A Hungarian Cryptological Manual in Berlin

Štefan Porubský
Institute of Computer Science of the Czech Academy of Sciences
Pod Vodárenskou věží 271/2, 182 07 Praha 8
Czech Republic
sporubsky@hotmail.com

Abstract

This is a report on some activities of the Hungarian SIGINT department and a Hungarian cryptographic manual written by the head of its Department X István Petrikovits as found in the Archive of the German Federal Foreign Office in Berlin.

1 Introduction

Archive file TICOM Box No. 3843 in the Archive of the German Federal Foreign Office (Politisches Archiv des Auswärtigen Amts) in Berlin contains a cryptographic typewritten manual entitled *Rejtjel – Segédlet* (A Cipher Aid) written by the head of the Hungarian military cryptological center István Petrikovits. The (slightly damaged) characterization of the file by a TICOM officer says: "*??y general notes on code and cypher, and ??tography, in Hungarian, undated. Includes letter frequencies counts to depth of 100,000 letters of following languages: Hungarian, German, Roumanien, Russian, Serbian, Croatian, Slovak, Czech. From the Hungarian Crypt. Unit, Eggenfelden.*"[1]The document is not dated, but from the given author's military rank "General Major" we can deduce that it was written after May 20, 1943, the date when Petrikovits was "exceptionally and of mercy" awarded this honorary rank (vezérőrnagy in Hungarian). There are no details at disposal on the prehistory of the manuscript or about the way how it got to the TICOM Archive. One possible indication is the fact that between 2 May 1945 and 28 July 1946, Petrikovits was a prisoner of war, detained by the USA (Szakály, 2016).[2]

2 Stephanus Petrikovics vs. István von Petrikovits

István Petrikovits was born on September 24, 1888 in the town of Hlohovec (Galgóc or Galgócz in Hungarian or Freistadt an der Waag in German or in its Slovak colloquial variant Frašták, at that time) which today lies in Slovakia. In that time it also was a predominantly Slovak town. In the church register of the local Roman Catholic church written in Latin we can read that he was baptized on September 30 as Stephanus Robertus Matheus Petrikovics. Here Petrikovics is a more usual Hungarian transcription of the Slavic surname Petrikovič. His god-father was certain Robertus Petrikovics an engineer (geometra) from Párdány, a village today lying in Serbia. It is predominately a Serbian village nowadays, but in that time it had originally two parts: Serb Pardanj and Slovak Pardanj. In the middle of the 18th century, Germans and Hungarians settled here, mainly in Slovak Pardanj and so its name changes in accordance with the structure of the population.[3]

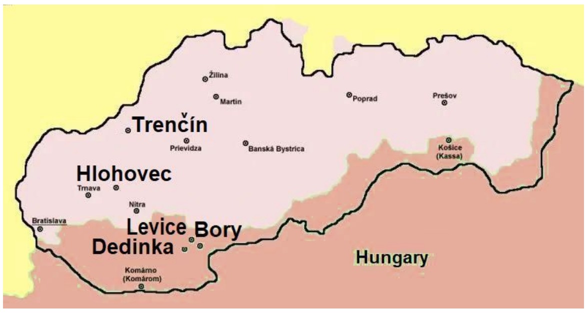

Figure 1. Borders of Slovakia 1939-1945.

Stephanus' father registered as Mathiaš Ignatius Franciscuš Petrikovics[4] (born April 4, 1852) came

[1] Notice that according to the last pre-Trianon 1910 census there lived numerous ethnic minorities within the boarders of the "Hungary-proper", i.e. excluding Croatia-Slavonia: 16.1% Romanians, 10.5% Slovaks, 10.4% Germans, 2.5% Ruthenians, 2.5% Serbs and 8% others.

[2] See also (Jakus, 2013) where however the author names him as Viktor Petrikovits instead.

[3] Two villages (the former Serb Pardanj and the former Slovak/German/Hungarian Pardanj) united into a single village in 1907 today called Meda. According to the 1910 census there lived 3,213 inhabitants in both settlements with the following ethnicity: German - 1,874, Serbian - 1,052, Hungarian - 243.

[4] His given names are written in this form in the local

from the village of Bory (Bori in Hungarian) in Slovakia which was predominantly Hungarian with a strong Slovak minority. His mother Natalia Maria Stephana Juliana Biróczy (born October 8, 1866) came from the village of Dedinka (Fajkürt in Hungarian) which at that time was a small predominantly Hungarian village with a small Slovak minority.

Mathias' father Eduardus had six children and his surname in their local church registers is written in three different ways: once Petrikovich, four times Petrikovics and once Petrikovits. When Stephanus (István in Hungarian) decided to write his surname employing the older Hungarian orthographic possibility[5] with *-ts* instead of *-cs* at the end of his name to stress his noble descent[6] is not known to the author.[7] On the list of the officers of the 15th Honved Infantry Regiment (Honved-Infanterieregiment Nr. 15 / Trencséni 15. honvéd gyalogezred)[8] which was intended for the front in Galicia against Russia and existed till the end of WWI, we can find this form of his surname on the list of 31 regiment Captains. Surprisingly,[9] his direct superior István Ujszászy[10] also writes his surname in the form Petrikovics or even as Petnikovics (Ujszászy, 2007). Petrikovits died on April 16, 1947 in Budapest several months after his return from the PoW camp. He is buried in Farkasréti cemetery in Budapest.

3 Hungarian Military Sigint

After the collapse of the Austria-Hungary Monarchy the new Hungarian military structure rose up on the ruins of the old Empire one. The structure of the later corresponded to that of the political framework of the country. The Empire army had three branches: the joint one, called the Imperial and Royal and recruited from the whole Empire, and then two brances recruited from each part separately, the Imperial-Royal Landwehr for the Austrian part and the Royal Hungarian Landwehr (Honvéd) for the Hungarian one. From our point of view, the directorate of military intelligence – the *k.u.k. Evidenzbureau* headquartered in Vienna, was a whole Empire unit. Thus the independent Hungarian national military intelligence and counter-intelligence services have been built out of its own and based mainly on the Hungarian staff from various military intelligence units of the Monarchy army. The basic structure of the Hungarian new unit undergone numerous structural changes since its establishment in 1918. At the beginning, after the Aster Revolution already on November 1, 1918 to build up such a unit was entrusted Dimitrije (Demeter) Stojaković (or Sztojakovics)[11] who in period 1917-1918 was the head of the Balkan section of the Evidenzbureau in Baden near Vienna. The primary aim ot the newly established unit was the intelligence service against the antagonistic neighbor states Czecho-Slovakia,[12] Romania and Serbia[13].

In 1919 the first Minister of Defense (MoD), the Hungarian Social Democrat Vilmos Böhm founded an intelligence department headed by Sztojakovics at MoD. Under the short-lived[14] communist Hungarian Soviet Republic (Hungarian: Magyarországi Tanácsköztársaság or Magyarországi Szocialista Szövetséges Tanácsköztársaság) the department changed only slightly and served as a subordinate unit called

church register contrary to the surname which is not written in the form Petrikovič. For his photo cf. (Sziklay and Borovzsky, 1898, p. 441).

[5] Older Hungarian texts are heterogenous due to the absence of the generally accepted spelling norms. For the phonem [tS] non existing in Latin (in the south Slavic denoted as ć or in the west Slavic as č) there were used the digraphs *ts*, *cs* or *ch*.

[6] To stress this fact he also used to write István von Petrikovits.

[7] In the second half of 19th century and later many inhabitants of Hungarian part of Austria-Hungary Magyarized their names.

[8] The nationality structure of the regiment was 85% Slovaks and 15% other nationalities and its recruitment was district of Trenčín (Trencsén in Hungarian and Trentschin in German) in north-west Slovakia. District of Trenčín was predominantly Slovak.

[9] Laxity or merely an indication of a not close service interrelationship between both of them?

[10] István Ujszászy served as the head of the Hungarian General Staff's counter-espionage department VKF-2 from 1939 to 1942.

[11] Born 1883 into a Serb family. He Magyarized his name to Sztójay Döme on November 4, 1935. In his birthplace Versec (Serbian: Vršac, German: Werschetz) a half of inhabitans were Germans and one third the Serbians in 1910. Sztójay, an avid supporter of the National Socialists, served as a military attaché in Berlin from 1925 to 1933. From 1933 to 1935 he served in the Ministry of Defence and from 1935 to 1944 as the Hungarian ambassador to Germany. Between March and August 1944 he was appointed the Prime Minister and Minister of Foreign Affairs of a pro-German goverment. After the war he was found guilty of war crimes and crimes against the Hungarian people, sentenced to death, and executed in 1946.

[12] Czecho-Slovakia, later Czechoslovakia, split into Protectorate of Bohemia and Moravia and the Slovak Republic in March 1939, a division which lasted till the end of WWII.

[13] More precisely, The Kingdom of the Serbs, Croats, and Slovenes from 1918 to 1929, and after October 3, 1929 The Kingdom of Yugoslavia.

[14] March 21, 1919 till August 1,1919

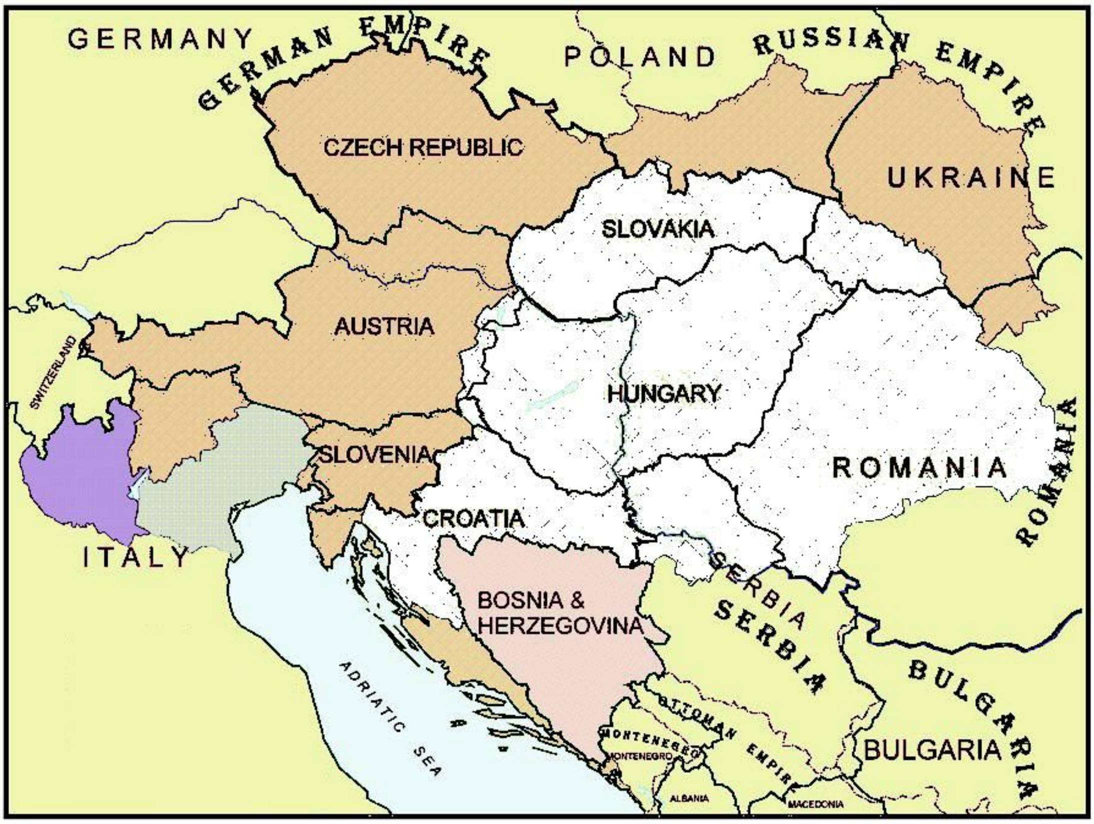

Figure 2. Austria-Hungary and its neighbours borders history ((a) state borders of Austria-Hungary around 1900; (b) states borders around 2000). (`https://i.pinimg.com/originals/d2/be/e3/d2bee3efc7fac13e655bd305788d3c4d.jpg`)

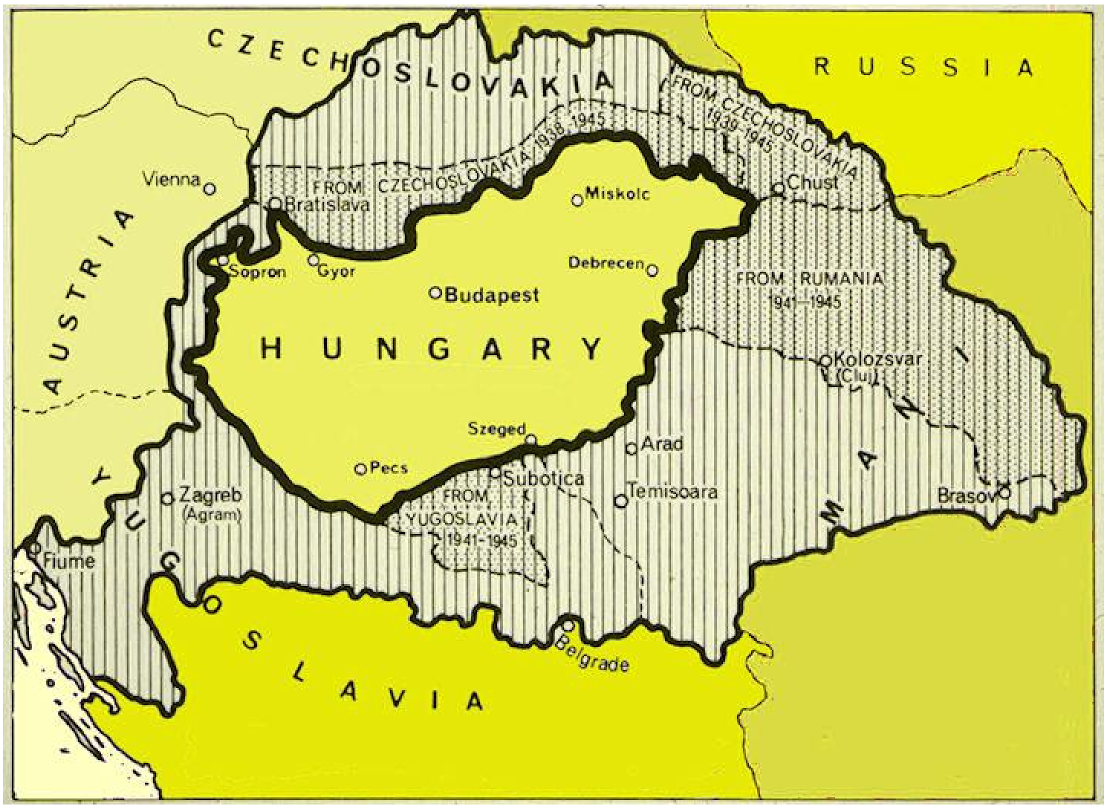

Figure 3. Hungary borders history 1900-1945. (`https://www.globalsecurity.org/military/world/europe/images/hu-map-1921-2.jpg`)

Department II (or VK II group) of the General Staff (Hungarian: VK II. csoportja, VK for Vezér Kar).

After the fall of the Hungarian Soviet republic, it was The Treaty of Trianon, the peace agreement of 1920, which regulated the status of the new independent Hungarian state. Conditions of the Treaty copied often those imposed on Germany by the Treaty of Versailles. The army was to be restricted, there was to be no conscription, heavy artillery, tanks and air force were prohibited, etc.[15] Since the army high command was also prohibited, the General Staff was established under the cover of the MoD on 1 July 1921 as the Main Directorate VI of the Ministry of Defence. Within this Main Directorate VI the 2nd Department was charged with intelligence and counter-intelligence. Its official name was VI-2 Department of the Ministry of Defence (VI/2. osztály). This Bureau of the Second Division operated mainly on the rules taken over from the time of the Evidenzbureau and essentially functioned in this form until 2nd March 1938, when the General Staff and the 2nd Department was officially established and Gyula Gömbös, the former head of Department VI was appointed as the main commander of the Hungarian royal army. From that point Department VI-2 was called "VKF-2" (General Staff 2nd Department, Hungarian: vezérkari főnökség 2. osztálya). The internal organizational structure of VKF – with unsubstantial modifications and extensions – principally remained in the form as it was designed by Colonel Döme Sztójay (Hajma, 2013):

- Register subdivision (Nyilvántartó alosztály, "Nyil"): military, political and defense data processing
- Central offensive subdivision (Központi offenzív alosztály "Koffa"): intelligence assessment, organization and control
- Defensive subdivision (Defenzív alosztály "Def"): anti-spy and cooperation with military police
- Directly subordinated groups (Közvetlenek); "*X*" Department, etc.

The *X* Department was charged with SIGINT and both cryptography and cryptanalysis. The "central figure" of the *X* Department was General Hermann Pokorny. Pokorny was born on April 7, 1882 into a German family in Kroměříž, (German: Kremsier), a Moravian town in a historical region in the east of the Czech Republic.[16] At that time the town was bilingual with 13% of German speaking minority to which belonged also the Pokorny's family. Actually, the word 'pokorný' in Czech or Slovak means 'the humble one'.

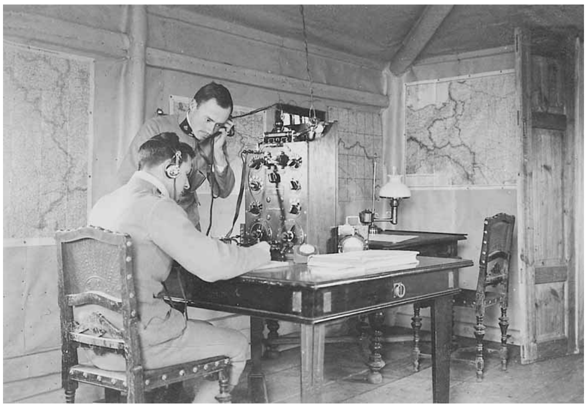

Figure 4. H.Pokorny in the radio intereception station on the East front in 1915 (Pokorny, 2000).

Major Pokorny[17] was one of the best "language expert" in the Evidenzbureau, who spoke German, French, Russian, Polish, Serbian, Czech, Slovak, Bulgarian etc. Immediately after the begin of WWI, as a member of the Austria-Hungary SIGINT group on the East front, he proved his brilliant cryptologic abilities by cracking Russian ciphers[18] during the Battle of Tannenberg, the Siege of Premyšl[19] or at the seizure of Brest-Litovsk. He was the head of Russsian subsection of the Austro-

[15] For instance, due to the strategic importance of the railway, no railway would be built with more than one track!!

[16] Kroměříž is one of the most beautiful cities in Moravia region called the "Athens of Moravia". In 1885, Emperor Franz Joseph and Tsar Alexander III met in Kroměříž to political talks.

[17] He joined the k.u.k. Austro-Hungarian Army in August 1900 as the cadet and by 1918, when the Austro-Hungarian Empire collapsed, his rank was Lieutenant Colonel. He was promoted to Colonel in 1925 and retired in 1935 in the rank of Major General (since 1928) and in October 1945 he was promoted to General.

[18] In the first 20 months of the war he solved several thousands!! intercepted Russian radiograms. For instance, he recognized that the Russians used a system in which they reduced the 35-letter Russian alphabet to 24 letters, while replacing the 11 missing letters with some of the used 24 ones. The results of his activity of tapping and decrypting Russian radio telegrams he described in his book (Pokorny, 2000). His effort to publish it in Germany in 1939 did not find a support there. In January 1945, however, the Russian General Staff took over a copy of this book, with all 18 of original Russian keys decryptions and approx. 12,000 deciphered radiograms. The book was translated into Russian and used later as a secret aid to their staff.

[19] Today a town in southeastern Poland, in that time in Galizia in Cisleithanian Austria-Hungary; German: Premissel, Czech: Přemyšl, Ukrainian: Peremyshl (Перемишль).

Hungarian Deschiffrierdienst. Thought being a German-language native speaker, Pokorny did not request neither Czechoslovak citizenship because of his German origin nor the Austrian one because he had been born in the Czech part of the Monarchy and feared that as a person born outside Austria, he would be considered a second-class citizen. Therefore he decided for the Hungarian citizenship after the WWI and moved to Budapest.

In 1919 Pokorny was charged to set up the Hungarian cryptological bureau on the bases in Vienna operating the so-called *S*-group. The new group was named, as mentioned above, the *X*-Department. Why *X* in its name, is not known. After Pokorny build up this cryptologic section in 1920 he acted as its head until the end of April 1925.[20] He was replaced by his deputy, Colonel Vilmos Kabina[21]. Kabina, as Pokorny, also served during WWI as a cipher officer. Kabina retired on March 1, 1927, but held the position as the head of the *X*-group until January 31, 1935 when he definitely left military service.[22] The next day the head of *X*-group became Colonel István Petrikovits who lead the unit until May 2, 1945, despite his retirement on 1 November 1942.

The main sections of the *X*-department were (Ritter, 2010):

- two radiocommunication intelligence batallions
- deployed interception stations
- central decryption section

The central decryption section was divided into subsections, each having 4-5 cryptologists, and covering specified regions or state groups. Their number changed according to the political situation and military importance. Around 1944 the sections had the following ”territorial competences”:

Turkish section: Turkey,

English section: British Commonwealth, Egypt, USA,

French section: Vichy France and its colonies, Swiss, Belgian, Holland and Greece emigrant governments,

Russian section: USSR, Bulgaria, Czechoslovak and Yugoslavian emigrant governments, Independent Croatia,

Romanian section: Romania,

Swedish section: Sweden, Danish and Norwegian emigrant governments,

Italian section: Italy and Vatican,

Spain section: Spain and Portugal,

Japan section: Japan and China.

István Petrikovits' language “expertise” were Slovak and Bulgarian. He participated on the work of the Russian section. Further members of the ‘Russian half’ of the section were lieutenant Pál Krisztinkovics and major Elemér Lajtos. The substantive part of work of the Russian section was oriented to follow radio communication and to gather intelligence information from and in the direction of the Soviet Union and Yugoslavia. The section was successful in cracking some ciphers used by the Soviets. They cracked at least one important cipher used by the Soviet Foreign Ministry.

In 1940 Petrikovits reciprocated the visit of representatives of the Finnish SIGINT group in Hungary and reported about the Finnish achievements in the deciphering of Soviet military ciphers.[23] Thus for instance, the Finns were able to gather the airdropped Soviet military material thanks to the information intercepted and deciphered from the Soviet radiograms. As a result of a close collaboration not only between both SIGINT groups, several Hungarian officers were awarded Finnish orders. One of them was I. Ujszászy and also I.Petrikovits who was awarded the Finish Order of the Cross of Liberty with swords of the 2nd Class (Sallay, 2014). This order was founded 1918 upon the initiative of General C.G.E. Mannerheim.

Another interesting collaboration was that with Japan. In July 1938 the Japan military attache moved his headquarter from Vienna to Budapest and an intensive military collaboration between Hungarian and Japan on the field of intelligence and decipherment started (Sallay, 2007). One aspect of this collaboration was an intensive ex-

[20] In 1935 already mentioned Gömbös, now premier minister of Hungary, forced Pokorny to leave his active military service arguing with his non-Hungarian origin.

[21] Born as József Vilmos János Zsigmond Kabina on May 4, 1876 in the town of Levice (Hungarian: Léva, German: Lewenz; the Old Slavic name of the town was *Leva*, which means “the Left One”, since the town lies on the left bank of the Hron river), now in Slovakia. In that time it was predominantly a Hungarian town. On June 17, 1951 the communist regime forced him and his wife, both barely able to walk, to leave their apartment in Budapest and move to a small town Kunszentmárton in the central Hungary.

[22] According to some source, e.g. (Ritter, 2010), H.Pokorny temporarily headed the *X*-Departmen for a half year period during 1935/36.

[23] The good relations between Hungarians and Finns goes back to the Finno-Ugric linguistic affinity cultivated since the end of the 19th century. Hungarian volunteers fought on the side of Finland during the Winter War (1939–1940) against the Soviet Union. Even Albert Szent-Györgyi offered all of his Nobel prize money which he received in 1937 to Finland in 1940.

change of distinctions. The Order of the Rising Sun awarded in nine classes was established in 1875 as Japan's first order. The third through sixth classes were conferred upon individuals who have made significant contributions to Japan. István Ujszászy was awarded this order twice: in 1940 it was its 4th Class and in 1942 the 3rd Class. In the 1942 "wave of honours exchange" István Petrikovits was awarded the Order of the Sacred Treasure of the 3rd Class, an imperial order established in 1888.

In November 1944, before the advancing Red Army, the X-department escaped to Und (German Undten: Croatian Unda), a mostly Croatian municipality in the Sopron-Fertőd region in western Hungary close to the border with Austria. Gradually moving to the west, the group gave up on May 2, 1945 to the Americans next to Eggenfelden, a small town in the Lower Bavaria. All transported and historically important material become a part of the TICOM archive.

The activities of VKF or of the army generality in general were not always completely consistent with the visible official pro-German politics of Hungary (cf. e.g. (Szakály, 1987)). On one side, Wilhelm Höttl (1915-1999), the young Austrian Nazi Party member serving in SD-Ausland (Sicherheitsdienst = Security Servis), and by 1944 acting as a head of the R.S.H.A.[24] branch for Central and South East Europe conveyed an impressive tribute to the work of the Hungarian secret intelligence during WWII (cf. (Kahn, 1996, p. 453)). According to Höttl, Hitler, who ensnared Admirál Miklós Horty[25] into Axis alignment by restoring some of Hungary lost territories, deeply distrusted Horty. The augury of a bleak outcome of the war forced Horty's cabinet[26] to secret negotiations with Western Allies where an important role was played by Major General István Ujszászy.[27] Contact with Western Allies led to the *Mission Sparrow* when OSS airdropped a three men group under Colonel Florimond Duke in Hungary. Three days later, on March 19, the Germans in *Operation Margarethe* invaded Hungary and captured all three members.[28] When on August 23 a cup replaced pro-Nazi Romanian government by a Soviet-aligned one, Horty plotted with Ujszászy and the commandant of Budapest to seize Budapest and to start secret negotiations with Moscow. But Germans were again ahead mainly due to intelligence activities of Höttl's SD-Ausland which penetrated Hungarian Secret Service.[29]

Finally, it would be perhaps interesting to the reader to note that a cousin of Hermann Pokorny, Major Franciszek Pokorny born June 15, 1891 in the village of Mosty[30] was a Polish Army offi-

[24] Reichssicherheitshauptamt = Reich Central Security Office

[25] Miklós Horthy de Nagybánya or German Nikolaus Horthy Ritter von Nagybánya (1868 - 1957) was a Hungarian admiral and statesman, who served as the Regent of the Kingdom of Hungary from 1 March 1920 to 15 October 1944.

[26] Already 1943 the Prime Minister Miklós Kállay (1942-1944) sent envoys to Istanbul. In 1944 one of them was the Nobel Prize Winner Albert Szent-Györgyi. Till the end 1944 also the Defence Minister L.Csatay, Chief of Staff General F.Szombathelyi and VKF's Department 2 all sent their representatives to Istanbul.

One of the key figures behind the scene in Istanbul was in Russia born and during WWI volunteer of the Russia army, Colonel Harold Gibson, SIS station head in Turkey. Gibson as a "visa clerk" of the British embassy in Prague played also a crucial role in the reorientation swap of the Czechoslovak military secret service from the French to the British secret service and in the organisation of a spectacular flight of Colonel Moravec, chief of the Czechoslovak secret service with 10 of his close collaborators, from Prague to London on the eve before the German invasion of Czechoslovakia on March 15, 1939, cf. (Porubský, 2017a; Porubský, 2017b). After his retirement 1958 Gibson was found shot dead under unexplained circumstances in his flat in Rome in 1960. Possible collaboration with the Soviet secret service as a reason for a suicide is not excluded.

[27] István Ujszászy was the head of the internal security apparatus subordinate to the Interior Minister known as the State Protection Center (Hungarian: Államvédelmi Központ) from 1942 to 1944 and he was one of the key figures in the preparation for the so-called "bail out" (Hungarian: kiugrás). After the German occupation of Hungary, he was arrested by the SS Security Service SD. Then since February 1945 by the NKVD. After interrogations in Moscow he was allegedly transferred back to Hungary to a detention camp of the infamous Hungarian secret police State Protection Authority (Hungarian: Államvédelmi Hatóság or ÁVH) in the summer of 1948. His final fate disappears in the fog.

Ujszászy's handwritten protocols written for the ÁVH kept in the archives of the Ministry of the Interior for decades are published in (Ujszászy, 2007).

In the interwar period 1930-1938 Ujszászy's served also as the military attache in Paris, Warszaw and Prague. For the comments on his stay in Prague see (Moravec, 1975). Hovewer his name is misspelled as Ujzazy here.

[28] Hungary's German occupation was justified via argument of the "unresolved Jewish question" and the "unfaithfulness" of the Hungarian political leadership. On the other hand, recent archive discoveries indicate (Peterecz, 2012) that the Allies played a two-faced game and that the aim of the airdrop was also to provoke the Germans to sent military forces to Hungary and thus to weaken the German military position in the West before the invasion of Normandy disregarding possible Jewish casualties in the Hungarian population.

[29] Höttl was recruited by the United States Army Counter Intelligence Corps (CIC) after the war.

[30] Mosty u Jablunkova (Polish: Mosty koło Jabłonkowa, German: Mosty bei Jablunkau or Mosty in den Beskiden), lies today in the Moravian-Silesian Region of the Czech

cer who, after World War I, from 1925 till 1929 headed the Polish General Staff's Cipher Bureau (Referat Radio i Szyfrów Oddziału II Sztabu Generalnego (Głównego)) the predecessor of the famous Biuro Szyfrów.

4 The Manual

The cryptological manual authored by István Petrikovits has 91 on one side typewritten pages with the following contents:[31]

In the introductory part[32] of the manual Petrikovics settles the basic terminology. He recognizes three main branches of crytpography:

- real (apparent) cryptography, mostly based on mathematical ideas
- covered (hidden) cryptography, for instance to use passphrases to initialize previously prearranged actions
- invisible writing using chemical processes (invisible ink, etc.)

What concerns (in his conception called *real*) cryptological systems he distinguishes between permutations and substitutions.[33]

Almost one half of the manual is devoted to a thorough description of the frequency analysis of the basic structural elements of written documents, as the frequencies of the letters, bigrams or words of the aforesaid languages. The selection of languages indicates that the manual arose from the needs of Department X since apart of Hungarian and German, they are languages used in the enemy states. On the other side, the briefness of the description of cryptological techniques suggests that it was not intended to be used as a textbook, rather as a succinct introductory guide, maybe for personal use or as a basis for a future project. Throughout the text scattered problems, with solution given at the end, indicate that the manual was not written as a report during the captivity.

This analysis of the written form of languages constitutes the 2nd Chapter called *Language analytics* (Nyelv-analytika). Petrikovits gives relatively detailed 'anatomy' of the Hungarian, German, Romanian, Russian, Serbian, Croatian, Slovak and Czech language. The corresponding reports follow the same structure for each of these languages. The given characteristics are based on the analysis of sample texts having approximately 100,000 characters in total (Russian as an exemption uses only 50,000 characters). Certain speciality is that these 100,000 characters stem from a collection of (not closely identified) independent sub-texts each having approximately from 3,000

Republic. At that time, during the Austria-Hungary Empire, with a predominant majority of population being native Polish-speakers.

[31] This is contents given by Petrikovits at the end of manual. Actual headings are partly different.

[32] Though not denoted as Chapter 1 it is so meant, as follows from the rest of the manual.

[33] For some concepts he also gives their German translation, thus substitutions are in Hungarian *helyettesittő* or in German *Ersatzverfahren* and permutations are *keverőrendszerek* or *Versatzverfahren*, respectively.

to 6,000 characters. The reason for considering such sub-divided collections of texts is a bit unusual. They are base for several tables of the letter frequencies. Besides the standard tables of letter frequencies based on the whole collections of 100,000 characters, interesting min-max tables of frequencies are given. These tables show the minimal and maximal letter frequencies in these sub-texts. For instance, for the computation of the characteristics of the Hungarian they have about 3,000 letters each. As an example, the letter with the maximal frequency in the Hungarian is *e*. It appeared in the whole sample 10,656 times, i.e. with frequency 10.66%, while in sub-texts it appeared with frequency lying between 8.26% and 14.70%. The six-columns Table a occupying one page and giving total absolute and relative, minimal or maximal frequencies is followed by an analogical Table b showing analogical recalculated frequencies of letters of the telegraphic alphabets (that is without diacritic accents). Petrikovits explains the significant differences of the frequencies in comparison with the previous global Table a arguing that some parts were written in dialects, or that some of them are written by uneducated persons, etc. For instance, letter *e* appears in the Hungarian alphabet as *e* or *é*. The general frequency of *e* is 14,14% while in min-max table the given frequencies are 10.80% and 19.90%. The next part contains comments on distribution of vowels and consonants. Actually there are no numerical characteristics here, only comments on their pattern alternations. The following section contains notes to the mixed patterns of vowels and consonants. The last part comments the words frequencies in the sample of 100,000 characters. Lists of the absolute frequencies of the most frequent one-, two-, three- and four-letters words are also given.

Then frequency characterizations of characters and words of German, Romanian, Russian (based on sample of 6× 8,333 characters texts), Serbian (16×6,250 characters), Croatian (16×6,250 characters), Slovak (16×5,900 + 16×5,600 characters) and Czech (17×5,900 characters) are given following the same pattern.

The third chapter of the manual is devoted to a very short description of the basic cryptographic techniques. It starts with the monoalphabetic cipher. The idea how to solve a monoalphabetic cipher is briefly demonstrated using an atbash like cipher. He points out its weakness when the characters are substituted by simple letters, or by couples of digits stressing the fact that we have 26 characters but only 10 digits when replacing letters by pairs of digits. To defuse this defect he shows two substitutions employing couples of digits or letters with more or less equidistributed components. He also mentions the usage of nulls.

In the part devoted to the polyalphabetic substitutions (called composite (in Hungarian *bonyolult*) substitutions in the contents) Petrikovits works with a periodic Vigenère's cipher. He shows Tritheim's and variants of Vigenère's tables with numeric or alphabetic heads[34] and show how to solve this type of a cipher. The solution is based on Kasiski's test without to mentioning Kasiski's name. To apply it he counts distances between repeating bigramms and trigramms. After finding the key pattern he shows how to recover the used keyword (and indirectly also the message language) and cipher alphabet taking into account also the frequency tables of different languages.

The next section is devoted to the autokey cipher. Petrikovits handles its text-autokey type where he uses either the message text or its enciphering to determine the next element in the keystream. He shows how to solve the Vigenère autoclav of the above first type based on the tabula recta when the key is a single letter.

The part dealing with transpositions starts with a short critics of Cardinal Richelieu's simple transposition cipher, and continues with the columnar transposition (with nulls) and the standardly given hints for its solution. Then Petrikovits presents the initiatory, and rarely given, ideas how to solve a 90° turning, in his case a 6×6, grid cipher. Provided we know that a turning grill was used, the solution idea is based on the observation of symmetries of bigramms in the 1st and 3rd or 2nd and 4th turns.

This part of the manual ends with short comments on what he calls composite transpositions. These are either transpositions of previously by a substitution encrypted texts or double columnar transpositions. An example of the second type is given with a comment that a double columnar transposition should be consider to be unsolvable from the cryptoanalytical point of view.

Then follows a section devoted to general description of the use of nomenclators in cipher

[34] He names them Vigenère's, Gronfeld's (not Gronsfeld?) ciphers.

texts. Petrikovits describes several possibilities for the form of the inserted codewords. For instance, their numerical or literal form, their most used length or possibilities to use tables or dictionaries. The description is a bit lengthly and too general, and was incorporated probably due to their general use in the intelligence and diplomatic correspondence.

The final 'scholarly' section is devoted to some general instructions for examining cryptographic materials.

The concluding part containing the solutions of the problems given in the text lists their solutions without any comment.

5 Appendix

In the TICOM collection fund by the author in the Archive of the German Federal Foreign Office there was another file registered as TICOM report No. 3870. Its characterisation says: *Bried notes in Hungarian on types of Bulgarian, Czech and Jugoslavian keys used 1921-35. From the Hungarian Crypt. Unit, Eggenfelden.*

The file contains two reports both covering period February 1, 1921 through August 1, 1936. Surprisingly, though they contain principally identical information about the cryptological activities, they are not identical.

Both reports are typewritten and each is 1 and half side long. They are classified as *strictly confidential* and are written in Hungarian. The (of this paper author's) translation of the substance of their contents is as follows:

Report

on the cipher keys of foreign countries which were deciphered by lieutenant-colonel István Petrikovits in the period February 1, 1921 – August 1, 1936.

Czechia[35]

- it was effective 1921/11/1 through 1922/7/30: small diplomatic cipher key.
- it was effective 1922/8/1 through 1923/8/1: big diplomatic cipher key.
- it was effective 1929/8/1 through 1934/10/1: cipher key of an army division (katonai csapat)
- it was effective 1930/8/1 through 1931/7/31: cipher key of an army division
- it was effective 1931/8/1 through 1932/7/31: cipher key of an army division
- it was effective 1932/8/15 through 1933/10/1: cipher key of an army division
- it was effective 1933/8/15 through 1934/10/1: cipher key of an army division

Remark in the Report: Every army cipher key changed on daily basis 5-5 within the cipher system and thus within every cipher system deciphering of 75-75 new recipherings were realized.

Yugoslavia

- it was effective 1923/6/1 through 1926/1/1: big diplomatic cipher key.
- it was effective 1926/1/1 through 1927/6/1: big diplomatic cipher key.
- it was effective 1927/6/1 through 1929/12/31: big diplomatic cipher key.
- it was effective 1930/1/1 through 1932/12/31: big diplomatic cipher key.
- it was effective 1933/1/1 through 1935/4/1: big diplomatic cipher key.
- since 1927/8/1 diplomatic cipher keys changed cipher tables every month. Altogether more than 100 reciphering tables.
- it was effective 1926/1/1 through 1934/12/31: consular cipher key.
- it was effective 1930/1/1 till today valid royal court cipher key

Bulgaria

- it was effective 1926/8/1 through 1933/3/1: diplomatic cipher key 975
- it was effective 1930/8/1 through 1933/1/1: diplomatic cipher key 03210
- since 1935/1/1 till today: diplomatic cipher key 00062
- since 1935/1/1 till today: diplomatic cipher key 67676
- it was effective 1930/1/1 through 1935/1/1: royal court cipher key.

Remark in the Report: Here listed Czech, Yugoslav and Bulgarian cipher keys were deciphered by lieutenant-colonel István Petrikovits who deciphered thousands of telegrams.

Date: Budapest August 10, 1936 and signed by Pokorny (followed by an unreadable sign part)

[35] Meant is Czechoslovakia. It was a custom in Hungary in the interwar time to use the name Czechia or Czech Republic (Csehország) instead of Czechoslovakia and all its citizens to call simply as Czechs. For some aspects of the relations between Czechoslovakia and Hungary (including some Ujszászy's activities) cf. (Miklós, 2017).

As mentioned the second report is not a copy of the first one. Its head reads: Report on the cipher keys of foreign countries on which decipherment there cooperated lieutenant-colonel István Petrikovits in the period February 1, 1921 – August 1, 1936. Further, the first Yugoslavian item report has the following footnote: decipering a code requires 6-12 months. Otherwise the contents (but not the form of the lists) are identical. Finally, the closing remark says: Here listed Czech, Yugoslavian and Bulgarian cipher keys also deciphered in a co-operation of lieutenant-colonel István Petrikovits who deciphered thousands of telegrams. This second report is again signed by Pokorny but in contrast to the first one on February 10, 1937.

Acknowledgments

The author thanks the unknown referees for their valuable comments. He was supported by the strategic development financing RVO:67985807.

References

Deborah S. Cornelius. 2011. *Hungary in World War II: Caught in the Cauldron*. Series: World War II: The Global, Human, and Ethical Dimension Fordham University Press, New York Project MUSE muse.jhu.edu/book/14532.

Lajos Hajma. 2001. *A katonai felderítés és hírszerzés története. (History of military reconnaissance and intelligence)*. Zrínyi Miklós Nemzetvédelmi Egyetem, Felderítő Tanszék (Miklós Zrínyi National Defense University).

János Jakus. 2013. A magyar rádió- és rádióelektronikai felderítés szervezeti változásai 1990-ig. (Organizational changes of the Hungarian radio- and radioelectronics reconnaissance until 1990). *Rendvédelem-történeti Füzetek (Acta historiae preasidii ordinis)*, 23 (27-30): 101–128.

David Kahn. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, New York.

Dániel Miklós. 2017. The Picture of the Czechs through the Eyes of Hungarian Politicians. In *Az első világháború irodalmi és történelmi aspektusai a kelet-európai régióban*. Tanulmánykötet, Trefort-Kert Alapítvány - ELTE Doktorandusz Önkormányzat, Budapest, pages 47–62.

František Moravec. 1975. *Master of spies: the memoirs of General Frantisek Moravec*. Doubleday, Garden City, N.Y.

Zoltan Peterecz. 2012. Sparrow Mission: A US Intelligence Failure during World War II. *Intelligence and National Security*, 27(2):241–260.

Hermann Pokorny. 2000. *Emlékeim: a láthatatlan hírszerző. (My memories. The invisible intelligence officer)*. Petit Real, Budapest.

Štefan Porubský. 2017. STP cipher of the Czechoslovak in-exile Ministry of defence in London during WWII. In *Proceedings of EuroHCC 2017 (3rd European Historical Cipher Colloquim, Smolenice, Slovakia, May 18-19,2017*, pages 47–66.

Štefan Porubský. 2017. Application and misapplication of the Czechoslovak STP cipher during WWII (report on an unpublished manuscript). *Tatra Mt. Math. Publ.* 70:41–91.

László Ritter. 2010. A Magyar rádiófelderítés a második világháborúban. (The Hungarian radio reconnaissance in the second world war. *Felderítő Szemle (Intelligence Review)*, IX (2):149–168.

Gergely Pál Sallay. 2007. Japán-magyar katonadiplomáciai kapcsolatok 1938-1944. (Japanese-Hungarian military diplomatic relations 1938-1944). *Hadtörténelmi Közlemények (Military History Bulletin)* 120:183–202.

Gergely Pál Sallay. 2014. Finn kitüntetések a Magyar Nemzeti Múzeum gyűjteményében. (Finnish honors in the collection of the Hungarian National Museum). *Folia Historica* 30:155–176.

Sándor Szakály. 1987. Wojskowy ruch oporu na Węgrzech v latach drugej wojny światowej (Polish) [The Hungarian military resistance movement in World War II]. In: *Razem w walce*, Węgierski instytut kultury & Wojskowy instytut historyczny, Warszawa, pages 65–91.

Sándor Szakály. 2016. From the Evidenzbureau to the Establishment of the Independent Hungarian Military Intelligence. *National Security Review* (Military National Security Service, Budapest), 2:13–28.

János Sziklay and Samu Borovszky. 1898. Magyarország vármegyéi és városai. (Counties and cities of Hungary), volume 4: Nyitravármegye. Apollo irodalmi társaság, Budapest.

István Ujszászy. 2007. *Vallomások a holtak házából Ujszászy István vezérőrnagynak a 2. vkf. osztály és az Államvédelmi Központ vezetőjének az ÁVH fogságában írott feljegyzései) [Testimonies from the House of the Dead (Protocols written by Major-General István Ujszászy the head of the VKF 2nd Department and of the AVK during his captivity by ÁVH)]*. G.Haraszti and Z.A.Kovács and Sz.Szita edts. Corvina, Budapest.