Bulgaria Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports, please use the following details: Mr. Jeremy Beale, ENISA Head of Unit - Stakeholder Relations, Jeremy.Beale@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared the **Bulgaria Country Report**: Dan Cimpean and Johan Meire.

Legal notice

Table of Contents

Bulgaria

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level*
    - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
        - *National authorities*
        - *CERTs*
        - *Industry organisations*
        - *Academic organisations*
        - *Other organisations active in NIS*
    - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
- *Country specific NIS facts, trends, good practices and inspiring cases.*

For more details on the general country information, we suggest the reader to consult the web site: http://europa.eu/abc/european_countries/index_en.htm

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

NIS as part of the information society strategy

The Bulgarian Council of Ministers has adopted a new programme aimed at accelerating the development of Information Society in the country for the period 2008-2010. The document defines the operational framework of the Bulgarian Information Society model. It addresses in particular the use of new knowledge, technologies and practices necessary for generating and implementing technology transfers.

The main national Bulgarian priorities in the establishment of the Information Society are identified as follows:

- building of a national universally available information and communication infrastructure;
- introduction of modern ICT in the management, economy, education, culture, health care, national security system, ecology;
- development of ICT industry as a leading branch;
- adapting the Information Society legislation to the respective EU legislation;
- creation of high qualification specialists for Information Society;
- preparation of the society for adequate realisation in Information Society.

Furthermore, the new programme focuses on the convergence of information and communication technology (ICT), electronic content and public services, as well as the improvement of the quality of life. In doing so, it takes account of the various options that ICT provide in terms of social and economic development. It is to be noted that the new programme covers the concept of 'inclusive Information Society' whose application is intended to integrate all layers of society in the Information Society while supporting the development of human capital.

The key elements of the national Bulgarian NIS strategy are also reflected in different strategies, initiatives and measures implemented or planned by the Government and the various Ministries, or in cooperation with private business. Key strategies or initiatives in the following areas with relevance for the NIS domain are listed below:

e-Governance national strategy

Several elements of the Bulgarian NIS national strategy are covered by the e-Governance initiatives undertaken by various authorities. In Bulgaria, the e-Governance is an element of the transition from industrial to information society and is a tool to increase the competitive ability of the Bulgarian economy and to improve the whole business climate. The goal for implementation of the e-Governance elements in Bulgaria is to allow for:

- Reduction of time, efforts and price for usage of administrative services by citizens and businesses, and for search and access to personal and public data;
- Increase of efficiency and reduction of cost of services provided by the administration.

The process of introduction of the e-Governance in Bulgaria is divided into three stages:

1. **preparatory stage**, related to the adoption of the strategic documents: strategy for modernization of the state administration from accession to integration and strategy for e-government;
2. **experimental stage**, related to the introduction of 20 indicative e-services for the citizens and businesses defined by the European Commission, introduction of e-documents and e-signature in the work of the administration and, as a whole, work on basic, conceptual and methodological projects;
3. **real stage of dynamic development**, during which a re-engineering of the business processes in the administration and total introduction of e-services, including also cross-border services within the frame of the single European market will be carried out.

A number of pilot projects for delivery of on-line administrative services have been implemented at central, regional and municipal level. Some of the most important projects are:

1. Council of Ministers - central portal for services of the e-government to integrate the e-services of the separate administrations as a single entry point of the e-government;
2. National Insurance Institute - e-services for enquiries related to the social and health insurance of citizens, filing statements on social and health insurance of employees by companies, filing of statements on labour contracts of employees by companies;
3. Ministry of Regional Development and Public Works - Citizen Registration and Administrative Services Directorate - change of registration of citizens on current address, verification of registration of election lists for citizens;
4. Ministry of Finance - General Tax Directorate - filing of VAT declarations by companies, income taxation declarations by citizens, corporate taxation declarations by companies; Customs Agency: filing of customs taxation declarations; Information Systems Directorate: filing of offers for placing of small public procurement orders by companies;
5. Ministry of Labour and Social Policy - Employment Agency: demand of jobs in Labour offices;
6. Ministry of Economy, Energy and Tourism - Public Procurement Agency: public procurement electronic register;
7. Ministry of Culture - National Library St. Cyril and Methodiy: search of publications by catalogue information;
8. Stara Zagora Region and Municipality - integrated portal for services of the region and municipality; e-services of the regional administration: issuing of State Property Act of Real Estate, filing of complains to the Regional Department of the Ministry of Interior; e-services of the municipality: issuing of copies of birth certificates, issuing of construction permits.

The Telecommunications Sector Policy

The Ministry of Transport, Information Technology and Communications (MTC) will continue the overall programme, commenced in 1991 by the Committee of Posts and Telecommunications (CPT), for implementation of the necessary reforms related to the transition of telecommunications to development under fully liberalised market conditions.

The Telecommunications Sector Policy gives an idea about the present state and identifies the future directions of development in the sector and outlines the transition in the sector from telecommunications to electronic communications in the sense used in the new EU legal framework 2002. The strategic goal in the telecommunications sector, as stated in the Bulgarian Government Programme in its section on the development of communications and information technologies, is:

- satisfaction of the needs of the business and citizens of modern,
- efficient and quality information and communication services as a necessary condition for Bulgaria's technical and
- technological development and as the basic driver of long-term conditions for growth.

NIS strategy elements in the Bulgarian National Strategy for Counteracting Crime

The Bulgarian National Strategy for Counteracting Crime recognises the cybercrime as an issue with an intensive growth. Therefore, the Bulgarian Council of Ministers has already considered drafting amendments to the Penal Procedure Code in view of the needs of the police authorities in the detection, investigation and drafting the relevant documents for criminal acts in local and network computer systems (searching and seizing computers and relevant devices, information carriers, data, etc.).

The regulatory framework

The following Bulgarian national regulations have relevance and applicability in the domain of network and information security:

e-Governance Legislation

e-Governance Act

An e-Governance bill was drawn up in October 2006 and the ensuing e-Governance Act entered into force on 13 June 2008. The act lays down arrangements for the handling of electronic documents by administrative authorities, the provision of administrative services by electronic means and the circulation of electronic documents among different Administrations.

The scope of the act also extends to other entities that carry out public functions (notaries, central and local educational authorities, etc.) and to providers of public services (health institutions, educational establishments, utilities, telecom operators, postal services, etc.).

One of the act's main principles is that, once a data set concerning an individual or a company comes into the possession of a public body, other public bodies cannot request the same data from this individual or company. On the contrary, they have to request it from the primary data administrator. For example, once an individual is born and the corresponding birth certificate issued, he/she should not need to produce copies of that certificate to any Administration for the rest of his/her life. It is the Administration concerned that has to request the certificate from the issuing authority.

Another important principle requires all public bodies to provide all of their services electronically, and not just manually. Exceptions are allowed only if another law/act explicitly provides for different arrangements. By its very nature, the new act requires strong inter-institutional cooperation. Implementation of the Act is also seen as a major driver of new IT developments. A number of projects are already under way to help different Administrations meet their requirements.

It is worth noting that a month before the entry into force of the e-Governance Act, in April 2008, the Bulgarian Government adopted four ordinances setting out detailed arrangements for the implementation of the future act. These regulations cover, respectively: the delivery of electronic administrative services; the registers of information sites and administrative services; the internal circulation of electronic and paper documents within administrations; and the use of e-Signature in administrations.

In 2008 the Ordinance on the General Requirements on Interoperability and Information Security came into force. It will further facilitate the implementation of the e-Governance Act in terms of information security.

Data Protection/Privacy Legislation

Law for Protection of Personal Data

Adopted in December 2001 and last amended in July 2007, the Law for Protection of Personal Data has been modelled on the EU Directive 95/46/EC on the protection of

individuals with regard to the processing of personal data and on the free movement of such data. It applies to the protection of individuals with regard to the processing of personal data, granting them the right to access and correct information held about them by public and private bodies. Like most of personal data protection laws, the Bulgarian Act defines lawful grounds for the collection, storage and processing of the personal data of individuals.

The application of the Act is overseen by the Commission for Personal Data Protection; an independent supervisory authority created in 2003. The members of this Commission are appointed by the Parliament.

According to the European Commission's Monitoring Report of May 2006 on Bulgaria's progress towards EU accession, Bulgaria's legislation had not yet been aligned with the ''acquis'', in particular with regard to the following aspects: automated processing of personal data; processing of personal data for defense, national security and public order purposes; mechanisms for adopting codes of conduct; tasks of data controllers; time limits to lodge complaints; and provisions concerning notification of processing operations.

eCommerce Legislation

Law on eCommerce

The Law on eCommerce was enacted in Parliament in 2006 in order to implement the EU Directive on electronic commerce (2000/31/EC). It regulates the obligations of service providers with regard to contracts by means of eDevices, and lays down the rules limiting the service providers' responsibilities as to the provision of access and transfer of information services. The law also introduces a definition of 'SPAM', as well as the development of a specialised registry of the people who do not wish to receive such messages.

eCommunications Legislation

Electronic Communications Act

Until May 2007 the telecommunications sector in Bulgaria was regulated by the Telecommunications Act 2003, which implemented the old EU regulatory framework (acquis 1998/2000). Following the country's accession to the EU on 1st January 2007, a new Electronic Communications Act ("ECA") was adopted in May 2007 (promulgated in State Gazette, issue 41, 22 May 2007). This implements into the national law the current EU regulatory framework for electronic communications ("acquis 2002").

The ECA substantially liberalises the telecommunications sector but the full transposition of the new EU regulatory framework is still to come with the adoption of the acts of secondary legislation provided for in the ECA and the forthcoming procedure of market review of the relevant markets.

The National Assembly adopted at the sitting on October 28, 2009, on second reading, amendments to the Electronic Communications Act, tabled by the Council of Ministers. They stipulate the non application of the Act when electronic communications are used by government authorities and their administrations in relation to the national security and by the Council of Ministers for its proper needs.

eSignatures Legislation

Law on Electronic Document and Electronic Signature

The Law on Electronic Document and Electronic Signature (EDESA) was adopted in March 2001 and published in April 2001. It transposed the EU Directive on a Community framework for electronic signatures (1999/93/EC) into Bulgarian law. The law regulates electronic documents and electronic signatures, as well as terms and procedures for providing certification services.

The specific of the Bulgarian legislation in comparison to the eSignatures Directive is related to the definitions of different types of electronic signatures. Indeed, the meaning of "electronic signature" under the Bulgarian EDESA is similar to that of "advanced electronic signature" under the Directive. Likewise, the definition of the "advanced electronic signature" under EDESA's could be equalled to the "qualified electronic signature".

According to EDESA, the universal electronic signature is the only type of electronic signature which has the effect of a handwritten signature, unlike the "basic" and the advanced electronic signatures which have such an effect only among individuals. A universal signature is a type of advanced electronic signature which is supported by a qualified certificate issued by a registered certification service-provider.

eProcurement Legislation

Public Procurement Law

A new Bulgarian Public Procurement Law entered into force in October 2004 and was amended in September 2006. It contains regulations pertaining to eProcurement, covering among others eNotification, eTendering, eAuctions. However, no specific mentioning of information security requirements for public procurements are included.

The only reference to special security measures needed as part of the public procurement is specified in the Art. 6: *"The law shall not apply for public works: 1. (SG 43/02; SG 45/02) connected with the defence and the security of the country which are subject to classified information representing state secret or which implementation shall be accompanied by special security measures in compliance with the effective legislation in the country. The conditions and the order of assigning these public procurements shall be determined by an ordinance adopted by the Council of Ministers upon proposal of the Minister of Interior and the Minister of defence."*

Cybercrime

Penal Code

Several articles of the Bulgarian Penal Code are of relevance in the NIS context:

Art. 319a	(1) A person who obtains unauthorised access to the resources of a computer and copies or uses computer data without permission, when such one is required shall be punished with a fine of up to 3000 leva. (2) In case the act under paragraph one has been committed by two or more persons that have conspired to commit the act, the punishment shall be imprisonment up to one year or a fine of up to 3000 leva. (3) In case the act under paragraph one is committed repeatedly the punishment shall be imprisonment of up to three years or a fine of up to 5000 leva. (4) If the acts under the previous items 1-3 are committed concerning information qualified as government secret, the punishment shall be imprisonment from one to three years, provided there is no heavier punishment prescribed. (5) If the act under item four causes grave consequences, the punishment shall be imprisonment from one to eight years.
Art. 319b	(1) A person who without the permission of the administrator or the user of the computer adds, changes, deletes or destroys a computer program or data when the impact is significant shall be punished with imprisonment up to one year or a fine up to 2 000 leva. (2) In case the act under the previous paragraph has caused significant damage or other grave consequences, the punishment shall be imprisonment up to two years or a fine of 3 000 leva. (3) In case the act under paragraph one has been committed with the purpose of obtaining material benefit the punishment shall be imprisonment from one up to three years or a fine of 5 000 leva.
Art. 319c	(1) A person who commits an act under the previous article with regard to data that by virtue of a law are provided through electronic means or through a magnetic carrier shall be punished by imprisonment of up to two year and fine of up to 3 000 leva. (2) If the act under the previous paragraph has been committed for the purpose of frustrating the execution of duties, the punishment shall be imprisonment up to three years and a fine of up to 5 000 leva.
Art. 319d	(1) A person who brings a computer virus in a computer or the information network shall be punished with a fine of up to 3 000 leva. (2) If significant damage has been caused by the act under the previous paragraph or it has been committed repeatedly the punishment shall be imprisonment up to three years and a fine of up to one thousand leva.

Art. 319e	(1) A person who distributes computer or system password and this results in disclosure of personal data or a government secret shall be punished with imprisonment up to one year. (2) If the act under the previous paragraph has been committed for material advantage or has caused significant damage, the punishment shall be imprisonment up to three years.
Art. 319f	A service provider who violates the provisions of Art. 6, paragraph 2, item 5 of the Electronic Document and Electronic Signature Act shall be punished with a fine of up to 5000 leva, provided he is not punishable with a heavier punishment.

Secondary legislation

The Bulgarian Communications Regulation Commission (CRC) publishes the Secondary legislation relevant to NIS:

- Secondary legislation as per the Law of Electronic Communications, like for example: technical requirements, rules for operation of electronic communication, methodologies, etc.
- Secondary legislation as per the Law on Postal Services, like for example: measures to secure confidentiality of correspondence, methodologies, etc.
- Secondary legislation as per the Law for the Electronic Document and Electronic Signature, like for example: Procedure for Registration of Certification-Service-Providers.

Self-regulations

Self-regulatory Code of Conduct for a Safer Mobile Use by Children and Younger Teenagers

The Bulgarian mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Bulgarian mobile electronic telecommunications market and complies with applicable European and national legislation.

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	• Ministry of Transport, Information Technology and Communications (MTITC) • Communications Regulation Commission (CRC) / Комисия за регулиране на съобщенията (КРС) • Ministry of the Interior / Министерство на вътрешните работи • Chief Directorate for Combating Organised Crime (CDCOC) • Ministry of Defence • State Commission on Information Security (DKSI) • State Agency for National Security
CERTs	• CERT Bulgaria
Industry Organisations	• Association of Bulgarian Telecommunication Companies / Асоциация "Телекомуникации" • Bulgarian Association of Information Technologies (BAIT) • Bulgarian Association of Software Developers (BASD) / Българска асоциация на разработчиците на софтуер (БАРС) • Association for Information Security (ISECA) • Bulgarian Web Association (BWA)
Academic Organisations	• National Laboratory of Computer Virology • Institute for Parallel Processing / Институт по паралелна обработка на информацията • Sofia University "St. Kliment Ohridski", Faculty of Mathematics and Informatics (FMI) • Technical University of Sofia • Technical University of Varna • Academy of the Ministry of Internal Affairs
Others	• Applied Research and Communications Fund • Public Council on Safer Internet Use in Bulgaria • Information Systems Audit and Control Association – Sofia Chapter (ISACA Sofia Chapter) • Bulgarian National Consumers Association • New Horizons Bulgaria

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who" – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory[1].

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

[1] http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation via the Bulgarian Ministry of Transport, Information Technology and Communications

The Bulgarian Ministry of Transport, Information Technology and Communications carries out a set of activities aimed at developing the existing mutually beneficial bilateral and multilateral cooperation on various NIS areas.

According to the General Rules and Procedures of the Ministry of Transport, Information Technology and Communications the key activities of the Ministry include:

- Drafting of programmes, conceptions and analysis for the development of the bilateral and multilateral cooperation of the Ministry;
- Accomplishing the procedures for joining of the Republic of Bulgaria to multilateral and bilateral agreements and other acts in the ICT area;
- Coordination of the participation of the Republic of Bulgaria in the activity of the specialized international and regional organizations in the ICT area, such as International Telecommunication Union, Universal Postal Union, European Conference of Postal and Telecommunications Administrations, satellite organizations, etc.;
- Coordination, preparation and participation in meetings and negotiations; in Bulgaria and abroad;
- Organization, coordination and preparation in international ICT fora held in Bulgaria.

The Ministry organises on a regular basis public discussions and consultations on NIS domain. However, no detail overview of public consultation actions held by the Ministry is currently publicly available.

Co-operation via the Bulgarian Communications Regulation Commission

The Communications Regulation Commission (CRC) organises public consultations on the following areas of regulation that are in its scope: Radio Frequency Spectrum, Electronic Signature, Radio & Telecom Terminal Equipment (R&TTE) and on Numbering. Providers, users, industry associations or public authorities have the possibility to provide their input on the different draft decisions of CRC. Usually, the consultations are open for 30 days. The latest public available annual report of CRC was issued in 2007.

The Bulgarian Ministry of Transport, Information Technology and Communications, being a public body, has the general competence of adopting the country's policy in the electronic communications sector. On the other hand, the Communications Regulation Commission, being the regulator in the electronic communications sector in Bulgaria, has the general oversight competence of the telecommunications sector, in terms of adoption of regulation and its enforcement.

Co-operation and information exchange via CERT Bulgaria

The Computer Security Incidents Response Team within the CERT Bulgaria (governmental CERT) provides the following reactive and pro-active services and information exchange to its constituencies:

Alerts and Warnings	This involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action

	for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected.
Incident Handling	Incident handling involves receiving, triaging and responding to requests and reports, and analyzing incidents and events. Particular response activities can include: • taking action to protect systems and networks affected or threatened by intruder activity • providing solutions and mitigation strategies from relevant advisories or alerts • looking for intruder activity on other parts of the network • filtering network traffic • rebuilding systems • patching or repairing systems • developing other response or workaround strategies.
Announcements	This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.
Security-Related Information Dissemination	Provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include:: • reporting guidelines and contact information for the CSIRT • archives of alerts, warnings, and other announcements • documentation about current best practices • general computer security guidance • policies, procedures, and checklists • patch development and distribution information • vendor links • current statistics and trends in incident reporting • other information that can improve overall security practices.

Co-operation on Safer Internet Use and prevention of child pornography on the Internet

The institutional framework for the hotline's operation already exists and national responsibilities with regard to safer Internet have been defined. The Bulgarian hotline is managed by the Applied Research and Communications Fund in partnership with the State Agency for Child Protection, the Ministry of Interior, the Ministry of Education and Science, the Ministry of Transport, Information Technology and Communications and under the general supervision of a Public Council on Safer Internet Use in Bulgaria.

The Bulgarian hotline supports the European network by co-operating with and assisting the network co-ordinator, exchanging reports with other members of the network, participating in network meetings and working groups established by the network, and in other collaborative activities, such as drafting of best practice papers and documentation or training schemes to exchange expertise between hotlines. The Bulgarian hotline is provisional member of the International Association of Internet Hotlines (INHOPE).

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

Security incidents could be reported to CERT Bulgaria and are handled during working hours between 9:00 and 18:00 h. Incident reports, submitted via WEB, e-mail or fax out of this window of service are handled as soon as a CERT Bulgaria team member is available. The CERT Bulgaria services are offered to employees of the state administration after being registered in the portal of the CERT.

Others

A particular focus of the Bulgarian authorities is on combating illegal software. As such, officers of the Bulgarian Chief Directorate Combating Organized Crime (CDCOC) have seized the biggest amount of illegal music, movies and software, to date, in Bulgaria[2].

As such, this was publicly reported as a key action. This has been a joint operation of the officers from the Computer Crime and Intellectual Property Section with the Chief Directorate Combating Organized Crime -Ministry of Interior and the Section for Fighting Organized Crime with the Ministry of Interior Regional Police Directorate in the coastal town of Burgas. The products have been seized from Internet provider at the territory of Burgas and Yambol. More than 27 terabytes software products of Microsoft, Adobe, Macromedia and Autodesk, the newest movies and music have been spread to all subscribers in Burgas violating the author's right legislation in the country and through optical high speed connection-to the towns of Yambol, Aytos and Karnobat. The total capacity of the server is about 29 000 optical carrier at CD-R format. The files have been divided in categories-movies, music, software and games as the movies category only contains about 5000 titles.

It is interesting to mention that during the first half of 2009, Bulgaria was mentioned in the global report[3] published by the Anti-Phishing Working Group (APWG)[4] with the following relevant statistics:

- 9 unique phishing attacks reported for this country;
- 7 unique domain names used for phishing reported for this country;
- A score of 4.5 phish per 10.000 domains registered in this country;
- A score of 5.7 attacks per 10.000 domains registered in this country.

---

[2] *Source: FOCUS News Agency quoting the Bulgarian Ministry of Interior, 7 November 2009*
[3] *Source: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf*
[4] *The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.*

Emerging NIS risks

The Bulgarian Institute for Parallel Processing (IPP) is an active partner in the FORWARD[5] initiative of the European Commission to promote the collaboration and partnership between academia and industry in their common goal of protecting Information and Communication Technology (ICT) infrastructures. The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defenses, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures.

As part of the "Days of Information and Communication Technologies 2009" conference held from 28th to 31st of October 2009 at Inter Expo Center – Sofia, the representative of the Institute for Parallel Processing, Bulgarian Academy of Sciences presented an overview of the FORWARD initiative and of the identified future and emerging threats in ICT[6].

No relevant information was identified on the participation of Bulgarian CERT, ISPs, etc in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviours and Attack Threats (WOMBAT)[7].

No particular NIS emerging risks reporting was observed being published by the Bulgarian Ministry of Defense or by the Ministry of Interior.

Resilience aspects

In Bulgaria, the specific local term that is preferred to "network resilience" is the term "network integrity". No specific network integrity related preparedness and recovery measures are in place. However there are measures in place when it comes to crisis situations that could affect national security. For these measures both exercises and training is organized.

---

[5] *See: http://www.ict-forward.eu/home*

[6] *See presentation "Future and Emerging Threats in ICT" - Edita Djambazova, Days of Information and Communication Technologies 2009, Sofia, Bulgaria, 28-31 October 2009 referred on http://www.ict-forward.eu/publications/*

[7] *See: http://www.wombat-project.eu/*

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Personal Data Protection Act, promulgated in the State Gazette, Issue No. 1 of 4 January 2002, last amended by the State Gazette, Issue 57 of 13 July 2007 (the "PDPA").

The Bulgarian competent national regulatory authority on this matter is the Commission for Personal Data Protection (the "Commission")

Personal Data and Sensitive Personal Data

The definition of personal data in the PDPA is closely based on the standard definition of personal data. In particular, it only applies to individuals as opposed to legal entities. Under the PDPA, sensitive personal data includes both: (i) the standard types of sensitive personal data; and (ii) information about the human genome.

Processing of such sensitive data may be initiated only if the data controller has obtained an express statement confirming registration with the Commission. The Commission shall issue a statement if after a preliminary inspection the Commission establishes that the data processing will be carried out in conformity with the applicable requirements of the PDPA and in particular the processing complies with the standard conditions for processing sensitive personal data. As a ground for data processing, the data subject's consent does not need to be in writing, although this is often preferred.

Information Security aspects in the local implementation of the Data Protection Directive

The data controller must apply the general data security obligations. The Commission regulates in detail the requirements of the general data security obligations by a regulation passed to this effect under the PDPA and effective as of the end of March 2007. By this regulation the Commission determines the minimum level of technical and organisational measures and the permissible type of security to be provided by a data controller to various types of data processing.

Data protection breaches

The data controller must apply the general data security obligations. The Bulgarian Commission for Personal Data Protection regulates in detail the requirements of the general data security obligations by a regulation passed to this effect under the PDPA and effective as of the end of March 2007. By this regulation the Commission determines the minimum level of technical and organisational measures and the permissible type of security to be provided by a data controller to various types of data processing.

Enforcement

The Bulgarian Commission for Personal Data Protection has full supervisory powers over the activity of data controllers and is competent to issue mandatory directions to, and impose fines and restrictions on, data controllers for breaches of the PDPA. Public prosecutors also have enforcement powers but their scope of competence is limited and they usually act on the request of the Commission.

NIS awareness at the country level

Awareness actions targeting the public authorities and security experts

Security incidents could be reported to and by CERT Bulgaria through several communication channels, including phone, email. The reporting via online forms is under development. CERT Bulgaria is active in providing a list of technical reports of recent vulnerabilities as well as alerts for cyber attacks on the IT systems. Security incidents are reported and useful security advices are provided on how to protect the systems against malicious attacks:

- Warnings - Non-technical reports of recent vulnerabilities, viruses, and other important security information. Warnings are intended for end users who want to be informed about the latest security issues.
- Alerts - Technical reports of recent vulnerabilities, viruses, and other important security information. Alerts are intended for system administrators, system and network security professionals.
- Security Advices - Security advices are short security best practice documents for end users.

Incidents could be reported to CERT Bulgaria by anyone, who had found a vulnerability in the system he/she supports. The information about incidents, vulnerabilities and attacks is available to the public.

The Centre for Security and Defence Management (CSDM) of the Institute for Parallel Processing (IPP)[8] is an academic unit, conducting theoretical and applied research according to highest professional standards.

It has an important role in the awareness raising efforts in Bulgaria, by providing unbiased, politically neutral support to the formulation and the implementation of security and defence policies. CSDM also facilitates informed, constructive, and innovative public debates on key security and defence issues, including the national contribution to European Security and Defence Policy (ESDP) and the NATO security strategy. CSDM conducts research, provides advice, focused training and interactive simulations in the fields of:

- Security and Defence Policy and Strategy
- Foresight-based, Capabilities-oriented Security and Defence Planning
- Organisational Design and Process Improvement
- Security and Defence Technological and Industrial Base
- Critical Infrastructure Protection & Civil Security
- Information Security
- Good Governance in the Security Sector: Transparency, Accountability, Integrity
- Knowledge Management and Organisational Learning

Based on its own research results, and in cooperation with its international partners, CSDM provides training and qualification opportunities for security and defence experts from parliament, the executive, and civil society organisations. In its projects, CSDM involves permanent researchers, associated senior fellows, support staff, and doctoral students, as well as other Bulgarian and foreign experts. CSDM disseminates its research results mainly through:

[8] *The IPP operates under the authority of the Bulgarian Academy of Science*

- Information & Security: An International Journal (English language quarterly),
- the monograph series in Security and Defence Management (in English, occasionally translated in other languages),
- the book series on "Information & Security" and "Managing Change in the Security Sector", in Bulgarian, and
- via other refereed journals, conference proceedings, and popular media.

The Information & Security journal of CSDM covers scientific, technical and policy issues related to national and international security in the information age, C4ISR technologies and systems, information operations, command and control warfare, and information assurance. The objective is to bridge the IT and the security communities, presenting state of the art, new findings, ideas and needs of the one community to the other, as well as to present latest research, conducted 'on the bridge' between the two communities. The journal is published in English four times per year both on paper and in electronic form on the web site[9].

Awareness actions targeting the consumers/citizens

The Bulgarian General Direction for Combating Organized Crime (CDCOC) maintains a web site aimed to provide useful information about essential cybercrime terminology, explained in a clear and understandable manner and advice on how to protect against it.

Other awareness-raising vehicles

The Bulgarian Hotline web site for illegal and harmful content on Internet site was built by Applied Research and Communications Fund in the framework of the SAFE-NET BG project supported by the European Commission. Its goal is to establish a national Safer Internet Hotline in Bulgaria that should enable local Internet users to report incidences of harmful and illegal content disseminated over the Internet, with a special focus on child pornography.

At the current stage of its implementation the hotline is primarily concerned with issues of child pornography on the Internet but the scope of activity may be extended to cover also other forms of harmful content and conduct, as well as other interactive technologies (incl. mobile, online games, chat channels, etc.).

For the past nine years the i-Security Forum[10] in Bulgaria has delivered information on security and storage systems. It is organized through a partnership between International Data Group and the local chapter of the Information Systems Audit and Control Association (ISACA). The forum presents the latest problems and solutions related to sustaining effective information security, covering such topics as COBIT, identity management, business continuity, access control, defining and defending against the latest security threats, data management and storage optimization. The audience description:

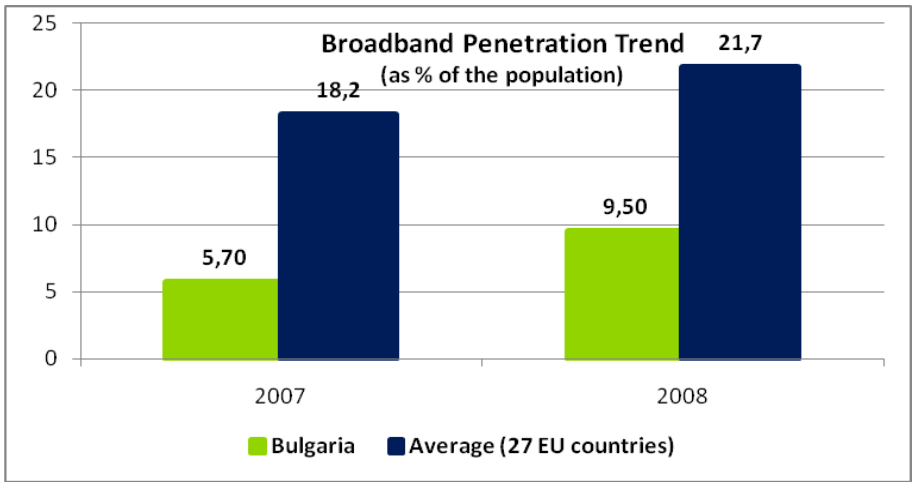
- 33% of attendees are CSOs and CIOs
- 23% are security experts
- 20% are senior managers (managing directors, CEOs, CFOs)
- 14% are auditors.

[9] *See: http://infosec.procon.bg/*
[10] *See http://events.idg.bg*

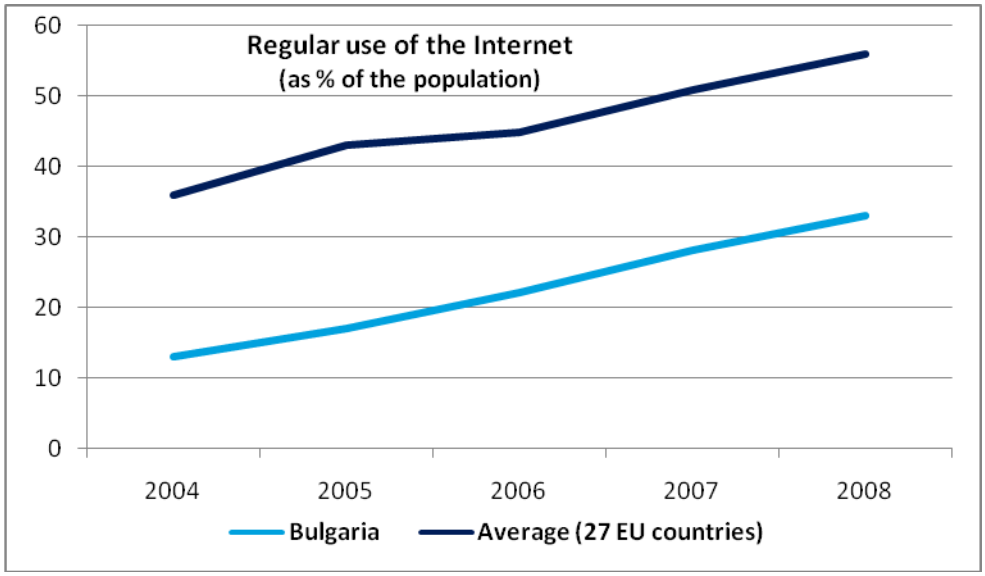
Relevant statistics for the country

The information society in Bulgaria is at a relatively early stage of development. Although progress has taken place since last year in the areas of broadband and internet usage, there is still significant room for improvement: very low rankings on broadband penetration, of Internet usage and e-Governance show the urgent need of further efforts to narrow the gap with the rest of Europe.

Based on the Eurostat[11] information, it appears that the broadband penetration trend for Bulgaria is significantly currently below the EU average:



Based on the same source of information, the regular use of Internet by the population (use as % of the population) is constantly below the EU average but it continues on an increasing path. Rates of internet usage have been gradually improving over the last few years. Nevertheless, take-up of the Internet in Bulgaria is still low and a major segment of the population has never used the Internet. Usage of Internet services is correspondingly low.



[11] *Source: Eurostat*

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of Transport, Information Technology and Communications (MTITC)	Policy in the NIS domain, keeping registers of standards on interoperability and information security. Keeping lists of accredited entities and certified information systems. Accreditation of entities for certification of information systems.	http://www.daits.government.bg
2. Communications Regulation Commission (CRC) / Комисия за регулиране на съобщенията (КРС)	The Communications Regulation Commission (CRC) implements the state sector policy in the field of telecommunications and postal services. CRC is a specialized independent state authority, entrusted with the functions of regulation and control over the carrying out of the electronic communications. In the context of equity and transparency and in compliance with the Bulgarian legislation, CRC strives to promote the competition of the telecommunications markets in the country. The national regulator proceeds, aiming at the increase of the sector investments, the new communications technologies' development and the protection of the end-users in Bulgaria.	http://www.crc.bg
3. Ministry of the Interior / Министерство на вътрешните работи 4. Chief Directorate for Combating Organised Crime (CDCOC)	Activities aimed at protection of information and communication systems related to national security. The Chief Directorate for Combating Organised Crime of the Bulgarian Ministry of Interior maintains a web site with the aim of increasing awareness on phishing, spoofing, pharming, viruses, etc. This site is linked to EuroISPA and provides useful information about the important phishing.	http://www.mvr.bg http://www.cybercrime.bg
5. Ministry of Defence	Strategic guidance to the armed forces related to information security; availability of CERT for defence purposes. The issue of critical infrastructure defence is closely monitored by the Bulgarian Ministry of Defence. Special attention is given to the new phenomenon – cyber security. The example with cyber attacks on Estonia (2007) and Georgia (2008) increased the focus on the fact Bulgaria is facing a relatively new threat for which it has to be prepared.	http://www.mod.bg
6. State Commission on Information Security (DKSI)	State body pursuing the policy of the Republic of Bulgaria on classified information. The State Commission on Information Security organizes, controls and is responsible for the fulfilment of obligations on classified information protection, arising from international treaties to which Bulgaria is a party.	http://www.dksi.bg
7. State Agency for National Security	The agency prevents destructive actions toward communications and information systems and provides help to institutions and business in case of security incidents.	N/A

Computer Emergency Response Teams (CERTs): roles and responsibilities

CERT	FIRST member	TI Listed	Role and responsibilities	Website
8. CERT Bulgaria	No	Yes	CERT Bulgaria is the Governmental Computer Security Incidents Response Team. Its mission is to provide information and assistance to its constituencies in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents when they occur. CERT Bulgaria is already accredited by Trusted Introducer.	www.govcert.bg

Industry organisations active in network and information security: role and responsibilities

Industry organisations	Role and responsibilities	Website
9. Association of Bulgarian Telecommunication Companies / Асоциация "Телекомуникации"	The Telecommunications Association was founded in April 2002 as a non-profit, non-governmental organisation. Its members are 50 reputable legal and natural persons, among which recognised public telecommunications operators, international and local manufactures and suppliers of communications equipment, legal and telecom consultants, IT and Internet businesses, Sofia's university 'St Kliment Ohridski' and the technical universities of Sofia and Varna as well the New Bulgarian University and the Higher College of Telecommunications and Post. The Telecommunications Association focus on co-operation in elaborating of the new legal framework, consulting the national policy and regulatory authorities in telecommunications market regulations, participation in EU fostered programs, promoting an improved information environment for telecommunications players, and enhancement of qualification and professional training of its members' staff. The Association supports the business and professional relationships of its members, their ongoing dialogue with governmental authorities as the Ministry of Transport, Information Technology and Communications, the Commission on Regulation of Communications, etc. The Association's would like to bring in local and foreign experts in Committees on issues like information technologies, R&S, legal, economic and others, directly relating to its members' activities.	www.astel-bg.com
10. Bulgarian Association of Information Technologies (BAIT)	The Bulgarian Association of Information Technologies (BAIT) is the biggest branch organisation in the field of information and communication technologies in Bulgaria. Established in 1995 by seven founder-member companies, there are more than 170 company members presently in it, the greatest part of which are leaders in hardware, software, system integration, telecommunications, Internet and other fields of the ICT market on the Bulgarian market. The mission of BAIT is to protect the interests of its	www.bait.bg

Industry organisations	Role and responsibilities	Website
	members by applying information technologies for priorities in the development of Bulgaria. BAIT is an active partner of the State and legislative authorities in the formation of a State policy in the sphere of information and communication technologies, and in order to achieve its goals it cooperates with other non-governmental branch and employers' organisations.	
11. Bulgarian Association of Software Developers (BASD) / Българска асоциация на разработчиците на софтуер (БАРС)	BASD is a non-profit organization that actively supports the professional development of the Bulgarian developers by various activities, aiming to improve their knowledge and skills in the area of software design and development. The Association organizes conferences, seminars and training courses for software development and software technologies specialists.	www.devbg.org
12. Association for Information Security (ISECA)	ISECA is a non-profit organization, aimed at building of awareness of the IS risks and protection necessity and at boosting the development of professional attitude and high standards in IT area.	www.iseca.org
13. Bulgarian Web Association (BWA)	BWA keeps up with the web technologies development for achieving professional standards for quality web services and products in Bulgaria. BWA promotes the advantages of web and Internet among the business society, general audience, and government and non-government organizations.	www.bwa.bg

Academic bodies: role and responsibilities, tasks

Academic organisations	Role and responsibilities	Website
14. National Laboratory of Computer Virology	Scientific organization in Bulgaria, specialized in the domain of computer virology and security.	www.nlcv.bas.bg
15. Institute for Parallel Processing / Институт по паралелна обработка на информацията	The Institute for Parallel Processing (IPP) is responsible for information security of the academic network in Bulgaria. Its Information Security department includes: **Centre for Security and Defence Management (CSDM)** - conducts research, provides policy advice, focused training and interactive simulations in: • Security and Defence Policy and Strategy • Foresight-based, Capabilities-oriented Security and Defence Planning • Organisational Design and Process Improvement • Security and Defence Technological and Industrial Base • Critical Infrastructure Protection & Civil Security • Information Security • Good Governance in the Security Sector: Transparency, Accountability, Integrity • Knowledge Management and Organisational Learning It also includes the **Joint Training, Simulation, and Analysis Centre (JTSAC).** It is active in providing support to security and defence policy formulation and implementation, including through concept development and experimentation and support to training. The interdisciplinary research team of IPP explores, advances and applies methodologies and tools	http://www.bas.bg www.caxbg.com/is

Academic organisations	Role and responsibilities	Website
	for IT governance and change management, design and analysis of architectures and capabilities, modelling and simulation for the security sector, and information security management.	
16. Sofia University "St. Kliment Ohridski", Faculty of Mathematics and Informatics (FMI)	The university conducts teaching, training and research and development in Information Technologies. The course "Information security in computer systems and networks" is a Master program and is 3 semesters long. The university cooperates with IT companies in the organization of different events and trainings in the IT security field.	www.fmi.uni-sofia.bg
17. Technical University of Sofia	The largest higher engineering school in Bulgaria. The Faculty of computer systems provides bachelor and master programs, which include courses in IT security. For example the course "Security Code Writing" is part of the bachelor program "Computer systems".	www.tu-sofia.bg
18. Technical University of Varna	The department of Computer Science and Engineering provides courses in IT security. The faculty is partnering with Cisco Systems and Microsoft.	http://www.tu-varna.bg/
19. Academy of the Ministry of Internal Affairs	The academy is educating professionals for the National Police and the other national security offices; the IT systems protection is part of the bachelor degree program "National security protection".	www.academy.mvr.bg/default.htm

Other bodies and organisations active in network and information security: role and responsibilities

Others	Role and responsibilities	Website
20. Applied Research and Communications Fund	The fund conducts applied research and analysis that assists the development and implementation of public policies. The organization was established to promote innovation in the European economy and facilitate the transfer of new and advanced technologies and know-how, and to support cross-border networking and capacity building of businesses, public agencies or private organizations, by using the advances in information and communication technologies.	www.arcfund.net
21. Public Council on Safer Internet Use in Bulgaria	The council supports the national Safer Internet Hotline in Bulgaria that enables local Internet users to report incidences of harmful and illegal content disseminated over the Internet. At the initial stage of its implementation the hotline will be primarily concerned with issues of child pornography on the Internet but, as the service gains experience and public recognition, the scope of activity will be extended to cover also other forms of harmful content and conduct, as well as other interactive technologies (including mobile, online games, chat channels, etc.)	www.web112.net/en/
22. Information Systems Audit and Control Association – Sofia Chapter (ISACA)	The organisation's prime focus is to expand its members' knowledge in the IT governance and control field by providing training, resource sharing, advocacy, professional networking and other benefits. The Sofia Chapter is part of ISACA worldwide. The organization certifies in a number of IT professional skills (CISA, CISM,	www.isaca-sofia.org

Others	Role and responsibilities	Website
	CGEIT) and CobiT.	
23. Bulgarian National Consumers Association	A consumer organisation, its aim is to protect and educate consumers. Has responsibilities in the Bulgarian educational strategy on Internet safety: • "Development and initial implementation of an educational strategy on Internet safety for multipliers, teachers and parents", focused on the creation of common strategy and action plan for the informal education of European adult citizens on how to protect their children on the Internet • "Initial application of an educational strategy measures on children Internet safety for teachers and parents"	www.bnap.org/en
24. New Horizons Bulgaria	New Horizons Bulgaria is a successor of all the activities performed by Consulting & Technical Education Company (CTEC-BG) and provides full range of solutions in the transfer of knowledge area: technical training (information security, ITIL, Microsoft, Cisco, IBM etc.).	www.newhorizons.bg

Country specific NIS glossary

Broadband Penetration Indicator	Number of total subscriptions to broadband connections (households, enterprises, public sector) by platform (DSL, all others) divided by the number of inhabitants. 3G subscriptions are not included in the total. Source: European Commission.
CDCOC	General Direction for Combating Organized Crime
CPT	Committee of Posts and Telecommunications
CRC	Communications Regulation Commission
CSDM	Centre for Security and Defence Management
DPA	Data Protection Act
ECA	Electronic Communications Act
EDESA	Electronic Document and Electronic Signature
ESDP	European Security and Defence Policy
IPP	Institute for Parallel Processing
Personal Data	The definition of personal data in Bulgarian legislation is closely based on the standard definition of personal data. In particular, it only applies to individuals as opposed to legal entities. We refer to the Bulgarian Personal Data Protection Act, promulgated in the State Gazette, Issue No. 1 of 4 January 2002, last amended by the State Gazette, Issue 57 of 13 July 2007.
R&TTE	Radio & Telecom Terminal Equipment

References

- European Commission, Europe's Digital Competitiveness Report, Volume 2: i2010 — ICT Country Profiles available at http://ec.europa.eu/information_society/eeurope/i2010/key_documents/index_en.htm#EDCR
- An overview of the eGovernment and eInclusion situation in Europe, available at http://www.epractice.eu/en/factsheets
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Bulgarian Personal Data Protection Act, promulgated in the State Gazette, Issue No. 1 of 4 January 2002, last amended by the State Gazette, Issue 57 of 13 July 2007.

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu