the significantly improved Enigma by new theoretical and practical methods. Together with his collaborators Jerzy Różycki and Henryk Zygalski, he broke the Enigma code in 1932, which, as I have already mentioned, greatly helped the British to read German messages sent via Enigma during World War II. The thinking behind the breaking of the Enigma was based on three basic questions:[18]

(1.) To understand the idea of the technical workings of the machine,

(2.) to find out how the rotors (scramblers) are connected and what cable connections they have,

(3.) to try a daily key that would include the types of rotors used (three out of five) and how they are fitted in the machine, as well as the wiring of the distribution board, changing pairs of letters.

The Polish success in breaking the Enigma was due to three factors: fear, mathematics, and espionage. The Poles successfully used Rejewski's system for several years. In 1934, they obtained information on Hermann Göring's visit to Warsaw, and his communications were decrypted. In 1938, however, the Enigma was further improved, and in this case, the Poles did not have time to decipher it before the start of World War II.

The first German despatches, based on the knowledge obtained from the Poles, were deciphered by the English in mid-1940 by the ULTRA system. Thanks to perfect secrecy, the Germans never managed to discover this fact. The secret of the ULTRA system was not revealed by the English until 30 years after the war, precisely because of the Germans. The Germans sold the Enigma to the Middle East after the end of the war, and they continued to crack foreign messages encrypted by the machine until 1976. In 1934, the Japanese purchased the Enigma and some other encryption machines and built their own encryption machine based on their principles. They called it 97-shiki-O-bun In-ji-ki, or the letter machine 97 (the number means the last two digits of the year 2597 according to the Japanese calendar). The Americans, without having seen the machine, built a model called MAGIC, which allowed them to decipher Japanese messages. They called this cipher Purple. The first

[17] Based on the publication [65].

[18] He described the code analysis thoroughly in [65, chap. 4 – Fighting the Enigma].

successes were achieved by American crackers, notably Leon Rosen, under Friedman's[19] leadership, in September 1940, a few days before the formation of the Allied axis Berlin-Rome-Tokyo.

7. Conclusion

The period immiediately after the end of the First World War was a time of euphoria about the freedom gained – for Czechoslovakia and Poland a double freedom – not only of free citizens, but also of free new independent states that had emerged as a result of the defeat of Germany and the collapse of the two great powers of Austria-Hungary and the Ottoman Empire. The Versailles Peace Treaties guaranteed these freedoms to all those involved in World War I. It was Czechoslovakia and Poland that gained their independence, and it was necessary for the two new Central European parliamentary countries to take care of their political, economic and cultural development (although still different – Poland was an agrarian, industrially underdeveloped country, Czechoslovakia, formed from the Czech lands and Slovakia, on the contrary, was an industrial hinterland of the former monarchy), but also their security. This was initially tied to France, the architect of the Peace of Versailles, which helped both countries to organise their armies. Both countries built on their legions, successfully fighting in the war on the side of the Allies, which formed the army's base and which, in the officer field, were educated in the countries that helped to create them. The closest links, therefore, militarily went to France, and later to Great Britain and the USA.

Intelligence centres and cryptologic services had to be built within the armies, as it was to be expected that Germany and Austria had intelligence structures left intact after World War I, which they could easily use for intelligence work against Czechoslovakia and Poland. Thanks to the French Military Mission, Czechoslovakia created an intelligence service within its General (later Main) Staff in the 2nd (Intelligence) Department. It was further divided into four groups: A – study and planning, B – search, C – foreign, and D – security and support. This branch of the army was highly regarded. In the 1920s, the defensive section focused on exposing the malign activities of communists and German nationalists, while the offensive section focused its attention on Hungary, which had consistently sought changes to the borders established after World War I. The army also had to focus on the establishment of training institutes, which were mostly based on French military schools. The most important was the War College in Prague for the training of officers for the Main Staff and the Command. It was joined by a system of secondary schools, academies, and various apprenticeships designed for both the reserve and regular soldiers. In these schools, in the French apprenticeships, and in the Second Department, the education of intelligence officers and cryptographers continued. Military intelligence officers were also assisted in their activities by modern technical means. Thus, in the mid-1930 s, under the leadership of Officer Josef Růžek, a technical department with a laboratory for the construction of special fasteners, photographic work, and the development of secret inks was established in the Intelligence Department of the Main Staff. Růžek was also involved in pedagogical work in the education of new cryptographers, for whom he produced a ten-volume work entitled Cryptographic Systems and Instructions for Cracking Cryptograms. By 1939, Czechoslovak intelligence officers had also achieved remarkable results in the development of agency stations and were able to monitor the radio communications of foreign armies and the telephone lines of embassies of states of interest. The international and domestic political developments during the 1930s placed great demands on both the defence and offence of intelligence. Nazi espionage had to be countered, as did sabotage from Hungary, Poland, and Germany.

Intelligence activities in the Polish Army were the responsibility of the Second Department of the General Staff. The skeleton of the Second Department of the Polish General Staff was made up of three departments: organisation, records and studies, and intelligence. The Polish Cryptologic Department fell under the Organisational Department. Within it, a cryptologic unit called Biuro Szyfrow was created during the war with the Soviets, headed by Major Gwido Langer. This service was divided into two other departments. One of them was responsible for domestic activities such as checking printed materials for foreign ciphers and also cooperated with the Polish police. The second department dealt with cracking foreign ciphers. In particular, it focused on Germany and the USSR, Poland's long-time enemies. Cryptologists in Poland were educated in regular universities, in mathematical departments, in courses in the military, and in foreign armies, especially in France.

But the inability to read German coded messages was not just a problem for the British or the French. There was another country in Europe in the late 1920s that considered it vital to know the secrets of a defeated (and again slowly growing) Germany. Poland, which had regained its independence after World War I, had plenty of experience and reason to be cautious. It fought for its territory and independence with the Russian Bolsheviks until 1921, and also took up the fight with Lithuania (1919–20) and Czechoslovakia (in the so-called Seven Days' War for Teschen during January 1919), for example. The Poles were very interested in exploring the Enigma cipher machine, whose materials and documents they had access to in the mid-1920s, and in 1932, with the help of mathemati-

[19] After Friedman's death, the Friedman Archive was established at the George C. Marshall's Friedman Center, convenient for researchers to crack codes. William Frederick Friedman (1891–1969) was a leading figure in American cryptanalysis in the first half of the 20th century.

cian Marian Rejewski and two other mathematician colleagues, they managed to crack the Enigma code. This helped not only Polish intelligence but also the Western powers, especially Great Britain, to crack German messages during World War II. After the Enigma was perfected in 1938, the cryptologic work was transferred to the UK.

References

[1] G. Kasparov. *Deep Thinking: Where Artificial Intelligence Ends and Human Creativity Begins*. John Murray Publishers, 2018.

[2] Z. Kárník. *České země v éře První republiky (1918–1938) [In Czech; Czech lands in the era of the First Republic]*, vol. 1–3. Libri, Praha, 2000–2003.

[3] L. Fasora. *Dějiny Polska v meziválečném období [In Czech; History of Poland in the interwar period]*. Akademické nakladatelství CERM, Brno, 1999. ISBN 80-7204-121-5.

[4] J. Opat (ed.). *První světová válka, moderní demokracie a T. G. Masaryk [In Czech; The First World War, Modern Democracy and T. G. Masaryk]*. Ústav T. G. Masaryka, Praha, 1995. ISBN 80-901971-0-8.

[5] R. Majzner. *Polski wywiad wojskowy wobec polityki III Rzeszy 1933–1939 [In Polish; Polish military intelligence against the policy of the Third Reich policy 1933–1939]*. Wydawnictvo Adam Marszalek, 2006. ISBN 978-83-7441-148-6.

[6] H. P. Willmott. *First World War*. Dorling Kindersley, 2003.

[7] M. Bečvářová, I. Netuka. *Dopady první světové války na mezinárodní spolupráci matematiků [In Czech; The effects of the First World War on international cooperation of Mathematicians]*. Česká technika – nakladatelství ČVUT v Praze, Praha, 2019. ISBN 978-80-0106-540-2.

[8] M. Bečvářová, J. Bečvář et al. *Matematický svět mezi válkami [In Czech; The Mathematical World Between the Wars]*. České vysoké učení technické v Praze, Praha, 2020. ISBN 978-80-01-06792-5.

[9] K. Kuratowski. *A Half Century of Polish Mathematics: Remembrances and Reflections*. Polish Scientific Publishers, 1980. ISBN 9780080230467.

[10] I. Kraus et al. *Věda v českých zemích: dějiny fyziky, geografie, geologie, chemie a matematiky [In Czech; Science in the Czech lands: history of physics, geography, geology, chemistry and mathematics]*. Česká technika – nakladatelství ČVUT v Praze, Praha, 2019. ISBN 978-80-01-06557-0.

[11] M. Tayerlová et al. *Česká technika = Czech Technical University*. České vysoké učení technické, Praha, 2nd edn., 2004.

[12] C. Christensen. Polish mathematicians finding patterns in Enigma messages. *Mathematics Magazine* **80**(4):247–273, 2007. https://doi.org/10.1080/0025570X.2007.11953492

[13] K. Pacner. *Československo ve zvláštních službách [In Czech; Czechoslovakia in Special Services]*, vol. 1. Themis, Praha, 2002.

[14] R. Gawłowski. *The First Enigma Codebreaker*. Pen & Sword, 2023. ISBN 9781399069106.

[15] M. Rejewski. How Polish mathematicians broke the Enigma cipher. *Annals of the History of Computing* **3**(3):213–234, 1981. https://doi.org/10.1109/MAHC.1981.10033

[16] M. Givierge. *Course in Cryptology*. Aegean Park Press, Laguna Hills, 1978. https://archive.org/details/courseincryptogr0000givi/page/n7/mode/2up

[17] E. Antal. The origin of military cryptanalysis in Czechoslovakia. *Cryptologia* **48**(3):193–218, 2023. https://doi.org/10.1080/01611194.2022.2158448

[18] H. Sebag-Montefiore. *Enigma: Bitva o kód [In Czech; Enigma: the battle for the code]*. B4U Publishing, 2012.

[19] R. A. Woytak. The origins of the ultra-secret code in Poland, 1937–1938. *The Polish Review* **23**(3):79–85, 1978.

[20] M. Grajek. *Enigma. Bliżej prawdy [In Polish; Enigma, closer to the truth]*. Rebis, 2007. ISBN 9788375101034.

[21] J. Sýkorová. *Československo-francouzské vztahy v letech 1918–1939 [In Czech; Czechoslovak-French relations in 1918–1939]*. Master's thesis, Charles University, Faculty of Social Sciences, 2010.

[22] M. Efmertová, P. Golan, B. Mannová. *Česká stopa v historii výpočetní techniky [In Czech; Czech footprint in the history of computing]*. České vysoké učení technické v Praze, Praha, 2021. [DVD-ROM].

[23] M. Kosman. *Dějiny Polska [In Czech; History of Poland]*. Karolinum, Praha, 2021. ISBN 978-80-246-1842-5.

[24] M. Koldinská, I. Šedivý. *Válka a armáda v českých dějinách: Sociohistorické čtrty [In Czech; War and the army in Czech history: Sociohistorical quartets]*. Nakladatelství Lidové noviny, Praha, 2008. ISBN 978-80-7106-034-5.

[25] J. Kudrna et al. *Dějiny Francie [In Czech; History of France]*. Svoboda, Praha, 1988.

[26] A. Klimek. *Jak se dělal mír roku 1919. Československo na konferenci ve Versailles [In Czech; How peace was made in 1919. Czechoslovakia at the Versailles Conference]*. Melantrich, Praha, 1989.

[27] Y. Lacaze. Contribution à l'histoire de la Mission militaire française à Prague sous le général Pellé et à celle du traité franco-tchécoslovaque du 25 janvier 1924. In Y. Lacaze (ed.), *L'Amitié franco-tchèco slovaque*, vol. 50, pp. 3–5. Bulletin de l´Association, 2000.

[28] Y. Lacaze. K cestě prezidenta Masaryka do Paříže v říjnu 1923: Vznik smlouvy o spojenectví a přátelství mezi Francií a Československem v roce 1924 [In Czech; On president Masaryk's trip to Paris in October 1923: The establishment of the Treaty of Alliance and Friendship between France and Czechoslovakia in 1924]. In J. Opat (ed.), *První světová válka, moderní demokracie a T. G. Masaryk*. Ústav T. G. Masaryka, Praha, 1995.

[29] M. Heimannová. *Československo, stát, který zklamal [In Czech; Czechoslovakia, the state that failed]*. Petrkov, Havlíčkův Brod, 2020. ISBN 978-80-87595-86-2.

[30] A. Marès. *Edvard Beneš od slávy k propasti. Drama mezi Hitlerem a Stalinem [In Czech; Edvard Beneš from glory to the abyss. Drama between Hitler and Stalin]*. Argo, Praha, 2016. ISBN 978-80-257-1895-7.

[31] J. Friedl, T. Jurek, M. Wihoda, M. Řezník. *Dějiny Polska [In Czech; History of Poland]*. Nakladatelství Lidové noviny, Praha, 2023. ISBN 978-80-7422-914-5.

[32] M. Sawicka (ed.). *Polské okamžiky. Významná polská výročí v článcích z archivu Orientace Lidových novin [In Czech; Polish moments. Important Polish anniversaries in articles from the Orientation Lidove noviny archive]*. Polský institut Praha, Lidové noviny, 2012–2019.

[33] P. Semka. Profesor a maršál [In Czech; Professor and Marshal]. *Polské okamžiky Významná polská výročí v článcích z archivu Orientace Lidových novin* pp. 6–8, 2017.

[34] J. Fidler. *Na čele armády – Náčelníci hlavního štábu branné moci 1919–1939 [In Czech; At the head of the army – chiefs of the Main Staff of the Defence Forces 1919–1939]*. Naše vojsko, Praha, 2005.

[35] R. Künzl-Jizerský. *V diplomatických službách ČSR [In Czech; In the diplomatic service of Czechoslovakia]*. Jos. R. Vilímek, Praha, 1947.

[36] E. Stehlík. *Srdce armády: Generální štáb 1919–2009 [In Czech; Heart of the Army: the General Staff 1919–2009]*. Ministerstvo obrany České republiky, Praha, 2009. ISBN 978-80-7278-515-5.

[37] M. John. *Září 1938 [In Czech; September 1938]*. Votobia, Praha, 2000. ISBN 80-7198-401-9.

[38] J. Kochanowski. Polsko v době autoritativního režimu Piłsudského [In Czech; Poland during the authoritarian regime of Piłsudski]. *Historický obzor : časopis pro výuku dějepisu a popularizaci historie* **10**(1–2):22–35, 1999.

[39] M. Efmertová, A. Grelon, J. Mikeš (eds.). *Des ingénieurs pour un monde nouveau: Histoire des enseignements électrotechniques (Europe, Amériques): XIX^{e}–XX^{e} siècle [In French; Engineers for a new world: History of electrotechnical education (Europe, Americas): 19th–20th century]*. P.I.E. Peter Lang, Brussels, 2016. ISBN 9782807600010.

[40] J. Fidler. Význam francouzské vojenské mise pro výstavbu československé branné moci [In Czech; The importance of the French military mission for the construction of the Czechoslovak armed forces]. *Vojenské rozhledy* **9**(2):117–122, 1999.

[41] J. Fidler. První náčelník hlavního štábu československé branné moci, général de division, Maurice-César-Joseph Pellé [In Czech; First chief of the main staff of the Czechoslovak armed forces, general de division, Maurice-César-Joseph Pellé]. *Historie a vojenství* **48**(1):178–189, 1999.

[42] R. Břach. *Generál Maurice Pellé. První náčelník hlavního štábu čs. branné moci [In Czech; General Maurice Pellé. First Chief of the General Staff of the Czechoslovak Armed Forces]*. Ministerstvo obrany České republiky, Praha, 2007. ISBN 978-80-7278-380-9.

[43] R. Břach. První kroky francouzské vojenské mise v Československu (únor–květen 1919) [In Czech; First steps of the French military mission in Czechoslovakia (February–May 1919)]. *Historie a vojenství* **46**(4):3–32, 1997.

[44] J. Hnilica. *Francouzský institut v Praze 1920–1951: Mezi vzděláním a propagandou [In Czech; The French institute in Prague 1920–1951: Between education and propaganda]*. Karolinum, Praha, 2009. ISBN 978-80-246-1663-6.

[45] M. Braunstein. *Z historie Francouzského institutu v Praze [In Czech; From the history of the French Institute in Prague]*. Francouzský institut, Praha, 1993.

[46] F. Jílek, V. Lomič, P. Horská. *Dějiny Českého vysokého učení technického, 1. díl [In Czech; History of the Czech Technical University, part 1]*, vol. 1,2. České vysoké učení technické, Praha, 1973, 1975.

[47] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Vojenské školství, 1919–1939 [In Czech; Military Historical Archive, fund Ministry of National Defence, Military educaton, 1919–1939].

[48] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Vojenské školství, 1919–1939. Dekret prezidenta Československé republiky, ref. 2982 [In Czech; Military Historical Archive, fund Ministry of National Defence, Military educaton, 1919–1939. Decree of the President of the Czechoslovak Republic, ref. 2982].

[49] S. Włoszczewski, G. d'Ostoya. *Les Militaires polonais dans les armées françaises [In French; Polish soldiers in the French army]*. Picart, Paris, 1935.

[50] P. Jung. *Rakousko-uherská armáda za první světové války [In Czech; Austro-Hungarian Army during the First World War]*. Computer Press, Brno, 2007. ISBN 978-80-251-1520-6.

[51] Dzieje.pl. 140 lat temu urodził gen. Józef Haller, twórca Błękitnej Armii [In Polish; 140 years ago Gen. Józef Haller was born, founder of the Blue army], 2013. [2023-08-10]. `https://dzieje.pl/aktualnosci/140-lat-temu-urodzil-gen-jozef-haller-tworca-blekitnej-armii`

[52] W. Kowalski. Dekret o utworzeniu armii Polskiej we Francji [In Polish; Decree on the creation of a Polish army in France], 2012. [2023-08-10]. `https://dzieje.pl/aktualnosci/dekret-o-utworzeniu-armii-polskiej-we-francji`

[53] A. Garlicki, A. Garlicka. *Józef Piłsudski życie i legenda [In Polish; Jozef Pilsudski life and legend]*. Wydawnictwo Sejmowe, Warszawa, 1993.

[54] A. Garlicki. *Józef Piłsudski: 1867–1935 [In Polish]*. Wydawnictwo Znak, Kraków, 2012.

[55] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Hlavní štáb (HŠ) – 2. zpravodajské oddělení, (1919–1939), especially Rozbor a tabulky šifrového klíče POS, 1933 (čj. 117 taj.), k. 98., Připomínky zpravodajského oddělení HŠ k návrhu nového polního řádu, 1934, k. 108., Služební zprávy o různých armádách, 1934, k. 108., Seznam frekventantů zpravodajského kursu HŠ pro důstojníky v záloze, 1935, k. 119., Směrnice pro obranné zpravodajství 1935 (čj. 8421 dův.), k. 119., Program pracovní skupiny D zpravodajského oddělení HŠ na rok 1936–1937 (čj. 34010 taj.), k. 133., Směrnice pro písemné kursy kryptologie, 1936 (čj. 14202 dův.), k. 133., Mapky vojenských a policejních radiotelegrafních sítí v Rakousku, 1936 (čj.

17091 dův.), k. 133., Námět na cvičení v rámci zpravodajského kursu HŠ v roce 1936 (k čj. 3093 taj. a čj. 3524 taj.), k. 133 [In Czech; Military Historical Archive, fund Ministry of National Defence, Main staff – 2nd intelligence department, (1919–1939), especially Analysis and tables of the POS cipher key, 1933 (čj. 117 taj.), k. 98., Comments of the HQ Intelligence Department on the new draft field regulations, 1934, k. 108., Service reports on various armies, List of participants of the HQ Intelligence Course for Reserve Officers, 1935, k. 119., Defence Intelligence Directive 1935, (čj. 8421 dův.), k. 119., Programme of Working Group D of the Intelligence Department of the General Staff for 1936–1937, (čj. 34010 taj.), k. 133., Guidelines for written cryptology courses, 1936 (čj. 14202 dův.), k. 133., Maps of military and police radiotelegraph networks in Austria, 1936 (čj. 17091 dův.), k. 133., Exercise for the 1936 HQ Intelligence Course, (k čj. 3093 taj. a čj. 3524 taj.), k. 133].

[56] F. Moravec. *Špión, jemuž nevěřili [In Czech; The spy they didn't trust]*. Rozmluvy, Praha, 1990. ISBN 80-946352-42-9.

[57] J. Plzák. *Český radioklub: Rádiové spojení zpravodajských služeb [In Czech; Czech Radio Club: Intelligence radio links]*. Český radioklub, Praha, 2005. [2023-07-07]. http://crk.cz/CZ/ROZVEDKAC.HTM

[58] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Hlavní štáb – 2. oddělení zpravodajské, osobní složka Josefa Růžka [In Czech; Military Historical Archive, fund Ministry of National Defence, Main staff – 2nd intelligence department, Personal file of Josef Růžek].

[59] J. Kokoška, S. Kokoška. *Spor o agenta A-54 [In Czech; The dispute over agent A-54]*. Naše vojsko, Praha, 1994. ISBN 80-206-0437-5.

[60] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Hlavní štáb – 2. oddělení zpravodajské, ročník 1919–1939, k. 133, inv. č. 57, č.j. 14 202, Směrnice pro písemné kurzy kryptografie, [In Czech; Military Historical Archive, fund Ministry of National Defence, Main staff – 2nd intelligence department, vintage 1919–1939, k. 133, inv. č. 57, č.j. 14 202, Guidelines for written cryptography courses].

[61] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Hlavní štáb, (1919–1939), kroniky a fotoalba [In Czech; Military Historical Archive, fund Ministry of National Defence, Main staff, (1919–1939), chronicles and photo albums].

[62] Vojenský historický ústav. Vojenský historický archiv, fond Ministerstvo národní obrany, Hlavní štáb, (1919–1939), Učební texty pro frekventanty zpravodajských kursů 1926 (čj. 1607), k. 82 [In Czech; Military Historical Archive, fund Ministry of National Defence, Main staff, (1919–1939), Teaching texts for students of intelligence courses 1926 (čj. 1607), k. 82].

[63] D. Alvarez. Wilhelm Fenner and the development of the German Cipher Bureau, 1922–1939. *Cryptologia* **31**(2):152–163, 2007. https://doi.org/10.1080/01611190601038225

[64] L. Erben. Úsvit hackerů: Marian Rejewski a Enigma [In Czech; Dawn of hackers: Marian Rejewski and Enigma], 2013. [2023-08-07]. https://www.root.cz/clanky/usvit-hackeru-marian-rejewski-a-enigma/

[65] S. Singh. *Kniha kódů a šifer [In Czech; Book of codes and ciphers]*. Argo, Dokořán, Praha, 2003.

[66] J. J. O'Connor, E. F. Robertson. Marian Adam Rejewski, 2007. [2023-08-05]. https://mathshistory.st-andrews.ac.uk/Biographies/Rejewski/