HADMÉRNÖK

X. Évfolyam 2. szám - 2015. június

PRISZNYÁK Szabolcs
prisznyak.szabolcs@bv.gov.hu

BORDERS AND THEIR IT SYSTEMS

Absztrakt

This study presents Information Technological support of border protection and its related activities. These solutions focus primarily on border traffic control but there are also IT innovations supporting border guarding forces. Border protection IT systems formerly used in Hungary as well as IT systems will be introduced that are currently applied in the EU and the Schengen Area. The paper will come up with the experiences so far and lists possible future solutions.

A cikk bemutatja a határellenőrzés – valamint ahhoz kapcsolódó egyéb tevékenységek - informatikai rendszerekkel történő támogatását. A megoldások elsősorban a határforgalom ellenőrzésére fókuszálnak, de a határőrizet támogatásában is sok az újszerű megoldás. A szerző áttekinti a korábbi magyar határőrizeti rendszereket, majd bemutatja a jelenlegi EU-s, Schengeni rendszereket. Összegzi a tapasztatokat, majd ismerteti a jövőben alkalmazható megoldásokat.

Keywords: *Schengen Treaty, IT systems, border control, Schengen Information System, border guard ~ Schengeni Egyezmény, informatikai rendszer, határellenőrzés, Schengeni Információs Rendszer, határőr*

INTRODUCTION

Computers and Information Technology of various grades of complexity and development are present in practically all areas of our everyday life. These systems range from printing simple forms and registering partners to operating power stations or supporting space exploration projects. Naturally, also governmental operations, including law enforcement and even more specifically, border protection are areas where information technology plays a cardinal role. Border protection, in particular, border control and border guarding of green (on land) and blue borders (on sea). In a broader sense, border control is related to foreign affair, domestic policy, law enforcement, refugee policy activities. From an information technological perspective, this means that the individual systems may be interconnected, may electronically exchange data, and in the various individual fields, may apply each other's databases. Today, the IT system are so highly developed that information is not only be processed only after the event in question but by systematising, identifying the data and the connections between them in a large pool of information, it enables us to forecast certain events with considerable certainty. To protect the territory of the European Union and the Schengen Area, increasingly developed and modern systems get implemented. The design, development and later, the operation of these IT systems are such a large-scale issue that the EU has established an independent agency to perform the relevant tasks. In this study, I will present the IT systems applied in Hungarian border protection prior to the Euro-Atlantic integration, then I will describe the systems that are used by the border guarding forces in Hungary and in other member states today, following the accession to the European Union then to the Schengen Area. Finally, I will sum up the experiences so far, the accomplishments, and will discuss possible future development ideas and the possibilities of their practical application.

FORMER IT SYSTEMS USED IN HUNGARY

The Yalta Conference (4 – 11 February 1945) [i] after the Second World War determined the future of Europe and in a broader sense, the world for more than 40 years. The term 'iron curtain' was first used by Winston Churchill in his speech in Fulton (5 March 1946.): „From Stettin in the Baltic to Trieste in the Adriatic, an iron curtain has descended across the Continent." [ii].

The new order of the world brought changes not only in a political, economic and a military sense but also determined the border protection activities of the individual countries. The iron curtain was built along the Austrian-Hungarian border, whose history between 1945 and 1989 was summarised in detail in János Sallai's book: An Impression of a Bygone Era[iii].

In Hungarian border protection and border traffic control, IT devices and computers have been used only since the 1980s. The reason for this is that only at this point had technological development reached the right level. It is also important to mention that because of the CoCom[iv] – a multilateral trade embargo - former Socialist countries, like Hungary, were not allowed to purchase IT devices developed and manufactured in Euro-Atlantic states (in total, 17 counties). Technologically speaking, however, the computers developed and produced in former Socialist states were seriously lagging behind the technology of Western states.

It was therefore in the 1980s, in accordance with the political expectations of the time, that the first computers popped up at the Western border of Hungary.[v]. Because of the reasons mentioned above, these were R-20 and R-20 type small computers developed by the Socialist industries for the Eastern Bloc. These computers were applied to support the border traffic control activities. Their main purpose was to perform checks in the database of expelled and observed individuals. These computers required special operation conditions, so air

conditioning was also necessary to operate them. Besides, technological failures were quite common, so there was lots of stand-by time. On these occasions, the checks had to be performed manually with the help of the printed database lists.

The real breakthrough of IT systems came when micro-computers started spreading worldwide. Simultaneously, the prices of computers were dropping, which increased procurement. It is also an important factor that fewer and fewer IT devices were listed by CoCom, and following the political and economic changes of the Eastern Bloc at the beginning of the 1990s, the list was completely eliminated. This gave the Border Guard Forces the opportunity to establish a new system with more modern devices, the so-called Photo-based System already based on micro-computers: the passport data could be read by a Closed Circuit video system and forwarded to computers. In addition to more modern, larger capacity and more operationally secure systems, also the electronic data transmission came about, which reflected the technical quality levels of the era, had the transmission speed of the telecommunication conditions in Hungary of the time and occurred once a day. The Border Guard Automated Data Transfer System meant another breakthrough. Following the political changes, the main objectives of border protection became the reconnaissance of weapon, drug and human trading and alongside these, of the activities of organised criminal groups. Hungary asked the USA for assistance to enhance the establishment of this system. The computers were placed in the passport control boxes, a Local Area Network (LAN) was set up, and the far-distance data transmission network was also developed. The Border Guard Forces benefitted greatly from the establishment of the system, but the governments could agree neither on the contents of the data exchange and nor on the system of the information transfer, so the system was never implemented live.

Following this, the Hungarian Border Guard Forces took over the establishment of their own national system. Some of the formerly implemented elements were adopted, but in other elements, they devised completely new solutions. The system introduced in 1994 was named Solarium 2i. The speed of the data transmission was continuously increasing. Due to the changes occurring in Eastern Europe, the number of crimes committed by foreigners was also growing, which brought about prohibition of entry and stay. As a result, the databases managed by the Border Guard Forces were also dynamically increasing. In the databases formerly containing a couple of thousand data now had to manage tens of thousands of data. The capacity of the machine park proved less and less sufficient with time. There was no possibility to develop it centrally because of financial reasons, so the regional organs of the Border Guard Forces were trying to develop their IT system according to their diverse economic possibilities. Consequently, the originally homogenous machine park started to become increasingly heterogeneous. More and more crossing points opened up, which had to be supplied with IT devices and telecommunication networks capable of data transmission. The Kaktusz-1 IT system was implemented in 1997, which technically was mostly based on the earlier Solarium2i. Its introduction was necessary because the government set the Border Guard Forces increasing law enforcement expectations in the field of border traffic control. In order to meet these, because of public and property security, search in arrest warrant databases was also essential. A further expectation was faster search in the databases, which could only be met by implementing new search methods. It is crucial to mention that in accordance with the political requirements at the time – especially because of the Balkan crisis – the largest scale developments were carried out along the southern and eastern borders. By 1999, illegal migration had begun stagnating, and the public was preoccupied by organised crime. The control methods which had continuously been simplified and differentiated according to nationality from 1990 onwards was replaced by a new act against organised crime [vi] and, as a consequence, universal checking methods. This task could not be performed with the then-existing machine park, thus a decision was made to replace it by devices that were able to

automatically scan passports and cameras capable of reading the license plates of cars crossing at road crossing points. The system was called Border Registration System. Besides the devices applied by the final users, the local networks and the central machine park were also renewed. The far-distance data transmission also developed technically. These developments were primarily funded by the EU before Hungary's accession to the European Union.

On 1 May 2004, Hungary received full membership in the EU. Due to this, the system of border police and in particular, border traffic control changed significantly. The Hungarian-Slovenian, the Hungarian-Austrian and the Hungarian-Slovakian border became internal borders of the EU, although the Hungarian-Austrian border remained the external border of the Schengen Area. The IT systems underwent a great development process, which mainly served the accessibility of the system, so back-up data transmission possibilities and databases were established. The database management system was modernised just like the query display screen. The renewed system was called Border Control and Registration System. Following this, the accession to the Schengen Area came closer, and all IT development activities were performed with this purpose in mind.

SCHENGEN INFORMATION SYSTEM

Hungary became part of the Schengen Area on 22 December 2007. Accordingly, at the Schengen internal borders – at the Slovakian-Hungarian, Austrian-Hungarian, Slovenian-Hungarian borders, border traffic control ceased. At the external borders of the Schengen Area, however, very strict regulations had to be complied with.

Based on the agreement signed on 19 June 1990 on the implementation of the Schengen Agreement, the member states would develop and maintain a joint information system (Schengen Information System – SIS). The Hungarian border traffic control system had to be connected to SIS to meet this expectation. The merge came about following a long professional preparation period both at national and international levels. The SIS enables the authorities appointed by the individual member states to access the warning signals related to persons and objects while performing automated query procedures. SIS also ensures the cooperation of the law enforcement forces and the judicial system in accordance with international law. At the same time, SIS also allows check activities related to border control, domestic police, customs control as well as to issuing visas and residence permits. Neither SIS nor the newly developed SIS I+ were able to serve the new member states joining in 2007, though. With the Regulation (EC) No. 2424/2001[vii], the Council of Europe acknowledged the necessity of the development of a second generation of the system (SIS II), which enables the access of newly joining member states. Its development was, however, procrastinated. When it became obvious that the planned improvement would not be carried out by the original deadline, Portugal came up with an alternative solution to cope with the IT challenges brought about by the accession of the new member states. The idea for the so-called SISone4ALL was that Portugal made the copy of her own individual system (original Portuguese system: N.SIS) available to all new member states free of charge. The Justice and Home Affairs Council accepted Portugal's offer at its meeting on 4-5 December 2006, so in the new member states – like Hungary – fulfilled the necessary IT requirements with its help until the completion of SIS II. The Council Decision of 21 December 2006, No. 2006/1007/JHA stated that the development of SIS II was taking longer than expected and further financial support was necessary for further progress. [viii]

The Portuguese clone was implemented in Hungary by the Central Office for Administrative and Electronic Public Services (KEK KH). The Border Guard Forces started further developments to enable the already applied system HERR (HERR I+) to be suitable to do queries in SISone4ALL and national data pools, to transmit, to receive data with the necessary

contents and forms and to manage and forward messages related to SIRENE and national visa system. It was also crucial to extend and implement the statistics functions and query functions from the registered data.

After Hungary's accession to the Schengen Area, from 1 January 2008, the Border Guard Forces merged with the Police Forces, so now the Police perform the tasks concerning border control.

In SIS, data are managed in the following categories: the data of wanted individuals due to transfer or extradition or based on European or international warrants for arrest of individuals subject to prohibition of entry and stay in the member states of the Schengen Area, of missing persons, of individuals participating in court procedures, of targeted or covertly monitored persons or objects, of wanted documents, vehicles or legally specified other objects serving as subject of confiscation or as evidence.

SIS II began operating on 9 April 2013, which allows the management of biometric data (fingerprints, face recognition), the sharing of information related to new data categories (stolen aircrafts, ships, containers or stocks), the connection of certain actors (e.g. individuals and vehicles as well as the storage and sharing of a copy of European warrants for arrest. The legal background of SIS II was provided by Act CLXXXI of 2012 [ix] on the exchange of information in the framework of the second-generation Schengen Information System and the Government Decree No. 15/2013. (28/I) [x] on the detailed procedures of the exchange of information in the framework of the second-generation Schengen Information System.

VISUM INFORMATION SYSTEM

The Visum Information System (VIS) covering the member states of the Schengen Area was implemented live on 11 October 2011. The purpose of VIS was to improve the implementation of a uniform visa policy, the cooperation of consulates and the consultation quality between the central visa authorities by exchanging data on short-term visas. Based on the Regulation (EC) No. 767/2008/ [xi], the system has been being introduced gradually between 2011 and 2015 distinguishing 23 regions.

VIS is extraordinary because of its modern technology, which allows central storage of fingerprints and face images and the electronic comparison of fingerprints. In practice, at embassies, the data, such as fingerprints and images of visa applicants, are forwarded to the central database operated in Strasbourg. Fingerprints are digitally scanned. Biometric identifiers are stored in the system for 59 months, so if a new visa application occurs within 5 years, the fingerprints do not have do be scanned again. When crossing external borders, the authority of the affected member state checks the genuineness of the visa and the identity of the owner of the VISA, for instance, by comparing the fingerprint scanned on the spot with that stored in VIS.

The new system simplifies the identification of visa applicants, the battle against abuse of visa application and the control activities performed at the external border crossing points and in the member states themselves. The VIS enhances refugee procedures, and it contributes to the prevention of threats affecting the internal security of any member state and by this, it greatly increases the safety of the citizens of the European Union.

EURODAC

In accordance with the Regulation (EC) No. 2725/2000 [xii], the EURODAC system facilitates the application of the Dublin II Regulation, determines which EU Member State is responsible to examine an application for asylum seekers within the European Union. EURODAC makes it possible to establish the personal identity of asylum seekers and individuals arrested for illegally crossing the external borders of the EU. By comparing the fingerprints, the member states can determine, whether the foreign national illegally residing and seeking asylum in one of the member states of the EU has ever sought asylum in any other member state of the EU and whether they have illegally entered the territory of the EU or not. The EURODAC consists of a central unit set up within the Commission with a central database capable of comparing fingerprints and the data transmission network between this database and the individual member states. Each country enters personal data, data concerning asylum seeking and fingerprints. They collect data of everyone over 14 years of age, and forward this information to the central unit by the national access point. The data of all asylum seekers are maintained for 10 years, but if the person in question is granted citizenship in any member state, their data must be immediately eliminated from the database. The data of foreign nationals arrested for illegally crossing the external borders of the EU are maintained for 2 years from the day their fingerprint is scanned. If a foreign national resides in a country illegally, his fingerprints can be compared to those in the central database, and it can be established whether he has sought asylum in any other member state. The fingerprints forwarded for the comparison are not stored after the comparison. As the personal data protection requires, the member states transmitting fingerprints to EURODAC must ensure that the scanning of fingerprint and all procedures connected to the processing, transmission, storage and elimination of the data are carried out in a lawful manner.

ELECTRONIC DOCUMENT MANAGEMENT

In order to prevent and combat the forgery of official documents, the European Union has set up FADO (False and Authentic Documents Online). The database contains the images of genuine and false documents and their data. The system can be accessed by investigators and document experts working for law enforcement forces. In Hungary, official documents are processed and registered in an additional system, as FADO is not available for the executive staff. This database is called NEKOR (National Complex Document Management Database), which contains genuine, false, forged and unreal documents. The system helps to establish the identity of the documents and to discover abuses related to them. In addition, it also plays a role in the training of border guard experts working with documents.

A PRADO (Public Register of Authentic Travel and Identity Documents Online) is a database containing identity and travel documents of individuals. This system is publicly available on the internet. The database is not complete but is continuously updated, which is necessary, as new documents keep being issued.

EUROSUR

EUROSUR (European Border Surveillance System) [xiii] was set in motion on 2 December 2013. The system is expanding and will eventually cover 30 countries. EUROSUR greatly contributes to rescuing those who risk their lives to reach European shores. It also provides good tools for the EU and its member states to prevent transnational crimes – such as drug trade or human trafficking – but also detects and helps small ships carrying migrants having drifted into danger. The backbone of EUROSUR consists of the national coordination centres, in which all national border guard authorities collaborate and harmonise their activities. These national authorities share information on events occurring at land and sea borders, the situation and positions of patrolling officers as well as analysis reports and intelligence data. This cooperation and information exchange allows that the affected member state can respond to any incident related to illegal migration, internal crime or event risking the life of migrants. FRONTEX, the European Agency for the Management of Operational Cooperation at the External Borders, plays an important role in collecting and analysing information from the member states and by this, it contributes to uncovering new routes and new methods applied by criminal organisations. These also contain the information gathered during the joint operations of FRONTEX and the information in the border zones. EUROSUR does not only facilitate more rapid response on the part of the member states when the incidents actually occur but also in critical situations occurring at the external borders.

FRONTEX

FRONTEX (European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union) was established by Regulations (EC) No. 2007/2004 on 26 October[xiv]. It manages the operative cooperation of the members states at the external borders of the EU; it provides the member states with border guard training opportunities as well as with setting up common training standards; it performs risk analysis, monitors the research activity of the control and surveillance activities at external borders; it supports the member states with their technically and operationally challenging situations at external borders; it provides support for the member states in joint return operations. It has separate units organising operations at land, air and sea borders. Upon the request of member states, in urgent cases, it also coordinates the deployment of the European Border Guard Teams, and it also devises operation plans for short-term application. At its headquarters in Warsaw, it has a Situation Centre, which permanently monitors the current state of affairs at the external borders. Within the framework of the European Border Surveillance System (EUROSUR), national and FRONTEX coordination centres have been set up, which have raised the standard of situational awareness and response capabilities to EU level. Its development focuses on extending licenses, organising and financing research and development activities regarding border control. It has begun establishing an information centre in the area of document security.

FRONTEX increases the security of borders by taking the responsibility for the coordination of the independent activities of the member states related to the community measures regarding the management of external borders. It plays a key role in the development of the theory and practice of integrated border management.

EU-LISA

Regulation (EU) No. 1077/2011/EU [xv], EU-LISA (EU Agency for large-scale IT systems) started its operations on 1 December 2012. The headquarters of EU-LISA are located in Tallinn, Estonia, but the tasks related to the operational management of large-scale IT systems is carried out in Strasbourg, France and in the backup site of the agency, in Sankt Johann im Pongau, Austria.

The job of the organisation is to develop and operate the IT systems serving freedom, security and law enforcement within the EU. With its activities, the agency contributes to the reinforcement of the refugee, migration and border management policies of the EU. Respecting basic human rights, the agency operates according to the strictest security and data protection rules. The tasks of EU-LISA is to coordinate the operations of the three most significant IT border managements systems: SIS II, VIS and EURODAC. It is also one of its important assignments to develop future IT system within the EU.

SUMMARY

In this article, I summed up the history of the IT support systems of border control in Hungary, I presented the most important systems applied in the European Union as well as the organisations managing and coordinating these systems and providing their technical background. Considering experience, it can be stated that –as it is the case in other areas of life – the theory and practice of IT systems are increasingly gaining foothold in the area of border protection too. The systems are more and more complex and technically more challenging, but the information provided by them is more multifaceted and accurate. While in the past only data used to be processed as figures and texts, today information in images is much more emphasised. Accordingly, biometric identification, the processing and computational interpretation of fingerprints, palm prints or face recognition play a significant role. In the EUROSUR system, the processing of images taken by various cameras – daylight or night cameras – are also important. It can also be crucial to process the images taken by drones, which is already practised in the EUROSUR [xvi].

Developments, however, have clearly not come to an end yet. EU-LISA has several challenges to cope with: one of these is the development of the Entry Exit System (EES), which facilitates the electronic registration of non-EU citizens entering and exiting the Schengen Area, by which the calculation of their time of residence could be simpler. (It is quite unique that Hungary used to have a similar system available already in the early 1990s.) Another significant task is the development of Registered Traveller Programme (RTP), which does not only categorise individuals by country, but also provides more personalised categories, which assist the authorities in decision-making.

In conclusion, we can state that IT system play a crucial role in maintaining law, order and security in the European Union and the Schengen Area. Today, life would be unimaginable without the support of these systems. Considering the large flow of refugees in recent times, however, we can also see that the issue of illegal migration can only be really and exclusively handled long-term by political and economic measures and by international facilitative assistance programmes of third world countries.

References

[1] [i] http://www.rubicon.hu/magyar/oldalak/1945_februar_4_megkezdodik_a_jaltai_konferencia/ download: 10. May 2015.

[2] [ii] http://history1900s.about.com/od/churchillwinston/a/Iron-Curtain.htm download: 10. May 2015.

[3] [iii] SALLAI János: An Impression of a Bygone Era, The History of the Iron Curtain = Hanns Seidel Foundation 2012 - ISBN 998−973−88484−3−7

[4] [iv] http://nyomaban.blog.hu/2014/08/21/cocom-lista_a_vagyott_nyugat_kereszthuzasai download: 10. May 2015.

[5] [v] PRISZNYÁK Szabolcs: A határforgalom ellenőrzés számítógépes támogatásának történeti áttekintése a kezdetektől Schengenig = Hadtudományi Szemle 4. évfolyam 4. szám, Nemzeti Közszolgálati Egyetem Budapest 2011., pp. 172-181 - ISSN 2060-0437

[6] [vi] 1999. évi LXXV törvény A szervezett bűnözés, valamint az azzal összefüggő egyes jelenségek elleni fellépés szabályairól és az ehhez kapcsolódó törvénymódosításokról

[7] [vii] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R2424&from=HU download: 10. May 2015.

[8] [viii] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006D1007R(01)&from=HU download: 10. May 2015.

[9] [ix]http://njt.hu/cgi_bin/njt_doc.cgi?docid=156598.291634 download: 12. May 2015.

[10] [x] http://njt.hu/cgi_bin/njt_doc.cgi?docid=158609.252717 download: 12. May 2015.

[11] [xi]http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0767&from=HU download: 12. May 2015.

[12] [xii]http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000R2725&from=HU download: 12. May 2015.

[13] [xiii]http://ec.europa.eu/dgs/home-affairs/e-library/docs/infographics/EUROSUR/EUROSUR_en.pdf download: 12 May 2015.

[14] [xiv] http://FRONTEX.europa.eu/assets/About_FRONTEX/FRONTEX_regulation_en.pdf download: 12. May 2015.

[15] [xv] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011R1077&from=HU download: 12. May 2015.

[16] [xvi] NYÁRI Éva: Technoligies, technical devices and equipment used in bordercontroll procedures, their developments in Schengen region = Hadtudományi Szemle 7. évfolyam 1. szám, Nemzeti Közszolgálati Egyetem Budapest 2014., pp. 201-210 - ISSN 2060-0437