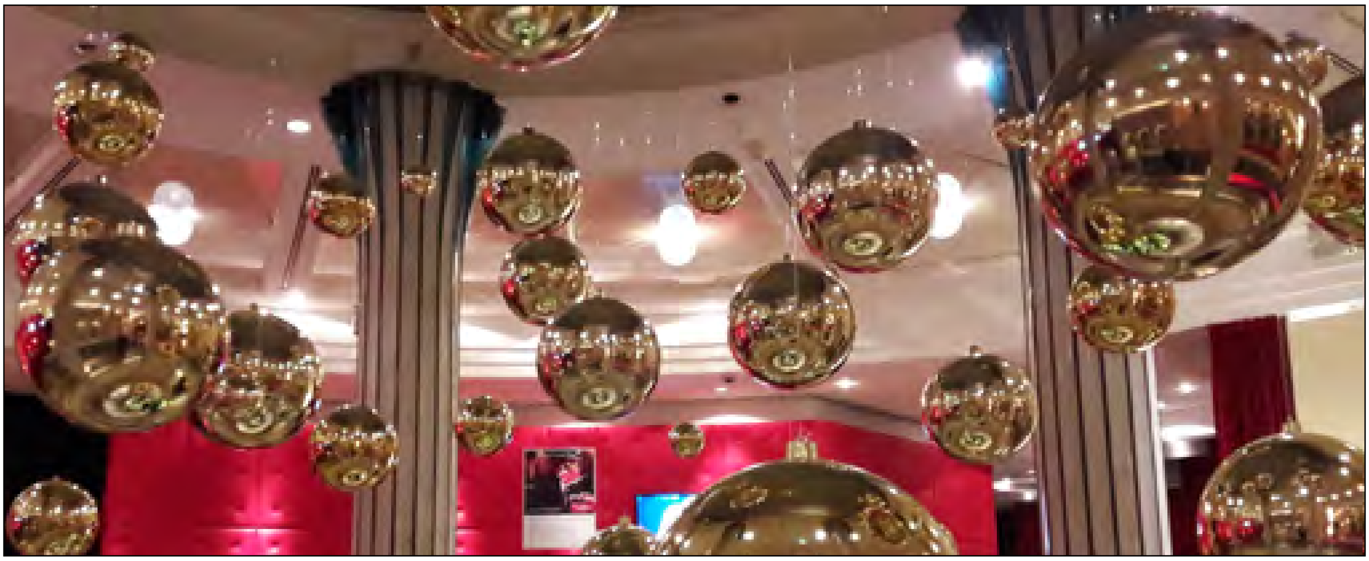
Newsletter - *Calibrated for Creative Communications*

Vol. 14, no. 4, Winter 2016/17



Dazzle Time

The Winter Issue is largely based on material related to the 10th IT STAR Workshop on IT Security held on 28 October 2016 in Milan, Italy.

We are pleased to publish the Milan Takeaway including the Conference statement, personal impressions of the Workshop from several participants, and a paper on Ensuring Security for Europe's Information Society from *Paolo Empadinhas*, representative of the European Union Agency for Network and Information Security (ENISA).

A Panel on Legal Informatics, Document Management, Privacy and Ethics was convened during the Milan event and the three panelists

Bruno Lamborghini, AICA Vice-President
Niko Schlamberger, SSI President
Daniel Olejar, Vice-Rector, Comenius University

kindly responded to the invitation of the Editor and prepared for the Winter NL issue short articles based on their Milan interventions.

We hope you will enjoy the Issue. We also take this opportunity to wish our Readers an enjoyable end-of-year.

Season's Greetings and Best Wishes for 2017!

The Newsletter Team

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

Editor

P. Nedkov, Halsriegelstraße 55
A-2500 Baden, Austria
e-mail: **info@starbus.org**, web-site: **nl.starbus.org**

Etude Esterhazy – Temple with Ducks on Ice

ADVISORY BOARD

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 acknowl-edgement of the source is made. In all cases, please apply for permission to the Newsletter Editor.

Special arrangements for the production and circula-tion 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.

10th Workshop on IT Security, 28 October 2016, Milan – The Takeaway

Plamen Nedkov

***Plamen Nedkov** is Chief Executive of IT STAR and Editor of the IT STAR Newsletter. He served as Moderator of the 10th WS on IT Security.*

Our objectives in organizing the 10th IT STAR Workshop on IT Security were similar to these of previous events: To convene a stakeholder forum of representatives coming from academia, business, government and professional organizations with stimulating debate, to encourage synergies between national and international activities, outlining policies, best practices and competences, hopefully leading to spin-off activities and projects, and to produce a post-conference book with the proceedings for further dissemination.

The program consisted of an overview presented by the President of Associazione Italiana per l'Informatica ed il Calcolo Automatico (AICA), host and co-organizer of the event, and then proceeded under three major topics:

- **EU and national strategies and activities in the IS field**, with presentations of representatives of the EU Agency for Network and Information Security (ENISA), Slovakia, Hungary and Bulgaria
- **Business related strategies and practices**, with presentations from representatives of business and academia in Germany and Italy, and
- **IS Competences**, including presentations of representatives of TC 428 on "Digital Competences and ICT Professionalism" and the WS on ICT Skills of the European Committee for Standardization (CEN) - also representing UNINFO and (ISC)², and a presentation on AICA's enriched eCF*plus* system and its ICT professional profiles related to security.

A Panel on legal informatics, document management, privacy and ethics complemented these topics.

The Takeaway

IT STAR as regional association focuses on issues that confront the countries of Central, Eastern and Southern Europe within the context of the European Union. This event helped identify success stories and shortcomings in the IS field as well as potential topics for networking and closer co-operation between individuals and institutions within Europe. The favorable mix of participants and choice of presentations influenced positively a debate, which we are confident, will continue after the close of the 10th WS on IT Security.

In addition to the excellent presentations and stimulating debate, the Workshop laid a solid base for further professional contacts between the participants and the institutions they represent. The Milan Statement, as a synthesis of the Workshop proceedings, was distributed widely and would hopefully be of further use to IT STAR's member societies and other professional organizations in their contacts with national and international authorities. Finally, we are hopeful that the post-conference book with the revised and edited proceedings would be a useful reference document for further consideration and research.

The slide presentations that were delivered during the workshop are available at www.starbus.org/ws10. The publication of the post-conference papers will further augment the excellent debate within the format of the 10th IT STAR event. ■

Partner Publication

http://mondodigitale.aicanet.net/ultimo/index.xml ■

Milan Statement

Based on the debate of the 10th IT STAR Workshop on IT Security, 28 October 2016 in Milan, Italy

The growing dependence on information and communication technology, on the one hand, and the vulnerability of the Internet to abuse, on the other, magnify the importance of IT security for governance, business, education and social activity, as well as for further development and application of ICT. Strategies, policies and legislation for IT Security, cybercrime prevention, awareness, knowledge, skills and responsible behavior in the Internet environment, are essential in avoiding intellectual, material and personal harm.

The following policy matters were highlighted and are offered for consideration to a wider circle of stakeholders in the field:

- The acceptable balance between privacy and security in cyberspace should be an important preoccupation of government, the private sector, professional organizations and individuals. Legislation initiatives should treat cyber crime as any other criminal activity with similar consequences as in cases of physical attack, theft, fraud and other. The responsibilities of Internet providers to protect customers need to be better regulated.

- The majority of EU member states have national cyber-security strategies but pan-European cooperation remains dependent on wider harmonization of regulations, sharing experiences and good practices, detecting and preventing treats. In this regard, ENISA, the EU Agency for Network and Information Security, has a distinct role to play.

- For large companies and SMEs, digitalization strategies and the associated digital leadership principles are essential within an increasingly volatile economic environment. Economic growth scenarios need to incorporate security competences and standards for Internet products and services.

- Competences and skills are the crux in addressing IT Security. CEN's TC 428 on "Digital Competences and ICT Professionalism", CEN's WS on ICT Skills, (ISC)² and AICA's enriched e-CF*plus* system provide a base for further developments, moreover, cybersecurity needs to be recognized and embedded within formal education, practice and skills standards.

The presentations and further details about the 10th IT STAR Workshop on IT Security are posted at www.starbus.org/ws10.

Shared Impressions

10th IT STAR WS on IT Security, 28 October 2016, Milan

All attendees liked the Workshop. It was held in the building housing the headquarters of Istituto dei Ciechi di Milano at via Vivaio 7,

Istituto dei Ciechi di Milano

an architectural masterwork constructed in 1892. The Institute presently serves as a center of excellence in research and planning in the field of typhlo-pedagogy and typhlo-information technology, and also offers meeting space for numerous events and cultural activities.

The facilities offered to the Workshop participants no doubt contributed to the creative debate.

We are very pleased to share some of the impressions that were received after the event:

"Thank you very much for the invitation. It was indeed a very pleasant conference with very good discussions".

Paulo Empadinhas
Head of Stakeholders Relations and Administration Department, ENISA

"I found the workshop useful since I got interesting information and met clever people dealing with similar problems".

Daniel Olejár
Vice-Rector, Comenius University, Bratislava

"... most interesting IT STAR Workshop".

Niko Schlamberger
President, Slovenian
Society INFORMATIKA

Securing Europe's Information Society

Paulo Empadinhas

***Paulo Empadinhas** is Head of Stakeholders Relations and Administration Department of the European Union Agency for Network and Information Security (ENISA).*

Introduction to ENISA

ENISA is the network and information security agency of the European Union. Created back in 2004, its primary goal is to support the European Member States protecting their network and information systems from cyber-attacks through implementing robust cyber security mechanisms. In 2014, extending its mandate to 2020, ENISA is one of the most important policy players in cyber security worldwide. Its role varies to accommodate the needs of the public and private sector in information security, namely ENISA is:

a) Supporting Member States **implementing European policy regulation**, i.e. Article 13a of the Telecommunications Directive on the notification of information security incidents in the sector, or Article 4 on notification of data breaches, or Article 19 of the electronic identification directive on Trust providers;

b) Issuing yearly **recommendations** for policy makers, the industry and academia on how to protect and enhance security levels in different sectors i.e. SCADA Security, Transport, or using different technologies i.e. Cloud Computing, Privacy Enhanced Technologies (PET), Smartphones etc.

c) Increasing the **operational capabilities** of the Member States providing organisation of specific technical trainings for the national Computer Security Information Response Teams (CSIRT) and through biannually organising Cyber Europe, the only Pan European Cyber Security exercise that brings together stakeholders from the private and the public sector to respond through collaboration to a major cyber crisis.

d) **Mobilising the community** by creating collaboration groups of subject matter experts and take into account their feedback and expertise when creating guidelines; organises workshops and conferences to disseminate this knowledge and through awareness raising effort i.e. the European Cyber Security Month, engages the society as a whole into enhancing cyber security.

However, ENISA cannot perform this important task alone; collaboration is set primarily with the European Commission, the national security authorities and policy makers of the Member States in different sectors, the industry experts spanning from IT devices manufacturers to IT service providers, the national and international standardisation bodies like ISO and ITU, the vast academic community in supporting research and development and of course the European society as a whole. All these stakeholders constitute the ENISA ecosystem, which constantly interacts with each component to provide expertise and guidance.

Network and Information
Security Directive

Enhancing cyber security in the Critical Sectors

The Network and Information Security Directive
In 2016 the European Commission adopted the Network and Information Security (NIS) Directive. The NIS Directive lays down measures to achieve higher level of security for network and information systems for the EU MS. To achieve this goal firstly, it creates two groups:

a) The cooperation group with a strategic role on the specific requirements of the Directive and
b) The CSIRTs network, where national CSIRT of MS constitute the operational force.

Starting with NIS national strategies as a prerequisite, the NIS Directive's provisions also require the establishment of information security incident notification schemes and the adoption of security requirements. The target of this directive is the Digital Service Providers meaning the cloud provides, online market places and search engines; and the Essential Services Operators meaning providers of services on sectors like transport, energy, water, health, finance and digital infrastructure. The Member States need to implement the provisions of this Directive effectively in 21 months from its adoption, and ENISA is the supporting body to assist both the Member States and the European Commission. The goal is to achieve, as much as possible, convergence of the different approaches the Member States will take towards this implementation and so collaboration is a requirement. ENISA is there to facilitate this collaboration between stakeholders and to give voice to both public and private sector.

Cyber Security Strategies

Everything starts with a national strategic document that clearly defines the priorities of the state towards network and information security for a given timeframe; this document is called national cyber security strategy.

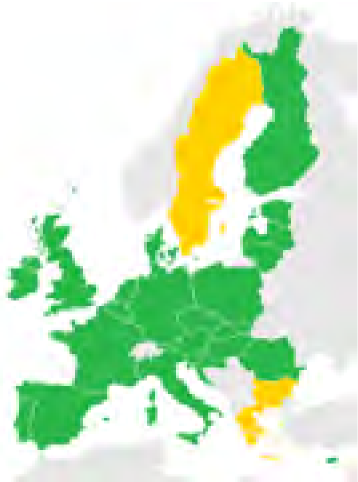


Figure 1 EU NCSS status (November 2016)

One of the provisions of the NISD is that all member states need to have a national cyber security strategy. Currently 25 out of 28 MS have a National cyber security strategy, however this is not an easy task to achieve. Many challenges arise when creating a strategy; where does the mandate for implementing and monitoring the strategy lay, how do the stakeholders communicate and collaborate, how are the responsibilities spread between those stakeholders and how do they report to the overarching authority. Establishing effective cooperation between stakeholders was named by many countries as one of the major challenges they were facing during the implementation of their NCSS.

ENISA is supporting MS since 2012 in the area of NCSS. Based on the ENISA lifecycle for NCSS (design, implement, evaluate and adjust), ENISA has launched many initiatives in the area. Some of them are:

- The NCSS EU map: a repository of the MS national strategies.
- ENISA studies: a good practice guide in designing and implementing a strategy (defines the objectives of a national strategy for both phases), the evaluation framework (provides a logic model and a set of KPIs to help MS evaluate their strategies)
- Establishment of an experts group that supports ENISA activities and provides input to ENISA's NCSS studies and workshops.

To increase resilience and security of global network and information systems, a national cyber security strategy needs to be flexible with planned actions and established strategic objectives. In the studies ENISA has identified the most important strategic objectives that should be included in a strategy document. For example, Critical information infrastructure protection (CIIP) is an essential part of many cyber and information security strategies. Other examples of usual security objectives included in the strategy are: raise awareness, organise cyber security exercise, foster research and development, establish reporting mechanisms, adopt security measures, strengthen education programs and training, establish incident response capabilities, invest on public-private partnerships, engage in international collaboration, address cyber-crime, formalise the collaboration between public agencies, balance security and privacy.

It is a matter of time that all Member States will soon have a NIS strategy in place.

Critical Information Infrastructures Protection

Critical is considered any information infrastructure which when breached, can cause impact to the society in a national or cross border level. Under the Critical Information Infrastructures fall[1] the following sectors: Energy, Transport, Telecommunications, Water, Finance, Health, public and legal order, civil administration, chemical and nuclear industry and space and research.

From the governance point of view according to another ENISA study[2] MS have developed three different approaches in CIIP governance:

- The centralized approach, in which one central authority is responsible for all sectors and a comprehensive legislation is that creates obligations and requirements across all sectors is established. For example, France's ANSSI has been declared the main national authority for the defense of the information systems in 2011. ANSSI has a strong supervisory role for "operators of vital importance" (OIVs). The agency can order OIVs to comply with security measures and is authorized to perform security audits on them. Furthermore, it is the main Single Point of Contact for OIVs, which are obligated to report security incident to the agency.
- The second approach is the decentralized one, in which the public agencies have developed strong cooperation and the adoption of laws and regulations remain sector specific and may vary across the different sectors. For example, Sweden has assigned the responsibility of different tasks (identification of vital services, coordination and support of operators, regulatory tasks, etc.) to different agencies (ex. MSB, PTS, etc.). In order to coordinate the actions between the different agencies and public entities, the Swedish government has developed a cooperative network comprised of authorities "with specific societal information security responsibilities". This Cooperation Group for Information Security (SAMFI), consists of representatives of the different authorities and meets several times a year to discuss issues related to national information security. Other examples are Austria, Cyprus, Finland, Switzerland and Ireland.
- The third approach is the co-regulation with the private sector, in which institutionalized cooperation like PPPs are established between the public and private

[1] Based on ENISA report "Methodologies for the identification of Critical Information Infrastructure assets and services"

[2] ENISA, Stocktaking, Analysis and recommendations on the protection of CIIs, 2015

sector. In this approach usually the public sector offers political legitimacy and funds, while private actors bring in expertise and efficiency. For example, Netherlands has a major CIP agency, the National Cyber Security Centre (NCSC). The NCSC consists of several partnerships between public and private actors, such as various Information Sharing and Analysis Centres (ISACs) and the ICT Response Board which analyses the situation during a large-scale IT crisis or threat. The NCSC emphasizes that cooperation with private stakeholders is based on equality and trust. In addition, the Dutch Cyber Security Council offers advice on a strategic and political level. The council is comprised of representatives from different Ministries, academia and the private sector and has a strong public-private character. Participation in the various Information Sharing and Analysis Centers is based on confidentiality, meaning that members are not forced or obligated to share information with the other participants but do so on a voluntary basis. All representatives are expected to respect the mutual agreement and treat information on threats, risks and other sensitive issues in a confidential manner.

Cooperation and incident reporting are very important aspects in CIIP. The Member States examined in ENISA's study have developed different forms of cooperation with the private sector with varying degrees of institutionalization. Public-Private partnerships are an institutionalized form of cooperation between public and private actors. They are usually characterized through a long-term commitment of the different stakeholders, a contractual agreement or a joint statement, which defines the goals and responsibilities of the partnership, and shared responsibility for the produced output. A less institutionalized form of cooperation are working groups and contact forums, which are often temporary and demand less resources and commitment from the different stakeholders.

Enhancing information security in critical sectors

Under the CIIP topic, ENISA has invested in cyber security for specific questions. In our portfolio the reader can find studies on Industrial Control Systems, Smart Grids and the energy sector, eHealth, Transport, Telecommunications, Internet Infrastructures, Maritime and Finance. Some indicative activities are summarised below:

- Energy: Cyber-attacks on CIIs are now the norm than a future trend. As a result there is an increasing interest by MSs in securing national power grids. It is noteworthy that Energy sector is among the critical sectors mentioned in NISD. Smart grid is the future of energy infrastructure. However, it should be secure, so that it provides reliable services in the power supply chain. ENISA fosters information sharing and for this reason has already established relationships with public sector as well as private sector European energy ISAC.
- Telecommunication: Incident reporting schemes have improved resilience and security in the EU telecoms sector. An example is Article 13a, which addresses security and integrity of public electronic communication networks and services. ENISA is supporting this regulatory framework since 2011 by publishing reports about significant incidents and outages across the EU.
- Finance: Many regulations exist in the Financial Sector, information security is scarcely addressed. Payment Services Directive 2 has some information on incident reporting and operational security. NIS directive has similar requirements. Harmonization will be of first priority. ENISA works with the regulators in a number of working groups with the European Banking Authority and the European Central Bank. ENISA also collaborates with the private financial industry where security experts from EU private banks discuss policy and technical issues.
- Healthcare: ENISA is working in this area since 2014. Several challenges have been identified in the health sector. For example, MS lack regulatory framework for the protection of network and information systems, there are no guidelines on how to share information in case of a cross border incident. Electronic health records are the most critical systems in all MS. ENISA publishes recommendations and guidelines on how to protect critical eHealth infrastructures, services and systems.
- Transport: Safety is the outmost priority for this sector. Due to the vast subcategories it covers, namely public transport, aviation, railways, ENISA decided to take a per sector approach and this year focused on the topic of aviation. More research and activities to follow.
- Maritime: Maritime cyber security awareness is currently low, to non-existent. ENISA has published the first EU report ever on cyber security challenges in the Maritime Sector. This principal analysis highlights essential key insights, as well as existing initiatives, as a baseline for cyber security.

ENISA strongly believes in sharing experiences and information as this leads to building knowledge intelligence. MS and private sector, with the assistance of ENISA, should co-operate to protect CIIs via PPPs or ISAC.

Outlook

Europe has come way ahead in cyber security in the past 5-10 years; it has become more mature, more highly skilled through trainings and exercises, more resilient and definitely more secure. Great progress is observed among all the Member States and the difficulties in the collaboration with the private sector have been set aside. However we always need to wonder if this is enough. Introducing new technologies, due to urging needs, means that the attack surface is widening; knowledge and capabilities are built both ways (to the ethnical and non-ethical entities) resulting into more sophisticated attacks emerging; on the other side, policy specifications take time and cannot catch up with the technology advancement. So the need for additional research, collaboration and initiatives is evident.

ENISA is at present appointed with the high task to support the Member States in enhancing their cyber security needs. And this is what we will continue doing in the future, to secure Europe's information society.

Panel on Legal Informatics, Document Management, Privacy, Security, Ethics

Panelists:
***Bruno Lamborghini**, AICA Vice-President*
***Niko Schlamberger**, SSI President*
***Daniel Olejár**, Vice Rector, Comenius University – Bratislava*

Big Data and Security Issues

Bruno Lamborghini

How can the transition from Bit Economy to Data Economy be fostered, supervised and if needed regulated, especially in terms of security control?

We see today only the tip of the iceberg of a dynamic digital scenario driven by technology, but also by new forms of human, social and economic evolution based on embedded diffusion in all activities and people life, of data flows coming from knowledge sharing, social networks, Internet of everything, machine to machine and machines to humans, creating enormous amounts of Big Data, trillions of data exchanged and stored every second.

To avoid disruptive change with risks of losing control of security and IPR, we need, from now on, to deeply invest in new e-skills and e-leadership competences, preparing young and senior people through lifelong education and training based on the right technology use, but more and more on social consciousness, security issues, ethics and self-responsibility.

This challenge is particularly relevant for Europe, due to some negative factors, which characterize the present socio-economic scenario in many European countries *vis-à-vis* the US and the most dynamic emerging areas.

The recent book on the second machine age by Brynjolfsson and McAfee has shown clearly the impact of the digital revolution, both in terms of new opportunities produced by Artificial Intelligence and risks of digital unemployment and computer dominance on people's decisions. The development of machine2machine networks and Internet of everybody systems could produce immense Data Prairies and human free decision processes.

All people in any organization are required to know and apply efficiently digital technologies. It is like a telephony network, where all telephone sets have to work in the same way, otherwise the network fails. This means to prepare e-skills at all levels of any organization. It does not mean to train all people to become ICT professionals but to provide them with all the useful knowledge of digital technologies in a dynamic way.

Digital technologies in innovating organizations are today like blood circulation in a human body or like the capacity of reading and writing.

E-skills preparation should become a strategic target in all organizations and should be a fundamental content of secondary or university courses.

The European Commission introduced the concept of e-Leadership, referring to people who can produce innovation in an organization through the digital technologies, becoming innovation Leaders. This requires creating the right mix of digital technologies with the so-called soft skills (team leadership, people motivation and collaboration, business negotiations, etc.).

Adam Smith at the beginning of the first industrial revolution was concerned about the impact of such revolution and said very clearly that the only possibility to face positively the change was to prepare people, recommending to follow three main objectives, skills, dexterity and judgment, adding also the need to include moral sentiments. Today we have only to follow the Adam Smith recommendations.

The main questions about the relation between BIG Data and security are:

- Who will manage this avalanche of data, who will control huge storage systems, who will be able to analyze these data mines and use them
- Which impact on Citizens/consumers, on Industry, on Government
- Which rules are available or will be provided to avoid disruptive economic and social change, on risks for security, privacy protection, data propriety
- How to manage Open data as Common Goods available to everybody

I would make short comments with regard to the three main producers and users of Big data:

Citizens/consumers: Every day, enormous amount of data about way of life, consumers spending, people geo-location through social networks, smart phones, sensors everywhere like wearable computers, going to few large data storages, server farms by companies such as Google, Facebook, Amazon and others. There are growing risks of losing privacy, identity, health data, freedom of decision, at the same time information sharing, active users, new opportunities for jobs and startups. The question is: market freedom as it is now or need of some regulation? Is it possible at national or European level even if the digital scenario is global?

Industry: Cloud management and Industry 4.0 are radically modifying value chains and firm organizations, Value chains will be driven and modified by Big data and relative data flows moving to widening ecosystems and open innovation. The question is about the data propriety and data protection in a widened participation environment with open access to all people in the company and in the supply chain. Digital fabrication is radically changing factory organization by additive manufacturing, distant digital manufacturing and IoT. Are there enough competences for adapting organizations to the speed of digital change?

Government: There are smart cities programs with big data flows connecting energy, transportation, education, healthcare, housing, entertainment. There are Open data programs, which can permit free access to citizens and companies for creating new jobs and business. The question is: which data are open at national or global level? Are there international rules? Not to consider the issue of Datagate and relevant public data protection.

But the most challenging question is: how to prepare people, companies and governments to this dynamic scenario?

At European level, through the ECDL Foundation and CEPIS, and in Italy through AICA, we are very committed to the diffusion of digital competences starting at primary and secondary school level but also with special regard to the e-skills and e-leadership education of digital competences for industry people and management and for public administrators in order to create the right approach to ICT security.

At European level, we are strongly supporting the e-CF approach (European Competence Framework), which could permit to reach common digital competences throughout Europe.

There is an urgent need to prepare people to manage Big Data and Analytics in all fields; for this reason there is an urgent need to define competences of Data Scientists and Digital Marketing profiles and to focus Universities courses to this target.

We believe that this is a primary and urgent request to be made by the European Commission.

The European countries have a major role to play and a major responsibility to define some of the rules of the new digital game following the European cultural heritage and our specific human values to promote ethics and humanistic informatics and shaping a more favorable digital living environment. We expect and we have to do any effort in order that the European Union can take the lead in driving the new conditions and the route of what will happen in the digital scenario of the near future.

The European Computer Associations like AICA and IT STAR have to represent the core of this effort and we should commit ourselves in promoting lifelong education for preparing the right e-skills and e-leadership competences for managing companies and public institutions towards a secure digital scenario.

Digital Security Revisited

Niko Schlamberger

During the 6th IT STAR Workshop on Digital Security on 30 March 2012 in Bratislava I had the pleasure and honor to chair a panel on privacy, data protection, and intellectual property rights. A synopsis of the contributions was published in IT STAR's Newsletter Summer 2012 issue.

I was invited now as a panelist to offer an overview of developments in the issues addressed during the first panel. A summary of my contribution follows, which is far from being a comprehensive analysis of the issues addressed but has nevertheless initiated an interesting discussion. I concentrated on three topics that were hot then but do not seem to have become any cooler after four years.

Data management and data retention has turned out to be very interesting both for administrations and non-government entities but also for commercial companies. Probably we all remember discussions about who and for what period should be entitled to collect various data and how long should the data be kept. There are two faces of this medal. One is a possible infringement of privacy with which no one can agree. Echelon which was started in the 1970s and has since collected zillions of bytes of data without us even knowing it, let alone to be able to prevent it. The battle seems to have been lost. However, we all remember WikiLeaks and the awareness it started in millions if not in billions of people. Were it not for data retention, legal or not, that would not have been possible. Also, in the meantime big data has become a big issue, one that I call new alchemy. The classical one attempted – unsuccessfully - to produce gold from lead. To transform not lead but quicksilver into gold has been a success of nuclear physics only in 20th century but the price of the process is prohibitive, so gold is still produced the classical way. The new alchemy is a method of turning data into money. Without data retention, big data accompanying algorithms and resulting new services, new jobs, and new income this could not be possible. The real issue is therefore not to try to prevent data collection and retention, illegal or not, but to penalize abuse. This is homework for governments and also partisans should better concentrate on that rather than fight windmills.

Privacy is another issue that persistently provokes discussions of various kinds. There seem to be two poles most active, governments and non-government entities. To simplify, the first tries to regulate the field and the second opposes to any kind of regulation, and nothing much has changed in the four years – except that many crimes were prevented, and quite some offenders were uncovered due to cameras in public places. There is obviously not a common understanding of privacy and one of the consequences is an opposition to public cameras. Obviously, one's privacy ends when one leaves one's home. Constitutions protect privacy of home, but not privacy in public places and that should be the most important standard when considering if privacy has been violated or not. In public we are entitled to physical integrity but not to privacy. It should be also remembered that nothing comes for free and that is also true in this case. There is a trade-off between security and privacy and there is no maximum privacy and maximum security available – at least for now. A special aspect of privacy is violating electronic mail. Probably everybody has experienced at least an attempt of harmful e-mail of some form. Some countries, Slovenia for one, have established organizations where one can report incidents of such kind. You report, and what next? You receive a thank-you message for having reported the incident and that is it; all the rest is up to you. This is simply not good enough and the result is that intruders are encouraged as they get away with it. If such attempts are criminal acts, and this is a common consensus, the institutions should be made to persecute felons by official duty. This is another commendable homework for governments.

Regarding intellectual property rights there seem to be no hot issues at this time. In 2012, Anti-Counterfeiting Trade Agreement, commonly known as ACTA, was much debated, opposed to, and finally more or less forgotten although some countries have signed it. Perhaps it has attempted to solve a non-existing problem although in my view ACTA was not harmful in itself, even more so as the signing country has had the possibility to revoke the signature. Obviously the existing intellectual rights protection mechanisms are sufficient.

Legal Aspects

Daniel Olejár

During the last 30 years our society has changed radically. We practically jumped into information society. The legislation, creating and maintaining the rules for society life, was not able to keep the pace with the "running" informatization. We have a new society without rules or with incomplete rules.

In Slovakia, we have partial acts and general formulations in traditional acts (Penal code, Personal information protection law, Law on the protection of classified information, Critical information protection act, Electronic signature act, Telecommunication act, Public administration information systems act, e-Government act, etc.) covering some problems and relations associated with the use and misuse of computers. The partial solutions are often insufficient and even contradictory. We need to write and adopt a general law (lexgeneralis), which will create a consistent legal framework of information security. The Slovak government approved the legislative concept of the information security law some years ago; but various interests and influences blocked the preparation of the law. Despite the obstacles the law is ready; it sets the competences of state bodies, incorporates the requirements of EU legislation (namely the NIS Directive), defines the basic terminology, sets the rules for classification of information and systems, defines the sets of minimal security requirements on systems, requires the security during the whole life cycle of a system, requires the introduction of the ISMS in state organizations, specifies the requirements on critical information infrastructure protection, supports the solution of cyber-crime by setting the obligations of the operators, requires the security testing of new technologies before their implementation and the harmonization of other laws with respect to the information security.

Adopting a reasonable law is only a necessary but not the sufficient condition. We need qualified experts (especially lawyers) able to implement the law. There are only a few such lawyers in Slovakia and we are trying to involve them to prepare the others. Comenius University created the Department of computer law and launched lessons on legal informatics for the students of computer science. The Cyber-security concept (the information security strategy approved by the Slovak government in 2015) and the subsequent Action plan set a very ambitious program in cyber-security/information security education and awareness raising; including the education of judges, attorneys, prosecutors, investigators and others.

The European Union is producing a large amount of regulations, directives, standards and other documents creating the regulation framework of information security in the whole EU. The implementation of the European legislation discovered another problem - the terminological one. There is no standard information security terminology in the Slovak language and the consequences are sometimes peculiar; e.g. the Regulation on trust services was officially translated as the Regulation on the trustful services. But even the more experienced translators encountered problems with distinguishing terms (and finding their adequate Slovak translations) such as fail, failure, mistake, error, fault; probability and likelihood, safety and security, and others.

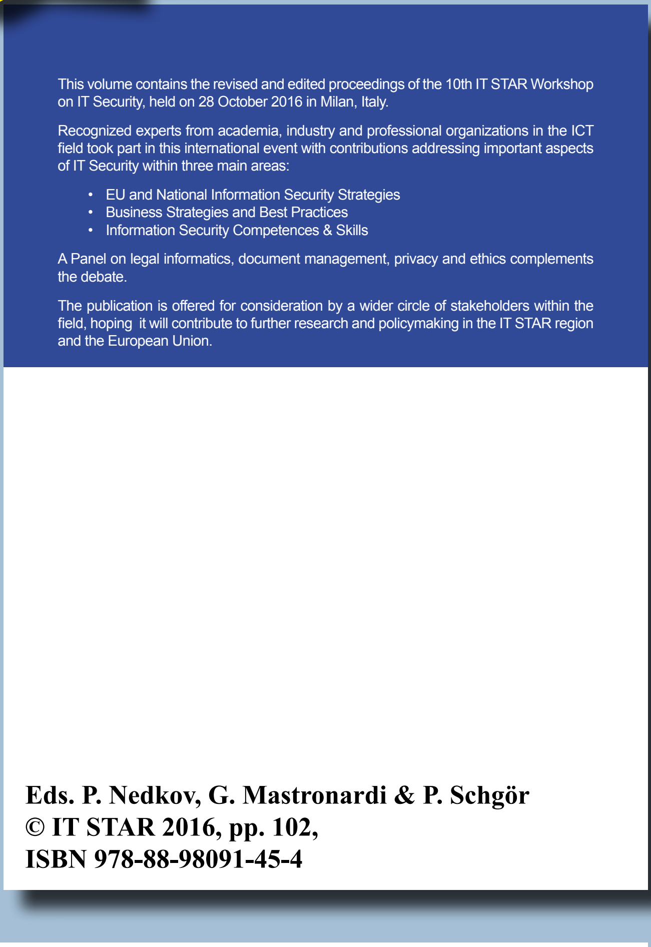
Slovakia created in 2016 a state committee on cyber-security and invited the leading experts from industry and academia to participate in its work. Legislation, education, standards, terminology, critical information infrastructure protection, cyber-crime and other hardcore problems of info-/cyber-security are the main topics of the agenda of the committee. The future will show, whether the committee will be only a discussion club, or it will be able to implement really the solutions of information security problems in Slovakia.

New IT STAR book

Plamen Nedkov, Giuseppe Mastronardi & Paolo Schgör (Editors)

IT Security

IT STAR Series



This volume contains the revised and edited proceedings of the 10th IT STAR Workshop on IT Security, held on 28 October 2016 in Milan, Italy.

Recognized experts from academia, industry and professional organizations in the ICT field took part in this international event with contributions addressing important aspects of IT Security within three main areas:

- EU and National Information Security Strategies
- Business Strategies and Best Practices
- Information Security Competences & Skills

A Panel on legal informatics, document management, privacy and ethics complements the debate.

The publication is offered for consideration by a wider circle of stakeholders within the field, hoping it will contribute to further research and policymaking in the IT STAR region and the European Union.

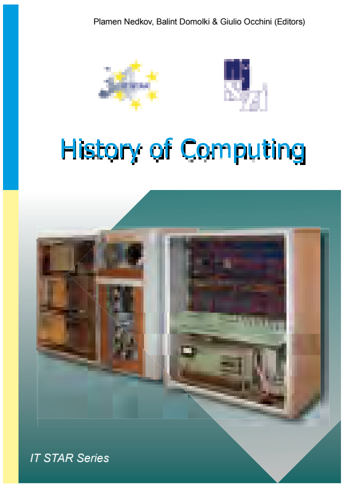
Eds. P. Nedkov, G. Mastronardi & P. Schgör
© IT STAR 2016, pp. 102,
ISBN 978-88-98091-45-4

CONTENTS

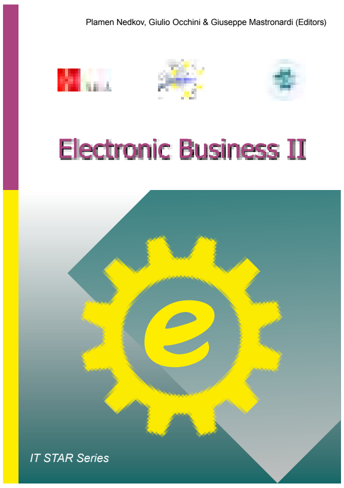
Other IT STAR Publications

Plamen Nedkov, Marek Holynski & Giulio Occhini (Editors)
ICT Strategies & Applications
IT STAR Series

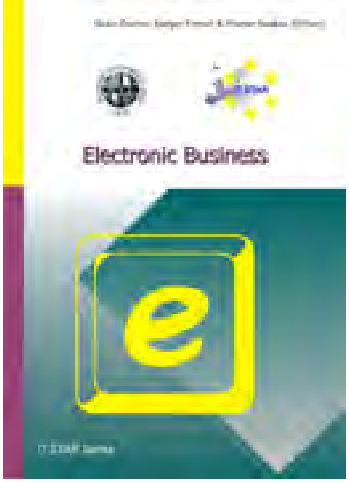
Eds. P. Nedkov, M. Holynski & G. Occhini
© IT STAR 2015, pp. 106,
ISBN 978-88-98091-39-3



Eds. P. Nedkov, B. Domolki & G. Occhini
© IT STAR 2014, pp. 168,
ISBN 978-88-98091-34-8


Plamen Nedkov, Giulio Occhini & Giuseppe Mastronardi (Editors)
Electronic Business II
IT STAR Series

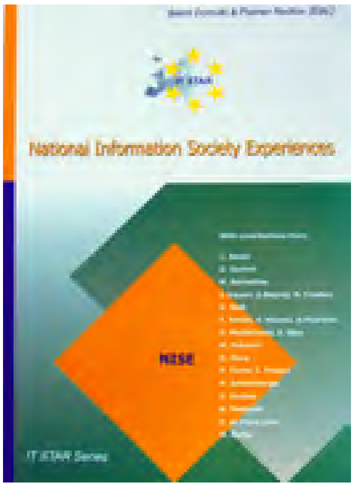
Eds. P. Nedkov, G. Occhini &
G. Mastronardi
© IT STAR 2013, pp. 139
ISBN 978 88 9809 1 11 9



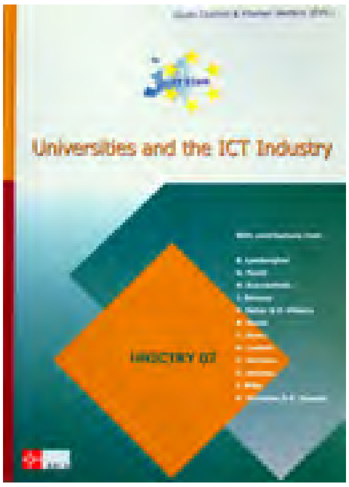
Eds. G. Occhini, M. Frkovic &
P. Nedkov
© IT STAR 2011, pp. 125
ISBN 978 88 9054 0615

ICT Skills, Education and Certification
The multi-stakeholder partnership
IT STAR Series

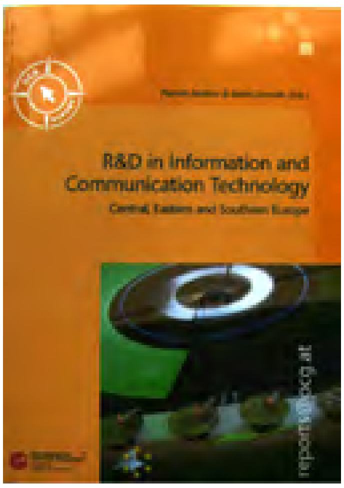
Eds. G. Occhini & P. Nedkov
© IT STAR 2010, pp. 165
ISBN 88-901620-5-8



Eds. B. Domolki & P. Nedkov
© IT STAR 2009, pp. 118
ISBN 88-901620-2-3



Eds. G. Occhini & P. Nedkov
© IT STAR 2007, pp. 104
ISBN 88-901620-1-5


R&D in Information and Communication Technology
Central, Eastern and Southern Europe
reports@ocg.at

Eds. P. Nedkov & B. Domolki
© IT STAR 2007, pp. 116
ISBN 978-3-902580-02-3

Further information about these and other IT STAR books is posted at http://starbus.org/publications.htm.

Member Society News & Events

Bulgaria

On 1 December 2016, **Julian Revalski**, Director of the Institute of Mathematics and Informatics (IMI), was elected President of the Bulgarian Academy of Sciences (BAS) for a period of four years.

Prof. Revalski is Doctor of Mathematical Sciences and Academician (full member) of BAS.

Forthcoming IT STAR Events

IT STAR Business Meeting
May/June 2017
Venue: To be decided

11th IT STAR Workshop, Bulgaria
Tentative Topic: Data Management
Second half of October 2017, Sofia

Other News and Events

United Nations
Educational, Scientific and
Cultural Organization

UNESCO - Challenges of a multilingual cyberspace

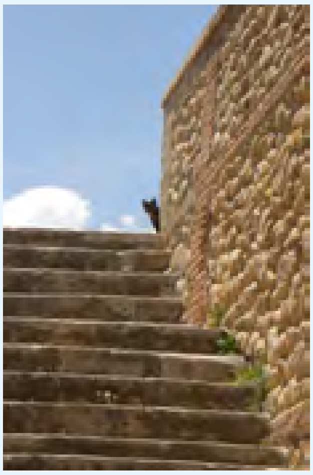
A round table and a high-level meeting on Russia's language policy and the situation of the multilingualism in the world was held in Moscow on 17 and 18 November at the ITAR-TASS News Agency, in cooperation with the Ministry of Education and Science of the Russian Federation, the Russian Committee of the UNESCO Information for All Programme, and the Interregional Library Cooperation Centre.

High on the agenda were the following topics: access to information in a truly multilingual cyberspace; the promotion of formal and informal open online education in all languages; and the development of the Russian language and the languages of some 100 indigenous peoples of the Russian Federation.

ITUNews Magazine (Link to download)

European
Commission

EUROPEAN CONFERENCE
High-Tech and Leadership Skills for Europe
26 January 2017, Brussels - www.leadership2017.eu



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

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

IT STAR Member Societies

Austrian Computer Society – OCG
Wollzeile 1,
A-1010 VIENNA, Austria
Tel. +43 1 512 0235 Fax +43 1 512 02359
e-mail: ocg@ocg.at
www.ocg.at

Bulgarian Academy of Sciences – BAS
Institute for Information and Communication Technology
Acad.G.Bonchev str.Bl.25A
SOFIA 1113, Bulgaria
Tel +359 2 8708494 Fax +359 2 8707273
e-mail: vomidiv@gmail.com
www.bas.bg

Croatian IT Association– CITA
Ilica 191 E/II,
10000 ZAGREB, Croatia
Tel. +385 1 2222 722 Fax +385 1 2222 723
e-mail: hiz@hiz.hr
www.hiz.hr

The Cyprus Computer Society – CCS
P.O.Box 27038
1641 NICOSIA, Cyprus
Tel. +357 22460680 Fax +357 22767349
e-mail: info@ccs.org.cy
www.ccs.org.cy

Czech Society for Cybernetics and Informatics – CSKI
Pod vodarenskou vezi 2,
CZ-182 07 PRAGUE 8 – Liben
Czech Republic
Tel. +420 266 053 901 Fax +420 286 585 789
e-mail: cski@utia.cas.cz
www.cski.cz

Greek Computer Society – GCS
Thessaloniki & Chandri 1, Moshato
GR-18346 ATHENS, Greece
Tel. +30 210 480 2886 Fax +30 210 480 2889
e-mail: epy@epy.gr
www.epy.gr

John v. Neumann Computer Society – NJSZT
P.O. Box 210,
Bathori u. 16
H-1364 BUDAPEST, Hungary
Tel.+36 1 472 2730 Fax +36 1 472 2739
e-mail: titkarsag@njszt.hu
www.njszt.hu

Associazione Italiana per l' Informatica
ed il Calcolo Automatico – AICA
Piazzale R. Morandi, 2
I-20121 MILAN, Italy
Tel. +39 02 760 14082 Fax +39 02 760 15717
e-mail: g.occhini@aicanet.it
www.aicanet.it

Lithuanian Computer Society – LIKS
Geležinio Vilko g. 12-113
LT-01112 VILNIUS, Lithuania
Tel. +370 2 62 05 36
e-mail: liks@liks.lt
www.liks.lt

Macedonian Association for Information
Technology – MASIT
Dimitrie Cupovski 13
1000 SKOPJE, Macedonia
e-mail: indovski.p@gord.com.mk
www.masit.org.mk

Polish Information Processing Society
Zarząd Główny
ul. Solec 38 lok. 103
00-394 Warszawa
Tel./Fax +48 22 838 47 05
e-mail: marek.holynski@gmail.com
www.pti.org.pl

Asociatia pentru Tehnologia Informatiei si
Comunicatii – ATIC
Calea Floreasca Nr. 167, Sectorul 1
014459 BUCAREST, Romania
Tel +402 1 233 1846 Fax +402 1 233 1877
e-mail: info@atic.org.ro
www.atic.org.ro

JISA Union of ICT Societies
Zmaj Jovina 4
11000 BELGRADE, Serbia
Tel.+ 381 11 2620374, 2632996Fax + 381 11 2626576
e- mail: dukic@jisa.rs
www.jisa.rs

Slovak Society for Computer Science – SSCS
KI FMFI UK, Mlynská dolina
SK-842 48 BRATISLAVA, Slovak Rep.
Tel. +421 2 6542 6635 Fax +421 2 6542 7041
e-mail: SSCS@dcs.fmph.uniba.sk
www.informatika.sk

Slovenian Society INFORMATIKA – SSI
Litostrojska cesta 54
SLO-1000 LJUBLJANA, Slovenia
Tel. +386 123 40836 Fax +386 123 40860
e-mail: info@drustvo-informatika.si
www.drustvo-informatika.si