



## Paint IT Fall

This is our Next IT STAR Newsletter and we proudly announce our new members of the Advisory Board from Germany, Russia, and Spain on board to provide further assurances of the growing interest in our publication!

The Fall issue will

- Take you through a developing project with a bottom-up approach on digital transformation of mature SME businesses
- Lead you further within the building blocks of the Slovak information security strategy
- Brief you about a unique national scientific society that precedes the nationhood of its country, with an extensive ICT research capacity nowadays, and
- Reward you with a visit to an important place of pilgrimage for Catholics in Central Europe and a paradise for mountain lovers.

It's all here!

Take the Journey!

Plamen Nedkov

## IT STAR representatives

**Austria**/OCG-R. Bieber, **Bulgaria**/BAS- I. Dimov, **Croatia**/CITA-M. Frkovic, **Cyprus**/CCS-P. Masouras, **Czech Rep.**/CSKI-J. Stuller, **Greece**/GCS-S. Katsikas, **Hungary**/NJSZT-B. Domolki, **Italy**/AICA-G. Occhini, **Lithuania**/LIKS-E. Telešius, **Macedonia**/MASIT-P. Indovski, **Poland**/PIPS-M. Holynski, **Romania**/ATIC-V. Baltac, **Serbia**/JISA-D. Dukic, **Slovakia**/SSCS-I. Privara, **Slovenia**/SSI-N. Schlamberger

## Contents

New members of the Advisory Board .....	3
Digital transformation .....	3
Information security in Slovakia.....	6
Olympiads in Informatics .....	11
Focus – BAS.....	12
MS News & Events.....	13
MultiCulti – Mariazell .....	14
IT STAR Snapshot .....	15
Member Societies .....	16

## Editor

P. Nedkov, Halsriegelstraße 55

A-2500 Baden, Austria

e-mail: [info@starbus.org](mailto:info@starbus.org), web-site: [nl.starbus.org](http://nl.starbus.org)

## Time to Fly



## Partner Publication



<http://mondodigitale.aicanet.net/ultimo/index.xml>

## ADVISORY BOARD

Ana Pont Sanjuan, Spain  
Angel Alvarez, Spain  
Ashley Goldsworthy, Australia  
Augusto Casaca, Portugal  
Blagovest Sendov, Bulgaria  
Cene Bavec, Slovenia  
Dudley Dolan, Ireland  
Giorgio Ausiello, Italy  
Giulio Occhini, Italy  
Irena Lasiecka, Poland/USA  
John Atanasoff II, USA  
Martin Przewloka, Germany  
Vladimir Kitov, Russia

*Ex officio:* IT STAR MS representatives (see page 1)

## EDITORIAL POLICY

This Newsletter maintains a world-class standard in providing researched material on ICT and Information Society activities from the perspective of Central, Eastern and Southern Europe (CESE) within a global context. It facilitates the information and communication flow within the region and internationally by supporting a recognized platform and networking media and thus enhancing the visibility and activities of the IT STAR Association.

The stakeholders whose interests this newspaper is addressing are

- IT STAR member societies and members
- ICT professionals, practitioners and institutions across the broad range of activities related to ICTs in government, business, academia and the public sector in general
- International organizations

Individual articles from the Newsletter may be re-printed, translated, and reproduced, except for denoted copyright protected material, provided that acknowledgement of the source is made. In all cases, please apply for permission to the Newsletter Editor.

Special arrangements for the production and circulation of the Newsletter could be negotiated.

The newsletter is circulated to leading CESE ICT societies and professionals, as well as to other societies and IT professionals internationally. Everyone interested in CESE developments and working in the ICT field is welcome to contribute with original material. Proposals for articles and material for the Newsletter should be sent two months before the publication date to [info@starbus.org](mailto:info@starbus.org).

## New Members – Honorary Advisory Board

*We are pleased to announce the following new members of the Newsletter's Advisory Board:*



**Ana Pont Sanjuan** is full professor of Computer Architecture at the Universitat Politècnica de València (UPV), Spain.

Between 1998 and 2004 Ana was head of the Computer Science High School at the UPV. Her research interest includes web and internet architecture. Ana is the Span-

ish representative to IFIP TC6.



**Martin Przewloka** is chief digital officer (CDO) responsible for the innovation management of msg systems AG, Munich, Germany.

Prof. Dr. Przewloka has more than 20 years of experience in the successful development, launch and scale-up of digital technologies. His special technical and scientific interests lie in

the field of digital assistance systems, sensor technologies, smart data and artificial intelligence.



**Vladimir Kitov** is professor of computer science at the Moscow Plekhanov University of Economics. He served as senior manager at DEC, Siemens Nixdorf and Fujitsu. He is permanent member of the Advisory Board of the Russian Virtual Computer Museum.

## Bottom-up digital transformation of mature SME businesses – first results

*Martin Przewloka, Justus Liebig University Giessen – Germany and Technische Hochschule Mittelhessen – Germany*

### Introduction

The author has developed a new methodology and best practices for initiating and implementing digital transformation processes in small and medium-sized enterprises (SMEs). The essential building blocks of this bottom-up method are a significant shift in responsibility towards the executive units in companies, the reduction of hierarchies, the use and integration of different skills and experiences (diversification), and the willingness to increase the level of risk.

This method has now been applied to various companies. In this article the results of two transformation projects are presented and discussed. Furthermore, the typical problem areas, which can be identified from the gained experience, are presented and illustrated how they can be mitigated.

### Basic principles of the new methodology

The newly developed and successfully applied methodology is based on the following basic principles<sup>1</sup>:

- the customer is at the center,
- avoidance of any complexity,
- digital Leadership must be distributed to all employees and each employee takes over this new responsibility,
- sharing knowledge and experiences with others using digital media has to be self-evident,
- adoption of collective decision-making skills and an expanded willingness to assume responsibility to execute and change,
- the (digital) integration of processes and the standardization of products or product components is imperative.

### The special importance of service transformations

One goal of applying the new bottom-up method was to foster service transformations. This includes the expansion of physical products through services or their complete replacement. It is only through the use of the special possibilities of information technology that these transformations become possible, in particular the extension

<sup>1</sup> See *Martin Przewloka* "Successful Digital Transformation for Mature SME Businesses" pp 51-55 in *IT Security – Proceedings of the 10<sup>th</sup> IT STAR Workshop on IT Security*, Eds. P. Nedkov, G. Mastronardi & P. Schgör, ISBN 978-88-98091-45-4, and slide presentation at <http://starbus.org/ws10>



of business fields and business models.

Three service variants can be distinguished<sup>2</sup>:

1. In the following so-called Integrated Digital Services (IDS) services are an integral part of a manufactured product and are generally made available to the customers at no extra cost. They increase the value of the solutions offered by the provider and can also be developed to a Unique Selling Point (USP).
2. Add-On Digital Services (ADS) are offered as digital extensions for manufactured products and generate additional charging fees. As a rule, the product characteristics will be extended by these additional services. As a consequence, these services can lead to an additional USP and significantly strengthen the supplier's competitive position..
3. Purely Digital Services (PDS) provide digital services, which are independent of, or a substitute for, the manufactured product. The importance of the physical product disappears completely<sup>3</sup> or at least partially. The value of the solution is calculated exclusively by the quality and value of this type of digital services.

#### ***First results: The concrete adoption of the new methodology***

The digital transformation bottom-up method has been successfully applied several times. The following case study explains the application of the method.

A very successful German SME offers extensive technical services. This includes for example carrying out the complete electrical installations as well as the end-to-end implementation of heating and cooling systems for large industry buildings. The implementation of these technical services is project-based, i.e. accurate planning, perfect organization, execution and costing are essential components for achieving a profitable business. Even this SME is actually very successful on the market, but the management faces fundamental challenges that can be classified as follows:

- High competitive pressure due to strong price hikes from foreign companies, which also enter the German market
- An increased shift from large-scale projects to more

2 Kloetzner, H./Przewloka, M.: „Studienbasierte Entwicklung eines Frameworks zur Ableitung von Strategieempfehlungen Digitaler Service Transformationen für produzierende Unternehmen“ in: Angewandte Forschung in der Wirtschaftsinformatik – Die Transformation gestalten; Publ. Barton, T./ Herrmann, F./ Meister, V.G./Müller, Chr./Seel, Chr., mana-Buch, P. 71 -79 (2017)

3 At least, the physical product is no longer placed in the foreground of any marketing or sales activity.

and more small projects. The administrative cost (fix cost) for each project also reduces the operational margin

- The dramatic shortcomings. The scaling of the existing business model is fundamentally dependent on the availability of technical, well-trained specialists. Here, too, the company is competing for filling vacancies against countless companies, also from other industry sectors
- The step-by-step (digitization) technology. This field challenges many SME's because there is often not enough time for training and development to keep up with these new technologies<sup>4</sup>
- The non-existence of continuous, predictable and secure revenue streams.

It was decided to use the existing knowledge in the company as the essential basis for the development of a future-oriented (digital) company. Initiated by the top management of the company, teams were formed across all departments. Service transformations have been set as the guiding principle related to new business models to be developed. Following the new methodology, the diverse teams proceeded as follows:

- Identification of strengths, weaknesses and future challenges from today's viewpoint
- The present and future view of the customer – “which types of new services would make the life of a customer much easier?”
- The investigation of the competitiveness of the SME (today and in future)
- The analysis of the key customer-centered processes (e.g. time to respond on customer inquiries)
- The internal processes and the investigation of the burden and complexity of internal administrative processes
- Today's adaptation of (digital) technologies
- The recognition of growth areas, focus service transformations
- The view on the personnel development
- The identification of USP's and quick wins
- The identification of disruptive solutions focusing on service transformations
- The balancing of opportunities and risks
- The development of concrete recommendations for action

These interdisciplinary teams quickly recognized the problem of today's concentration of exclusive concentration on the execution and charging of technical craftsmanship. In addition, complex internal processes bind a large amount of administrative resources, slow down the process of invoicing, with the consequence that the margin is additionally reduced.

4 As an example: the technology areas of augmented and virtual realities (AR/VR) has been identified as very promising for this SME, but the daily workload and the shortage of resources doesn't allow to deal with it intensively enough.

As a consequence, one sub-team concentrated on the reduction of complexity in internal processes, while the other team developed (disruptive) ideas for service transformations. It quickly became clear that the current and future structures of the company do not allow the development of PDS. Therefore, attention was focused on the development of ADS to solve the above problems.

More concretely and as an example, the development of a service called “digital twin for craft services” was invented. This is the exact, digital copy of all the works carried out by the SME. All related data is provided to the customer as a digital service. The customer is thus able to find exactly the power and water lines that are no longer visible, to plan and implement extensions of the installation more easily, but also to carry out simulations and the like. These services are additionally offered in form of an ADS and represent a direct added value for the customer. Pricing in the form of a so called Freemium<sup>5</sup> model makes it very attractive for the customer to enter into this new service model.

Followed by an extended SWOT analysis, the findings were presented a decision board. The board decided positively on several recommendations and initiated the setup of small and agile project teams to develop the ideas further and to finally execute. The complexity reduction in the area of administrative processes was executed immediately with significant success. The expansion of the service portfolio by the development and implementation of IDS and ADS has been started as well but requires significant more time.

### ***Learnings***

To date, a total of 6 transformation projects have been carried out according to this new methodology. The company's sizes ranged from 1,000 to 4,000 employees, sales of € 100 million to € 700 million per year. All companies were in an excellent economic situation with healthy growth figures.

It was common to all projects:

- The identification of weak points with regard to a promising product and solution portfolio succeeded very quickly in all projects
- The identification of weak points in the internal and customer centric processes also succeeded very quickly. This is precisely where the most direct approaches to digital technologies were found, on the one hand, to increase efficiency and, on the other, to drastically reduce the complexity of today's processes
- Today's presence of digital services is not existing or very weak. The philosophies of all 6 companies are still product or hardware centric

<sup>5</sup> Freemium = Free + Premium. This means, the basic service is free of charge, premium services will be charged per use or regularly.

- The development of ideas for IDS and ADS is comparatively easy. However, the development of proposals for PDS, on the other hand, has been inadequate. To be more successful to develop PDS, it requires a lot of external impulses. It became clear that a team without external input is hardly able to develop PDS.
- Since IDS are normally associated with the existing business models and no additional revenue sources are generated, the implementation of these types of services is also comparatively simple. In contrast to this, it is more difficult to generate new revenue models based on ADS. It is also important to note that external support is required to validate implementation variants.
- The necessary risk assessment of all service types shows that PDS have not only the highest risk, but that due to the disruptiveness, considerable change management efforts will be required in case of execution. This is one of the reasons for the fact that the PDS risks are often judged to be too high. The experience for alternative implementation variants such as the implementation in a company spin-off in order to keep the risks for the parent company comparatively manageable is hardly possible.

After applying the bottom-up method, all 6 companies have started transformation projects. All projects are more cautious rather than disruptive. However, it has become clear that the developed bottom-up method has been essential for the development and implementation of these projects. Without the involvement and the direct assumption of responsibilities of the various teams, none of these projects would have been launched.

### ***Conclusion***

Digital transformation for SME's requires new approaches and new ways of execution. The proposed bottom-up methodology has shown its significant potential as it has been applied at 6 companies very successfully.

The transfer of responsibility to heterogeneous teams was a decisive success factor to develop new, customer-oriented service models. At the same time, internal and external business processes were examined with regard to complexity reduction and digitized in parts. It was found that especially in the digitization of the business processes a very fast implementation success can be realized (quick win). The development of purely digital services (PDS) which can reduce the existing product offer or even replace it, has only been successful in parts. The risks are (still) considered as too high. In addition, external advisory support is required in this area.

■

## Information security in Slovakia - from concepts to implementation <sup>1</sup>

Daniel Olejár



**Daniel Olejár** is Vice-Rector of Comenius University, Bratislava and lectures on discrete mathematics, mathematical logic, set theory, computability theory, computer architectures, coding theory, combinatorics, cryptology and IS.

### Abstract

*The paper deals with the development and problems of information security (InfoSec) in Slovakia. It shortly describes the period of a nonsystematic development of InfoSec (1992-2007) and concentrates on the period from 2008 to present days. The Slovak Government in 2008 approved National strategy for information security and Action plans for its implementation. The paper briefly analyzes the goals, which the Strategy has been settled and what Slovakia has done to fulfill the set tasks. The raising InfoSec awareness and the European legislation are changing the attitude to InfoSec. The state engagement in InfoSec is growing. The paper discusses the last development (the change of competencies, InfoSec and/or cyber security in state strategic programs) and perspectives for the future.*

### Introduction

The human society depends on its information and communication technologies (ICT). Modern ICT present critical infrastructure of our society, they are very powerful, but vulnerable, too. Moreover, the failure of a large information system, computer network or computer based control system can cause a large or even global catastrophe. There is no alternative to modern ICT available today and therefore the sufficient level of information security is a necessary condition of the future development of our (information) society. Information security is a multidiscipline area, covering selected areas of mathematics, computer science, management, psychology, law and other disciplines. Ensuring adequate protection of various individual systems, of the national ICT infrastructure as a whole and participating in the protection of the global virtual space is a very difficult task of a complex nature. We will describe the development of information security (InfoSec) in Slovakia, the current problems and the perspectives for the future.

### The prehistoric period - perceiving the need for InfoSec

The history of information security in Slovakia takes about 25 years. During these years InfoSec passed three different stages of development. The first one (1992-2000) was from the InfoSec point of view “pre-historic”, the second (2000-2007) is characterized by growing InfoSec awareness and the third (since 2008) is the period of growing state engagement and attempts to solve the InfoSec systematically.

During the first period Slovakia (i.e. state institutions, schools and private sector) concentrated primarily on building ICT infrastructure. The information security awareness was low (more precise, zero), the functionality of ICT was (for their owners and users) more important than their security. Nevertheless, the occurrence of malware, sporadic attacks on computer systems and other forms of computer crimes spoiled the idyllic picture of information society.

The state traditionally protected selected kinds of information (classified, sensitive, personal) and recognized the necessity to extend the protection from the paper world to virtual space. Even in the nineties the existing laws in Slovakia reflected the role of computers in information processing and the state generalized its security requirements on information protection (confidentiality, integrity, availability).

People from the private sector and universities played a very active role in InfoSec in this prehistoric period. In the early nineties some young enthusiasts founded the first Slovak CERT, but the response from state and industry was minimal and without financial and logistic support CERT's activities terminated soon. The lack of qualified specialists in InfoSec motivated the small, but active community to various activities: their members organized regular seminars, conferences, CISA exams, they included cryptology and information security into university computer science curricula, provided expertise for state institutions; transferred ISO standards into Slovak technical standards system, etc. In the end of the nineties two professional organizations were created – SASIB (Slovak association for information security) and ISACA Chapter Slovakia. InfoSec became a topic of Slovak computer science society, too.

Industry adopted a hesitating attitude to InfoSec; the ICT companies recognized the need for InfoSec, but the market demand was too low. Two kind of commercial subjects were able to do business in InfoSec in these years: auditors and other InfoSec experts operating individually, in small companies or as employees of consulting companies and companies with stable contracts with banks or state institutions. The important exemption presented Eset, antimalware company with its own research and successful product, established in 1992.

<sup>1</sup> This paper was first published in IT Security, Proceedings of the 10th IT STAR Workshop on IT Security, Eds. P. Nedkov, G. Mastronardi & P. Schgöör, ISBN 978-88-98091-45-4

The prehistoric period ended symbolically on January 1<sup>st</sup>, 2000. The medialized problem of year 2000 (2K problem) attracted public attention and forced companies and state institutions to realize the potential impact of their systems failure and the need for InfoSec.

### **Raising InfoSec awareness**

The second period in the history of information security in Slovakia spans the years 2000-2007. At the beginning of a new millennium Slovakia was preparing to join the European Union. It had to adapt its legislation to European law and to participate in European initiatives and programs, too. Slovakia adopted new and amended some existing laws. Three of them have played an important role in raising the level of InfoSec awareness: Personal data protection act (adopted in 2002), Electronic signature law (2002) and Public administration information systems act (2006).

Personal data protection act covered a large number of systems (in private and public sector) and defined strict requirements on personal data processing and use, including security projects and information security management based on risk analysis.

Electronic signature law was even more promising, since electronic signature was considered one of the necessary conditions of e-Commerce and e-Government. The Act introduced into Slovak legislation electronic (digital) signatures, the concepts and basic rules of Public key infrastructure (PKI) and became a base for more detailed technical and administrative standards. Slovak National security authority<sup>2</sup> enlarged its competency and it became the main body of state administration responsible for electronic signatures. Expecting large e-Commerce boom, the industry built several certification authorities, but the lack of suitable applications of electronic signatures delayed the advent of mass e-Commerce and slowed down the development of PKI. Nevertheless, PKI and electronic signatures attracted attention of both commerce and academic sectors and resulted (at least) in the development of know-how; the numbers of people with theoretical knowledge (cryptography, InfoSec and PKI) and with practical experience (in the implementation of PKI or the provision of certification services) increased significantly.

The public administration information systems (ISVS in Slovak) act contains<sup>3</sup> three simple requirements: the owner of the system must

- Ensure continuous, secure and safe operation of the system,
- Protect the system,
- Run the system in compliance with standards.

The Ministry of finance (which has been responsible for

<sup>2</sup> Národný bezpečnostný úrad, NBÚ

<sup>3</sup> the act is still valid

informatization of Slovakia) issued mandatory standards, containing detailed information security standards. The first version was a little bit chaotic list of isolated requirements, but the later security standards for ISVS have been based on ISO/IEC 27000 series of standards and required continuous and complex protection of ISVSs, including risk analysis, audit, security policies and finally the introduction of Information security management system.

At the end of the second period the basic technical ICT infrastructure (in Slovakia) was completed, informatics (at a user level) became a standard component of elementary and secondary school curricula and a significant part of the middle-aged and elderly generation was forced by circumstances to gain necessary computer literacy. Users discovered the dark side of virtual space (mostly malware incidents) but the general level of InfoSec awareness remained low.

Despite the adopted laws and partial initiatives (Lisbon Strategy, e-Europe+ and e-Europe) the protection of Slovak virtual space remained fragmented and uncoordinated.

During this period Eset became one of the global IT security companies developing leading-edge security solutions against cyber threats. Besides Certification authorities specialized in certification service providing, InfoSec became an object of commercial interests and many ICT companies introduced InfoSec solutions into their portfolio. Most of state institutions and private companies recognized the relevance and the need for InfoSec, but insufficient resources and particularly the lack of qualified specialists were the main reasons of a low level of InfoSec in Slovakia at the end of this period.

### **OPIS and the National InfoSec strategy**

The main stimulus for systematic development of information security at a national level provided European Operational program informatization of society (Slovak abbr. OPIS), launched in 2007. To administrate the Program, the Ministry of Finance (the control body for OPIS was the Government Office of the Slovak Republic), created several advisory bodies and working groups and engaged external experts for cooperation. One of such advisory bodies was a Commission for Information security. The Commission spent a lot of time in discussions on various particular problems and their members recognized very soon the need for a complex solution. The National information security strategy (Strategy) was created in 2007/8 and was approved by Slovak Government in 2008. The authors of the Strategy utilized the experience of the most developed countries; the comprehensive knowledge of the development and the current state of InfoSec in Slovakia; they identified the main problems and proposed solutions. The Strategy set three strategic goals for building InfoSec at the national level:



1. **Prevention.** The owners of particular systems and state institutions responsible for information security (responsible subjects) ought to know the vulnerabilities of systems belonging to their domain, relevant threats and risks following from vulnerabilities of assets and relevant threats, they ought to be able to assess the risks and to introduce, to maintain and to review the adequate measures mitigating or eliminating the identified risks.
2. **Preparedness.** The responsible subjects ought to be able to detect a developing security incident as soon as possible, to stop its development, to minimize its negative impact, to ensure the continuity of operations and to manage the recovery of the affected system or asset.
3. **The sustainable level of InfoSec.** The responsible subject ought to develop their know-how to be able to protect their systems against new threats and ought to review the security of their systems to maintain the adequate level of their protection.

To reach the above mentioned strategic goals the Strategy defined seven strategic priorities:

1. Protection of human rights in activities concerning virtual space.
2. Rising security awareness and building competence in InfoSec
3. Creating secure environment
4. Introduction of effective InfoSec management
5. Protection of the state ICT infrastructure and the ICT infrastructure supporting the state critical infrastructure
6. Cooperation at the national and international levels
7. Improvement of national InfoSec competence (the support of scientific research, creating and introducing the system of education in InfoSec and the preparation of experts).

During the next six years the Ministry of finance initiated, organized or sponsored various activities aimed at tasks defined in the Strategy. The most important of them were

1. Creation and long term support of CSIRT.SK,
2. Elaboration of the system of InfoSec education,
3. Elaboration of the InfoSec terminology,
4. Creating and implementing security standards for ISVS based on ISO/IEC series 27000,
5. Preparing the Information Security Act (it remained in the form of draft)
6. Pilot project in InfoSec education.

The Slovak legislation in this period has marked two new important laws; the Critical infrastructure act (2011) and the e-Government act (2013). The first one stressed the importance of ICT and identifies a part of critical information

infrastructure<sup>4</sup>, but did not solve the systematic critical information infrastructure protection. The second act defines conditions, requirements and processes enabling to grant electronic documents the same legal value as in the case of classic paper documents. The act deals with identification and authentication of persons, integrity and authenticity of documents, non-repudiation of origin and receipt and other important security issues.

Education and building know-how in InfoSec have reached a higher level; Slovak technical university (STU) introduced a special study program devoted to cryptology and Comenius University (and STU, too) provided the specialization in information security in the frame of computer science programs. Comenius University, Slovak technical university and the company Eset signed a memorandum on cooperation in InfoSec and created a common research laboratory.

### Information security and/or Cyber security

The Strategy and the Action plans were originally designed for a five-year period (2009-2013). Then the Strategy ought to be reviewed and the Action plans ought to be modified and/or updated. It did not happen. OPIS (gently speaking) was not a very successful program and the enthusiasm for informatization at the Ministry of Finance gradually faded. When the key persons left the Ministry and the support for InfoSec dropped to minimum, the Ministry was not able to continue its activities in InfoSec and to perform the tasks of the Action plan. The Government Office took over some powers in informatization from the Ministry of finance and the National security authority became the state body responsible for cyber security (2015).

The old question – information security or cyber security – was once again opened. The Strategy considered information as a key asset and the protection of information as its main task. Since the failure of infrastructure can threaten the integrity, authenticity, availability or confidentiality of information, InfoSec includes the protection of the infrastructure, too. The Cyber security concept<sup>5</sup>, adopted by Slovak Government in 2015 defined *cyber security as a set of legal, organizational, and technical measures for ensuring the protection of cyberspace, and cyberspace as a virtual space without borders, composed from global, interconnected networks, hardware, software and data*. The Cyber security concept is a political document and the definitions are broad but a little bit vague. Though there are many other definitions of cyberspace and cybersecurity,

<sup>4</sup> The Act applied a sector approach. This approach is not suitable for critical information infrastructure, which elements belong to various sectors. The sector approach enable to discover the critical information infrastructure elements/systems only in the finance and banking sector, the other critical information systems were hidden in or behind technological or industry systems.

<sup>5</sup> The general main tasks formulated in the Concept were elaborated in the Action plan for the implementation of the Concept, adopted by Slovak Government in 2016.[3]



from practical point of view the society needs to ensure the correct and safe operation of its information and communication infrastructure and therefore the protection (whether provided under InfoSec or cyber security flag) must include infrastructure, data which are processed by this infrastructure and its environment, since the failure of every component (infrastructure, data, environment) can threaten the functioning of the whole ICT system, consequently the data processing and providing services. Despite the formal difference between InfoSec and cyber security in Cyber security concept, the Cyber security concept defines 7 main tasks covering the same or similar problems as were identified by Strategy.

#### 1. Creating institutional framework for cyber security governance

Attaining the adequate level of cyber security requires cooperation of various institutions and organizations. The competencies of state institutions, the rights and obligations of private subject are to be defined. The set of CSIRTs at various levels will be created. Some of the tasks National security authority (Slovak abbr. NBU) is already a state body responsible for cyber security and it has created the Commission for cyber security

#### 2. Creating legislative framework for cyber security

The key element of the cyber security legal framework will be the Cyber security act. This act is in preparation and utilizes the advanced draft of InfoSec Act written at the Ministry of finance. The act is crucial for the implementation of the Concept, since it will specify the rights and obligations of state institutions and other subjects participating in cyber security governance, particularly it will define subjects responsible for tasks presented in the EU Directive 2016/1148<sup>6</sup>. The act will also introduce security classification of information and ICT systems, it will define categorization of systems and sets of mandatory security measures, unify InfoSec and cyber security terminology, etc.

The Act will certainly open many questions which will require more detailed elaboration. This will be the task of the NBU and the Commission for cyber security.

#### 3. Cyber security management

The Concept distinguishes two levels of cyber security management, global, dealing with the cyber security at a national level and local, dealing with the cyber security at a level of organization or a system. The Concept concentrate on the cyber security management at the global level and set the following tasks: elaboration of

a risk assessment methodology, building a system of early warning, coordination and cooperation in protection of the critical ICT systems, elaboration and implementation of classification schema and the minimal sets of security measures. At the local cyber security management level the Concept requires the implementation of measures, business continuity planning, regular risk assessment and stresses the need of penetration testing of critical ICT systems.

#### 4. Creating, introducing and supporting the system of cyber security education and training

The education in cyber security would cover large groups of people (pupils of elementary schools, students of secondary schools, teachers, soldiers, judges, lawyers, police officers, etc.) Most of them will need only an elementary knowledge and basic skills in cyber security and the key problem is how to manage the training of such mass of people. A multilevel system (experts, trainers of trainers, trainers, "students") combined with e-learning ad supported by publicly available textbooks can be the solution. The educational pilot project of the Ministry of finance followed several goals and yielded results, which can be immediately used in the system of cyber security education: methodology of education, classification of users, knowledge requirements for different roles, curricula, textbooks and practical experience in organizing the education of large number of adults with different knowledge and needs.

#### 5. Risk management and communication

#### 6. Governmental bodies and other subjects would create CSIRTs; these CSIRTs shall communicate and cooperate. A secure communication channel and a system for security incident announcement shall be created.

The last two tasks do not need an explanation:

#### 7. Active international cooperation

#### 8. The support of scientific research in cyber security

The strategic priorities of the Strategy and the main tasks of the Concept are similar (except for the human rights protection, which was not mentioned in the Concept). The Concept recognized the same main problems as the Strategy has identified and took the work in InfoSec/cyber security again.

### Conclusions

In the early nineties a small group of enthusiasts from IT companies and universities in Slovakia found out the risks emerging from the growing dependence of society on in-

<sup>6</sup> DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

formation and communication technologies. They laid foundations of information security in Slovakia, raised the security awareness of the state administration, developed know-how, prepared standards and even laws.

The state administration dealt with special information security problems (the protection of classified information, personal data protection, electronic signatures, telecommunication security, etc.) and there was no state institution responsible for information security of Slovakia. The first attempt for a comprehensive solution (the National strategy for information security) appeared in 2008. The Strategy defined reasonable goals, but did not gain the broader support of state institutions and the private sector and did not reach the stated goals. A new initiative (the Cyber protection concept) appeared 6 years later. Despite the different terminology the Concept uses and elaborates the ideas of the Strategy. The main difference between the Strategy and the Concept are following. The Strategy defined the tasks as recommendations and the Concept set mandatory requirements; the Strategy did not define an organizational structure able to force the stated requirements and recommendations; the Concept defines explicitly the structure of bodies and executive units dealing with cyber security issues. The Strategy assumed that the Information security act could define or redefine competencies of state bodies and institutions in information security and establish an Information security authority. Though the Information security act was almost completed, but it was not formally processed. The Concept appeared in more favorable conditions; the level of information security awareness is much higher than it was 6 years before, NBU was already explicitly defined as a state body responsible for cyber security, the roles defined in the Conception can be affirmed in the cyber security act, which can be completed very quickly, using the draft of information security act and the newest European legislation.

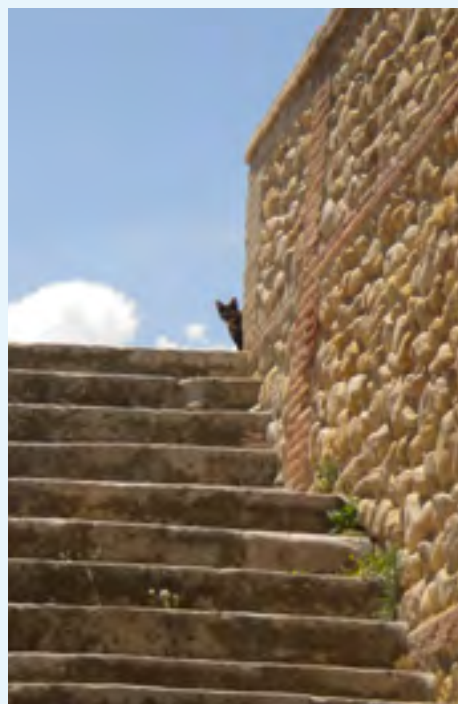
The Concept has set very ambitious goals and it will be interesting to know how the tasks defined in the Action plan will be completed.

## References

Národná stratégia pre informačnú bezpečnosť v Slovenskej republike [www.informatizacia.sk/ext\\_dok-narodna\\_strategia\\_pre\\_ib](http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib)

Koncepcia kybernetickej bezpečnosti Slovenskej Republiky naroky 2015-2020 [http://www.nbusr.sk/ipublisher/files/nbusr.sk/kyberneticka\\_bezpecnost/koncepcia\\_kybernetickej\\_bezpecnosti\\_sr\\_na\\_roky\\_2015-2020.pdf](http://www.nbusr.sk/ipublisher/files/nbusr.sk/kyberneticka_bezpecnost/koncepcia_kybernetickej_bezpecnosti_sr_na_roky_2015-2020.pdf)

Akčný plan realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky naroky 2015-2020 [http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-197723?prefixFile=m\\_](http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-197723?prefixFile=m_) ■



**Curious in the IT STAR scene?**

**This is your place to promote your projects,  
services and products.**

**We will help you reach the ICT specialists of  
Central, Eastern and Southern Europe and  
beyond.**

**To advertise in the NL and at [www.starbus.org](http://www.starbus.org)  
contact [info@starbus.org](mailto:info@starbus.org)**



## Olympiads in Informatics



**B**alkan Olympiad In Informatics, 2 – 8 July 2017, Chisinau, Moldova

<http://www.boi2017.md/>

Participants – teams from 12 countries:

*Bosnia and Herzegovina*  
*Bulgaria*  
*Cyprus*  
*Greece*  
*Italy*  
*Macedonia*  
*Moldova*  
*Montenegro*  
*Romania*  
*Serbia*  
*Slovenia*  
*Turkey*

The following participants were awarded Gold medals:

1	Alex Tatomir	Romania
2	George Chichirim	Romania
3	Radoslav Dimitrov	Bulgaria
4	Gabriel Cojocaru	Moldova



<http://ioi2017.org/>



Teams from 84 countries took part in the annual IOI Competition in Teheran, held from July 28 to August 4, 2017.

The Iranian government extended full support for the organization of IOI 2017.



*Dr. Sorena Sattari, Vice President of Iran for Science and Technology, at Closing Ceremony*

At the closing, 76 contestants were awarded with the Bronze medal, 54 contestants with the Silver medal, and 25 contestants with the Gold Medal.

The results and ranking are available at <http://scoreboard.ioi2017.org/Ranking.html>. Yuta Takaya, from Japan, came first in IOI 2017, followed by representatives of Mingkuan XU (China) and Zhezeng Luo (US).

The first 5 best performing participants from countries in the IT STAR region were ranked as follows:

Rank	Name	Country
7	Encho Mishinev	Bulgaria
11	S. Constantin-Buliga	Romania
12	Mariusz Trela	Poland
14	Attila Gaspar	Hungary
15	Tamio-Vesa Nakajima	Romania

During the formal closing of the event, Iran passed the IOI flag to Japan, the next host of IOI 2018. ■



## Focus



**B**ulgarian Academy of Sciences (BAS) - Host of IT STAR's WS and BM, 29 September 2017

BAS was founded in September 1869 in Braila as the Bulgarian Learned Society.

Its mission is to promote scientific research for the enhancement of the country's intellectual and material wealth in conformity of universal values and national interests.

The Academy is governed by its General Assembly, Executive Council and Consultative Scientific Councils. The Executive arm of BAS is its Presidency consisting of the BAS President, currently Prof. Julian Revalski, three Vice-Presidents, the Scientific Secretary General and eight Scientific Secretaries.

Its institutes and other research units are grouped within the following research areas:

- [Information and Communication Sciences and Technologies](#)
- [Energy Resources and Energy Efficiency](#)
- [Nanosciences, New Materials and Technologies](#)
- [Biomedicine and Quality of Life](#)
- [Biodiversity, Bioresources and Ecology](#)
- [Climate Change, Risks and Natural Resources](#)
- [Astronomy, Space Research and Technologies](#)
- [Cultural-Historical Heritage and National Identity](#)
- [Man and Society](#)

In the ICT field, the following research units are in operation:

- [Institute of Mathematics and Informatics](#)
- [Institute of Mechanics](#)
- [Institute of Robotics](#)
- [Institute of Information and Communication Technologies](#)
- [National Laboratory of Computer Virology](#)
- [Laboratory of Telematics](#)

The Institute of Information and Communication Technologies (IICT) is IT STAR's focal point at BAS. It covers the

following areas:

- [Parallel Algorithms](#)
- [Scientific Computations](#)
- [Mathematical Methods for Sensor Data Processing](#)
- [Linguistic Modelling and Knowledge Processing](#)
- [Information Technologies for Security](#)
- [Grid Technologies and Applications](#)
- [Modelling and Optimization](#)
- [Information Processes and Decision Support Systems](#)
- [Intelligent systems](#)
- [Embedded Intelligent Technologies](#)
- [Communication Systems and Services](#)
- [Hierarchical Systems](#)

BAS is a member of IT STAR since 2003. The focal point for IT STAR activities within the Academy is the Institute of Information and Communication Technologies.

### Key reference officers for IT STAR

#### **Julian Revalski**



Before his election as President of BAS, **Julian Revalski** was Director of the Institute of Mathematics and Informatics (IMI). He is Professor and Doctor of Mathematical Sciences, and Academician (full member) of BAS.

#### **Ivan Dimov**



**Prof. Ivan Dimov** replaced Acad. Kiril Boyanov as representative to IT STAR in 2015. Ivan chairs the Scientific Council of the Institute for ICT, and currently serves as Vice-Minister for Science at the Ministry of Education and Science.

#### **Kiril Boyanov**



**Academician Kiril Boyanov** is Member of the Bulgarian Academy of Sciences. He was the first BAS representative to IT STAR.

Kiril has provided leadership within the Bulgarian ICT industry and in ICT R&D, notably as Director of IICT.

■

## Member Society News

### Italy



**International Conference on Computer Safety, Reliability and Security**, 12-15 September 2017, Trento, Italy – <http://safecomp17.fbk.eu/home> ■

### IT STAR

*29 September 2017, Sofia, Bulgaria* - Extraordinary IT STAR Business meeting and WS on Data Processing.

Workshop Topics:

- Big Data
  - Open Data
  - National and EU Policies
  - Business Strategies
  - Education and Research
- 

### International

#### UNESCO

#### World Conference on Intangible Capital for Communities



The 13th edition of the World Conference on Intangible Capital for Communities was co-organized by UNESCO and its Information For All Programme (IFAP), the University Paris-Sud and the European Chair on Intellec-

tual Capital on 3 and 4 July at the UNESCO Headquarters in Paris.

It was held under the theme of “Information and knowledge for all: towards inclusive innovation”, with the objectives to explore the prospects for inclusive innovation as a way for improving the flux of information and knowledge sharing and its impact on the overall livelihood of people.

The issues that were considered concern both developed and developing countries and underlines (delete) the role of data and digital resources in fostering capacities of communities to innovate.

Further information about the conference is posted at <http://en.unesco.org/news/2017-edition-world-conference-intangible-capital-communities-opened-today> ■



ITU Press Release

#### ITU releases 2017 global information and communication technology facts and figures

**Geneva, 31 July 2017**

New data released by ITU, the United Nations specialized agency for information and communication technologies (ICTs), show that 830 million young people are online, representing 80 per cent of the youth population in 104 countries. ITU's *ICT Facts and Figures 2017* also shows a significant increase in broadband access and subscriptions with China leading the way.

This much-anticipated annual release of global ICT data shows that youths (15-24 year olds) are at the forefront of Internet adoption. In Least Developed Countries (LDCs), up to 35 per cent of individuals using the Internet are aged 15-24, compared with 13 per cent in developed countries and 23 per cent globally. In China and India alone, up to 320 million young people use the Internet.

(The full text of the press release is posted <http://www.itu.int/en/mediacentre/Pages/2017-PR37.aspx> where you could also download the 2017 edition as well as facts and figures for previous years.) ■

**Mariazell**

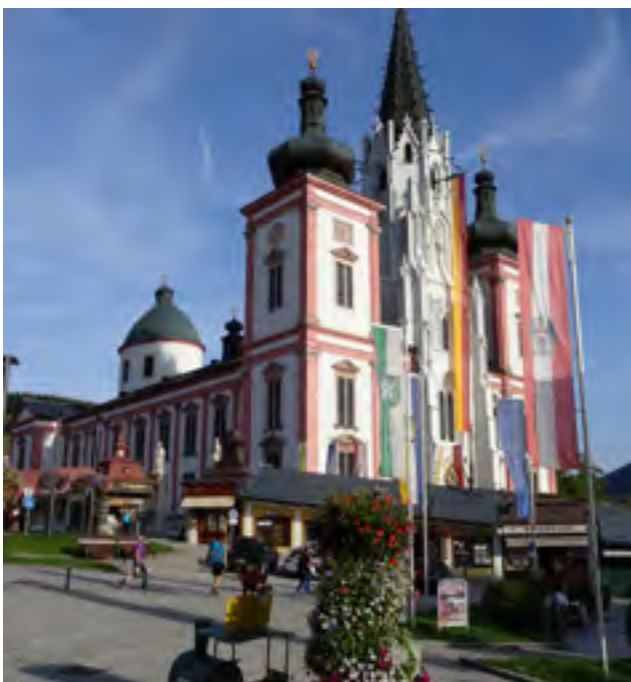
*Dorothy Hayden*



Last week I was in Mariazellerland and thought this destination will make a nice story for the MultiCulti column.

Mariazell (referring to a sculpture in basswood of the Virgin Mary and child, said to do miracles, brought here in 1157) is a site of pilgrimage for Catholics in Austria and the neighboring countries, a summer resort and a winter sports haven.

The main attraction for pilgrims is the Basilica, originating from the 13th century, reconstructed in baroque-style in 1644 around a smaller church built by King Louis I of Hungary, after a victory over the Turks in 1363. It was recently restored and holds a dominating place in the square around it.



*The Basilica*

My hotel was just across the Church – a comfortable refuge and obviously a popular place for pilgrims. There are

many other nice hotels, which border the square around the Basilica.



*One of the many hotels on the main square*

There are some fine things to see in Mariazell - the main square, the pharmacy (under UNESCO patronage), the many stores selling 'Lebkuchen', (= gingerbread) and souvenirs around the church.

Mariazell has a great location as a summer and winter paradise – a cable car from the town's center takes you to the top of the Bürger Alpe, and not far away is the Gemeinde Alpe, with prime summer and winter facilities. The Erlauf Lake offers attractive swimming and diving possibilities and the Erlauf River itself is a challenge for diverse sporting possibilities.



*View fm the Gemeinde Alpe with Erlauf Lake*

One of the greatest mountains in Lower Austria is the Ötscher, right across the Gemeinde Alpe, and to visit the Ötscher Graben – a crevice in between with a pristine brook at the bottom and a winding hiking path along it – is a life-time experience. ■







# SNAPSHOT

REGIONAL ICT ASSOCIATION IN CENTRAL, EASTERN & SOUTHERN EUROPE



## Type of organization

Regional non-governmental and non-profit professional association in the ICT field.

## Date and place of establishment

18 April 2001, Portoroz, Slovenia

## Membership

Countries represented (*see next page for societies*), year of accession, representatives

- Austria (2001) G. Kotsis, E. Mühlvenzl, R. Bieber
- Bulgaria (2003) K. Boyanov, I. Dimov
- Croatia (2002) M. Frkovic
- Cyprus (2009) P. Masouras
- Czech Republic (2001) O. Stepankova, J. Stuller
- Greece (2003) S. Katsikas
- Hungary (2001) B. Domolki
- Italy (2001) G. Occhini
- Lithuania (2003) E. Telesius
- Macedonia (2003) P. Indovski
- Poland (2007) M. Holynski
- Romania (2003) V. Baltac
- Serbia (2003) G. Dukic
- Slovakia (2001) I. Privara
- Slovenia (2001) N. Schlamberger

## Mission

*“To be the leading regional information and communication technology organization in Central, Eastern and Southern Europe which promotes, assists and increases the activities of its members and encourages and promotes regional and international cooperation for the benefit of its constituency, the region and the international ICT community.”*

## Governance

IT STAR is governed according to the letter of its Charter by the Business Meeting of MS representatives:

- 2016 Milan, **Italy** (October)
- 2015 Warsaw, **Poland** (October)
- 2014 Szeged, **Hungary** (September)
- 2013 Bari, **Italy** (May)
- 2012 Bratislava, **Slovakia** (April)
- 2011 Portoroz, **Slovenia** (April)
- 2010 Zagreb, **Croatia** (November)
- 2009 Rome, **Italy** (November)
- 2008 Godollo, **Hungary** (November)

- 2007 Genzano di Roma, **Italy** (May)  
Timisoara, **Romania** (October)
- 2006 Ljubljana, **Slovenia** (May)  
Bratislava, **Slovakia** (November)
- 2005 Herceg Novi, **Serbia & Montenegro** (June)  
Vienna, **Austria** (November)
- 2004 Chioggia, **Italy** (May)  
Prague, **the Czech Republic** (October)
- 2003 Opatija, **Croatia** (June)  
Budapest, **Hungary** (October)
- 2002 Portoroz, **Slovenia** (April)  
Bratislava, **Slovakia** (November)
- 2001 Portoroz, **Slovenia** (April)  
Como, **Italy** (September)

## Coordinators

- 2015 – Marek Holynski
- 2010 – 2015 Igor Privara
- 2006 – 2010 Giulio Occhini
- 2003 – 2006 Niko Schlamberger
- 2001 – 2003 Plamen Nedkov (cur. Chief Executive)










## Major Activities

- 10<sup>th</sup> IT STAR WS on IT Security  
<http://www.starbus.org/ws10>
- 9<sup>th</sup> IT STAR WS on ICT Strategies and Applications  
<http://www.starbus.org/ws9>
- 8<sup>th</sup> IT STAR WS on History of Computing  
<http://www.starbus.org/ws8>
- 7<sup>th</sup> IT STAR WS on eBusiness -  
<http://www.starbus.org/ws7>
- 6<sup>th</sup> IT STAR WS on Digital Security -  
<http://www.starbus.org/ws6>
- IPTS - IT STAR Conference on R&D in EEMS -  
<http://eems.starbus.org>
- 5<sup>th</sup> IT STAR WS and publication on Electronic Business - <http://starbus.org/ws5/ws5.htm>
- 4<sup>th</sup> IT STAR WS and publication on Skills Education and Certification - <http://starbus.org/ws4/ws4.htm>
- 3<sup>rd</sup> IT STAR WS and publication on National Information Society Experiences – NISE 08  
<http://www.starbus.org/ws3/ws3.htm>
- 2<sup>nd</sup> IT STAR WS and publication on Universities and the ICT Industry  
<http://www.starbus.org/ws2/ws2.htm>
- 1<sup>st</sup> IT STAR WS and publication on R&D in ICT  
<http://www.starbus.org/ws1/ws1.htm>

## Periodicals & Web-site

The IT STAR Newsletter ([nl.starbus.org](http://nl.starbus.org)) published quarterly.  
[www.itstar.eu](http://www.itstar.eu)

## IT STAR Member Societies

<b>Austrian Computer Society – OCG</b> Wollzeile 1, A-1010 VIENNA, Austria Tel. +43 1 512 0235 Fax +43 1 512 02359 e-mail: <a href="mailto:ocg@ocg.at">ocg@ocg.at</a> <a href="http://www.ocg.at">www.ocg.at</a> 	<b>Bulgarian Academy of Sciences – BAS</b> Institute for Information and Communication Technology Acad.G.Bonchev str.B1.25A SOFIA 1113, Bulgaria Tel +359 2 8708494 Fax +359 2 8707273 e-mail: <a href="mailto:vomidiv@gmail.com">vomidiv@gmail.com</a> <a href="http://www.bas.bg">www.bas.bg</a> 
<b>Croatian IT Association– CITA</b> Ilica 191 E/II, 10000 ZAGREB, Croatia Tel. +385 1 2222 722 Fax +385 1 2222 723 e-mail: <a href="mailto:hiz@hiz.hr">hiz@hiz.hr</a> <a href="http://www.hiz.hr">www.hiz.hr</a> 	<b>The Cyprus Computer Society – CCS</b> P.O.Box 27038 1641 NICOSIA, Cyprus Tel. +357 22460680 Fax +357 22767349 e-mail: <a href="mailto:info@ccs.org.cy">info@ccs.org.cy</a> <a href="http://www.ccs.org.cy">www.ccs.org.cy</a> 
<b>Czech Society for Cybernetics and Informatics – CSKI</b> Pod vodarenskou vezi 2, CZ-182 07 PRAGUE 8 – Liben Czech Republic Tel. +420 266 053 901 Fax +420 286 585 789 e-mail: <a href="mailto:cski@utia.cas.cz">cski@utia.cas.cz</a> <a href="http://www.cski.cz">www.cski.cz</a> 	<b>Greek Computer Society – GCS</b> Thessaloniki & Chandri 1, Moshato GR-18346 ATHENS, Greece Tel. +30 210 480 2886 Fax +30 210 480 2889 e-mail: <a href="mailto:epy@epy.gr">epy@epy.gr</a> <a href="http://www.epy.gr">www.epy.gr</a> 
<b>John v. Neumann Computer Society – NJSZT</b> P.O. Box 210, Bathori u. 16 H-1364 BUDAPEST, Hungary Tel.+36 1 472 2730 Fax +36 1 472 2739 e-mail: <a href="mailto:titkarsag@njszt.hu">titkarsag@njszt.hu</a> <a href="http://www.njszt.hu">www.njszt.hu</a> 	<b>Associazione Italiana per l' Informatica ed il Calcolo Automatico – AICA</b> Piazzale R. Morandi, 2 I-20121 MILAN, Italy Tel. +39 02 760 14082 Fax +39 02 760 15717 e-mail: <a href="mailto:g.occhini@aicanet.it">g.occhini@aicanet.it</a> <a href="http://www.aicanet.it">www.aicanet.it</a> 
<b>Lithuanian Computer Society – LIKS</b> Geležinio Vilko g. 12-113 LT-01112 VILNIUS, Lithuania Tel. +370 2 62 05 36 e-mail: <a href="mailto:liks@liks.lt">liks@liks.lt</a> <a href="http://www.liks.lt">www.liks.lt</a> 	<b>Macedonian Association for Information Technology – MASIT</b> Dimitrie Cupovski 13 1000 SKOPJE, Macedonia e-mail: <a href="mailto:indovski.p@gord.com.mk">indovski.p@gord.com.mk</a> <a href="http://www.masit.org.mk">www.masit.org.mk</a> 
<b>Polish Information Processing Society</b> Zarząd Główny ul. Solec 38 lok. 103 00-394 Warszawa Tel./Fax +48 22 838 47 05 e-mail: <a href="mailto:marek.holynski@gmail.com">marek.holynski@gmail.com</a> <a href="http://www.pti.org.pl">www.pti.org.pl</a> 	<b>Asociatia pentru Tehnologia Informatiei si Comunicatii – ATIC</b> Calea Floreasca Nr. 167, Sectorul 1 014459 BUCAREST, Romania Tel +402 1 233 1846 Fax +402 1 233 1877 e-mail: <a href="mailto:info@atic.org.ro">info@atic.org.ro</a> <a href="http://www.atic.org.ro">www.atic.org.ro</a> 
<b>JISA Union of ICT Societies</b> Zmaj Jovina 4 11000 BELGRADE, Serbia Tel.+ 381 11 2620374, 2632996 Fax + 381 11 2626576 e- mail: <a href="mailto:dukic@jisa.rs">dukic@jisa.rs</a> <a href="http://www.jisa.rs">www.jisa.rs</a> 	<b>Slovak Society for Computer Science – SSCS</b> KI FMFI UK, Mlynská dolina SK-842 48 BRATISLAVA, Slovak Rep. Tel. +421 2 6542 6635 Fax +421 2 6542 7041 e-mail: <a href="mailto:SSCS@dcs.fmph.uniba.sk">SSCS@dcs.fmph.uniba.sk</a> <a href="http://www.informatika.sk">www.informatika.sk</a> 
<b>Slovenian Society INFORMATIKA – SSI</b> Litostrojska cesta 54 SLO-1000 LJUBLJANA, Slovenia Tel. +386 123 40836 Fax +386 123 40860 e-mail: <a href="mailto:info@drustvo-informatika.si">info@drustvo-informatika.si</a> <a href="http://www.drustvo-informatika.si">www.drustvo-informatika.si</a> 	