

Romania Country Report



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:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@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 this country report on behalf of ENISA: **Dan Cimpean, Johan Meire, Andrei Ionescu and Bogdan G. Petre.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

Table of Contents

ROMANIA	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	7
NIS GOVERNANCE	13
OVERVIEW OF THE KEY STAKEHOLDERS	13
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	14
FOSTERING A PROACTIVE NIS COMMUNITY	18
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	19
SECURITY INCIDENT MANAGEMENT	19
EMERGING NIS RISKS	19
RESILIENCE ASPECTS	20
PRIVACY AND TRUST	20
NIS AWARENESS AT THE COUNTRY LEVEL	21
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY	23
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	23
RELEVANT STATISTICS FOR THE COUNTRY	25
INTERNET ACCESS OF POPULATION AND ENTERPRISES	25
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	26
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	27
OTHER STATISTICS	28
APPENDIX	29
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY	29
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	33
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	34
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	35
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	36
REFERENCES	36

Romania

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:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
 - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
 - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Government Programme 2009-2013 (e-Romania)

During 2009, the Romanian Government has approved the “e-Romania” national strategy proposed by the Romanian **Ministry of Communications and Information Society (i.e. the MCIS)**. For the 2010-2013 the above national strategy aims the state modernization through an improved computerized interaction with citizens and businesses.

The policy is aimed at leading the entire public sector to the information society and knowledge based society. The eGovernment system would be the main tool for building a national integrated system for the online public services designed for citizens and businesses.

The main objectives stipulated by the National Government Plan of the Romanian Government with regard to ICT include the increase of:

- Citizens’ comfort;
- Public administration's performance through coherent and efficient implementation of IT integrated systems;
- Competitiveness of national economy by promoting information society.

The national goals and priorities are based on the current requirements of the Romanian society, in accordance with the European provisions and making use of cooperation and financing mechanisms. The main objectives are:

- The economic and social development through the use of ICT in the eGovernment system;
- Providing high quality public services, financially accessible and acceptable;
- Increased capacity of the Government to make decisions regarding the participative and consultative process;
- The responsible and efficient approach, together with lowering the costs, of all the involved parties;
- Transparency in implementing, designing, maintaining and revising policies.

All national ICT policies and strategies in place recognise that the construction of the new society model requires a series of major socio-political changes. These changes are related to the decrease of the exclusion phenomena thanks to the benefits of the new technologies ('digital pide') to certain social categories and geographical regions/areas; these problems concern the social cohesion, the promotion, and conservation of the specific culture of the nation and local community, the protection of the citizen and consumer.

According to the programme, particular focus will be placed on adopting the large-scale use of IT in the business environment, in relation with the citizens and the Public Administration.

For implementing the current strategy, MCSI will elaborate national guidelines, standards, national priorities, interoperability framework, while the local and regional authorities will formulate their own strategies that would have to address to main user groups. The implementation of the strategy will be completed according to different protocols of cooperation and funding.

Government Programme

The key NIS-related objectives objectives from the Government Programme for 2004-2008 are still valid and also included as part of the new Government Programme for 2009-2013.

Part of the Romanian Government political programme 2004-2008, under the sections **"eGovernment Programme"** and **"Policy in the field of information technology and communications"** a series of specific measures are included, with relevance on the domain of network and information security.

The Romanian Government is aimed to promote a set of measures that will allow the improvement of IT indicators, will make flexible the structures of central and local administration for the initiation, sustaining and starting IT projects by the small and medium sized enterprises, as well as open some programs of financing the projects in cooperation with internal and international institutions.

The eGovernment has been actively promoted in the last years, being considered as the best way of organising public management in order to increase efficiency, transparency, accessibility and responsiveness to citizens, while reducing bureaucracy and corruption.

Lack of Internet access and IT skills are the main barriers in Romania in the implementation of the NIS strategies and initiatives, but never the less the resistance to the Internet cannot be neglected as a large part of population seems to be not aware its benefits. In order to overcome those challenges, e-inclusion actions have been promoted under the objective of "increasing the citizens' comfort".

IT strategy developed by Ministry of Communications and Information Society(MCIS)

The mission of the MCIS is to create solid premises that will ensure the transition to the Information Society in Romania. The Information Society is an objective of the development and not a desideratum in itself; it is an essential component of the politic and economic programme for development 2004-2008.

The government policies applied by MCIS are going to strengthen the benefits that ICT brought to Romanian economy and society, to create new opportunities and to include all citizens in the knowledge based economy.

MCIS is managing the following relevant NIS Romanian national strategies¹:

- The Romanian national strategy for development of the broadband eCommunications 2009-2015;
- The strategy for the universal service;
- The strategy for the transition from analogue to digital television and for digital multimedia services.

In addition, it also manages a set of nation-wide initiatives that are relevant for the NIS context:

- National-wide guidance for public authorities for managing their web sites;
- Electronic signature;
- Electronic archiving, etc.

¹ We refer to the strategy documents published on the website of the Ministry (only in Romanian): <http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Comunicatii-electronice/Strategii>

The regulatory framework

Since beginning of 2010 there were no major changes related to the Romanian regulatory framework applicable to NIS domain.

The main regulatory elements which define the regulatory framework are: the Law on Electronic Signature (2001); the Law on Free Access to Information of Public Interest (2001); the Law on the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data (2001); the Law on Electronic Commerce (2002); the Law regarding the electronic payment of local taxes (2002); the Law on the processing of personal data and the protection of privacy in the electronic communications sector (2004) and the Ordinance concerning the award of public contracts, public works concession contracts and services concession contracts (2006).

Romania was the first country in Europe to transpose the European Union regulatory framework for eCommunications into national legislation, between 2002 and 2003. The following Romanian national regulations have relevance and applicability in the domain of network and information security:

eGovernment Legislation

Government Decision no. 1085/2003

The Romanian Government has dedicated a lot of effort in recent years to develop a legal framework favoring the development of the Information Society and eGovernment. The Government Decision no. 1085/2003 concerns the application of some provision of Law no. 161/2003, regarding certain measures for assuring transparency in exerting public dignities and public functions as well as in business environment, regarding the prevention and prosecution of corruption and the implementation of a National Electronic System.

eCommunications Legislation

During 2010, a draft law on electronic communications issued by ANCOM was posted for public debate on ANCOM website.

Ordinance on access to the electronic communications networks and to the associated facilities, as well as their interconnection

Romania was the first country in Europe to transpose the European Union regulatory framework for electronic communications into national legislation. On January 2002, the Government approved the Ordinance on access to the electronic communications networks and to the associated facilities, as well as their interconnection (no. 34/2002). Its provisions are organised around the following points of interest: defining new concepts related to electronic communications, rights and obligations of the operators, powers of the national regulatory authority and possibility for the regulatory authority to impose specific obligations on operators with significant market power.

Special attention was paid to the obligations for unbundled access to the local loop: the regulatory authority may impose on the operator with significant power on the market for local loop the obligation to publish a reference offer for unbundled access to the twisted metal pair local loop. This law transposes the 2002/19/EC (Access Directive) into national legislation.

Law regarding the Universal Service and the Users' Right related to the Networks and Electronic Communications Services

The total liberalisation of the Romanian telecom market took place on 1 January 2003. In July 2003, the law regarding the universal service and the users' right related to the networks and electronic communications services (no. 304/2003) came into force.

The law implements principles such as the interdiction to grant any special or exclusive rights for the provision of directory services and transposes the 2002/22/EC (Universal Service Directive) into national legislation. This law is of particular importance and impact on the Romanian eCommunications, due to the lower maturity of the market, the low penetration rate of eCommunications in general, and due to the historical monopoly of the Romanian major telecom operator.

Law on the processing of personal data and the protection of privacy in the electronic communications sector

The Law on the processing of personal data and the protection of privacy in the electronic communications sector (no.506/2004) transposes the 2002/58/EC on privacy and electronic communications into Romanian law

Data Protection/Privacy Legislation

Transposition into national law of the Data Retention Directive 2006/24/EC²

The directive DIRECTIVE 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks was transposed during 2008 into the national law no. 298/2008.³ This new law triggered the reaction of the Constitutional Court of Romania and during 2009 the Court decided through the Decision no 1.258/2009⁴ that the law violates constitutional rights, that the transposing act violated the constitutional rights of privacy, of confidentiality in communications, and of free speech.

Law for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data

The basic law (no. 677/2001) allows individuals to access and correct personal information held by public or private bodies. It was complemented by recent additions such as law no. 55, (OJ. no. 244/23.03.2005), which ratifies the Additional Protocol to The Convention for the Protection of Individuals with regard to automatic processing of personal data, referring to control authorities and cross-border data flow.

Furthermore, a National Supervisory Authority for Personal Data Processing was established in 2005 by law no. 102/2005 (O.J. no. 391/ 09.05.2005). All of the data protection files previously kept by the Ombudsman have now been handed over to the Authority, which supervises and controls the legality of the personal data processing falling under the law no. 677/2001.

² Directive 2006/24/EC available at: : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

³ More details about national law 298/2008 available at: http://www.cdep.ro/pls/legis/legis_pck.http_act?ida=83447

⁴ More details about Decision no 1.258/2009 available at: http://www.cdep.ro/pls/legis/legis_pck.http_act?ida=92800

Law on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector

This law (no. 506/2004) on the processing of personal data and the protection of privacy in the electronic communications sector replaced Law no. 676 of 21 November 2001 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. It closely follows the Directive 2002/58/EC on personal data processing and privacy protection in the electronic communications sector.

eCommerce Legislation

Law on electronic commerce

This law was adopted in June 2002 (no. 365/2002) and modified in May 2006 by law no. 121/2006. It transposes the main provisions of the Directive 2000/31/EC on eCommerce. The law defines eCommerce and other basic concepts, such as electronic messaging or exchange of data over the Internet.

The main points addressed by the law are the following: free movement of Information Society services, contracts concluded by electronic means, commercial communications through electronic means and ePayments forgery. The law stipulates heavy punishments for the possession of equipments for falsifying electronic payments instruments.

ePayment Legislation

In January 2006, an amendment to an ordinance regulating electronic payments between the Government and citizens was adopted.

As the first stage of the Ministry of Communications and Information Society (MCIS) Virtual Payment Office project, it allows for the electronic payment of fines, taxes and other fiscal obligations.

eProcurement

Government Emergency Ordinance concerning the Award of Public Contracts, Public Works Concessions Contracts and Services Concession Contracts

Adopted in June 2006, this ordinance (no. 34/2006) revoked all the previous acts containing provisions on public procurement and merged the two EC eProcurement directives ([2004/17/EC](#) and [2004/18/EC](#)) in a sole act.

Law no. 337/2006

Law for the approval of the Government Emergency Ordinance no. 34/2006 regarding the award of public procurement contracts, public works concession contracts and service concession contracts, introducing amendments and supplements.

Government Decision no. 1660/2006

Decision on the approval of Application Norms for the award of public contracts by electronic means from the "Government Emergency Ordinance no. 34/2006, concerning the award of public contracts, public work concession contracts and services concession contracts".

Government Decision no. 925/2006

Decision on the approval of the Application Norms for the provisions concerning the award of the public procurement contracts using electronic means, according to the G.E.O. no. 34/2006, regarding the award of the public procurement contracts, public works concession contracts and service concession contracts. This decision has been supplemented by the *Government Decision no. 1337/2006*.

Government Ordinance no. 94

The Government Ordinance no. 94 on the modification and completion of the Government Emergency Ordinance no. 34/2006 on the award of the public procurement contracts, public works concession contracts and service concession contracts was published in the Official Gazette no. 676 of October 4, 2007, introducing important changes in the existing eProcurement legal framework.

Government Decision no. 198/2008

Decision on modifying and supplementing application norms concerning the award of public contracts by electronic means from the "Government Emergency Ordinance no 34/2006 concerning the award of public contracts, public work concession contracts and services concession contracts" approved by Government Decision no 1660/2006. This legal act is the legislative expression of Manchester Declaration from 2005 of ministers in charge for eGovernment politics from the Member States, candidate states and EFTA countries.

Secondary legislation from National Authority for Management and Regulation in Communications (ANCOM)

Methodological norms (implementation guidance) for the authorization of data centres

ANCOM submits to public notice and comment the methodological norms for the authorization of data centres methodological norms for the storage of documents in electronic archives. The Order of the Ministry no. 489/2009 on the methodological norms for the authorization of data centres, published in part I of the Romanian Official Gazette no. 435 of June 25, 2009 basically lays down the procedure and conditions with respect to the grant, annulment and withdrawal of the authorization of data centres where electronic archives are stored.

The prior authorization of data centres seeks thus to meet some elementary conditions regarding the integrity and security of documents in electronic form and of the space used by the hardware hosting electronic archives, as well the recovery of information as a result of unforeseen situations.

The data centres used by electronic archive administrators represent the secured spaces where any and all electronic documents filed to be kept by the beneficiaries are stored. Therefore, for the proper operation of such data centres it is essential that adequate information equipment and special facilities be used so that the security and accessibility of the information kept be ensured. Data centres must provide a safe infrastructure for the operations carried out by electronic archive administrators, limiting thus the chances of incidents likely to trigger security breaches or the failure of the service supply to the public. Furthermore, the data centre must ensure the security and integrity of the stored information, both in terms of physical access to the employed equipment, and of the remote access to the archived documents.

Other department regulations

Department regulations are effective in the domain of responsibility of their respective issuing authority. The following department regulations have relevance and applicability in the domain of network and information security:

- Other regulations of the National Authority for Management and Regulation in Communications (ANCOM);
- ORNISS directives: national classified information; NATO classified information; EU classified information.
- Various orders of the Ministry of Internal Affairs;
- Romanian Intelligence Service recommendations;
- Foreign Intelligence Service recommendations;
- Special Telecommunications Service recommendations;
- Ministry of Justice recommendations
- Ministry of Defense recommendations
- Provisions of National Bank of Romania;

Cybercrime

Computer crimes covered by the Romanian Anti-corruption Law

Several articles of the Romanian Anti-corruption Law are of relevance in the NIS context, as they directly address the computer misuse and the unlawful access to, or use of, information. This is an aspect very relevant for Romania, in particular due to the overall higher-level of computer criminality in this new Member State.

As such, there is significant focus from Romanian NIS stakeholders on awareness, prevention and correction of computer criminality. The most relevant computer-related illegal acts addressed relate to acts that involve:

- Illegal access to data;
- Illegal transmitting, altering, deleting or deteriorating computer data;
- The production, sale, import, distribution of a device or a computer programme designed to be used for illegal purposes.

The Service for Combating Cybercrime under the Romanian Directorate for Investigating Organised Crime and Terrorism Offences of the Prosecutor's Office of the High Court of Cassation and Justice (DIICOT) is the competent Romanian Authority in enforcing the legal measures against the cybercrime. The competences of DIICOT for combating cybercrime meet the requirements set out in the Convention on Cybercrime on international cooperation, being also the contact point available 24/7.

Self-regulations of telecommunications providers

Code of Conduct for safely using the content provided on the mobile phone

The Romanian 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 Romanian mobile electronic telecommunications market and complies with applicable European and national legislation.

eSignatures Legislation

Law on electronic Signature

The law no. 455/2001 grants to an eSignature the same legal status as a written one. This effectively places electronic and printed data on an equal footing and allows electronic data to be admitted as evidence in court in the event of a dispute. The Ministry of Communications and Information Society (MCIS) is the authority in charge of the regulation of eSignatures. The procedure for approving, delaying and recalling the decision of accreditation of the certification services providers is also defined (OJ no.209/ 11.03.2005).

eIdentification/eAuthentication

The National Person Identity System is a large project of the Ministry of Administration and Interior, under development, concerning the computerised record of civil status for all citizens. Modules include the Civil Information System, the Identity Card System, the Passport system, the Driving Licence and Car Registration system, and the Personal Record System. Of those, the Civil Information System concerns issuance and renewal of civil information and documents for Romanian citizens, such as birth certificates, marriage certificates and death certificates, among other.

Furthermore, work on biometric passports and electronic ID cards has started and an international auction has been launched.

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	<ul style="list-style-type: none"> • Ministry of Communications and Information Society (MCSI) • National Authority for Management and Regulation in Communications (ANCOM) • National Centre for Management of Information Society (CNMSI) • National Centre "Digital Romania" (CNRD) • National Authority for the Supervision of Personal Data Processing / Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) • ORNISS (The National Registry Office for Classified Information) • IT&C Commission – Chamber of Deputies • Ministry of Internal Affairs and Public Administration Reform (MIRA) • Special Telecommunications Service (STS) • Ministry of Defence • Romanian Intelligence Service (SRI) • Foreign Intelligence Service (SIE) • Service for Combating Cybercrime under the Romanian Directorate for Investigating Organized Crime and Terrorism of the Prosecutor's Office of the High Court of Cassation and Justice (DIICOT)
CERTs	<ul style="list-style-type: none"> • RoCSIRT (ex. RoEduNet CSIRT) • CORIS-STs • CERT-RO
Industry Organisations	<ul style="list-style-type: none"> • Aries (Romanian Association for Electronic and Software Industry) • National Association of Romanian ISPs (ANISP) • Employers' Association of the Software Industry and Services (ANIS) • Association for IT&C (ATIC) • Association of Telecommunications Operators • Cable Communication Association
Academic Organisations	<ul style="list-style-type: none"> • Military Technical Academy • National Communications Research Institute / Institutul Național de Studii și Cercetări pentru Comunicații (INSCC) • National Institute for Research and Development in Informatics (ICI)
Others	<ul style="list-style-type: none"> • Information Systems Audit and Control Association – Romanian Chapter (ISACA) • Foundation for promoting Information and Communication Technology (FICT) • Romanian Association of Telecommunications' Engineers • Association for Consumers' Protection / Asociația pentru Protecția Consumatorilor din România (APC)

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁵ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁶.

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,

⁵ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

⁶ See: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

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

In November 2008, the **Agency for Information Society Services (ASSI)** published its strategy which provides an overview of the eGovernment strategy in Romania. It summarizes the generic and specific principles of the Agency and it proposes ways to proceed towards the fulfillment of its mission. On 2009 based on **Law No. 329/2009** the ASSI was disbanded

Since March, 2010 the work and duties of ASSI were taken over by the **National Centre for Management of Information Society (CNMSI)** and **National Centre "Digital Romania" (CNRD)** based on the **Government Decision No 1439 of 18 November 2009**.

Their mission remains to increase citizen's comfort by improving the Public Administration performances. It specifically aims:

- To ensure unique access between the public institutions and the beneficiaries of their services;
- To become the central provider of back office services for common and specific processes of several institutions;
- To ensure data reusability between public institutions.

National Interoperability Framework (NIF)

The Romanian NIF is emerging. It will build on existing initiatives such as the National Electronic System (Sistemul Electronic National – SEN). At the time of this analysis, a law on interoperability is in the parliament. This law will mandate the NIF and define the governance structure surrounding it.

Ownership of the NIF will lie with the National Centre for Management of Information Society (Centrul Național de Management pentru Societatea Informațională – CNMSI), part of Ministry of Communications and Information (Ministerului Comunicațiilor și Societății Informaționale – MCSI). An Interoperability Working Group with representatives from multiple ministries has been installed. Implementation of new eServices under the NIF will also be directed by this working group.

In addition to the recent legislature, the new eRomania strategy (Strategia națională eRomania) 2010-2013, described above in this report, is a key driver for interoperability efforts in Romania. It builds on existing eGovernment initiatives, such as SEN, which is a common platform for providing several eServices to businesses and citizens via a portal. CNMSI aims to formalize and extend existing interoperability assets.

The following objectives are stated in the draft NIF document:

- Providing standardized and accessible web interfaces for electronic public services and information;
- Standardization, embracing and promoting the use of XML as the current standard for data exchange between electronic public services;
- Standardization, adoption, use and refine models used to structure data (metadata) using ISO or open international standards;
- Alignment of standards and specifications used in the Internet, developed by professional organizations and supported at European level (W3C, ISSS, OASIS, IETF, etc.); aligning systems providing electronic public services to those standards or specifications;

- Adopt, support and use open standards and the specifications widely used and supported by the private market to reduce overall costs for maintenance and development of electronic public services;
- Promoting the benefits arising from the use of open technologies;
- Review of policies, standards and specifications already implemented in existing systems for providing electronic public services.

Emphasis will be placed on semantic and technical interoperability. Although no plans for a central repository of semantical assets were observed, national base registries will be defined. Technical interoperability is expected to be the most extensive part of the Romanian NIF. An existing set of technical standards and guidelines exists (SEN-SDK and XML schemas).

In addition to defining the semantic and technical standards, CNMSI plans to guide implementation of a number of basic infrastructure services. A common authentication tool (single sign on) for citizens and businesses, coupled with a national communications infrastructure for secure data exchange, is one of the services planned. In addition, a common portal will be created, which will form the single point of access to all eServices. It is expected that this portal will build on the existing eGovernment portal⁷.

Co-operation via the National Authority for Management and Regulation in Communications (ANCOM)

Since the beginning of 2010, the ANCOM is still key driver for the stakeholder's co-operation on NIS topics. ANCOM adopted a public consultation procedure in the process of elaborating the regulations with applicability in the network and information security domain, as all the decisions with a significant impact on the market are published for the purpose of public consultation on the Authority's website, according to art. 50 of the Government Emergency Ordinance no. 79/2002. Therefore, the text of a draft decision published on the ANCOM website is accompanied by details regarding the publishing date, as well as the deadline for sending comments and the estimated date on which the measure under consultation is to be adopted.

In this process are involved the representatives of ANCOM, those of the providers and of their professional associations, as well as of the other public institutions ancillary to the regulatory activity in the field of electronic communications and postal services. An overview of public consultation actions held by ANCOM is published on the web site⁸ of the regulator.

Other co-operation of NIS stakeholders to combat spam and malware

The National Authority for Management and Regulation in Communications and the competent national data protection authority have signed a cooperation protocol with regard to the breaches of the legislation regarding unsolicited commercial communications and the supervision regarding the protection of personal data sent by electronic communications. However, the protocol between the two authorities is not public.

Also, the telecom regulator has a protocol with the Ministry of Administration and Internal Affairs with respect to the cooperation between the telecom regulator and the department for organized crime, as both authorities are in charge with the investigation of computer-related crimes. In most cases, the telecom regulator forwards computer crime related complains when they exceed its investigation and punishment powers. However, the protocol between the two authorities is not public.

⁷ eGovernment portal available at www.e-guvernare.ro

⁸ See the list of public consultation actions held by ANCOM at: <http://www.anrcti.ro>

Not much public information is available on the cooperation between the Romanian government, industry and other NIS stakeholders on combating spam and malware.

Information exchange managed via the Romanian national Emergency Management Information System (EMIS)

The Romanian national Emergency Management Information System (EMIS) still plays a key role in the overall set of measures for improving the exchange of information on NIS aspects, especially in emergency situations.

EMIS represents a reference IT project for the public administration in Romania with immediate effects on the improvement of the response capacity of the emergency system at the regional and national level as well as on the increasing capacity of the Government to take the optimum decisions and to act in emergency situations.

EMIS is the integrated information system of the National System for Emergency Situations which connects all operation centers for emergency situations as well as other organizations interested in sharing relevant information. It also represents a support in taking decisions both in every day emergency cases and in major emergency situations which involve management by the emergency committees. The system is used in all the stages of the emergency situations management: prevention, planning, response and return to the normal state of things.

The project has as a purpose to improve the exchange of information between the institutions involved in the management of emergency situations and to facilitate a fast adoption of the best decisions for the respective situations. The Emergency Management Information System – EMIS – is an integrated system meant to ensure the information support to the decision makers by collecting and distributing information about emergencies from and between those institutions involved in the management of these situations, evaluating the emergency situations and their effects, coordinating interventions, monitoring situations. EMIS also ensures the preparation, implementation, coordination of the plans and standard operational procedures dedicated to each particular situation.

Information exchange and co-operation via the Romanian CERTs

On 16th March 2010 the government decision no16/2010 approved the CERT-RO's internal regulations (i.e. "*Regulament de Organizare si Functionare*"). CERT-RO was established by the CSAT's decision nr. 56/2007⁹. Compared with 2009, there were recorded no other significant changes regarding the Romanian CERTs.

RoCSIRT (ex. RoEduNet CSIRT)

This CSIRT¹⁰ is Computer Security Incident Response Team of RoEduNet¹¹ and has been established as a operative service under the umbrella of AARNIEC/RoEduNet.

RoCSIRT constituency is formed by all RoEduNet connected institutions (research centers, universities, high schools, primary schools, etc) who will be named from this point forward, institutions. Additionally this CSIRT may provide services to other entities within Romania. Those entities will be considered part of this CSIRT constituency. Its mission is to provide information to the RoEduNet community and help it to handle computer and network security incidents. The

⁹ More details about Csat's decision nr.56/2007 available at <http://csat.presidency.ro/?pag=43>

¹⁰ Computer Security Incident Response Team

¹¹ Romanian National Research and Education Network

CSIRT coordinates investigations and information flow regarding security incidents in which its constituency is involved, whether as source or as victim of an incident.

The full extent of the services offered by this CSIRT is largely based on BELNET CERT service definition document, available on <http://cert.belnet.be>. At this moment the CSIRT provides information to its constituency by means of this web site or email lists.

RoEduNet (ex. RoEduNet CSIRT) provides:

- Reactive Services (Alerts and Warnings, Incident Handling, Vulnerability Handling, Artifact Handling);
- Proactive Services (Announcements, Technology Watch, Configuration of Tools, Security-Related Information Dissemination);
- Security Quality Management Services (Awareness Building, Education and Training, Advice to Legislative Bodies).

We would also to indicate other very active CERTS¹² that, however, do not exactly have a nation-wide, but that play a relevant role in the CERT/CSIRT interaction in Romania:

CERT-DRT

CERT-DRT¹³ represents the initiative of a Romanian Computer Emergency Response Team, currently working as an abuse team, in order to prevent and address Internet threats such as phishing, pharming, spam and malware distribution.

The CERT-DRT (i.e. CERT-DRT, or CERT.ro) has a mandate to support the Romanian society in working with protection against IT incidents and be the central report and coordination point for relevant security incidents for the government. Its constituency covers all hosts in the government domain as well as all addresses assigned to any local or national governmental body. CERT-DRT does not respond with technical assistance to individual users incidents.

It is important to mention that CERT-DRT does not work directly with the private sector or with the individual users. However, some of the proactive services of the Romanian CERT (information, advice on IT security, statistics) are available for everyone, especially via the website provided by the CERT-DRT or via the public distribution mailing lists.

The CERT-DRT is maintaining a set of black lists being set up for Romanian based hosts in order to avoid spam and other issues originating from Romania, as follows:

- SBL - a Spam Black List that will contain information about the email address, domain and IP address of the spam messages;
- XBL - an Exploits Black List that includes a list of hijacked/infected hosts;
- PBL - a Phishing Black List.

The CERT-DRT was also very active in informing its constituents on the European Commission's public consultation with the title "Towards a Strengthened Network and Information Security in Europe".

¹² CERT - Computer Emergency Response Team

¹³ See: <http://cert.org.ro/>

CERT-RO

Services and information exchanged offered by CERT-RO¹⁴ include:

- Information (statistics, reports, regulations, news);
- Alert – specific threats;
- Informational support and cooperation infrastructure;
- Training.

The CERT-RO also maintains a permanent online forum that encourages exchange of information between stakeholders on: co-operation with other Romanian CERTs and NIS stakeholders, on the actual NIS-relevant legislation, on current incidents, vulnerabilities, etc.

CORIS-STIS

The Operational Response Centre for Security Incidents (CORIS-STIS) is the CERT type entity designated to prevent and respond to security incidents related to information and communications systems of the Special Telecommunications Service and its clients

CORIS-STIS's aim is to provide a range of services and information in order to be used to a better protection of the computer systems, as well as to assist in handling security incidents.

CORIS-STIS is authorized to respond to all types of events/incidents and all types of threats that may occur in its area of responsibility, being able to perform on the request of a beneficiary or by own initiative, following a probable ongoing threat that may lead to a security incident.

Fostering a proactive NIS community

During 2010 Romania took part in the first pan-European exercise on critical information infrastructure protection, Cyber Europe 2010, so that European experts tested defense systems against cyber attacks.

This exercise is part of the measures stipulated by the Digital Agenda for Europe (strategy launched by the European Commission) in order to increase confidence in the Internet and improve network security.

The exercise scenario called "Cyber Europe 2010 foresaw the gradual loss or considerable reduction of Internet connections between European countries and in the worst case, the effective cancellation of the main cross-border connections in Europe.

To this exercise, from Romania were attended representatives of the National Center for Computer Security Incident Response (CERT-RO), National Institute for Research and Development in Informatics (ICI), Ministry of Administration and Interior and the Special Telecommunications Service, and European experts in information security.

¹⁴ See: <http://www.cert-ro.eu>

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

Security incident management

Local Romanian information security incidents are reported as public information on the web site of RoCSIRT. This reporting is voluntary - users from within RoCSIRT constituency report mainly on the received phishing emails in which they are invited to disclose security related information.

For 2010, the most recent local Romanian information security incidents reported by CERT-DRT cover phishing incidents related to the following Romanian entities (mainly financial institutions):

- Bancpost Phishing;
- Millenium Bank Phishing;
- Okazii.ro Phishing;
- Public Finance Ministry Phishing;
- BRD- Groupe Société Générale Phishing.

Other NIS-related incident reporting

In the last report published by the Directorate for Investigating Organized Crime and Terrorism the facts which concerning the IT criminality and fraud, focused on incidents related to:

- Electronic commerce frauds
- Fictitious auction of goods
- Credit card transactions frauds
- Information security attacks
- Child pornography.

No particular NIS incident reporting is either published by the Romanian Intelligence Service (SRI); the Foreign Intelligence Service (SIE); Ministry of Defence or by the Special Telecommunications Service (STS).

In general, providers in Romania do not voluntarily report security incidents. Such cases are usually reported by media, by NGOs and by consumer protection organizations.

Emerging NIS risks

Compared with 2009 , there were no major changes to the key aspects of the national stakeholders involved in the identification of the emerging NIS risks . The main key players are still the Ministry of Telecommunications and Information Society, Romanian Intelligence Service and the Supreme Council of National Defence.

No other relevant public information is available on the emerging NIS risks at the national level. Also, no relevant public information was identified regarding the participation of Romanian CERT, ISPs, etc in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT)¹⁵.

¹⁵ See: <http://www.wombat-project.eu/>

Emerging NIS risks highlighted by the Romanian Ministry of Telecommunications and Information Society

A consolidated list of emerging NIS risks that are officially considered by the Romanian Ministry of Telecommunications and Information Society is included in the specific procedure (public document) concerning "The management of emergency situations related to the risks in the scope of the Ministry" – published in 2005¹⁶.

According to this document, the following emerging risks were considered at the level of Romanian NIS authorities:

- Risks of major eCommunications network disruptions and risks of major disruptions to IT systems, caused by incidents like: fire, nuclear accidents, earthquakes, explosions, natural disasters, cyber attacks;
- Risks of cyber attacks affecting the data flows of NIS stakeholders, leading to denial of services, data theft or fraud.

Resilience aspects

Since the beginning of 2010, no significant changes or new developments were noted at national level regarding network resilience aspects. The network resilience related aspects in the primary or secondary legislation are still vague, expressed in general terms, which makes enforcement problematic – as such, the key responsibility on network resilience stays with the telecom operators that manage the respective networks.

No particular/specific network resilience enforcement rules were noted for Romania, therefore neither specific enforcement action were taken towards operators who infringed resilience rules.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Romanian Law No. 677/2001 concerning the Processing of Personal Data and Free Circulation of Such Data, published in the Romanian Official Gazette No. 790 of 12 December 2001 (the "DPA").

The competent national regulatory authority on this matter is the Romanian National Supervisory Authority for Personal Data Processing (i.e. the ANSPDCP).

Personal Data and Sensitive Personal Data

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

¹⁶ See the procedure "Regulament Privind Managementul Situațiilor de Urgență Specifice Tipurilor de Riscuri din Domeniul de Competență al Ministerului Comunicațiilor și Tehnologiei Informației – 2005" available at: <http://www.mcsi.ro/>. Note: the procedure is available in Romanian only.

In general, sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. However, personal data related to the commission of an offence by a data subject or proceedings for an offence or related to the criminal or administrative sanctions that a data subject has suffered may be processed only under the supervision of public authorities.

Information Security aspects in the local implementation of the Data Protection Directive. Data protection breaches and enforcement aspects

Romanian data controllers must comply with the general data security obligations. No specific customisation of these are noted for Romanis;

The DPA does not contain any obligation to inform the Supervisory Authority (i.e. ANSPDCP) or data subjects of a security breach. ANSPDCP is independent of any public authority or private entity and it receives notifications from personal data processors and complaints filed by people whose rights have been infringed. ANSPDCP has the power to control personal data processors and to apply administrative sanctions.

NIS awareness at the country level

In Romania, NIS awareness raising measures are still undertaken by both competent authorities as well as by private companies, academic bodies and NGOs.

Like in almost all EU Member States, Romania has several informative website and one or more complaint channel to present NIS awareness actions. Most of these websites are related to spam and/or malware, including advice on how to best protect against them.

Awareness measures to combat spam and/or malware

The Romanian Ministry of Communications and Information Society (MCIS) still plays a key role in this field and informs end users about spam and other internet related crimes via its website¹⁷.

More information about the spam phenomena and guidelines regarding the measures to be taken by an end user against unsolicited commercial communications, are provided by private associations through their websites. The Romanian Association for Technology and Internet provides the first Romanian black list of spammers through its website.

Several Romanian ISPs offer their clients packages for internet protection including antivirus, antispam and/or antispysware. Such technical solutions are developed together with software producers. Some ISPs have included an explicit spam policy in their terms and conditions, reserving the right to suspend user access for an unlimited period of time in the case of spam-related abuses are noted.

Awareness actions related to the Internet safety for children

For 2010 the involved Romanian NIS stakeholders, still pays particular attention towards the awareness aspects related to the Internet safety for children.

The Romanian Programme – Safer Internet RO AN-HL-HELP SIGUR.INFO¹⁸ - was establishing a Romanian combined node consisting of a hotline, a helpline and awareness activities with the aim

¹⁷ See: <http://www.mcsi.ro>

¹⁸ See: <http://www.sigur.info>

to provide teachers, parents and child protection specialists with knowledge and tools to protect their children in the new technological environment. The node is created by a consortium comprising two non-governmental organisations - Save the Children Romania as a National Coordinator, Focus Romania - Hotline Coordinator and the company Positive Media, with expertise in areas directly connected to children's rights, child protection and current new information technologies.

The awareness node is providing information regarding the ways of avoiding the online risks that children are exposed to, through extensive web based awareness and PR campaigns in e-media: on-line publications, e-zones, websites for parents, educators and children, forums and blogs, adword campaigns, online banner campaigns, online clip campaigns, e-mailing campaigns and a continuous web presence.

The multi-stakeholder approach on this (the Advisory Board acting as a national reference point and a discussion platform) makes possible professional exchange and open dialogue among representatives of the educational community, political decision-makers, media and technical industry. Based on members' professional expertise, the Advisory Board is seen as a main promoter of the best technical and legal solutions.

The Hotline is a civil contact point which provides internet users with the possibility of reporting any material of a child abusive nature (chatboxes, sites, discussion groups, e-mails) and also for reporting other types of illegal content. The information received is transmitted to the Fight against Cyber Crime Service of the Romanian Police, where it is examined. As stipulated in a protocol of collaboration signed between the Romanian Police and The Romanian Centre for Missing and Sexually Exploited Children – FOCUS, the Police Service has to confirm the reception of the information and the way with which it has been dealt by Police specialists.

Awareness measures towards cybercrime

For 2010 the main key player regarding measures towards cybercrime is still The Service for Combating Cybercrime under the Romanian Directorate for Investigating Organised Crime and Terrorism Offences of the Prosecutor's Office of the High Court of Cassation and Justice (DIICOT), which is promoting a series of permanent measures in order to fight against cybercrime, such as:

- Actions to increase public awareness and education about the danger of the computer crimes;
- Hotlines allowing citizens who discover online illegal activities to report the conduct to relevant authorities;
- Cooperation activities between all institutions (at national and international level) and law enforcement agencies in fighting against cybercrime;
- Encourage the private sector (including Internet Service Providers) and civil society (including teachers, non-governmental organizations, the media) to report any information they might obtain concerning cybercrime to the appropriate law enforcement or social service authority;
- Stimulate the Internet service providers to contribute by facilitating the referral of relevant information to law enforcement authorities;
- Training for criminal justice professionals (law enforcement, prosecutors and the judges) is a necessary as a part of a comprehensive program designed to fight these crimes. Provide special training for judges, prosecutors and police officers.

Other awareness-raising events

An annual International Conference on Computers, Communications and Control (ICCC)¹⁹ takes place annually in Romania. The publishing policy of ICCC is to encourage particularly the publishing of scientific papers that are focused on the convergence of the 3 „C” (Computing, Communications, Control).

The event is open to government, academic and industry bodies and provides a forum for international scientists to present and discuss their latest research findings on a broad array of topics in computer networking and control.

No public information is available on the awareness raising results of this annual event.

For 2011, Agency ARNIEC/RoEduNet's ([Romanian Education Network](#)) is organising the tenth annual Conference²⁰, under the patronage of [Ministry of Education, Research, Youth and Sports](#). The conference is offering special opportunities for information exchange in computer networking: technical and strategic aspects and communication issues.

Country-specific activities for identifying and promoting economically efficient approaches to information security

During 2010 the STS started several projects as part of Operational Programme "Increasing Economic Competitiveness" – they have a strong component related to economic efficiency aspects:

- Information systems development project within the single national system for emergency calls (SNUAU) for intervention stations in municipalities;
- Infrastructure development project of GIS (Geographic Information System) for national system for emergency calls (SNUAU);
- Emergency dispatches interconnection at the county capitals with the intervention stations located in the other municipalities in the same county.

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

During 2010 the representatives of the Ministry of Communications and Information Society (MCIS) participated in the conference "Critical Infrastructure Protection in Romania" in which one major theme addressed was the protection of telecommunications infrastructure as part of the Critical Information Infrastructure Protection (CIIP).

Since the beginning of 2010, MCIS is working on a project related to the cyber security strategy and contributes to developing the National Defense Strategy and Defense Cyber Law.

In order to improve the critical information infrastructure protection, Romania established an intergovernmental commission which has as a main objective the Critical Infrastructure Protection which includes also the CIIP .

¹⁹ See: <http://www.iccc.univagora.ro>

²⁰ See: <https://conference.roedu.net/index.php/roedunet/2011/schedConf/cfp>

On August 24, 2010, Ministry of Communications and Information Society (MCIS) received from the European Commission, official financing contract for a complex project, national and European importance. The project is called "Learning to develop an integrated cybernetic system at European level, using a pilot system to the main national providers of Internet

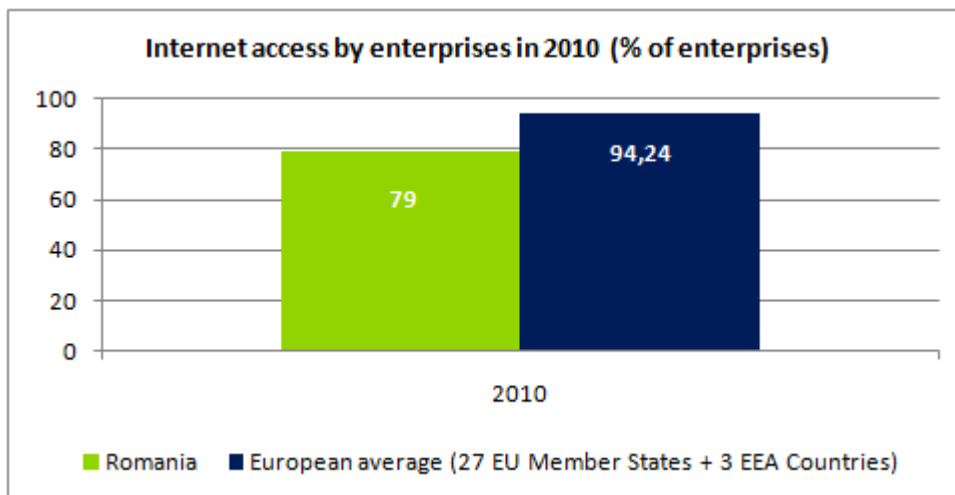
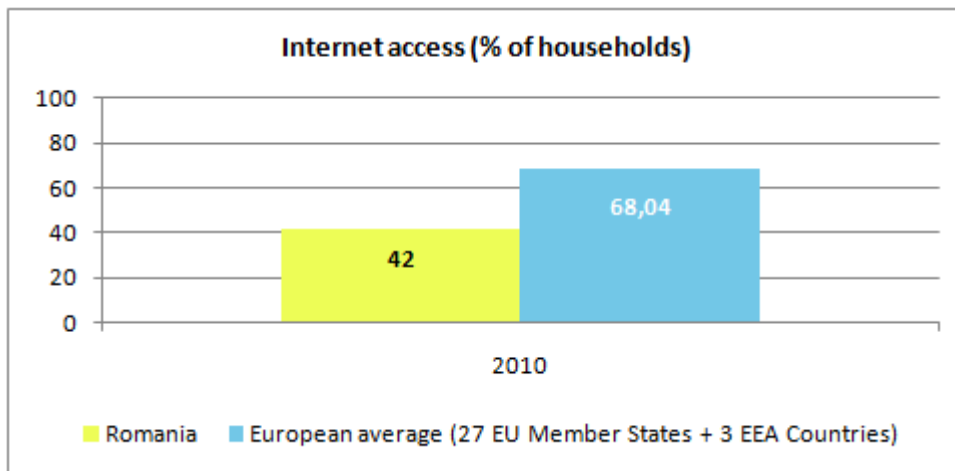
The project will be implemented over a period of 22 months and requires a study to develop a European system of protection against cyber attacks massive on Critical Infrastructure IT & C, made through public networks, the Internet providers, banks, etc.

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Romania, a series of relevant statistics are included in this section. Some of them indicate that the information society in Romania is at a relatively early stage of development, while others show progress and interesting trends.

Internet access of population and enterprises

The following graphs provide an overview of the situation²¹ of Internet access in Romania for enterprises and respectively households, relative to the European average.

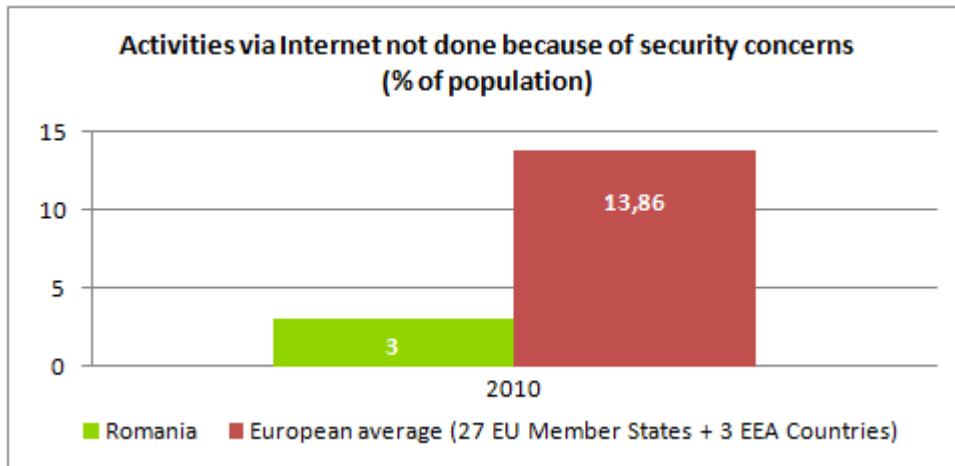


In 2010, the statistics indicate that, in Romania, both enterprises and households require efforts to close the gap on the European average.

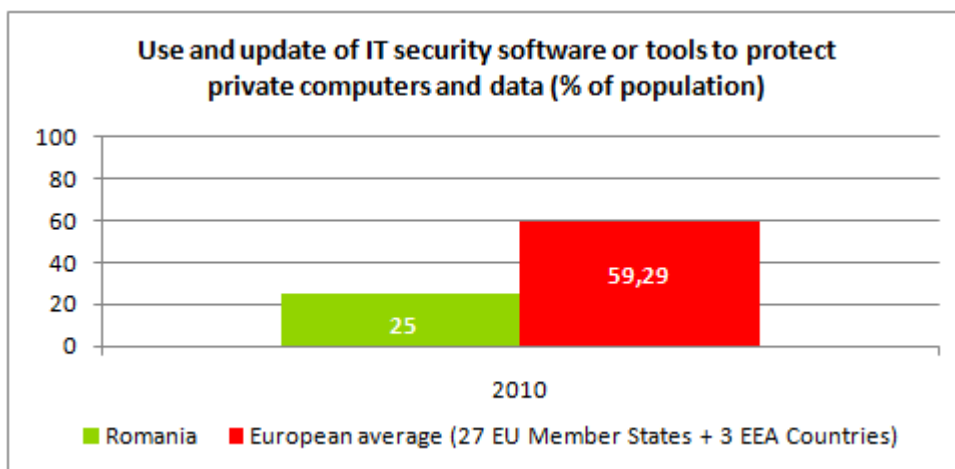
²¹ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Romania that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is almost a fifth of the European average:



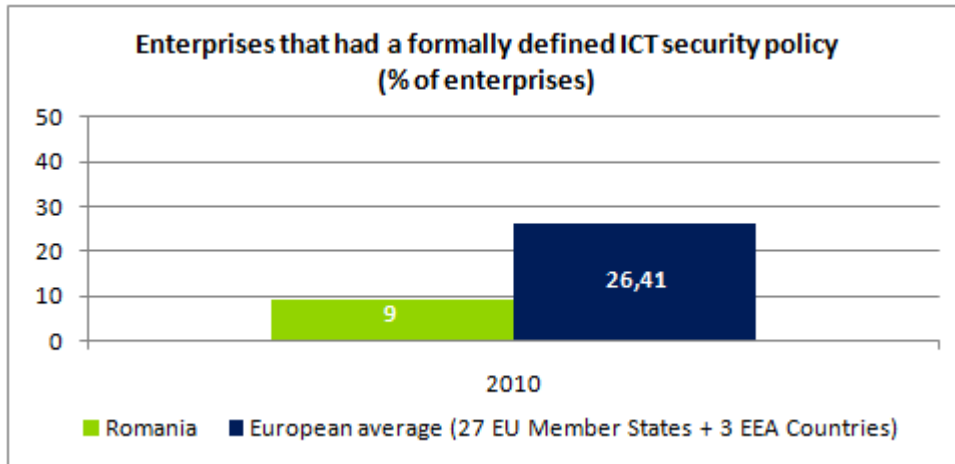
This can be an indication of either much confidence in web-based transactions or of a lack of awareness of the general public regarding IT security threats.



It also appears that the use of security tools to protect private computers and data is less than half the European average.

Statistics on use of Internet by enterprises and related security aspects

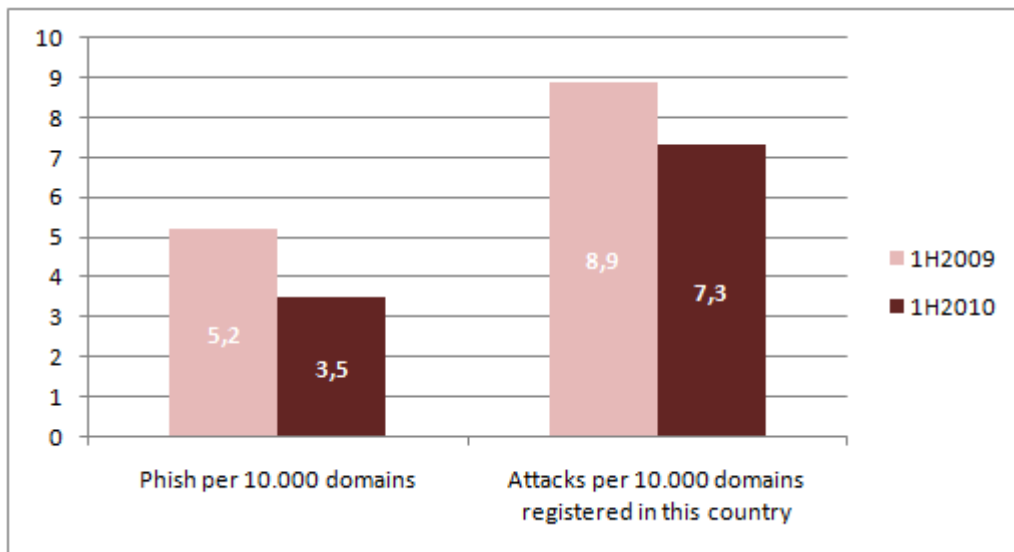
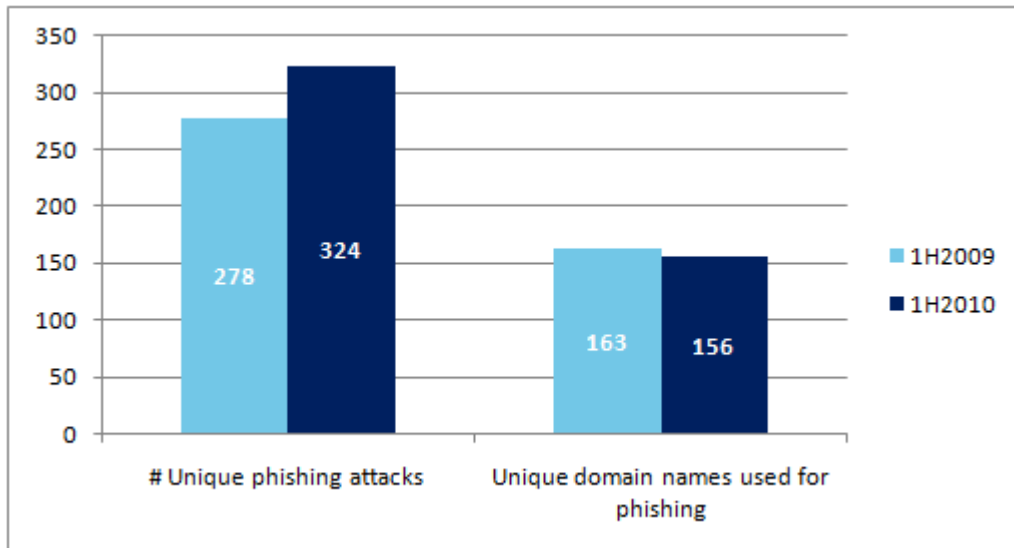
Fewer enterprises in Romania²² have a formally defined ICT security policy, compared with their European peers. See below:



²² Source: Eurostat

Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Romania was mentioned in the global report²³ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



²³ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Ministry of Communications and Information Society (MCSI)	<p>The Ministry of Communications and Information Society is the main policy and strategy producer. As the specialised body of central public administration in the ICT sector, it was established in 2001 with the objective of implementing the Romanian Government policy in this sector. It is responsible for defining the restructuring policies, coordinating the privatisation process in the ICT sector, financing the main projects to make the transition of the Romanian society to an Information Society and promoting the development of the Internet. Moreover, the MCSI is in charge of the harmonisation of the specific legislation with the European Union provision.</p> <p>According to its mandate mentioned above, the MCSI is also responsible for coordinating the implementation of policies and strategies, together with the subordinated agencies and departments.</p>	www.mcsi.ro
2. National Authority for Communications (ANCOM)	<p>The ANC was established in September 2008 by Government emergency ordinance (no. 106/200) through the reorganisation of both the National Regulatory Authority for Communications and Information Technology (ANRCTI – which was dissolved) and the National Institute of Research and Development in Informatics (ICI). ANCOM is the institution that sets the rules in the Romanian communications market and watches the enforcement of these rules.</p> <p>Since March 2009, ANCOM is under the parliament supervision.</p> <p>ANC took the role of national administration of the Top Level Domain (TLD), “.ro”, and the Second Level Domain (SLD), “.eu” for the domain names reserved for Romania and became the unique administrator of the policies in the field of electronic communications and information technology.</p> <p>The main activity of ANCOM, as a regulatory authority in the electronic communications and information technology sector, is elaborating the secondary legislation in the field. Thus, ANCOM:</p> <ul style="list-style-type: none"> • elaborates and updates the general authorisation regime, under which the providers of electronic communications networks and services are granted the right to enter the market and operate; • designates the providers of electronic communications networks and services with significant market power and imposes on them obligations meant to ensure that these providers will not abuse their dominant position, thus preventing them from affecting competition; • adopts the National Numbering Plan and issues regulations regarding the use of the numbering resources; • regulates the regime of interconnection between the electronic communications networks; 	www.anrcti.ro

National authorities	Role and responsibilities	Website
	<ul style="list-style-type: none"> ensures the implementation of the universal service mechanisms issuing regulations in the field. <p>In order to ensure compliance of the primary and secondary legislative frameworks, ANCOM is mandated to:</p> <ul style="list-style-type: none"> monitor and control the compliance with the obligations imposed on the providers of electronic communications networks and services by the general authorisations; oversee the national management of the numbering resources and the issuance of licenses for the use of the numbering resources; elaborate the methodology for conducting market analyses and identifying the relevant markets in the electronic communications sector; conduct market analyses with a view to identifying the relevant markets and, subsequently, to designate, if necessary, the significant market power companies and impose them specific obligations; manage the financing mechanisms related to ensuring access to universal service, as provided in the special legislation; control the compliance with the obligations imposed on the universal service providers, under the provisions of the special legislation. 	
3. National Management Center for Information Society	NCHM took over operation of the systems: www.e-guvernare.ro (Sistem Electronic National), www.e-guvernare.ro (National Electronic System) www.e-licitatie.ro (Sistem Electronic de Achizitii Publice), www.e-licitatie.ro (Electronic Procurement System) www.ghiseul.ro (Ghiseul Virtual de Plati), www.ghiseul.ro (Virtual Payment Desk) www.autorizatiiauto.ro (Serviciul de Atribuire Electronica a Autorizatiilor de Transport) www.autorizatiiauto.ro (Electronic Tender Service Transport Authorisations)	www.cnmsi.ro
4. National Center "Digital Romania" (CNRD)	National Center "Digital Romania" (CNRD), a public institution under the Ministry of Communications and Information Society, aims to provide informational content management and information services within the portal e-Romania	http://www.cnrd.ro/
5. National Authority for the Supervision of Personal Data Processing / Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)	The National Supervisory Authority for Personal Data Processing is a public authority, autonomous and independent in relation with any other public authority, natural or legal person, with legal personality, exercising the attributions it has been invested with by the present law, as well as by the special laws regulating the activity of personal data processing and the free movement of the data.	www.dataprotection.ro
6. ORNISS (The National Registry Office for Classified Information)	ORNISS performs regulation, authorization, evidence and control tasks in conformity with the provisions of Law no.182/2002 on the protection of classified information, the National Standards for the protection of classified information in Romania, approved by Government Decision no. 585/2002, and the Norms of the North Atlantic Treaty Organization on the protection of classified information in Romania, approved by Government	www.orniss.ro

National authorities	Role and responsibilities	Website
	<p>Decision no. 353/2002.</p> <p>In order to accomplish the tasks assigned, ORNISS is empowered to require the necessary information from the heads of public authorities and bodies, of economic operators with integral or partial state share capital and of other public or private legal persons. The heads of the authorities and public bodies, of economic units with integral or partial state share capital and of other public or private legal bodies are bound to place at ORNISS' disposal the data and information related to the protection of classified information in their field of activity, except for the cases stipulated by law</p>	
7. IT&C Commission – Chamber of Deputies	<p>The chamber is a parliamentary commission whose objective is to launch legislative initiatives in the field of technology of information and communications, advanced specific technologies in the field, coming into line with the international regulations, respectively standards, and the intellectual property</p>	<p>http://www.cdep.ro/</p>
8. Ministry of Administration and Interior	<p>According to the law, the ministry sets measures for defending the human fundamental rights and liberties, as well as for defending the public and private property; according to its competence, it organizes and develops, through specialized structures, activities for preventing and countering terrorism, organized crime, illicit trafficking and consumption of drugs, trafficking in persons, illegal migration, computer crime, as well as other crimes and antisocial deeds; monitors the enforcement of provisions contained by the strategies and programs of reform and restructuring of the central and local public administration, elaborated on basis of the Governing Programme, in compliance with the European Union standards and the domestic law. The ministry has also prerogatives in the domain of information security and electronic delinquency.</p>	<p>www.mai.gov.ro</p>
9. Special Telecommunications Service (STS)	<p>STS manages, operates and develops special telecommunications networks under its management or assigned to it for use. Key attributions:</p> <ul style="list-style-type: none"> • manages, operates and develops the special telecommunications networks under its management or assigned to it for use; • develops programs and documents for the modernisation, development, operation and maintenance of the special telecommunications networks; • establishes the communications security policy and ensures application of the methods and measures required for the protection of the information processed, stored or transmitted through the special telecommunications networks according to the national standards for information protection; • manages and ensures protection of the government-assigned frequency bands used to achieve its legal attributions or those of the institutions competent in the field of national security and public order; • monitors across the country, for protection purposes, the government-assigned frequency bands under its management and 	<p>www.stsnet.ro</p>

National authorities	Role and responsibilities	Website
	<p>keeps a record of their use;</p> <ul style="list-style-type: none"> develops co-operation relations with other institutions within the national system of defence and provides special communications for the High National Headquarters and the National Command and Control Authority, under the terms of the law; co-operates with the institutions within the national system of defence, as well as with other legal entities carrying out activities in this field, in order to harmonise and ensure compatibility of their communication systems; installs, operates and maintains the National Unique System for Emergency Calls – 112, according to the quality requirements; applies the procedures related to Public Key Infrastructure technology within the national system of defence; organises the electronic signature authentication system; together with the Ministry of Administration and Interior, takes part in applying specific measures for the integrated management of the national border; provides telecommunications services for private or public legal persons, according to the law. <p>Additionally, the Special Telecommunication Service is the EURid accredited registrar for the .eu domain. This service is intended for STS beneficiary institutions, according to the Romanian Law 92/1996 concerning the organisation and functions of STS</p>	
10. Ministry of Defence	<p>The Ministry of Defence is a specialized body of the central public administration submitted to the Government conducting national defence activities according to the stipulations of the law and to the strategy of national security, with a view to safeguarding national sovereignty, state independence and unity, territorial integrity and constitutional democracy.</p> <p>The ministry has also prerogatives in the domain of information security and electronic delinquency</p>	www.mapn.ro
11. Romanian Intelligence Service (SRI)	<p>The Romanian Intelligence Service is the official institution of Romania with competences in gathering and making the effective use of national security-related intelligence. The activities are carried out mainly on the national territory but also outside borders, in cooperation with other institutions with responsibilities in the field of monitoring and preventing cross-border threats. The service has also prerogatives in the domain of information security and electronic delinquency.</p>	www.sri.ro
12. Foreign Intelligence Service (SIE)	<p>The activity of the Foreign Intelligence Service is organized and coordinated by the Country's Supreme Defence Council (CSAT); Cooperates with other public institutions such as the Ministry of Defence, MIRA or SIE for matters of national security. The service has also prerogatives in the domain of information security and electronic delinquency</p>	www.sie.ro
13. Service for Combating Cybercrime under the Romanian Directorate for Investigating	<p>Responsible for combating cybercrime and crimes against intellectual property. Also responsible for combating crimes with credit cards and other means of electronic payment.</p>	www.diicot.ro

National authorities	Role and responsibilities	Website
Organized Crime and Terrorism of the Prosecutor's Office of the High Court of Cassation and Justice (DIICOT)	The competences of DIICOT for combating cybercrime meet the requirements set out in the Convention on Cybercrime on international cooperation, being also the contact point available 24/7.	

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST²⁴ member TI²⁵ listed 	
14. RoCSIRT	<p>RoCSIRT is the AARNIEC/RoEduNet Computer Security Incident Response Team. RoCSIRT has been established as a operative service under the umbrella of AARNIEC/RoCSIRT. Its mission is to provide information to the RoCSIRT community and help it to handle computer and network security incidents.</p> <p>The CSIRT coordinates investigations and information flow regarding security incidents in which its constituency is involved, whether as source or as victim of an incident. RoCSIRT constituency is formed by all RoCSIRT connected institutions (research centers, universities, high schools, primary schools, etc) who will be named from this point forward, institutions. Additionally RoCSIRT may provide services to other entities within Romania. Those entities will be considered part of RoCSIRT constituency</p> <p>RoCsirt is FIRST member & not TI listed.</p>	www.csirt.ro
15. CORIS-STIS	<p>The Operational Response Centre for Security Incidents (CORIS-STIS) is the CERT type entity designated to prevent and respond to security incidents related to information and communications systems of the Special Telecommunications Service and its clients. CORIS-STIS aim is to provide a range of services and information in order to be used to a better protection of the computer systems, as well as to assist in handling security incidents</p> <p>The CORIS-STIS purpose is to provide its beneficiaries with the needed services that allow security incidents handling, assuring preventive measures and complete information.</p> <p>CORIS-STIS is authorized to respond to all types of events/incidents and all types of threats that may occur in its area of responsibility, being able to perform on the request of a beneficiary or by own initiative, following a probable ongoing threat that may lead to a security incident.</p> <p>CORIS-STIS is not FIRST member & is TI listed.</p>	corisweb.stsisp.ro
16. CERT-RO	<p>Information Security Expertise Center is a new organisation created under the tutelage of the Romanian Ministry of Communication and Information Technology as part of the National Institute for Research and Development in Informatics (ICI - Bucharest). The organisation</p>	www.cert-ro.eu

²⁴ See: <http://www.first.org/members/teams/>

²⁵ See: <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST²⁴ member TI²⁵ listed 	
	<p>aims at creating a solid research center for information, equipment, network and system security and tries to focus both the IT&C specialists and the authorities on the security of virtual environment in Romania</p> <p>CORIS-STIS is not FIRST member & is not TI listed</p>	

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
17. Aries (Romanian Association for Electronic and Software Industry)	<p>Aries is the association of electronics and software companies of Romania and aims at promoting and protecting the Romanian IT and electronic business environment, as well as the professional and commercial interests of its members.</p> <p>With more than 280 members, Aries is the largest ICT association in Romania.</p> <p>It has developed a national strategy to increase Romania's hi-tech potential, as well as two strategies on turning Romania into an important software producer and exporter globally and research funds for SMEs.</p>	www.aries.ro
18. National Association of Romanian ISPs (ANISP)	<p>ANISP does lobbying for the members and involves actively in legislative initiatives related to the communications market.</p>	www.anisp.ro
19. Employers' Association of the Software Industry and Services (ANIS)	<p>The Employers' Association of the Software and Services Industry – ANIS upholds the interests of Romanian software producers and services providers. The association was founded in 1998, and at present, counts more than 100 members, some of which are the foremost IT companies in the field. One of ANIS strategic objectives is to be involved in legislative issues impacting the IT sector, by collaborating in the process of elaborating and applying national IT policies, with main focus on software production and service providing.</p>	www.anis.ro
20. Association for IT&C (ATIC)	<p>The Information Technology and Communications Association of Romania (ATIC) was the first independent non-governmental organization in the IT&C field in Romania. The association, registered in 1990 as the Romanian Software Association, changed its name into ATIC in 1996. ATIC includes the important Romanian IT&C companies as full members as well as well-known professionals from universities and research field as individual members.</p> <p>ATIC organizes and promotes the information exchange, collaboration and cooperation between its members, establishing as a fundamental principle the support of science practice in this field, honouring the creativity, respecting the law, in a wide exchange of opinions for the utilization with maximum efficiency and professionalism of the new scientific novelties. ATIC deems itself as active part of the Romanian civil society, sensing to participate in the name of its members in the elaboration process as well as the public debate of the strategic orientations, lawmaking initiatives, written and audio-visual</p>	www.atic.org.ro

	communication regarding the development of the IT&C field in Romania. ATIC is currently member of World Information Technology Software Alliance (WITSA), of Council of European Professional Societies (CEPIS) and also of ITStar.	
21. Association of Telecommunications Operators	ATO does lobbying for the members and involves actively in legislative initiatives that relate to the communications market. Build co-operation between members.	www.aotr.ro
22. Cable Communication Association	This is the industry association of the cable network operators in Romania.	www.cablu.org

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
23. Military Technical Academy	The Military Technical Academy provides both basic engineering and post-academic training for the Ministry of National Defence and the other structures of the national defence system (The Ministry of the Interior and Administrative Reform, The Special Communications Service, The Romanian Intelligence Service, The External Intelligence Service, The Guard and Protection Service). It also provides training upon request for other various partners. The Military Technical Academy has two departments: <ul style="list-style-type: none"> • The Department of Integrated Armament Systems and • The Department of Military Electronic and Information Systems. 	www.mta.ro
24. National Communications Research Institute / Institutul Național de Studii și Cercetări pentru Comunicații (INSCC)	National Communications Research Institute - INSCC Bucharest performs fundamental and applicative research, technological development, technical and economical studies. INSCC also carries out tests, measurements and trials, conformity assessment and certification of communications equipments and services.	www.inscc.ro
25. National Institute for Research and Development in Informatics (ICI)	The National Institute for Research and Development in Informatics (ICI) is involved in the Romanian information science and technology development. It is one of the leading Romanian ICT research - development and innovation centre. Information Security Expertise Center within ICI is a new organisation created under the tutelage of the Romanian Ministry of Communication and Information Technology as part of the National Institute for Research and Development in Informatics (ICI - Bucharest). The Expertise Center has been created as a core for the future development of CERT type (Computer Emergency Response Team) structures in Romania.	www.ici.ro www.cert-ro.eu

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
26. Information Systems Audit and Control Association – Romanian Chapter (ISACA)	ISACA Romania is a Romanian chapter of ISACA International. The association builds knowledge and facilitates the CISA and CISM exams and certifications for IT security professionals.	www.isaca.ro
27. Foundation for promoting Information and Communication Technology (FICT)	The Foundation for Promoting Information And Communication Technology is formed as a Romanian juridical person with private law, nongovernmental, non-political, non-profit, impartial, independent and with no patrimonial purpose, for promoting Information and Communication Technology in all Romanian social environments.	www.fict.ro/
28. Romanian Association of Telecommunications' Engineers	Non-profit, non-governmental organisation of Telecommunications' Engineers.	www.airt.ro
29. Association for Consumers' Protection / Asociatia pentru Protectia Consumatorilor din Romania (APC)	A consumer organisation, its aim is to protect and educate consumers.	www.apc-romania.ro

References

- An overview of the eGovernment and eInclusion situation in Europe available at <http://www.epractice.eu>
- eGovernment Factsheets – eGovernment in Romania available at <http://www.epractice.eu/files>
- 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
- NIS strategies available on the site of the Romanian Ministry of Communications and Information Society (in Romanian only) available at: <http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Comunicatii-electronice/Strategii>
- ENISA inventory of CERT activities in Europe available at <http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe>
- Details about the Cyber Security 2010 available on ENISA website at: <http://www.enisa.europa.eu/media/press-releases/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded>
- More details regarding phishing reported attacks during 2010 available at: <http://cert.org.ro/stiri-si-evenimente.aspx>



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