SECURING EUROPE'S INFORMATION SOCIETY

GENERAL REPORT 2010

enisa
European Network and Information Security Agency

CONTENT

A MESSAGE FROM
THE EXECUTIVE DIRECTOR

The year 2010 was a very exciting year. A new Commission and a new Commissioner for the Digital Agenda were approved by the European Parliament. The Digital Agenda, one of the flagship initiatives of the European Commission, was announced by Vice President Neelie Kroes in May 2010, while in September the new draft ENISA regulation was published. We are now looking forward to a very promising future.

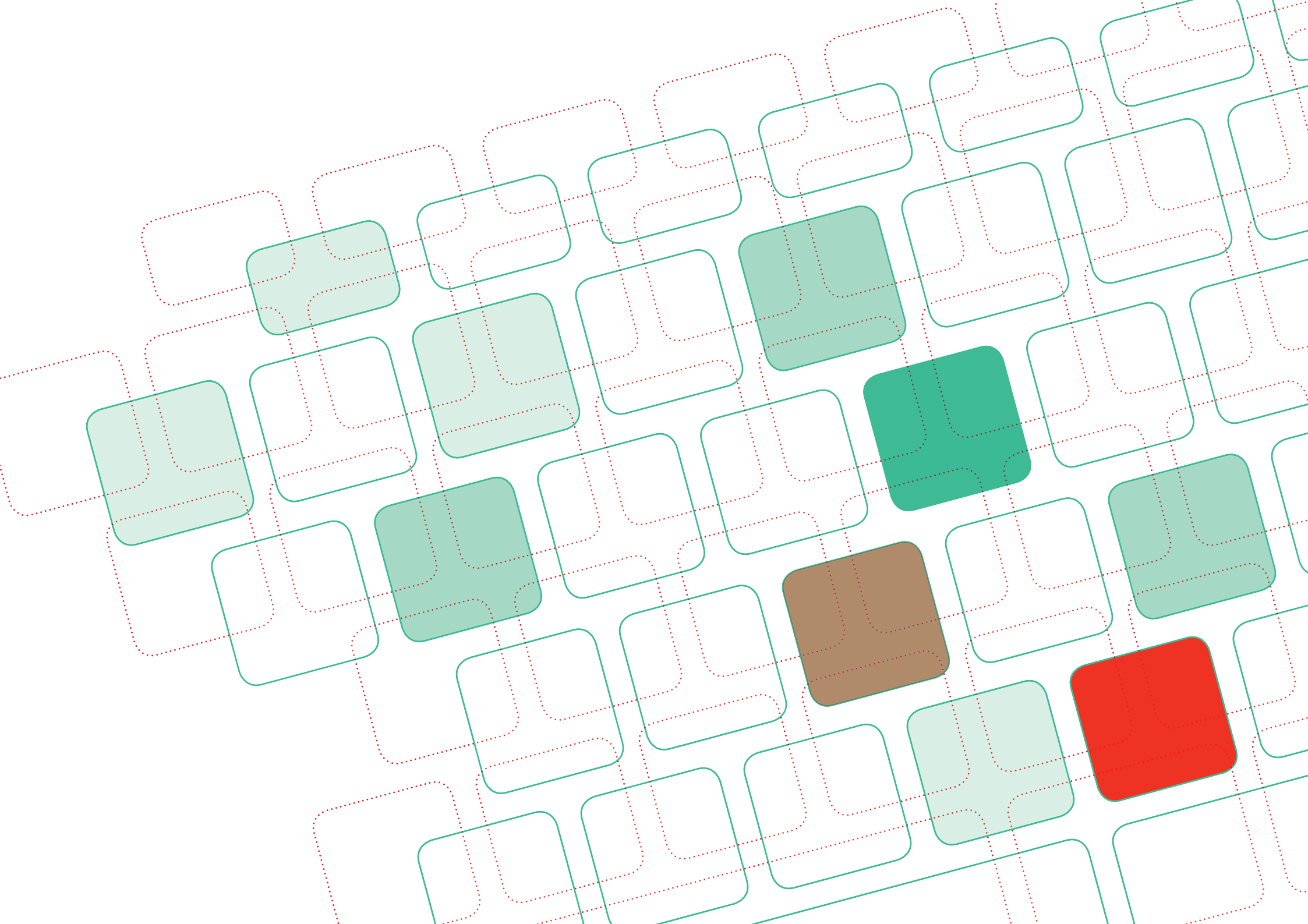
In February 2010, I appointed ENISA's new Permanent Stakeholder Group (PSG). We now have representatives from diverse fields including the information and communication technology (ICT) sector, ICT user organisations and academic experts in network and information security. In June, a joint meeting between the PSG and the Management Board (MB) took place. The objective of the meeting was to align the work programme of ENISA with the expectations and needs of our stakeholders for the benefit of EU institutions, Member States and Europe's citizens.

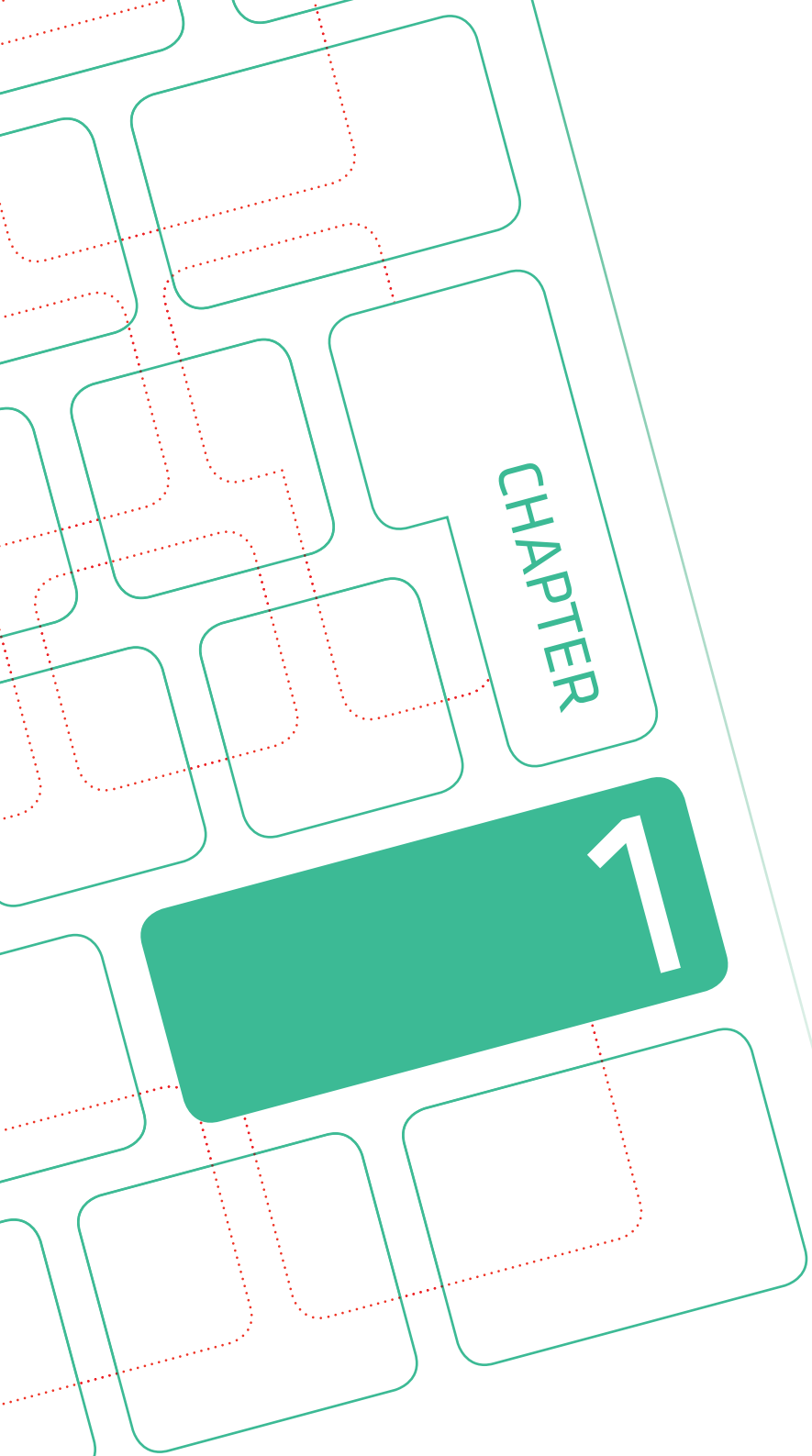
ENISA's work programme is an important means for achieving and implementing the EU's strategic objectives for 2020. Through the work programme, ENISA leverages Network Information Security (NIS) knowledge towards an IT security culture in Europe. Some examples of ENISA's deliverables are the Good Practice Guide for Incident Management, the Information Assurance Framework for Cloud Computing and the Country Reports. The latter provide an overview of the "state of the art" in NIS in 30 countries, i.e., the 27 European Union Member States and the 3 members of the European Economic Area.

In November 2010, and for the first time ever, ENISA and the JRC (the EU's Joint Research Centre) organised and conducted a pan-European Exercise for Critical IT Infrastructure Protection (CIIP). More than 150 experts from 70 public bodies around Europe participated in this exercise. They were exposed to more than 320 incidents, which as an exercise, was a first key step for strengthening Europe's cyber defences. This table top simulation fully met its objective of testing Europe's communication-readiness in the face of online threats to critical infrastructures used by citizens, governments and businesses.

IT security is crucial for governments, businesses and consumers alike – an essential element for prosperity in Europe. It is ENISA's mission and duty to secure Europe's Information Society to help EU Member States and private stakeholders develop their capabilities to prevent, detect and respond to cyber-security challenges.

Udo Helmbrecht





Introduction

NETWORK INFORMATION SECURITY
IN EUROPE: AN EVER-EXPANDING NEED

Information and Communication Technologies (ICTs) have transformed the way we live and work. Email, social networks, online banking and online shopping are just a few of the innovations that have made life more convenient for consumers and businesses alike. These technologies have become essential tools in political, social and economic interaction.

While providing many benefits, however, the new technologies have also brought with them risks. Communication networks and related technologies are now the central nervous system of our economy and society; they play an important role in employment, growth and personal interactions. Like a central nervous system, however, they can be vulnerable. For this reason, network and information security (NIS) is a major concern for both citizens and businesses throughout the European Union. For their part, citizens expect the EU to ensure the security of their communication networks, enforce online privacy and prevent cyber crime.

As our dependence on ICT has grown, NIS has gained increasing political attention within the EU. So much so, in fact, that the Digital Agenda is one of the seven flagship initiatives of the Europe 2020 Strategy, Europe's strategy for smart, sustainable and inclusive growth. The Digital Agenda underlines the key role that secure ICT will play in enabling Europe to achieve its economic ambitions – a speedy economic recovery and a sustainable digital future – by 2020. It outlines seven priority areas for action, and attributes an important role to ENISA in relation to the priority area of 'Trust and security'.

To achieve its goals for improving network and information security, however, Europe will need to act in unison. Mrs. Neely Kroes, Vice President of the European Commission with the Digital Agenda portfolio, has stated that "…cooperation of relevant actors needs to be organised at the global level to be effectively able to fight and mitigate security threats", and that "internationally coordinated actions targeting information security should be pursued, and joint action should be taken to fight computer crime, with the support of a renewed European Network and Information Security Agency." The Commission Communication on Critical Information Infrastructure Protection (CIIP) of March 2009 and the conclusions of the Council Presidency of the Tallinn Ministerial Conference on CIIP have laid the foundations for ENISA's work in this area. Moreover, in a resolution in December 2009, the Council of the European Union, which is composed of Europe's top political leaders, issued a strong statement in favour of a collaborative European approach to NIS. The resolution provided political direction for how the Member States, the European Commission, ENISA and stakeholders can each play their part in enhancing the level of NIS in Europe. It concluded an ongoing debate on the future of NIS policy in Europe and the role of ENISA. By identifying a clear need and the willingness of EU Member States to act in concert, the Council resolution marked a milestone for NIS in Europe.

> "Communication networks and related technologies are now the central nervous system of our economy and society"

ENISA's mandate to enhance NIS at the European level has received further impetus in 2010. In its conclusions of the 26th of April 2010, the Council (General Affairs) noted the importance of promoting "relationships with European Agencies (EMSI, CEPOL, EUROJUST, EUROPOL, ENISA, etc.), international bodies (INTERPOL, ONU, etc.) or third countries on new technology subjects, in order to reach a better understanding of the trends and modus operandi" of cyber crime. Furthermore, in September 2010, the Commission issued a proposal for the strengthening of ENISA. The proposal provided several recommendations regarding the role and contribution of ENISA, and noted that several of the ongoing developments in NIS policy, notably those announced in the Digital Agenda for Europe, benefit from the support and expertise of ENISA. These developments include the Commission working with ENISA to draft guidance on promoting NIS standards, good practices and a risk management culture, and ENISA organising, in cooperation with the Member States, the "European month of network and information security for all", featuring national/European Cyber Security Competitions.

ENISA's work in NIS is highly appreciated, and with an ever-growing need for a safe economy, the Agency is considered a crucial asset in ensuring the overall security of Europe's network and information systems.

ABOUT ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for network and information security (NIS). ENISA bridges the gap between citizens, industry and governments by acting as a knowledge broker in NIS matters and as a promoter of good NIS practices within EU Member States.

ENISA is a decentralised agency of the European Union. It was established in 2004 and is based in Heraklion, Greece.

ENISA's objectives are to:

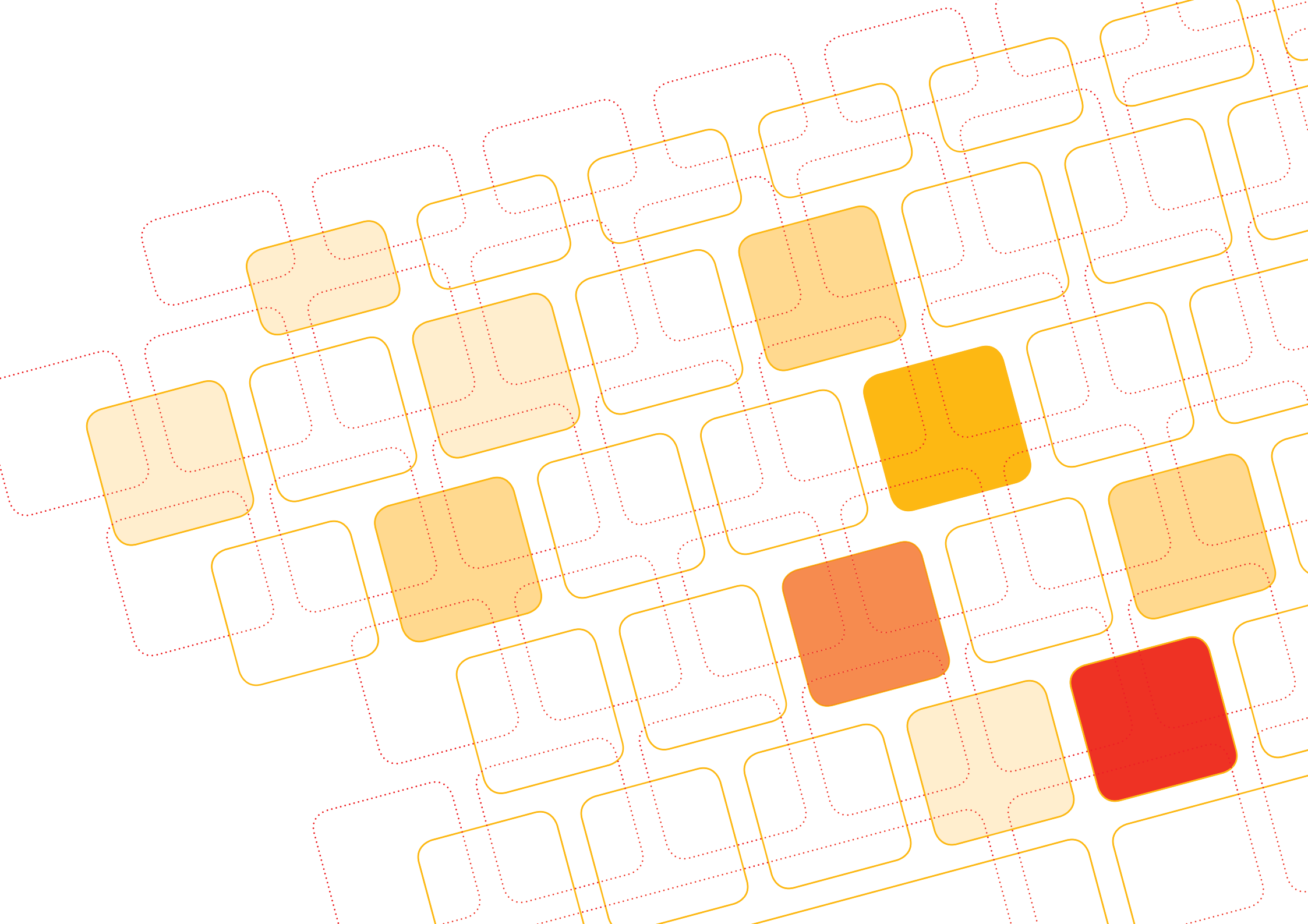
1. secure Europe's information infrastructure
2. cultivate e-privacy, i.e., trust and confidence in the use of Information and Communication Technologies (ICT)
3. promote information security standards, guidelines and certification schemes
4. educate the wider public on ICT

ENISA has published numerous reports and studies on a range of NIS issues including the security of USB drives, printers, spam, social networking, botnets, standards, risk assessment, risk management, business continuity, 'digital fire brigades', and how to obtain the CEO's support for awareness raising. The Agency also conducted a study of the European Information Sharing and Alert System (EISAS) for SMEs and citizens. ENISA co-organises conferences, runs workshops, publishes position papers, and produces the ENISA Quarterly Review to foster debate on NIS matters.

As a European agency, ENISA is uniquely positioned to bring together a wide range of key players in the Network and Information Society by acting as a neutral and independent advisor. With its technical expertise, its central position and its independence, the Agency is well placed to ring the alarm bells on emerging and future risks.

EU AGENCIES

From Helsinki to Crete and from Lisbon to Vilnius, specialised agencies have been established to carry out specific legal, technical or scientific tasks within the European Union. The agencies were setup to help implement EU policies more efficiently and to respond to particular needs identified by the EU institutions and Member States. They provide meaningful advice, facilitate exchanges of best practice among Member States, and support consensus-building through networks and exchanges. All agencies work in the public interest, and as they are spread throughout the EU, they can facilitate outreach to EU citizens. The EU agencies are involved in varied activities: safeguarding freedom, justice and security; improving health, safety and the environment; supporting education, business and innovation; and developing transport and satellite infrastructure. Today the agencies play a key role in implementing EU policies and are making a valuable contribution to the EU 2020 strategic objectives.



CHAPTER 2

ENISA operational activities

COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)

Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have the capability to respond effectively and efficiently to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens. At the same time, they must act as awareness raisers and educators.

Not every country connected to the internet possesses CERT capabilities. And the level of maturity among those who do varies dramatically. It is ENISA's mission to clear out the 'white spots' on the CERT world map and to minimise the gaps by facilitating the setting-up, training and exercising of CERTs.

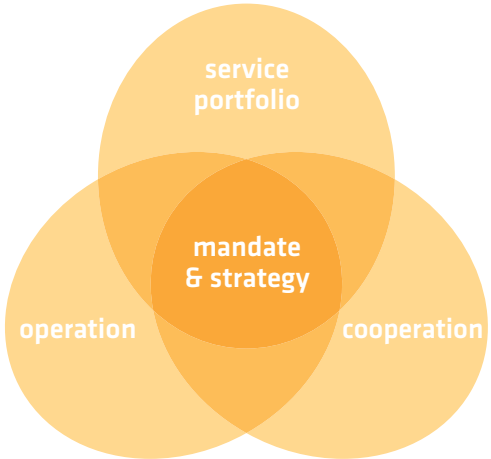
What we do

The activities and tasks related to CERTs are defined within the ENISA Work Programme 2010 - "Build on Synergies - Achieve Impact". For 2010, the CERT activities are included within Multi-annual Thematic Programme (MTP) 2: Developing and maintaining cooperation models. The work package dedicated to CERTs is Work Package (WPK) 2.2: Security competence circle and good practice sharing for CERT communities.

Baseline capabilities of national/ governmental CERTs – policy recommendations

Since 2009 ENISA has actively worked on defining a minimum set of capabilities that a Computer Emergency Response Team in charge of protecting critical information infrastructures in the European Union Member States should possess. The purpose is to ensure that CERTs can take part in and contribute to cross-border information sharing and cooperation.

The operational aspects of baseline capabilities, which were created in 2009, have been very well accepted by the CERT community. In 2010 ENISA has made further improvements and presented a set of policy recommendations on the baseline capabilities of national / governmental CERTs.



The primary aim of the recommendations is to support policy- and decision-makers in the Member States in the establishment of a suitable framework that enables their national or governmental CERTs to operate properly. This is done by shedding light on policy requirements and experiences in the Member States and also by providing background information on the operations of CERTs so that their requirements and needs are better understood.

The recommendations presented in the main document focus on the proper implementation of national / governmental CERTs in order to strengthen the security and resilience of national (critical) information infrastructures. These recommendations are in line with the communications of the European Council and the Commission which address the challenges and priorities for network and information security (NIS) and critical information infrastructure protection (CIIP). They also address the establishment of the most appropriate instruments to tackle these challenges at the level of EU Member State. The recommendations do not constitute a one-size-fits-all guide, however. Member States need to scrutinise the recommendations and, with the help of ENISA, decide if they are appropriate in the context of their present national situation.

ENISA 5th workshop "CERTs in Europe"

The annual ENISA Workshop "CERTs in Europe" took place in May 2010 near Heraklion, Crete. After having focused on cooperation among key players in network and information security (NIS) on a national level in order to guarantee the resilience of national public communication infrastructure, this year the workshop focused on the role of national / governmental CERTs in national and cross-border exercises.

Representatives from different European Union Member States, the USA, Malaysia and NATO shared and discussed their experiences in organising and participating in different exercises.

The following points were mentioned by presenters as possible roles and areas of contribution by national / governmental CERTs in national and cross-border exercises:

- participation in the development of good exercise scenarios
- technical and operational support
- information retrieval
- situation awareness
- management and coordination activities
- countermeasures
- provision of networking and communication facilities

During the workshop, the main current and future activities in the area of NIS were presented also by representatives of the European Commission (EC) and ENISA. In addition, participants used the opportunity to discuss with the representatives of the EC and ENISA topics such as possible changes resulting from the upcoming modernisation of NIS Policy in the EU, challenges in implementing article 13 of the new Telecom Package, and cooperation between CERTs and law enforcement.

Good practice guide for Incident Management

To reinforce the capabilities of national / governmental CERTs, and as a follow-up to the ENISA CERT setting-up guide, this year ENISA produced the *Good practice guide for incident management*. The guide describes good practices and provides practical information and guidelines for the management of network and information security incidents with an emphasis on incident handling.

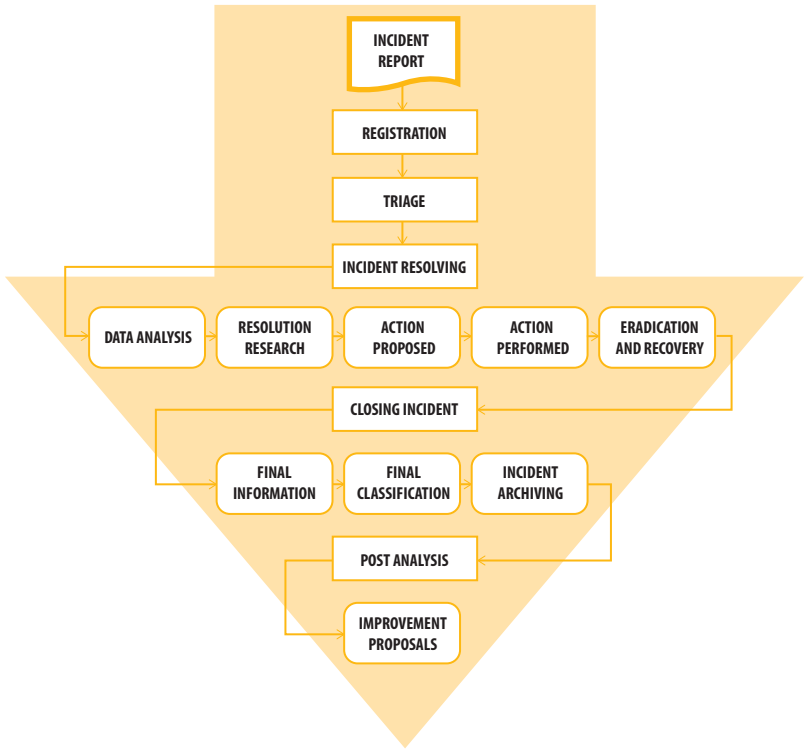
The primary audiences for this guide are the technical staff and management of governmental and other institutions that operate (or will operate) a CERT in order to protect their own IT infrastructure or that of their stakeholders.

For a CERT at the set-up stage, this guide provides very valuable input on how to actually shape incident management, and the incident handling service, in particular. For existing CERTs, it can serve as a means to enhance their current services and to obtain input and ideas for improvement.

In general, any group or team that handles information or network security incidents, not just CERTs, but also abuse teams, WARPs (Warning Advice and Reporting Point) and other security professionals, can benefit from reading the guide.

THE GOOD PRACTICE GUIDE: WHAT'S INSIDE?

The guide provides information on all aspects related to incident management, with an emphasis on incident handling. It starts from the basics of a CERT: its mission, constituency and authority. This is followed by a discussion of the basic issues in incident management and handling. Later chapters describe, for example, how to outsource parts of your incident management service and how to make presentations to management. The focus of the guide is the incident handling process – the core service carried out by most CERTs. Incident handling involves the detection and registration of incidents, followed by triage (classifying, prioritising and assigning incidents), incident resolution, closing and post-analysis.



A case study – the FI-ISAC Europe Workshops

The FI-ISAC Europe (Financial Institutions – Information Sharing and Analysis Centre) was established in 2008 with the aim of building a network between financial institutions, law enforcement agencies and national CERTs. The idea was to share information on incidents, threats, vulnerabilities and good practices. The Agency has grown significantly since its founding.

Two FI-ISAC Europe Workshops were held in 2010: the first on 15-16 April in Helsinki, Finland, the second on 29-30 November in Karlsruhe, Germany. These workshops were organised by the CERT Hungary, the Theodore Puskas Foundation (Hungary), MELANI (Switzerland), UK Payments (UK), FI-ISAC (The Netherlands), NVB (The Netherlands) and NICC (The Netherlands). The workshop in Helsinki was supported by the Federation of Finnish Financial Services, while the one in Karlsruhe was supported by BFK, Germany. ENISA supported the FI-ISAC workshops by providing input on the agenda, identifying speakers and participants, participating in the workshops, and maintaining a dedicated mailing list.

The FI-ISAC workshops aimed to create a trusted environment where stakeholders could freely share information about cybercrime in the financial sector and their experiences with national co-operation. The events brought together banks, Computer Emergency Response Teams and policy-makers, as well as an increasing number of representatives from law enforcement agencies throughout Europe. Only invited and trusted members were allowed to participate in the workshops and information was exchanged using a traffic light protocol.

It became clear during the meetings that international collaboration is greatly facilitated by the Europe-wide use of the same or similar ways of working and structures. Case studies were presented and good practice in the field was fruitfully exchanged.

IDENTITY & TRUST

As society becomes increasingly dependent on information and communication technologies, Identity, Privacy and Trust are the parallel lanes of the road towards communication networks that safeguard the EU society. The Declaration of the Future Internet Assembly (FIA) "Towards a European approach to the Future Internet" envisages the development and deployment of technologies that ensure the robustness and security of networks, managing identities, protecting privacy and creating trust in the on-line world.

ENISA is approaching this area with the following strategy:

- Facilitating the rapid deployment of research results: focusing on alternative trust models such as reputation and web-of trust, as well as a stock-taking of authentication methods.
- Fostering a Pan-European approach to privacy: focusing on rights and obligations of users as well as service-providers. Providing guidelines on the use of available privacy enhancing technologies and their implications for anonymity.
- Developing guidelines for regulatory review and interpretation: focusing on identity and authentication in new scenarios (e.g. RFID, cloud computing). And seeking to avoid the imposition of unrealistic requirements on commercial bodies or the infringement of personal liberties.

In parallel, ENISA publishes position papers in various domains, such as Security in Social Networks, and, in accordance with its Regulation, tracks standardisation activities in the area of network and information security.

What we do

The activities and tasks related to Identity & Trust are defined within the ENISA Work Programme 2010 - "Build on Synergies - Achieve Impact". The work packages dedicated to Identity & Trust are part of Preparatory Action (PA) 1: Identity, accountability and trust in the future Internet. Work Programmes may also include Preparatory Actions (PAs). A PA is an activity that is designed to complete in one year and is used to determine whether or not a new Multi-annual Thematic Programme should be initiated. A decision is taken once the results are available.

Identity, accountability and trust in the Future Internet

In 2010, ENISA launched a new activity in the area of "Trust and Privacy in the Future Internet". The main objective of this activity is to ensure that Europe maintains a high level of security and confidence of both users and industry in the ICT infrastructure and provided services, while at the same time limiting the threats to civil liberties and privacy. The Agency has formed a working group comprised of five well-known experts in ICT. Their task is to provide advice on short- and medium-term goals and objectives in the area of Privacy, Accountability and Trust.

Stock taking of authentication and privacy mechanisms

The introduction of a European data breach notification requirement for the electronic communication sector was included in the review of the ePrivacy Directive (2002/58/EC). This is an important development with the potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data is being secured and protected by operators in the electronic communication sector. Against this backdrop, ENISA reviewed the current situation in order to develop a consistent set of guidelines that address the technical implementation measures and procedures, as described by Article 4 of the reviewed Directive 2002/58/EC.

Since the beginning of the 21st century, Member States have been planning, developing and implementing new solutions to offer electronic services to citizens and businesses on a digital platform. The goal is to improve administrative efficiency, accessibility and user-friendliness and, above all, reduce costs. Policy makers and experts agreed on the desirability of finding solutions that would allow all stakeholders to work together across (digital) borders, while respecting the autonomy of each Member State. One of the directions taken defined a model, which included levels of authentication.

" …Identity, Privacy and Trust are the parallel lanes of the road towards communication networks that safeguard the EU society."

ENISA reviewed the authentication levels and their mapping to public electronic services in the eGovernment programme framework. The framework requires user authentication (security services).

For approximately the last ten years, Member States and EEA (European Economic Area) countries have been implementing electronic identity management (eIDM) systems based on their national requirements, which include improving administrative efficiency, accessibility and user-friendliness, and reducing costs. These requirements can be enhanced at the European level by improving the interoperability of electronic identification/authentication systems currently operated at national level. In 2010, ENISA identified general techniques for managing multiple identities and provided guidelines for three communities – technical, policy and end users.

Stock taking of service models supporting electronic services

In recent years, a continuously increasing number of users have been able to transfer their use of commercial or governmental services to the online environment. Online shopping, e-banking, social networks, emailing, e-taxation, etc. are now part of everyday life. As an individual user, however, it has been difficult to judge the extent to which an online service provider respects your individual rights, particularly the protection of your personal data. In 2010, ENISA conducted a survey to evaluate which mechanisms Member States have deployed in available online services for accountability, consent, trust, security and privacy.

Trends such as new technologies and globalisation are making the protection of personal data ever more complex. Against this background of rapid change, a review of the EU's data protection regulatory framework has been initiated, with a view to enhancing individuals' confidence and strengthening their privacy rights. ENISA has studied available technologies and research that addresses privacy and data protection, as well as topics related to privacy such as consent, accountability, trust, tracking and profiling. The objective of the ENISA study was to provide a comprehensive and realistic view of both limitations generated and possibilities provided by technologies in the context of personal data protection rights.

Cookies are a good example of the complexity of privacy and data protection. Originally used to facilitate browser-server interaction and as a convenience for users, more recently they are used by the advertising industry for other purposes such as advertising management, profiling or tracking. The possibilities to misuse cookies exist and are being exploited. The newer types of cookies, for example, support user-identification in a persistent manner and do not have enough transparency on how they are being used. Therefore, their security and privacy implications are not easily quantifiable. ENISA has identified and analysed some of the most common new types of cookies for security vulnerabilities and privacy concerns, and has provided recommendations for the mitigation of privacy risks.

RESILIENCE

Reliable communications networks and services are now critical to public welfare and economic stability. Disruptions due to physical phenomena, software and hardware failures, human mistakes or intentional attacks on networks and services all affect the proper functioning of public eCommunication networks. Such disruptions reveal the increased dependency of our society on these networks and their services. Experience proves that neither single providers nor a country alone can effectively detect, prevent and respond to such threats.

"Experience proves that neither single providers nor a country alone can effectively detect, prevent and respond to threats."

Recent European Commission Communications have highlighted the importance of network and information security and resilience. They have stressed the importance of dialogue, partnership and empowerment of all stakeholders to properly address these threats and increase citizen's confidence in infrastructures. Indeed, the Commission's recent Communication on CIIP recognises the importance of the area and confirms ENISA's role and expertise in the field.

Fully recognising this need, ENISA devised a Multi-annual Thematic Programme (MTP) with the ultimate objective of collectively evaluating and improving the resilience of public eCommunication Networks and Services in Europe. To achieve this objective, **ENISA organised its work in three different but complementary areas of interest:**

- The Policy and Strategy area deals with the national policies and regulatory environments across the EU Member States
- The Providers area focuses on practices, norms, procedures and techniques adopted by providers to enhance the resilience of their networks
- The Technology area analyses related technologies and highlights their security and resilience aspects.

What we do

The activities and tasks related to Resilience are defined within the ENISA Work Programme 2010 - "Build on Synergies - Achieve Impact". For 2010, the Resilience activities are included within Multi-annual Thematic Programme (MTP) 1: Improving resilience in European e-Communication networks. The work packages dedicated to Resilience are Work Package (WPK) 1.1: Underpin stakeholders' efforts to deploy ENISA s information sharing and incident reporting good practice guides; WPK 1.2: Assist providers in enhancing the resilience of their networks; and WPK 1.4: Empower stakeholders towards the first pan-European exercise.

Spreading information sharing and incident reporting good practice

Incident Reporting and the implementation of Article 13a

In 2010, ENISA started discussions with Member States on how to best implement the provision on incident reporting that is included in Article 13a of the revised Framework Directive on electronic communication and services. The final objective is to achieve a consistent and harmonised transposition and implementation of Article 13a in all 27 Member States. Moreover, the focus is on the mandatory incident reporting scheme introduced by the Directive and the security measures that Member States should enforce on the providers of public communication networks and services.

In the context of this project, ENISA is acting as a facilitator, identifying the appropriate regulatory authorities and engaging them in a structured dialogue on the relevant issues. These issues include incident reporting (e.g., conditions, parameters, and impact), minimum requirements for security and resilience, and how incidents should be reported to ENISA on an annual basis.

These activities have been pursued through the organisation of workshops, closed meetings and conference calls, in which all the Member States were invited to participate, as well as by providing appropriate tools, such as a dedicated portal for information sharing and a mailing list.

The main objectives of ENISA, as regards the reporting of security incidents and the implementation of article 13a, are to:

- identify, disseminate and consolidate the use of good practices in the area of incident collection and reporting;
- assist Member States in developing a common understanding of the main issues of article 13a and thus avoid fragmentation across Member States;
- define a unified scheme for reporting to ENISA and the European Commission that delivers added value to the Member States;
- work together with Member States and the private sector to increase their level of preparedness by developing minimum security requirements for addressing risks to resilience and security;
- support the creation of a trusted environment or community for information sharing between Member States.

As the project on Article 13a implementation spans over 2 years, ENISA, in cooperation with Member States and private stakeholders, is already planning the next near-term steps. In particular, we will continue to perform our role as a facilitator in assisting Member States with the harmonious implementation of article 13a. We will also establish a permanent communication platform to engage Member States and the private sector in a dialogue. The purpose of the dialogue is to establish a framework for data collection and analysis. ENISA will also prepare guidelines and good practices to assist Member States in implementing the "appropriate technical and organisational measures" described in paragraphs 1 and 2 of Article 13a. Finally, we will define a framework for the collection and analysis of information reported by the Member States.

Information Sharing

Information sharing is among the most common form of co-operation between stakeholders. It is considered a means to better understand a changing environment and learn in a holistic manner about intrusions, vulnerabilities, and threats. It involves joint action to develop recommendations for reducing network security vulnerabilities and threats, and to develop methods to continuously assess existing measures.

The most popular structure to facilitate this sharing is a 'trusted' forum or platform where owners or operators of private infrastructure can meet face-to-face at regular intervals to hold informal discussions. This may be through Public-Private Partnerships (PPPs) or other more formal or informal mechanisms.

Many countries have established sector-specific information sharing partnerships between government and the private sector. There are different approaches to sharing across the EU, with some Member States preferring a vertical, sector stratification while others prefer a horizontal one.

In 2009, ENISA issued its *Good Practice Guide (GPG) on Information Sharing*. The guide aims to assist Member States and other relevant stakeholders in setting up and running Network Security Information Exchanges in their own countries. Building on its work, in 2010, ENISA aimed to create awareness among Member States about the importance of Information Sharing. For that reason, in March 2010, ENISA organised an international workshop with keynote speakers from Industry, Academia, National Regulatory Authorities (NRA) and the public sector. ENISA also participated in a special session at the RSA Conference in London (12-14 Oct) on the future of pan-European information sharing, and organised, in the context of the Pan-European Forum of Member States in October, a special session on information sharing.

At the events, leading experts from Industry and Academia presented their experiences on information sharing and debated the opportunities for Member States and Industry. Some of the key findings were:

- Only a limited number of Member States has a national information sharing platform; Member States asked ENISA to promote the concept across EU countries and continue its efforts to raise awareness among both the public and private sectors on its importance.
- There is significant interest among existing national information sharing platforms to better understand each other, develop working relationships, effectively share information, and even develop a small pan-European information sharing platform.

- There is no cross-country operational information sharing platform on ICTs at the moment. The expectation was that the EU's Public Private Partnership for Resilience (EP3R) would fulfil this role. On the strategic level, the European Forum for Member States (EFMS) was mentioned.
- Analysing shared information is very important. Apparently almost all Information Exchanges focus mainly on sharing information but not on analysing it. The US Information Sharing Analysis Centres (US-ISAC) are a good example on how information could be analysed.
- Typical problems with the analysis of information include 1) the ownership of data; 2) the quality of data; 3) the trustworthiness of data; 4) the correlation of data; and 5) the combination of different analyses into a single integrated one.

These conclusions confirm that the private and public sectors should work closely to share information. The advent of EP3R should help Europe's public and private organisations to reach this goal.

Enhancing network resilience

Botnets

Botnets are networks of compromised, remotely controlled computer systems. They are used for the distribution of spam e-mails, coordination of distributed denial of service attacks, and the automated theft of identities (e.g. credit card information and general banking data) for financial fraud.

"To efficiently allocate the limited funds available for fighting botnets, it is essential to have accurate assessments of the relative size and impact of different botnets."

To efficiently allocate the limited funds available for fighting botnets, it is essential to have accurate assessments of the relative size and impact of different botnets. Current data on botnets provides, at best, estimates of numbers of infections based on very limited samples and poorly documented methodologies. Most statistics are based on the number of IP addresses on which bots are detected. Even if such data were accurate, however, the actual impact of botnets is not related solely to such numbers.

To address the lack of complete or reliable data on botnets, in 2010, ENISA produced a report, *Botnets: Detection*, Measurement, Disinfection & Defence which addresses the effectiveness of various strategies for measuring botnets, different measures for disinfecting and defending against botnets and the kinds of policies that are effective in reducing the number of infections.

Botnets are a serious threat that can only be handled through cooperation and the cooperative efforts of all affected stakeholders. Recommendations and good practices can be organised according to three categories: 1) mitigation of existing botnets and infections; 2) preventive measures for reducing the acquisition of new bots and growth of botnets; and 3) approaches that target botnet usability as seen from the botherder's view.

Alongside the main report, ENISA will also publish a report entitled *Botnets, 10 hard questions*, summarising the most important aspects of the discussion in the expert group. A separate document will discuss the legal issues in depth (based on a separate consultation with legal experts). ENISA will use the consultation group to drive forward the technical, policy and legal recommendations in a European policy context in 2011 and beyond.

BOTNETS: DETECTION, MEASUREMENT, DISINFECTION & DEFENCE

ENISA's Botnet report covers two main topics:

1. **Strategies for measuring botnets**
   - An assessment of uncertainty in a methodology.
   - The extent to which a technique is detectable by botnet controllers.
   - The relative impact of different species of botnets.
2. **Measures for disinfecting and defending against botnets. ENISA engaged with over 70 botnet experts to discuss methodologies and best practices. We examined the problem from all angles including technical, legal, economic, and policy initiatives. Areas covered include:**
   - How best to discover and disinfect botnets, and, just as important, take down the botnet herders' command and control centres. There are increasingly sophisticated ways of hiding command and control channels.
   - Legal issues – some defensive measures which might be effective are not practical because of legal obstacles. Either they are illegal or they take too long because of red tape.
   - Economic issues – botnets only exist because they make money for their owners. How can we find ways of 'cutting off the food supply'? Another important issue is that an organisation tends to lose revenue and suffer damage to its reputation if it informs its users about a botnet infection, even though it is not responsible for the infection.
   - Policy initiatives – what kinds of policies are effective in reducing the number of infections? For example, how effective are so-called 'walled gardens' – in which ISPs redirect infected machines to a safe online environment where they are provided with guidance on how to disinfect their machines.

Incentives and Challenges for Information Sharing

The importance of Information Exchange (IE) in ensuring network and information security is widely acknowledged by both policy makers and by the technical and practitioner community.

This study, Incentives and Challenges for Information Sharing, identifies barriers to and incentives for information sharing in the field of network and information security, in the context of peer-to-peer groups such as Information Exchanges (IE) and Information Sharing Analysis Centres (ISACs).

As a part of this research we asked practitioners to rank a list of barriers and incentives in terms of their relative importance. The findings indicate that many of the barriers and incentives commonly identified in the available literature are of relatively low importance to practitioners and security officials currently working in IEs.

According to the study, the most important incentives are economic (cost savings) or derived from the quality, value, and use of the information shared. The most important barriers were identified as poor quality of information, misaligned economic incentives stemming from risks to reputation, and poor management.

The report provides specific recommendations for both public decision-makers and private sector stakeholders. According to the report, European institutions should play an active role in developing a platform at the European-level and in linking different, existing

national IEs. European institutions should also address issues regarding the legal framework for information sharing (e.g. better understanding of legal regimes, legal barriers, encourage consistency) and map the legal environment for information sharing across the EU. Finally, they should encourage information sharing beyond the confines of the ICT sector.

National governments should establish IEs where none exist or host IEs. They should ensure that the legal framework is conducive to information sharing and publicise the benefits of IEs. National governments should also identify sectors in which platforms already exist which could be used as forums for information sharing.

The Private Sector should be transparent and share information responsibly. The report notes that IEs provide an excellent opportunity for openness. The private sector should also use IEs to improve security voluntarily. Used in this way, IEs can help avoid regulatory interest and strong regulatory action which might be counterproductive. The private sector could also set up one or more private sector only IEs as a pilot.

ENISA will continue its efforts in the area of information sharing. The main objectives are to make Member States more aware of the importance of Information Exchange, increase the number of Member States running IEs, and to develop knowledge and expertise on the subject that can then be used in the Public Private Partnership for Resilience (EP3R).

Resilience metrics

The ENISA study on metrics frameworks (Measurements Frameworks and Metrics for resilient networks and services) concentrates on providing ENISA's stakeholders with an overview of the mechanisms used to measure resilience. By presenting the frameworks currently used to measure the performance and availability of networks and suggesting a new taxonomy for metrics, ENISA has established the baseline for achieving better results in the area of quality of service.

The hierarchy of metrics that ENISA proposes covers individual providers and operators, but extends to the cross-border and even pan-European level. The framework is an essential ingredient for improving security in network architecture and in improving information sharing and security incident reporting. Developing this common framework will require commitment from Member State stakeholders – either the public or private sector.

The main challenges related to resilience metrics and measurements are a lack of standard practices and that organisations use their own specific approaches for measuring resilience, if they measure it at all. Resilience metrics, however, are difficult to deploy mainly due to the lack of knowledge and awareness on the subject.

With regard to improving the current state of resilience metrics, a number of policy recommendations emerged from the analysis of the information received during the online survey and the interviews with participants. It was felt that the European Commission and the Member States should:

- create a common understanding and good practices or standards on resilience metrics.
- stimulate investment in the research and development of resilience measurements, open issues frameworks and metrics.

>>

	Dependability	Security	Performability
Recovery	• Mean down time • Mean time to repair • Maintainability	• Mean time to incident recovery	
Service Delivery	• Operational mean time between failures • Operational availability • Operational reliability • Fault report rate	• Incident rate • Illegitimate network traffic • Percent of systems without known severe vulnerabilities	• Delay variation • Packet loss • Bandwidth utilization
Preparedness	• Mean time to incident discovery • Mean time to patch • Patch management • Vulnerability scanning coverage	• Risk assessment coverage • Security testing coverage	• Tolerance

Domain-based classification

MEASUREMENTS FRAMEWORKS AND METRICS FOR RESILIENT NETWORKS AND SERVICES

The complete study consists of two reports. The first report identifies the main challenges and lists the recommendations as they were revealed from the consultation with stakeholders and the state of the art review. The second report is a technical document that already attempts to address some of the most important recommendations. It includes the full state of the art review as well as the first time ever attempt to encapsulate all resilience metrics within a single, two dimensional taxonomy. The latter report is considered a working document. ENISA plans to update and revise it in 2011 based on consultation, presentations in workshops and expert forums including both academia and industry.

- Increase the awareness of resilience metrics and the relevant regulations related to resilience.
- Assist in the creation of tools to automate the deployment of resilience measurement (mainly data collection and data analysis).
- Facilitate co-operation between countries, public and private organisations, and encourage the sharing of information and good practice in resilience metrics. The creation of closed or sector-specific information sharing groups about metrics and measurements could possibly increase the trust needed for organisations to share information.

Regulators, industry consortia and public-private partnerships also have a role to play. They should create clear and practical good practices, or even standards, for the measurement of resilience. ENISA will continue working on this topic in the coming years. Our aim is to relate metrics with minimum security requirements for telecommunication providers and interconnection.

The first pan-European exercise: Cyber Europe 2010

On 4 November 2010, in an act of unity, all European Union (EU) Member States and three European Free Trade Association (EFTA) countries (Norway, Switzerland and Iceland) participated in **CYBER EUROPE 2010**. This was the first ever pan-European Cyber Security Exercise. The objective was to increase the understanding of how cyber-incidents are handled and test communication links and procedures in case of a large scale cyber-incident. The exercise was facilitated, organised and managed by ENISA and supported by JRC, the European Commission's Joint Research Centre.

CYBER EUROPE 2010 was first envisaged in the European Commission's Critical Information Infrastructure Protection (CIIP) action plan and reinforced by the Tallinn Ministerial Declaration and the Council Resolution of December 2009. The activity was foreseen in the 'Digital Agenda'. In its recent Digital Agenda, the European Commission (EC) called for ENISA to continue supporting EU and EFTA Member States in organising and running national exercises. Member States will develop their expertise and capabilities in the field through dedicated good practice guides, seminars and training.

The exercise was the result of extensive planning and intensive discussions. The first phase of CYBER EUROPE 2010 was a dry run at the end of September 2010. The after-exercise events included a de-briefing session immediately after the exercise. The exercise will be evaluated in depth, with additional evaluations to be conducted at the national level. These will later be fed into an overall public, EU-wide report on the

" CYBER EUROPE 2010 was a useful 'cyber stress test'"

exercise. The full report is to be published at the beginning of 2011 and a major workshop will be held to disseminate the results.

The exercise scenario concerned incidents affecting the availability of the Internet in several European countries, with Internet interconnectivity between countries gradually becoming unavailable. As a result, citizens, businesses and public institutions would have difficulty in accessing critical online services, unless the traffic from affected interconnections could be re-routed. As the phenomenon continued, one country after another would suffer increasingly from this problem throughout the day. In such circumstances, all playing Member States would have to cooperate in a joint response to the crisis.

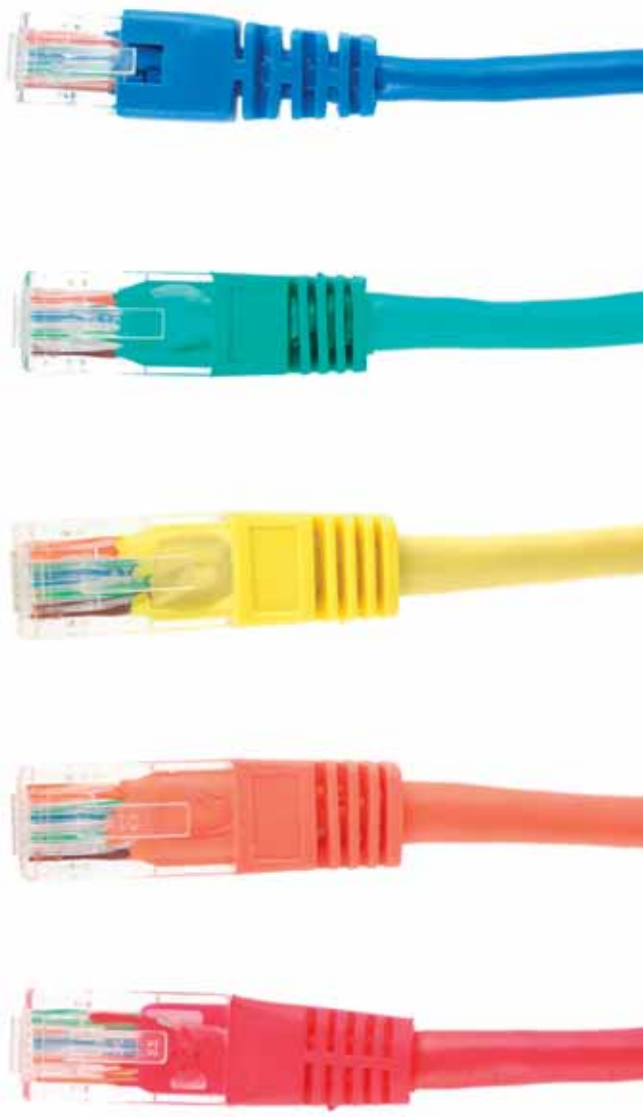
Participants in CYBER EUROPE 2010 were public authorities of EU Member States. The private sector did not take part in the exercise as the objective was to test the communication links and procedures among competent national bodies. The set-up of the exercise required public authorities in one Member State to make contact with participating public authorities, also called players, in other Member States.

Participating organisations varied by Member State, but the players included: communications ministries, communications regulators, critical information infrastructure protection authorities, crisis management organisations, law enforcement organisations, media and external communications teams, national Computer Emergency Response Teams (CERTs), national information security authorities and national intelligence departments.

The interim findings and recommendations of EU Member State participants indicate that CYBER EUROPE 2010 was a useful 'cyber stress test' for Europe's public bodies. It fully met its objective of testing Europe's readiness to face online threats to the critical infrastructure used by citizens, governments and businesses.

A number of observations and recommendations were made by Member State participants at the workshop on 5 November, immediately following the exercise. Participants stated that exchanging 'lessons learnt' with other (national or international) exercises would be useful. They also felt that the private sector should be part of the next pan-European exercise. Participants noted that incident handling in Member States varies a lot due to the different roles, responsibilities and bodies involved in the process. Member States had difficulty in fully grasping how incidents are managed in other Member States. ENISA was commended for its role in organising and managing the exercise, which participants said fully met its objectives. They felt that ENISA should continue to play this role.

The subject of CIIP is global, not just European, and discussions opened recently on collaboration between the EU and the US. The agenda includes dialogue on a future joint exercise. The CYBER EUROPE 2010 exercise was just the beginning.



National Exercises

In 2010 ENISA continued to support Member States in organising National Exercises. The *Good Practice Guide* on Organising National Exercises that was prepared in 2009 was used in 2010 to organise and plan the first pan-European exercise. In parallel, ENISA worked on material for a seminar based on the guide. The seminar material was made available to interested Member States. ENISA has already given the seminar in one Member State, and other Member States have already agreed to organise seminars with the help of ENISA in early 2011. ENISA will continue to support the organisation of national exercises by further organising seminars on how to plan, organise and conduct national exercises. Interested Member States should contact ENISA about future opportunities.

Resilience of the Internet Interconnection Ecosystem (extra mile)

This study looked at the resilience of the Internet interconnection ecosystem. The Internet is a network of networks, and the interconnection ecosystem is the collection of layered systems that holds it together. The interconnection ecosystem provides the basic function of reaching anywhere from everywhere. It is complex and has many interdependent layers. This system of connections between networks occupies a space between and beyond those networks and its operation is governed by their collective self interest – the Internet has no central Network Operation Centre, staffed with technicians who can leap into action when trouble occurs. The open and decentralised organisation that is the very essence of the ecosystem is essential to the success and resilience of the Internet as a whole. Yet there are a number of concerns.

The Internet is vulnerable to various kinds of common mode technical failures in which systems are disrupted in many places simultaneously; service could be substantially disrupted by failures of other utilities, for example, particularly the electricity supply. Moreover, there are concerns about the sustainability of current business models. Internet service is cheap and rapidly becoming cheaper. Because the costs of service provision are mostly fixed costs and marginal costs are low, competition forces prices ever downwards. Ultimately, there is a risk that consolidation might reduce the current twenty-odd providers to a mere handful. At that point the providers would start to gain pricing power and the regulation of transit service provision might become necessary as in other concentrated industries.

Another challenge is that dependability and economics interact in potentially pernicious ways. Most of the things that service providers can do to make the Internet more resilient, from maintaining excess capacity to route filtering, benefit other providers much more than the firm that pays for them, leading to a potential 'tragedy of the commons'. Similarly, security mechanisms that would help reduce the likelihood and the impact of malicious acts, error or accident, are not implemented because no one has found a way to roll them out that gives benefits that are sufficiently incremental and local.

> "…the Internet has no central Network Operation Centre, staffed with technicians who can leap into action when trouble occurs."

There is also remarkably little reliable information about the size and shape of the Internet infrastructure or its daily operation. This hinders any attempt to assess its resilience or the true impact of particular inci-

dents. The opacity also hinders research and development of improved protocols, systems and practices by making it hard to know what the issues really are and harder yet to test proposed solutions.

In view of the above, there may be significant troubles ahead which could present a real threat to economic and social welfare and lead to pressure for regulators to act. Despite the origin of the Internet as an initiative funded by the US government, the more recent history of government interaction with the Internet has been less successful. Various governments have made ham-fisted attempts to impose censorship or surveillance, while others have defended local telecommunications monopolies or have propped up other industries that were disrupted by the Internet. As a result, Internet Service Providers, whose good will is essential for effective regulation, have little confidence in the likely effectiveness of state action, and many would expect it to make things worse.

At this stage, there are four types of activity that can be useful at the European (and indeed the global) level. The first is to understand failures better, so that all may learn the lessons. This means consistent, thorough investigation of major outages and the publication of the findings. It also means understanding the nature of success better by supporting the long term measurement of network performance and by sustaining research in network performance. A second activity is to fund key research on topics such as inter-domain routing – with an emphasis not just on the design of security mechanisms, but also on developing an understanding of how solutions are to be deployed in the real world. Thirdly, we should continue to promote best practice. Diverse service provision can be encouraged by explicit terms in government contracts, and by auditing practices that draw attention to an over-reliance on systems that lack diversity. There is also a useful role for regulators to play in promoting the independent testing of equipment and protocols. Finally, public engagement is important. Greater transparency may help Internet users to be more discerning customers, and create incentives for improvement. The public should be engaged in discussions on potentially controversial issues such as traffic prioritisation in an emergency. Ultimately, if regulation of the Internet interconnection system is ever needed, governments need to figure out who's going to do it and start the discussions needed to prepare the ground for such regulation.

The objective of these activities should be to ensure that when global problems do arise, the European Commission has a clear understanding of the problems and of the options for action, including local regulatory actions that Europe can encourage when needed. ENISA will continue this work in 2011 with a focus on economic and market drivers (incentives, Service Level Agreements, etc.), as well as the policy and technical aspects of routing, traffic engineering and prioritisation.

Resilience / Secure technologies

Secure routing

Routing infrastructure is critical infrastructure and needs to be protected in order to secure public communication networks. In 2010, ENISA assessed the impact of deploying secure routing technologies. A survey of network operators in the EU was conducted on their use of or (concrete) plans to use secure routing technologies. ENISA will use the assessment to produce guidelines and/or recommendations for the deployment of secure routing technologies targeting policy makers.

End-to-end resilience

Public communications networks constitute the basis upon which a plethora of applications and services are offered, in many cases independent of the network operator. Users of ICT services are interested in end-to-end resilience and security, as well as resilient and secure transportation networks. Identifying high-performance architectures is, therefore, important; however, there is the risk that architectures may be strongly bound to the particularities of the technologies they deploy. Design principles, on the other hand, are likely to remain the same across technology platforms. In 2010, the Agency extended its work on assessing the impact of networking trends on the resilience of public communications networks. It identified and promoted architectural design principles that would enable true end-to-end security for any communication over the network.

RISK MANAGEMENT

Decision makers in both the public and private sector need a clear insight into the nature and impact of emerging and future network and information security challenges in the Information Society. Such challenges are connected to security risks pertinent to emerging and future applications and technologies entering the European market. Better insight into Emerging and Future Risks would allow public and private sector stakeholders to take more appropriate decisions and to have a better basis for policy making.

"Better insight into Emerging and Future Risks would allow public and private sector stakeholders to take more appropriate decisions and to have a better basis for policy making."

In 2008-2009, the Agency established a framework that enables stakeholders to better identify and understand Emerging and Future Risks (EFR) arising from new technologies and new applications. The framework is referred to as the Emerging and Future Risks Framework (EFR Framework). In 2010, ENISA delivered risk assessment reports on Emerging and Future Risks for specific application and technology scenarios. The scenarios reflect the views of various stakeholders across Europe, but also take account of other ENISA activities in the identification of emerging risks as a transverse issue. The ENISA work on EFR is designed to promote a proactive approach to dealing with emerging and future challenges generated by new and emerging technologies and applications. This activity aims to boost trust and confidence in the information society, particularly in important areas such as Resilience and Identity & Trust. As such, EFR is developing into a transverse support function for other ENISA MTPs when it comes to identification of emerging risks.

What we do

The activities and tasks related to Risk Management are defined within the ENISA Work Programme 2010 - "Build on Synergies - Achieve Impact". For 2010, the Risk Management activities are included within Multi-annual Thematic Programme (MTP) 3: Identifying emerging risks for creating trust and confidence. The work packages dedicated to Risk Management are Work Package (WPK) 3.1: Framework for assessing and discussing emerging and future risks – Analysis of specific scenarios; WPK 3.2: Maintenance of EFR framework; and WPK 3.3: Enhancing national risk management preparedness.

Security and privacy risks of life-logging technologies

Life-logging is not a new concept: people have always felt the need to capture and share moments from their lives. The advent of many new and exciting technologies such as social networking websites has, however, broadened and facilitated life-logging to an extent that would not have been possible before: individuals can now capture anything they want as they go about their daily activities and this data can be easily collected, copied, shared, and stored forever. Just because we can record it, however, does it mean we should? There are serious security and privacy risks underlying the use of such technologies, which impact the individual, industry, the government and society at large. These risks may go well beyond the social networking risks already identified. In this context, ENISA performed a study with a working group consisting of multi-disciplinary experts, and based on a prospective life-logging scenario. The working group explored the major benefits of these technologies, as well as the serious risks they pose. The experts provided some high-level recommendations that address those risks [report to be published].

Contribution to the PIA framework development process

The European Commission recommendation "on the implementation of privacy and data protection principles in applications supported by radio frequency identification" (12 May 2009), calls on Member States to ensure that industry develops a framework for privacy and data protection impact assessments (PIA). On 31 March, the industry published a draft proposal on A Privacy and Data Protection Impact Assessment Framework, and sent it also to the Article 29 Working Party for endorsement. According to the Commission's RFID recommendation, the development of the

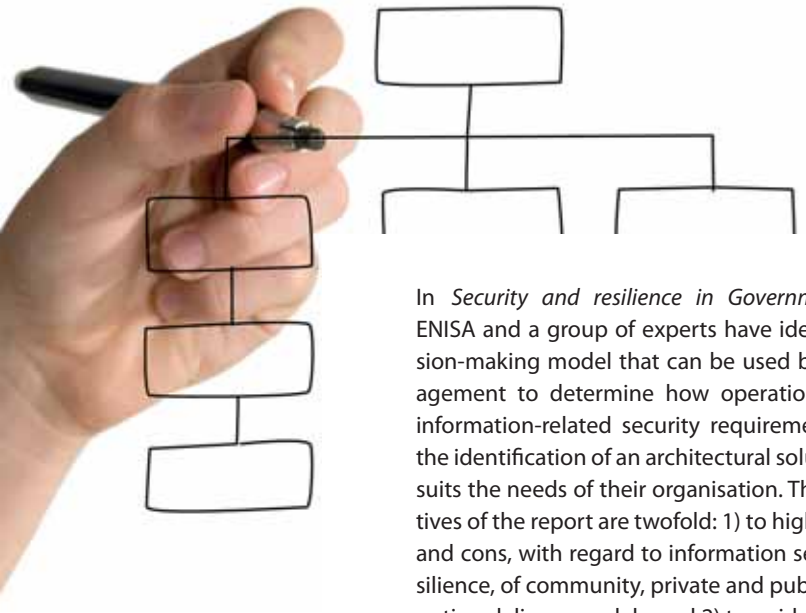
PIA Framework should build on existing practices including the work conducted by ENISA. Given ENISA's expertise and experience in the field of risk management and the development of a risk assessment framework, the Agency has been asked by the European Commission to provide comments and recommendations on the draft of the PIA framework and appropriate support, when needed. In view of the above, **in 2010 ENISA has contributed to the process in the following ways:**

- Made an informal presentation to the Article 29 Technology Sub-group meeting (on the 16th of June) on the Agency's initial comments on the draft submitted by the industry to Article 29 on 30 March 2010.
- Issued an official opinion in July 2010 based on the draft submitted by the industry on 30 March 2010. The opinion was also referenced in the Article 29 Working Party opinion of July 2010. In its opinion, ENISA identified issues and areas for improvement. Based on these, the Agency made some recommendations which could substantially improve the current PIA draft. Given our experience and expertise, our comments are mainly related to the methodology used (particularly regarding risk management and impact assessment) rather than legal issues. The text of the formal opinion is available on the ENISA web-site at: Agency Opinion on the Industry proposal for Privacy Impact Assessment for RFID.
- Assisted the European Commission in moderating a discussion between industry parties in a meeting held on the 22nd of October, with a view to facilitating the delivery of the updated version of the PIA framework proposed by the industry.
- Assisted the European Commission in moderating a discussion between industry parties in a meeting held on the 22nd of October, with a view to facilitating the delivery of the updated version of the PIA framework proposed by the industry.
- After receiving appropriate requests from the industry and the Article 29 Working Party, ENISA provided informal comments on the latest version of the PIA framework during November 2010.

Security and resilience in Governmental Clouds: making an informed decision

We are seeing some government agencies and Public Administrations (PA) moving towards a "cloud approach". This is happening all around the globe, from the USA, Japan, and Singapore to Europe, where early adopters such as the Netherlands, the UK, and Germany are announcing or planning to move into the cloud.

In the short to medium term (1 to 3 years), an increasing number of public institutions in Member States are expected to adopt the cloud computing service delivery model. This is why ENISA believes it is important to provide guidance on the security and resilience factors influencing the choice for (or decision against) cloud computing solutions for public bodies and organisations.



In *Security and resilience in Governmental Clouds*, ENISA and a group of experts have identified a decision-making model that can be used by senior management to determine how operational, legal and information-related security requirements can drive the identification of an architectural solution that best suits the needs of their organisation. The main objectives of the report are twofold: 1) to highlight the pros and cons, with regard to information security and resilience, of community, private and public cloud computing delivery models; and 2) to guide public bodies in the definition of their requirements for information security and resilience when evaluating cloud computing service delivery models.

The report seeks to support Member States in the definition of their national cloud strategy with regards to security and resilience, and follows work done by ENISA during 2009, and particularly the report: Cloud Computing: Benefits, risks and recommendations for information security.

Enhancing National Risk Management Preparedness

Critical Information Infrastructure Protection (CIIP) and the resilience of communication networks is an area that involves many stakeholders and addresses many areas, from technology to policy to coordination and communication between organisations. The proactive management of information risks is a key issue in building up and maintaining resilient information infrastructures. When looking at the elements of risks pertaining to information assets (both technical and organisational), different aspects have to be taken into account, depending on the nature, importance and impact this information has in a CIIP context. Furthermore, when considered at the level of a Member State, the establishment or enhancement of National Risk Management (NRM) preparedness has to involve multiple stakeholders from both the private and public sectors.

ENISA has defined the elements of a framework for the governance of National Risk Management (NRM) in relation to a country's Critical Information Infrastructure (CII). As such, it deals only with the management of information security risk, rather than risk management in the broader sense. **Three essential processes for the governance of Risk Management at the national level have been identified:**

- Process 1: national risk management policy making.
- Process 2: implementation coordination and support (of risk management in CII stakeholder organisations)
- Process 3: reviewing, reassessing and reporting on national risk management.

The framework for the governance of National Risk Management, as described in this document, is not intended to be used as a blueprint for the creation of a fully functioning NRM programme. However, it is intended to enable stakeholders in a nation's CII to gain an overview of the elements that are required to build such a programme, and to understand the relationships between these elements.

In addition to the description of the framework for the governance of NRM, this document contains the following elements:

- Questionnaires for use in assessing national capability maturity in relation to NRM preparedness.
- Guidance on how a framework for NRM governance can be developed and implemented.
- A process to test NRM preparedness and areas in which tests might be conducted.
- A brief report on NRM preparedness in four EU countries.

The document may be used by national governments in a number of ways. They may use it, for example, to identify strengths and weaknesses in the implementation of NRM in their country and examine how their government's NRM implementation is perceived by national CII stakeholder organisations. They can also use the document to assist with the development of a framework for their governance of NRM or to help the government assist in the development of risk management in their national CII stakeholder organisations.

AWARENESS RAISING

With the proliferation of increasingly sophisticated security breaches, the information security solutions used today will be obsolete by tomorrow. The security landscape is continually changing. But if, as most analyst reports claim, the human component of any information security framework is the weakest link, then only a significant change in user perception or organisational culture can really reduce the number of information security breaches. Consequently, a high personal awareness of the risks as well as the available safeguards is recognised as the first line of defence in securing information systems and networks. To improve NIS, all actors, including the industry and stakeholders, as well as end-users as individuals, must assume a share of responsibility.

What we do

The activities and tasks of the Awareness Raising (AR) Project are defined within the ENISA Work Programme 2010 - "Build on Synergies - Achieve Impact". For 2010, the awareness activities are included within Multi-annual Thematic Programme (MTP) 2: Developing and maintaining cooperation models. The work package dedicated to awareness raising is Work Package (WPK) 2.1: Cooperation platform for Awareness Raising Community.

Developing and maintaining co-operation models

During 2010, ENISA focused on building the information security awareness community and showing what public institutions and private companies can do to enhance users' information security awareness. To this end, ENISA worked to identify relevant information security experts and activities with which it could be involved, along with security topics which may be relevant for raising information security awareness. In particular, ENISA supported organisations in their efforts to raise the information security awareness of

> "…a high personal awareness of the risks as well as the available safeguards is recognised as the first line of defence in securing information systems and networks."

their employees and/or customers. The Agency provided educational and promotional material such as training modules, posters, illustrations, screensavers and video clips. This material is available for download and use in any information security training programme, awareness raising activity or company website. ENISA also supported organisations by providing customised communication material, and by identifying key awareness messages and areas in which information security awareness should be raised.

The Awareness Raising Community

The Awareness Raising (AR) Community is subscription-free and open to experts who have an interest in engaging in raising information security awareness within their organisations. The AR Community was launched in February 2008 and is designed to work with ENISA in fulfilling its mission to foster a culture of information security. The community shares emerging good practice and discusses cutting-edge topics and key issues in the information security field.

The AR Community sees different people and cultures as an asset in promoting a culture of information security. In a very short time, the Community has grown to 46 nations, comprising 406 members. All EU and European Economic Area (EEA) countries are represented and members are welcome from any country, within or outside Europe.

The AR Community now serves as an effective point of contact for matters related to information security awareness. Though members have a diverse range of skills and knowledge of ICTs, as well as differing interests, priorities and levels of expertise, they are united in their desire to help the AR Community become the intellectual backbone for the exchange of information security good practices.

The AR Community's work increased in 2010 through a combination of activities supported by the continuous involvement of members of the community. ARNews and a calendar of events were prepared

using inputs received by experts and were then distributed to community members. Alongside this, the AR Community offers the chance to participate in presentations at events. To enhance its capacity, and to promote knowledge sharing and dialogue within Member States and stakeholder organisations, a new way of coming together and sharing information was established. An awareness raising portal was launched at the beginning of 2010. This has enabled the AR Community to exchange emerging good practices and to discuss cutting-edge topics and key issues in the information security field.

In addition, a number of AR Community members have participated in virtual working groups which have enabled the preparation of white papers on topics such as the use of social networks, mobile phones and how to shop safely online.

Awareness Raising virtual working group publishes white paper on smartphones

Eighty million smartphones were sold worldwide in the third quarter of 2010, accounting for 20% of the total of mobile phones sold in the quarter. In the EU5 alone (UK, Germany, France, Spain, and Italy) the number of smartphone users increased to a total of 61 million. Smartphones are becoming increasingly important across the EU. Therefore, ENISA conducted a study to give an overview of the main information security risks and opportunities. The study mainly targeted IT officers (CIO's, CSO's, CTO's, etc.) in business and public organisations, and was intended to facilitate their evaluation and mitigation of the risks associated with adopting smartphones. The report assesses and ranks the most significant information security risks and opportunities for smartphone users, and gives prioritised recommendations on how to address them.

Awareness raising publications and activities

Training material for small and medium enterprises

This training material was developed for small and medium enterprises to raise awareness among their employees about important information security issues. The training modules were created by ENISA in conjunction with train-the-trainer reference guides for small and medium enterprises. The guides raise employees' awareness about fundamental issues regarding e-mail security, malicious software, identity theft prevention, use of the Internet at home, and security while travelling or working remotely.

The documents are designed to provide easy to understand information that focuses employees' attention on information security and encourages them to recognise and respond accordingly to threats. The training material may be used by individuals or presented in a classroom setting by instructors who are involved in their organisation's security awareness efforts. The train-the-trainer reference guides provide additional notes and external references for trainers and presenters to utilise while performing security awareness training.

Online as soon as it happens

This report describes the major risks and threats related to the social networking world and the mobile phone services that enable users to experience social networking sites (SNSs) on their handsets. While many of the privacy issues originating from web-based access to SNSs also apply to mobile social networks, there are also a number of risks and threats which are unique to mobile social networks. The publication points out risks and threats such as identity theft, corporate data leakage and reputation risk. The report provides Member States with a set of recommendations for raising the awareness of social network users – and in particular of social mobile users – regarding the risks and the possible consequences related to the improper use of mobile social networks.

The New users' guide: How to raise information security awareness

Two years after the publication of *The New users' guide*: How to raise information security awareness, ENISA reviewed this document in the light of new research and analysis conducted in the field. The updated version contains new activities and case studies as well as templates and samples. The guide presents an analysis of the main processes required to prepare

and implement information security awareness programmes in public and private organisations. Each process is analysed and time-related activities and dependencies are identified. The process modelling can be used to jumpstart awareness programme development.

How to shop safely online

This report analyses the anatomy of 'Online Shopping' and warns about the risks and threats. It suggests different countermeasures and guidelines to consumers – summed up in 5 'golden rules' – on how to shop safely online. The publication also displays a comprehensive checklist for the online seller who would like to operate a secure online shop. As many citizens lack trust in online purchases, this paper aims to increase awareness of the real risks involved and how to tackle them.

The biggest barrier to ordering online is the fear of potential fraud or identity theft. This fear still keeps millions of consumers from buying goods or services online. The report gives a comprehensive overview of the definition, history, main drivers and trends in online shopping. It discusses banks' payment services, the underlying Internet Infrastructure Services, and online fraud. The 'golden rules' list for consumers includes tips on avoiding fraudulent sites, how to protect your data when shopping online, tips for safe transactions when paying online, legal rights that protect online customers and how to deal with completion issues (mainly order fulfilment). As many citizens lack trust in online purchases, this publication aims to increase awareness of the real risks involved and how to tackle them. It concludes that online shopping offers great benefits to consumers and will continue to grow worldwide.

Protecting children...and organisations

In 2010 ENISA produced material to help raise information security awareness among two different groups: parents and organisations. The first set of material includes Internet safety tips and is designed to make parents more aware of what they can do to enhance the safety of children using the Internet. ENISA believes that awareness of what children can do online and parental involvement are crucial. Parents must be educated, empowered and engaged to ensure truly positive and valuable experiences for their children, while reinforcing safe online habits in the process.

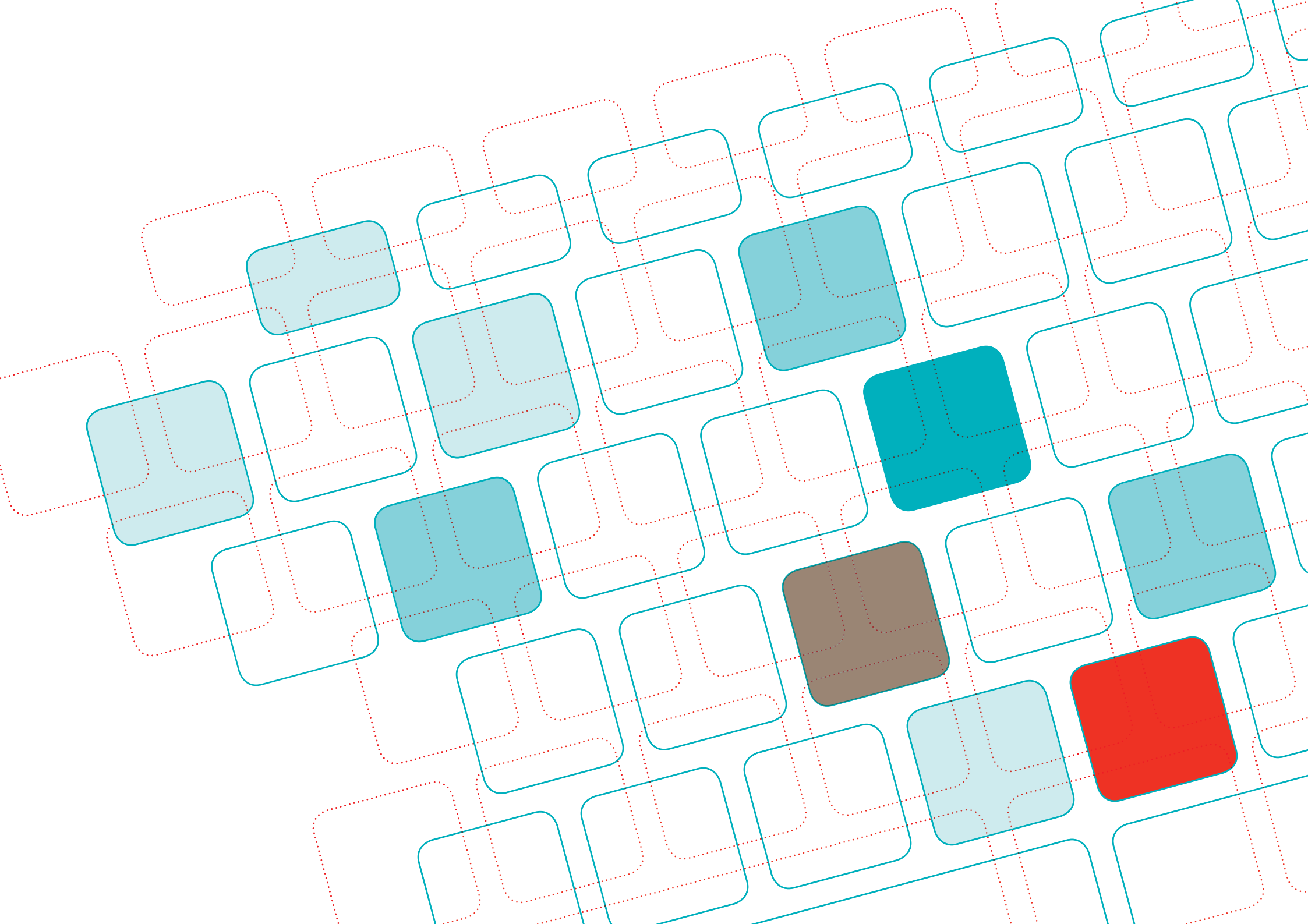
The second set of material was produced to help organisations keep their computers and networks safe. Information security tips were created for employees to ensure that they understand their roles and responsibilities in safeguarding sensitive data and protecting company resources.

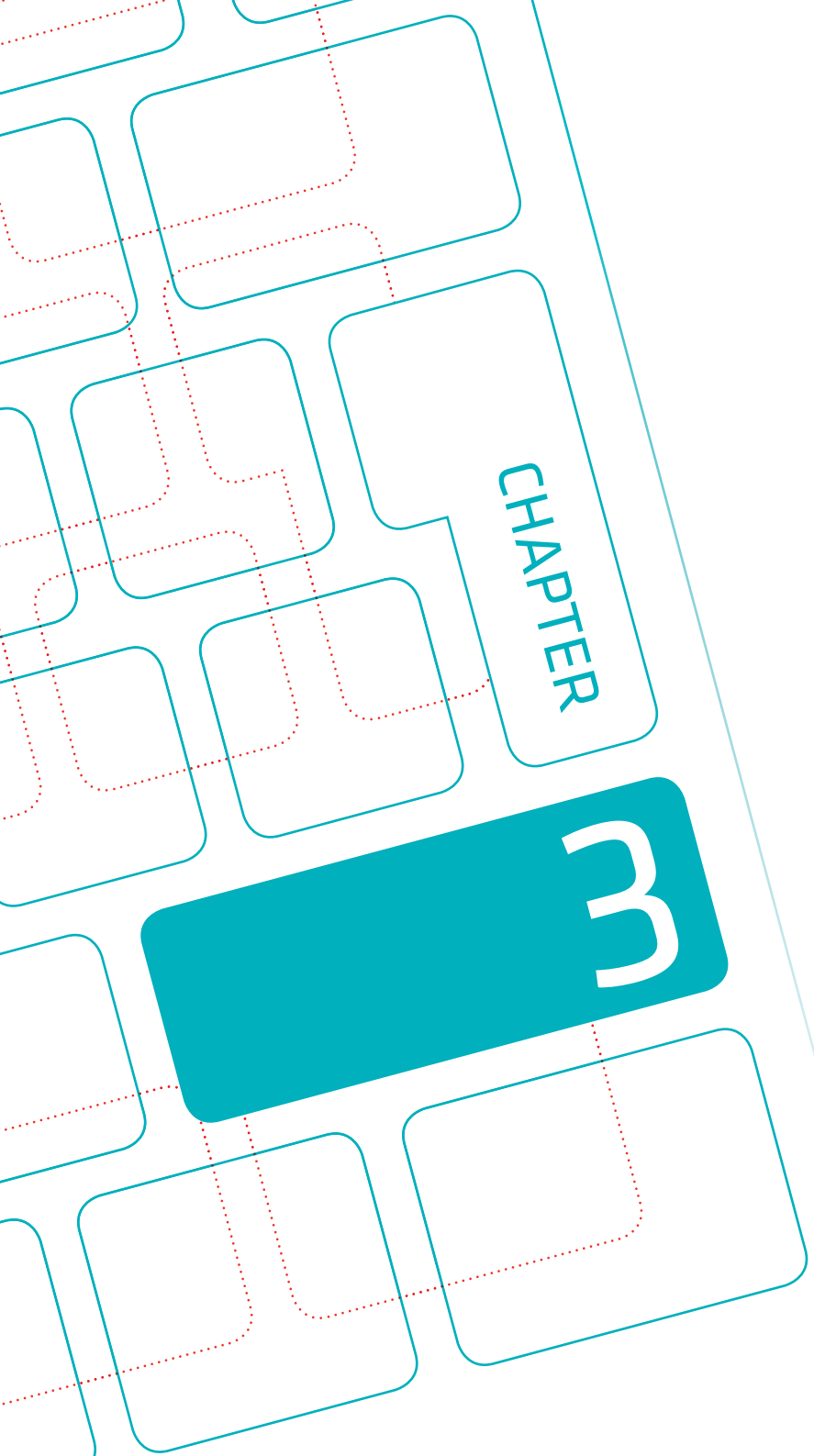
Spreading the Message

To promote its awareness raising findings faster and more effectively, ENISA published a volume, entitled *Promoting information security as a cultural and behavioural change*, which includes selected 2010 publications: *Online as soon as it happens, Email security, Malicious software, Online security at home, Preventing identity theft, Security when working remotely and Security while travelling.*

An awareness raising portal has also been launched, thereby giving AR Community members the possibility to receive up-to-date information on AR project activities, publications and events, and most importantly connect with other members of the community.

Finally, ENISA continues to strengthen its relationship with the Member States through collaborative efforts, regular dialogue and the exchange of good practices. The translation of awareness publications into different languages and the awareness pages of the ENISA website have both helped to create awareness around Europe and to disseminate ENISA's findings.





Public Affairs

PUBLIC AFFAIRS

The European Union has long recognised the importance and need to better and more effectively convey its work and achievements. As an EU agency, ENISA also recognises the strategic value of communications, supporting the EU Commission in its endeavours, and at the same time promoting the results of the Agency. Communicating ENISA studies and findings is critical to attaining the Agency's key operational objectives. It is crucial to make the Agency results known – and thus to actually change behaviour. It is the only way to fulfil the ambition of the Agency's founding regulation to develop "a culture of Network and Information Security". Communication, therefore, is indispensable for achieving impact and fulfilling the Agency's mission.

ACHIEVING IMPACT IN EUROPE

In mid-2010, the Agency set up a new team, the Public Affairs Unit, which brings together the Agency's management of public affairs, communication and outreach. Agency communication activities include press and media relations, maintaining and updating the ENISA website, organising high level events, producing corporate publications, supporting the Executive Director in public affairs, outreach to all Agency stakeholders, and supporting agency co-organised events and speaking engagements at conferences, workshops, and other venues.

COHERENCE AND CONSISTENCY - COMMUNICATION PLANNING

In order to achieve a higher impact for its reports, studies and operations, ENISA endeavours to achieve consistency and coherence across all its communication channels. Corporate communications are closely aligned with the operational activities of the Agency, from their inception, to optimise resources and improve the effectiveness of communications planning. This strategy is proving useful in achieving tangible results, maintaining the high quality of ENISA's relations with other stakeholders and enhancing the visibility of the Agency. For this purpose, a Media Communications Grid is maintained, and a new, updated Draft Communication Strategy was produced to accommodate changes in the organisation during the year. Advance planning enables ENISA to better integrate with its stakeholders' information and communication channels, and thus achieve even higher visibility for the Agency.

INCREASING THE AGENCY'S VISIBILITY

A major media exercise was yet again successfully organised in conjunction with the NIS Summer School, so as to enhance background knowledge and understanding of network and information security.

The NIS Summer School also provided an excellent opportunity for liaising and networking with key stakeholders. Another major media event was the Cyber Europe security exercise, and the subsequent media briefing in Berlin on the intermediate results. The two press releases and the Commission's public relations activities were the result of effective inter-service collaboration which generated a high impact, according to our media monitoring.

To overcome the most common and difficult communication barrier in Europe – languages – press releases

are translated. The impact and reach of ENISA's press releases were further enhanced by the addition of two more languages for translation and distribution to the media. During the year, through supporting services contracts, the Agency followed Commission best practice to make its content and activities more easily digestible by producing Frequently Asked Questions (FAQs) to accompany press releases. Moreover, more web content, such as focus articles and interviews, has been produced.

Brand marketing material was produced in 2010 and repetitive, brand recognition through print advertising was maintained during the year, as was an online advertising campaign designed to increase website traffic.

WEB SITE FOCUS

The ENISA website underwent a major overhaul in 2010 to make better use of and further develop the technical platform that was introduced in 2009. This will enable the Agency to more easily upgrade the web site in the future with new, innovative features such as interactive online services. Moreover, to accommodate these future web site enhancements, a Digital Communications Officer was appointed to ensure the ongoing development of the web site.

VISUALLY COMMUNICATING OUR RESULTS

As we are visual beings with approximately 75-90% of our perceptions coming through our eyes, visual communications can, when correctly used, be extremely useful for achieving higher impact. Using appropriate images, the Agency can support its messages and thereby more effectively achieve a higher level of outreach. To this end, the Agency has subscribed to an image library that contains approximately 7 million images. The image library is widely used within the Agency (for example, for the website, PowerPoint presentations, Intranet, studies, reports, print and brand material which require high quality, etc.). Moreover, the Agency also realised its ambition to increase the audiovisual display of its reports, produce a number of corporate video clips, and use modern communication tools and social media. We have also enhanced the audiovisual content of the website and presented results in a different, more accessible way in order to reach out to new target audiences.

PUBLICATIONS

The regulation bound ENISA General Report, a new corporate brochure, and the ENISA Quarterly Review (EQR) are key publications produced during the year. The General Report is published both as a hard copy and on CD-ROM to reach out to as many readers as possible. The EQR is focused on reaching out to specialised target audiences of the Agency. It has been integrated into the website as part of the ambition to reduce the amount of print material produced.

INTERNAL COMMUNICATION

Regular staff meetings, meetings at Department/ Unit levels, and the Agency's intranet, have ensured a sound and interactive flow of communication internally. Moreover, a team building exercise occurred at the end of 2010. In 2010, the wider use of the intranet has offered common ground for all staff to deal with a variety of information sources.

CONFERENCES AND JOINT EVENTS

ENISA was involved in a selection of high-level European conferences in 2010. One of the key events during the year was the well-attended high-level panel discussion on the future of European cyber security that was held at the end of September in Brussels. This was the first time the Agency organised such a meeting. The high-level panel included the Chair of the EP-ITRE Committee, MEP Reul, the Council's EU Counter-Terrorism Co-ordinator Mr. Kerchove, and Mr. Vassallo of 'DigitalEurope', as well as Vice President and Commissioner Nellie Kroes, who outlined the Commission's Regulation proposal for the Agency, which was presented in full the following day.

Often, these conferences are run in partnership with a third party such as a professional conference organiser, or a not-for-profit organisation. Such events allow the Agency to network and promote its work in a cost-effective way. During 2010, ENISA participated in or co-ordinated numerous conferences and other events throughout Europe and further afield.

NIS SUMMER SCHOOL

The 3rd Network and Information Security (NIS) Summer School – NIS'10 – was held over five days in September and proved another resounding success for its joint organisers, ENISA and the Institute of Computer Science (ICS) of the Foundation for Research and Technology – Hellas (FORTH). The Summer School is a forum for experts in information security, policy-makers from European Union Member States and EU Institutions, decision-makers from industry and members of the research and academic community. The event provides an opportunity to discuss cutting-edge and ground-breaking NIS topics.

More than 80 participants came together this year to discuss "Privacy and Security in the Future Internet". The Future Internet promises an exciting world: new

services, new infrastructures and new capabilities at all levels such as devices that will automatically exchange information to facilitate users, services that take into account information from different and multiple sources, and protocols and systems that are able to handle complex interactions. The Future Internet also creates many concerns, however, both technical and in relation to privacy issues, for individuals, organisations and society in general.

NIS'10 brought together an impressive list of speakers including Mario Campolargo, Director of the Emerging Technologies and Infrastructures, DG INFSO (Directorate General Information Society and Media); Bruce Schneier, Chief Security Technology Officer of BT, UK; Mikko Hyppönen, Chief Research Officer, F-Secure, Finland; and Peter Hustinx, Supervisor with the European Data Protection Supervisor. A keynote address was given by Dr. Silvia Adriana Ticau, Member of the European Parliament. There were also numerous distinguished lecturers, and for the first time, two panel sessions were held to increase involvement from the participants.

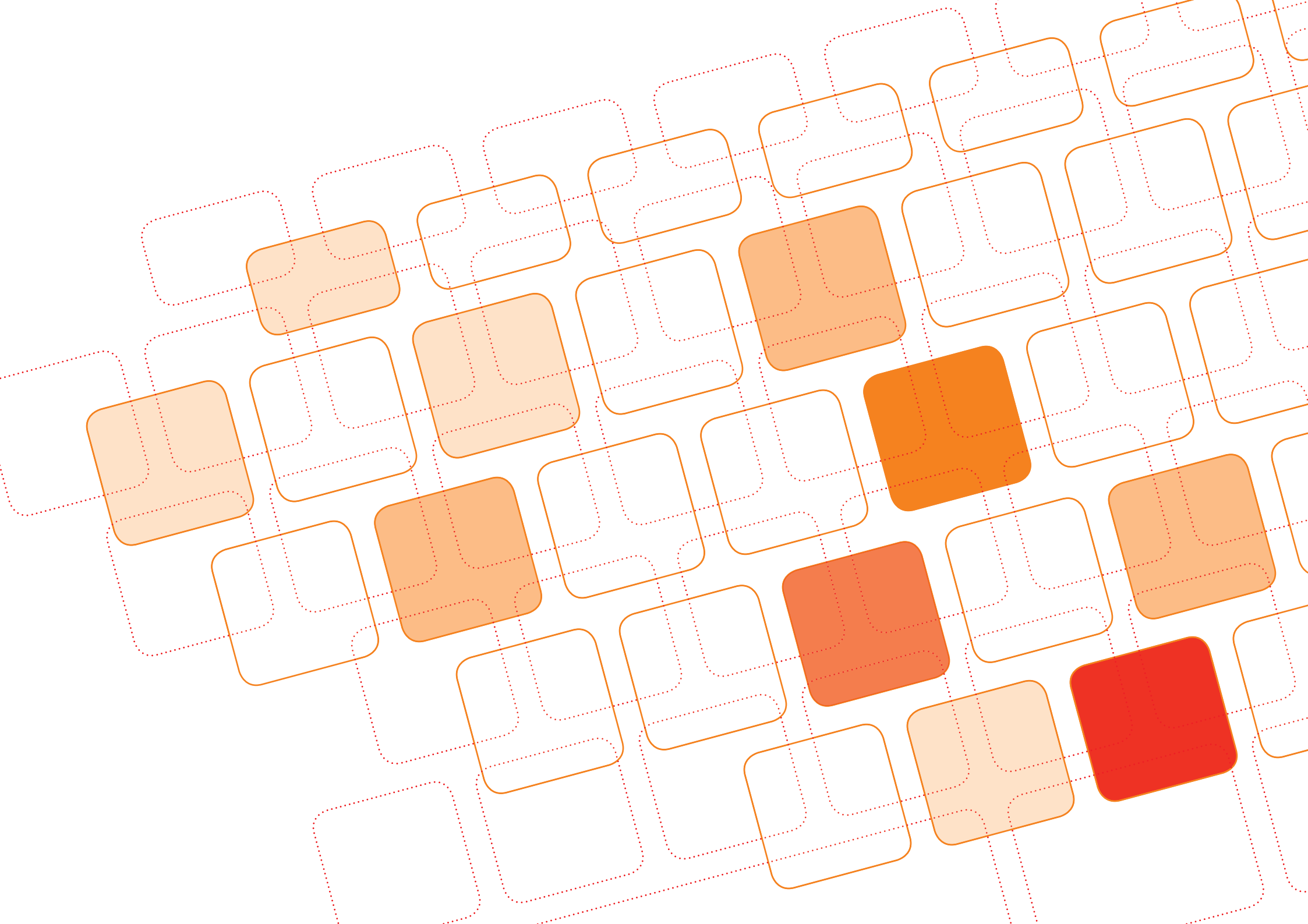
There was a clear increase in interest in 2010 from governments, European organisations and industry, which augurs well for next year's Summer School. Plans are already underway for NIS'11; it will take place in Crete between 27 June and 1 July.

For further details, contact Louis Marinos at ENISA (**louis.marinos@enisa.europa.eu**).

The full proceedings and talks of the NIS'10 Summer School are available at: **www.nissummer-school.eu/**.

SPEAKING ENGAGEMENTS

ENISA accepted more than 76 speaking engagements, and staff attended conferences and other events to fulfil ENISA's role in gathering and disseminating the latest results and discussing current trends in Network and Information Security. One example was the 1st Interpol conference which took place in Hong Kong. The event, like many others, was very useful for building new relationships. Such relationships are vital for an Agency like ENISA.



CHAPTER 4

Relations with ENISA stakeholders

EXTERNAL STAKEHOLDERS, ENISA BODIES AND GROUPS

ENISA's stakeholder relations are a key factor in the success of its overall mission of contributing to the security of the EU internal market. The Management Board (composed of the Commission, Member State and private sector representatives) and Permanent Stakeholder Group (composed of multi-stakeholders), as well as our informal networks and expert working parties, give us unparalleled insights and access to public and private sector Network and Information Security (NIS) experts. This in turn enables us to identify emerging risks, to forge new insights in order to help Member States and private sector organisations better prepare themselves for challenges in a proactive and professional manner, and to build novel public and private sector partnerships.

Management Board

The Management Board's task is to define the general strategic orientation for the operation of ENISA, to ensure consistency between the Agency's work and activities conducted by Member States as well as at Community level, as laid down in the ENISA founding Regulation. The Management Board also approves ENISA's Work Programme, ensuring that it is in line with the Agency's scope, objectives and tasks, as well as with the Community's legislative and policy priorities for Network and Information Security. It also adopts the Agency's budget.

The full Management Board met twice in 2010: in March and October in Athens, Greece.

The preparation and subsequent adoption of the Work Programme for 2011, the (amended) 2010 budget and the adoption of the IAS Strategic Audit Plan 2010-2012 were important activities during the year.

Furthermore, an informal joint meeting between the Management Board and the Permanent Stakeholders' Group took place in May 2010 in Athens, Greece. The meeting focused on prioritisation and themes of the Work Programme 2011. In addition, an informal Management Board meeting on Strategic Guidance for Work Programme 2012 was held in Brussels in December 2010.

Minutes and decisions of the Management Board are available on the ENISA website.

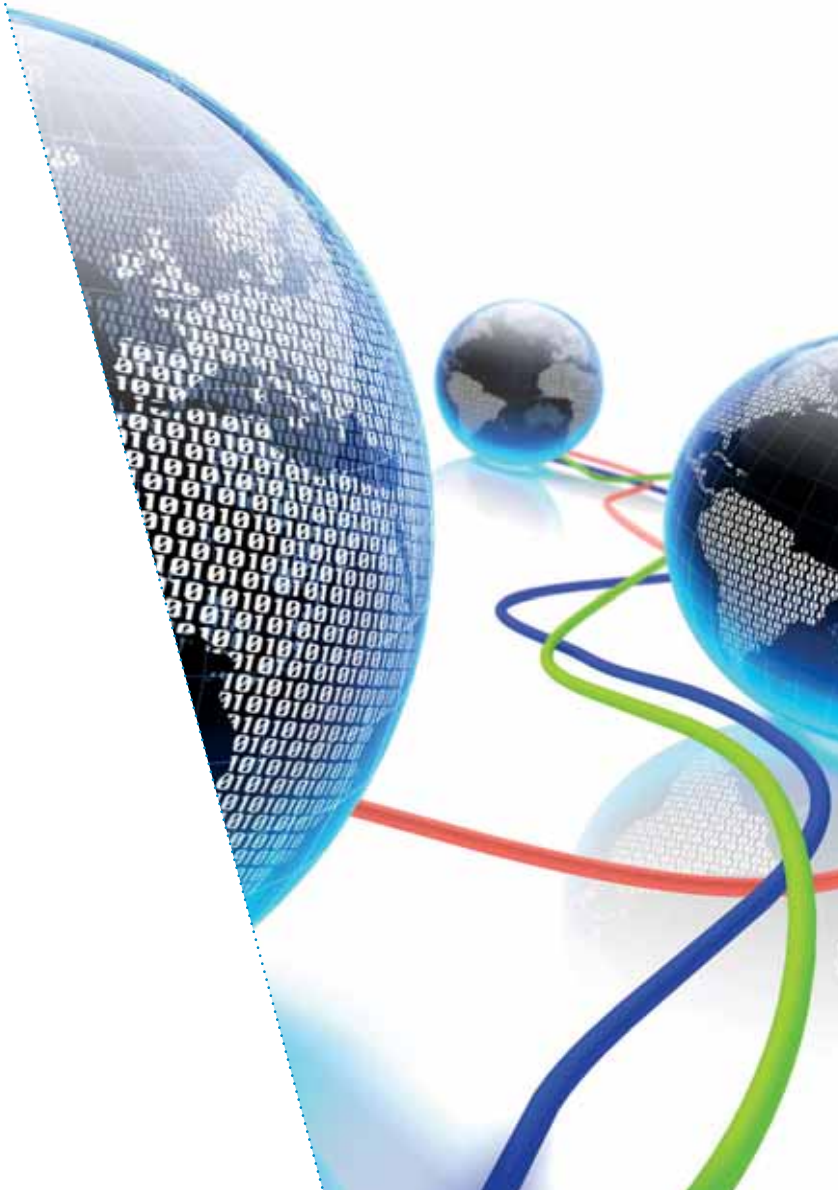
For a list of members of the Management Board, see **APPENDIX 1**: Members of the Management Board.

The list of Management Board members is also available on the ENISA website at: **http://www.enisa.europa.eu/about-enisa/structure-organization/management-board**

Permanent Stakeholders' Group (PSG)

The ENISA Permanent Stakeholders' Group (PSG) facilitates the Agency's regular dialogue with the private sector, academia, consumer organisations and other relevant stakeholders. The PSG is composed of 30 experts in Network and Information Security who provide valuable advice to the Executive Director and input for the development of the Work Programmes. The term of office for members of the PSG is two and a half years. Following an open Call for Members in 2009, a new composition of the PSG was established in 2010. This was also the first PSG to be appointed by Prof. Dr. Udo Helmbrecht in his capacity as Executive Director of ENISA. The 30 appointed members formally started their term of office on 17 February.

The PSG met formally twice in 2010, in March and November. An informal joint meeting with the Management Board was also held in Athens in June. The purpose of that meeting was to continue discussing ENISA's Work Programme 2011.



RESPONDING TO REQUESTS FOR ASSISTANCE FROM MEMBER STATES

In 2010, the Agency received two requests. One was a request from Romania to help set up a CERT by organising appropriate training. The second request was sent by the European Parliament and related to the establishment of an agency for the operational management of large-scale IT systems.

By providing prompt, independent and high quality responses to requests received from EU Institutions and Member States, ENISA is fulfilling its statutory task of advising and assisting the Member States and EU Institutions, giving the Agency a bridging role between the EU and national institutions. This role is specific to ENISA and currently it is unique in the world. Similar requests are expected to emerge in 2011.

A major change was introduced by the Executive Director with regards to the process of developing a new Work Programme and the role of the PSG. In order to kick-off the development process of the 2012 Work Programme earlier and let the PSG provide first input, the second formal PSG meeting in 2010 was organised in November. That meeting was later followed by an informal Management Board meeting in December in Brussels where the PSG had appointed the member Nick Coleman as rapporteur to present the input for the Management Board.

For a list of the members of the PSG, see APPENDIX 2: Members of the Permanent Stakeholders' Group

THE NETWORK OF NATIONAL LIAISON OFFICERS

Although not formally based on ENISA's Regulation, the network of National Liaison Officers (NLOs) is very helpful to the Agency: on the one hand, the NLOs serve as ENISA's primary contact point within the Member States; on the other, they are well placed to reinforce the work of the Agency in the Member States, and to exchange information amongst themselves.

In addition, thanks to valuable input from the Member States through the NLOs' network, ENISA was able to conduct various surveys and studies in the field.

RELATIONS WITH INDUSTRY
AND INTERNATIONAL INSTITUTIONS

Industry relations

In addition to the regular dialogue held with the members of its Permanent Stakeholders' Group, ENISA has established relationships with relevant national industry associations in all EU Member States as well as with a number of pan-European umbrella organisations representing ICT and software industries, telecommunications network operators and Internet Service Providers. These organisations are important partners for ENISA in its drive to foster a culture of NIS in Europe.

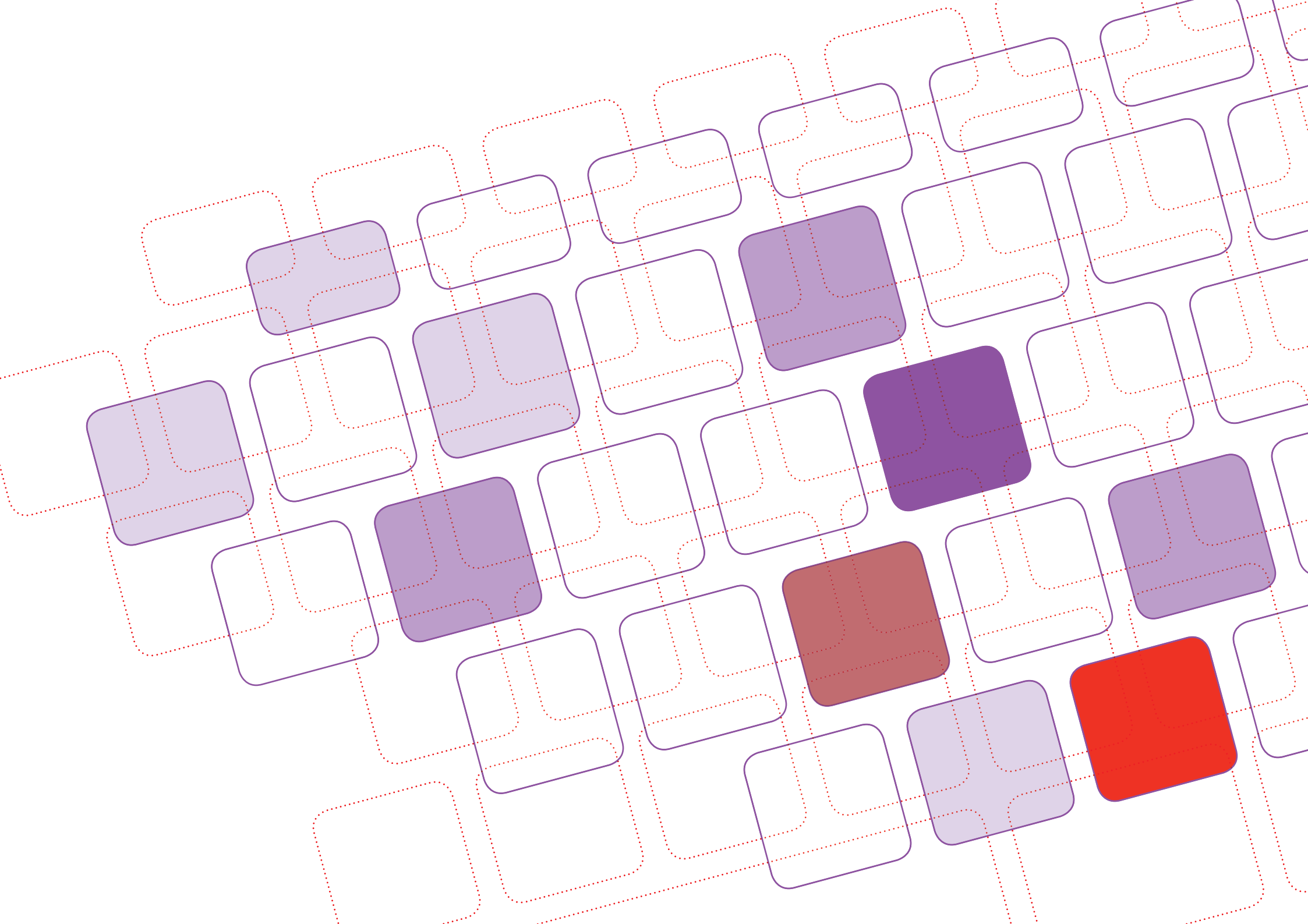
Numerous formal and informal meetings between industry representatives and ENISA experts took place throughout 2010. Establishing and maintaining relations with relevant NIS professionals and European organisations is imperative for the successful implementation of the ENISA Work Programme and is therefore an integral part of the activities of all ENISA Experts

International relations

NIS is a global challenge and does not recognise borders. In endeavouring to foster good European practice, the Agency has regularly participated in the different working bodies of international organisations such as the Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP). ENISA experts have also taken part in meetings and in the work of the Council of the Europe Convention on Cybercrime as well as the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) and Telecommunication Development Sector (ITU-D) groups.

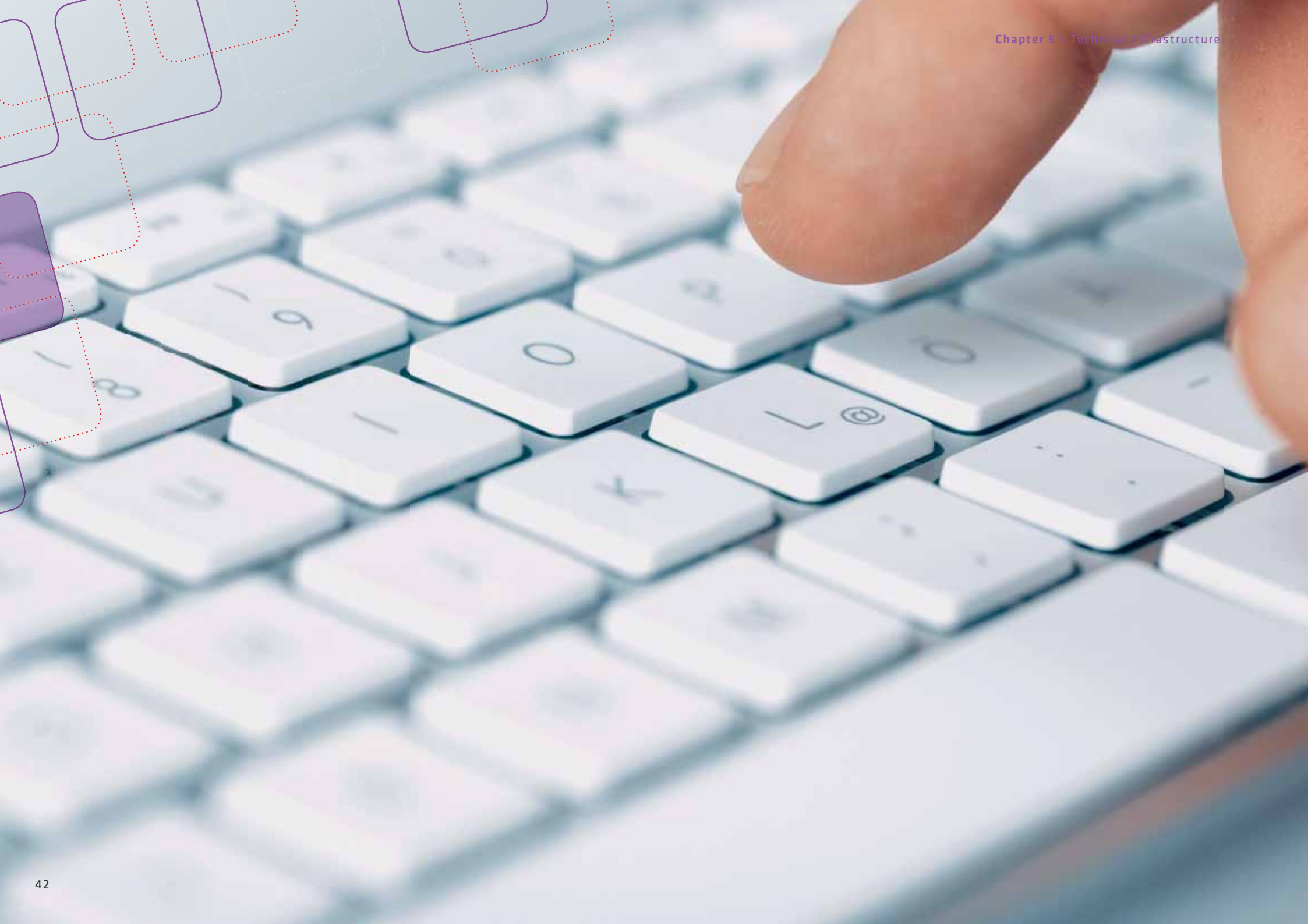
Speaking engagements of the Executive Director

The Executive Director had 102 speaking engagements in 2010.



CHAPTER 5

Technical Infrastructure



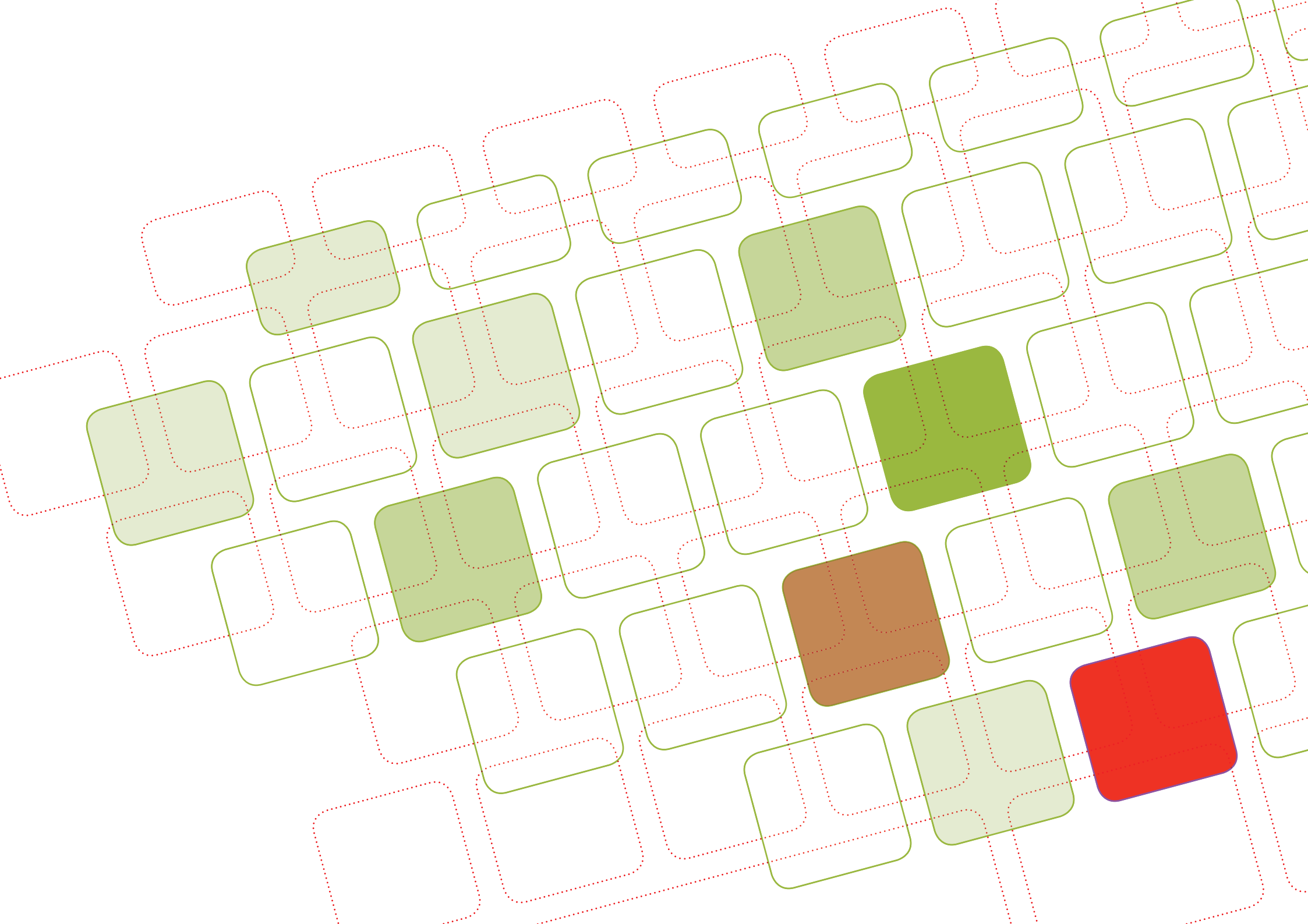
Work continued on expanding the use of the Intranet with the roll-out of several e-workflows and document management sites. In future, the use of the Intranet will be favoured over the use of the traditional file server for data storage due to the many advantages that it offers. Whereas previously the IT Help Desk was based on a mailbox, it was shifted to the Intranet, thus making it possible to use reporting and statistics functionality, and making the management of the Help Desk much easier.

Several large procurement projects were concluded during the year. New client computers were ordered to replace the currently fully depreciated ones, for delivery and roll out in early 2011. The contract for the outsourcing of the hosting and development of the ENISA website and Extranets was concluded for implementation in early 2011. Also concluded was the new contract for mobile telephony services.

As part of its strategy to outsource IT services where possible, several studies were carried out on Cloud services. These studies concluded that the benefits from outsourcing to the Cloud were indeed substantial and that ENISA should consider shifting services to the Cloud. As a first step, web security services will be implemented on the Cloud in early 2011, shortly followed by email and related services.

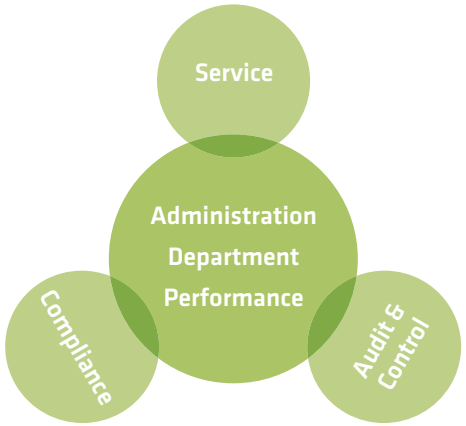
A business continuity project was undertaken, culminating in a "paper-based" exercise. The exercise simulated a natural disaster resulting in the unavailability of the ENISA building and internal IT services. This first exercise in business continuity proved invaluable and has highlighted many areas for improvement. It will be followed up with additional exercises in the near future.

Various important maintenance projects were also undertaken during the year, including the upgrade of the firewall, the upgrade of the backup and recovery infrastructure, and the upgrade of the VMWare virtualisation infrastructure to VCentre 4. Work also started on the preparation for the move to the new ENISA building in 2011.



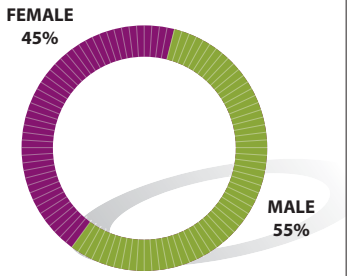
Administration

The Administration Department seeks to ensure compliance and further enhance the functionality of the administrative procedures of the Agency that are mandated by the regulatory framework, in order to deliver dependable services. The main components concerning the tasks of the administration are presented in the diagram below:

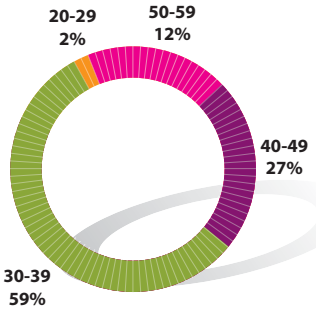


As a knowledge-based organisation, ENISA relies on its personnel to deliver its services to its stakeholders and ensure compliance in line with the regulatory framework. Some statistics regarding personnel at ENISA are as follows (Updated 31 December 2010):

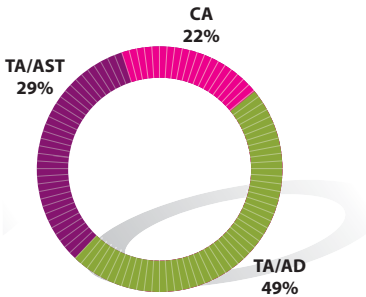
STAFF MEMBERS BY GENDER



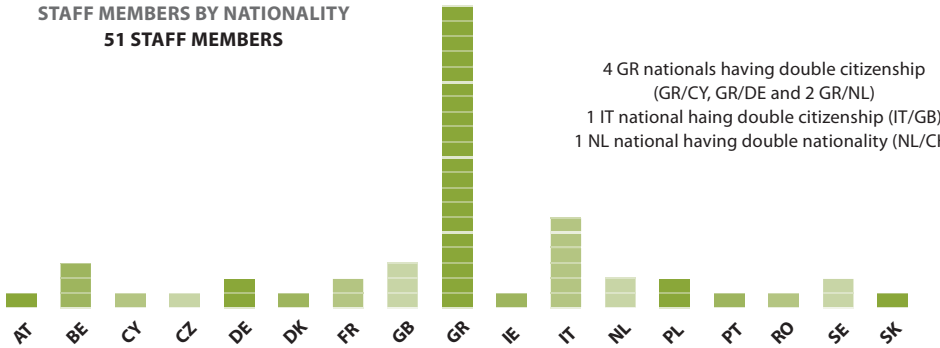
STAFF MEMBERS BY AGE



STAFF MEMBERS BY FUNCTION GROUP



STAFF MEMBERS BY NATIONALITY
51 STAFF MEMBERS



4 GR nationals having double citizenship
(GR/CY, GR/DE and 2 GR/NL)
1 IT national haing double citizenship (IT/GB)
1 NL national having double nationality (NL/CH)

In 2010 the Agency committed its appropriations at a rate of 99.95% (in 2009, the commitment level was 94.40%) in order to carry out the operational activities specified in the Work Programme 2010, as well as administrative tasks that are necessary to ensure compliance and services made available by the Agency. Payments reached the level of 75.46% (75.67% paid in 2009) of the total appropriations managed. An overview of the year's performance follows below:

Budget Title	Description	Budget €	Committed €	%	Paid €	%
Title 1	Staff expenditure	5,107,202.98	5,104,865.96	99.95%	4,565,452.69	89.39%
Title 2	Administrative expenditure	650,997.02	649,182.79	99.72%	422,169.38	64.85%
Title 3	Operating expenditure	2,354,987.93	2,354,987.93	100.00%	1,134,403.16	48.17%
Total		**8,113,187.93**	**8,109,036.68**	**99.95%**	**6,122,025.23**	**75.46%**

The outturn of contracts awarded as a result of procurement procedures launched in 2010, is as follows:

- **Contracts:** 52, including 20 service contracts and 9 framework service contracts
- **Purchase orders:** 233, 79 of which were issued under an existing framework service contract
- **Procurement procedures launched:** 36, including 13 open procedures

Finally, in 2010, the Agency carried out a risk assessment concerning prevailing risk areas, and concluded its preparations with regard to business continuity concerning its core activities.

FINANCIAL REPORTING

Balance Sheet

	Notes	31/12/2010	31/12/2009
I. Non Current Assets		**300.781**	**396.580**
Intangible fixed assets	1	19.232	34.138
Tangible fixed assets	1	281.550	362.442
II. Current Assets		**3.184.067**	**3.437.593**
Short-term receivables	2	66.686	169.384
Cash and cash equivalents	3	3.117.381	3.268.209
Total Assets		**3.484.849**	**3.834.173**
III. Non Current Liabilities		**0**	**13.441**
Long-term provision for risk and charges	4	0	13.441
IV. Current Liabilities		**2.076.973**	**2.620.499**
EC Pre-financing Received	5	774.858	1.324.500
EC Interest Payable	5	83.506	46.948
Accounts payable	5	498.817	879.117
Accrued Liabilities	6	669.792	319.934
Short-term provision for risk and charges	7	50.000	50.000
Total Liabilities		**2.076.973**	**2.633.940**
V. Net Assets		**31.12.2010**	**31.12.2009**
Accumulated result		1.200.233	1.082.999
Result for the year		207.643	117.234
Total Net Assets		**1.407.876**	**1.200.233**
VI. Contingent assets and liabilities			
Contingent liabilities		1.253.158	905.364
Total Contingent assets and liabilities	8	**1.253.158**	**905.364**

Economic Outturn Account

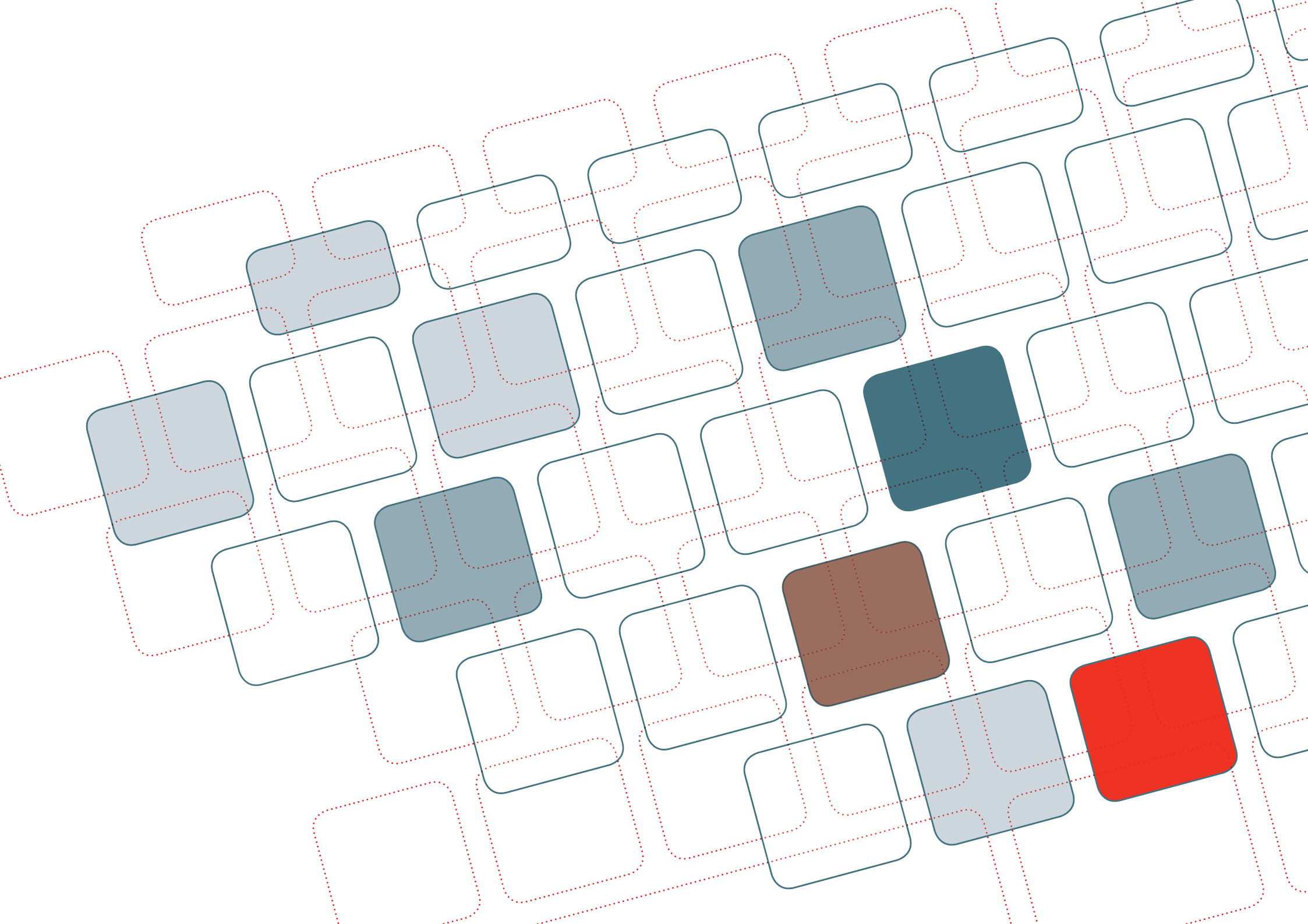
	Notes	2010	2009
Revenue from the Community Subsidy	9	8.021.504	7.434.025
Other revenue	10	0	54.008
Total Operating Revenue		**8.021.504**	**7.488.033**
Administrative expenses		-5.553.227	-5.217.390
Staff expenses		-4.448.485	-4.259.042
Fixed asset related expenses		-155.919	-196.176
Other administrative expenses		-948.823	-762.172
Operational expenses		-2.257.823	-2.150.129
Total Operating Expenses	11	**-7.811.050**	**-7.367.519**
Surplus/(Deficit) from Operating Activities		210.454	120.514
Financial expenses		-1.158	-2.137
Exchange rate loss		-1.653	-1.143
Surplus/(Deficit) from Ordinary Activities		**207.643**	**117.234**
Economic Result for the Year		**207.643**	**117.234**

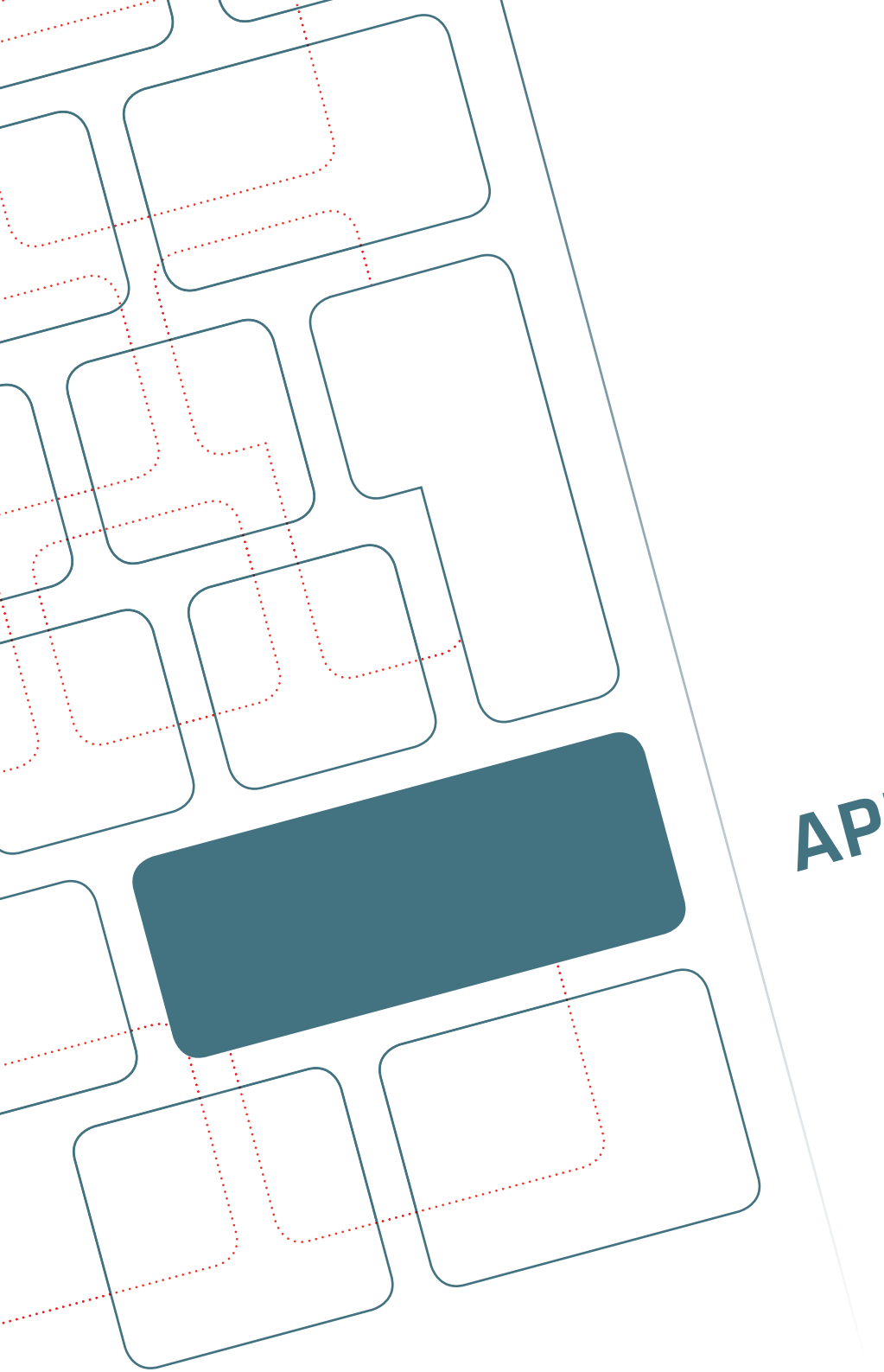
Cash Flow Statement

	2010	2009
Surplus/(deficit) from ordinary activities	207.643	117.234
Operating activities		
Amortization (intangible fixed assets)	15.419	20.940
Depreciation (tangible fixed assets)	140.500	**175.236**
Increase/(decrease) in Provisions for liabilities	-13.441	13.441
(Increase)/decrease in Short term Receivables	102.698	-13.071
Increase/(decrease) in value reduction for doubtful debts	0	45.200
Increase/(decrease) in Accounts Payable	-543.526	692.166
Gains on sales of Property, Plant and Equipment	0	-5.975
Net cash Flow from operating activities	**-90.707**	**1.045.172**
Cash Flows from investing activities		
Purchase of tangible and intangible fixed assets	-60.120	-224.257
Proceeds from tangible and intangible assets	0	10.600
Net cash flow from investing activities	**-60.120**	**-213.657**
Net Increase/(decrease) in cash and cash equivalents	-150.827	831.515
Cash at the beginning of the period	3.268.209	2.436.694
Cash at the end of the period	**3.117.381**	**3.268.209**

Statement of Changes in Capital

	Reserves	Accumulated Surplus / Deficit	Economic result of the year	Capital
Balance as of 1 January 2010	0	1.082.999	117.234	1.200.233
Allocation of the Economic Result of Previous year		117.234	-117.234	0
Economic result of the year			207.643	207.643
Balance as of 31 December 2010	**0**	**1.200.233**	**207.643**	**1.407.876**





APPENDIX

APPENDIX 1:
MEMBERS OF THE MANAGEMENT BOARD

At 26 January 2011

A key pillar of ENISA, the Management Board includes one representative of each EU Member State and three representatives appointed by the European Commission. There are also three members, proposed by the Commission and appointed by the Council, without the right to vote, who represent respectively:

- The information and communication technology industry
- Consumer groups
- Academic experts in Network and Information Security.

Finally, there are also three observers from the European Economic Area (EEA) Member States – Liechtenstein, Norway and Iceland. The Management Board is chaired by Prof. Dr. Reinhard Posch (Austria).

Representative	Alternate
Robert MADELIN *Director-General* *DG Information Society and Media* tel: +32 229 63338 robert.madelin@ec.europa.eu	**Andrea SERVIDA** *Deputy Head of the Unit in charge of network and information security policy* *DG Information Society and Media* tel: +32 2 29 58186 andrea.servida@ec.europa.eu
	Jakub BORATYNSKI *Head of the Unit in charge of the fight against organised crime* *DG Home Affairs* tel: +32 229 69452 jakub.boratynski@ec.europa.eu
Francisco GARCIA MORÁN *Director-General* *DG Informatics* tel: +352 430134561 francisco.garcia-moran@ec.europa.eu	**Marcel JORTAY** *Director in charge of infrastructure services provision* *DG Informatics* tel: +352 430134235 marcel.jortay@ec.europa.eu

MEMBER STATE REPRESENTATIVES

Member State	Representative	Alternate
Austria	**Reinhard POSCH** *CHAIR OF ENISA MANAGEMENT BOARD* *Chief Information Officer* tel: +43-1-53115/6152 reinhard.posch@cio.gv.at	**Herbert LEITOLD** *Institute for Applied Information Processing and Communication* tel: +43-316-873-5521 herbert.leitold@iaik.at
Belgium	**Luc HINDRYCKX** *Chairman of the Council of IBPT (Belgian Institute for Postal Services and Telecommunications)* tel: +32 2 266 8962 fax: +32 2 223 2478 luc.hindryckx@ibpt.be	**Charles CUVELLIEZ** *Member of the Council of IBPT (Belgian Institute for Postal Services and Telecommunications)* tel: +32 2 266 8825 fax: +32 2 223 2478 charles.cuvelliez@ibpt.be
Bulgaria	**Valeri BORISSOV** *Director of eGovernance Directorate in the Ministry of Transport, Information Technologies and Communications* tel: +359 2 9492992 vborissov@mtitc.government.bg	**Vasil GRANCHAROV** *Director of Communication and Information Systems Directorate in the Executive Agency 'Electronic Communications Networks and Information Systems'* tel: +359 2 9492666 vgrancharov@esmis.government.bg
Cyprus	**Antonis ANTONIADES** *Senior Officer of Electronic Communications and Postal Regulation* tel: +357 22 693 115 fax: +357 22 693 070 antonis.antoniades@ocecpr.org.cy	**Markellos POTAMITIS** *Officer of Electronic Communications and Postal Regulation* tel: +357 22 693 132 fax: +357 22 693 070 Markellos.Potamitis@ocecpr.org.cy
Czech Republic	**Pavel TYKAL** *Head of Unit* *Department of eGovernance Project and Service Development* *Ministry of Interior of the Czech Republic* tel: +420 974 817 559 pavel.tykal@mvcr.cz	**Marie SVOBODOVÁ** *Senior Counsellor* *Communication Infrastructure Department* *Ministry of Interior of the Czech Republic* tel: +420 974 817 544 marie.svobodova@mvcr.cz
Denmark	**Flemming FABER** *Senior Advisor* *IT-Security Division* *National IT and Telecom Agency* tel: +45 3545 0364 ff@itst.dk	**Thomas KRISTMAR** *Senior Advisor* *National IT and Telecom Agency* tel: +45 3337 9104 tkr@itst.dk

Member State	Representative	Alternate
Estonia	**Mait HEIDELBERG** *IT-Counsellor of the Ministry of Economic Affairs and Communications* tel: +372 6 397 613 mait.heidelberg@mkm.ee	**Jaak TEPANDI** *Head of the Chair of Knowledge-Based Systems, Department of Informatics, Tallinn University of Technology* tel: +372 6 202 308 jt@tepinfo.ee
Finland	**Mari HERRANEN** *Ministerial Adviser* *Ministry of Transport and Communications* tel: +358.9.160 28305 fax: +358.40.720 1693 mari.herranen@lvm.fi	**Mikael KIVINIEMI** *Ministry of Finance* mikael.kiviniemi@vm.fi
France	**Patrick PAILLOUX** *Director General of ANSSI* *(French Network and Information Security Agency)* tel: +33 1 71 758401 patrick.pailloux@ssi.gouv.fr	**Sylvain LEROY** *ANSSI (French Network and Information Security Agency)* tel: +33 1 71 758264 fax: +33 1 71 758260 sylvain.leroy@ssi.gouv.fr
Germany	**Michael HANGE** *President of the Federal Office for Information Security (BSI)* tel: +49 228 99 9582-5200 fax: +49 228 99 9582-5420 michael.hange@bsi.bund.de	**Roland HARTMANN** *Head of International Relations* *Federal Office for Information Security (BSI)* tel: +49 228 99 9582 5328 fax: +49 228 99 109582 5328 SIB@bsi.bund.de
Greece	**Constantine STEPHANIDIS** *Director* *Institute of Computer Science* *Foundation of Research and Technology (FORTH)* tel: +30 2810 391741 fax: +30 2810 391740 cs@ics.forth.gr	**Theodoros KAROUBALIS** *Hellenic Ministry of Transport and Communications* tel: +30 210 6508568 fax: +30 210 6508560 t.karoubalis@yme.gov.gr
Hungary	**Ferenc SUBA** *VICE-CHAIR OF ENISA MANAGEMENT BOARD* *General Manager of CERT-Hungary* tel: +36 1 301 2030 fax: +36 1 353 1937 Ferenc.Suba@cert-hungary.hu	

Member State	Representative	Alternate
Ireland	**Aidan RYAN** *Telecommunications Adviser* *Department of Communications* tel: +353 1 678 3183 fax: +353 1 678 2126 Aidan.Ryan@dcmnr.gov.ie	**Paul CONWAY** *Head of Compliance and Operations* *Commission for Communications Regulation* tel: +353 18 04 97 61 fax: +353 18 04 96 80 paul.conway@comreg.ie
Italy	**Rita FORSI** *Director General* *Ministry of Economic Development* tel: +39 06 54442360 fax: +39 06 54442020 rita.forsi@sviluppoeconomico.gov.it	**Alessandro RIZZI** *Audiovisual and Telecommunications* *Permanent Representation of Italy to the European Union* tel: +32 2 22 00 574 tlc@rpue.esteri.it
Latvia	**Edmunds BEĻSKIS** *Director of Communications Department* *Ministry of Transport and Communications of the Republic of Latvia* tel: +371 67028100 fax: +371 67820636 edmunds.belskis@sam.gov.lv	**Maris ANDZANS** *Head of Transport and Communications Security Division* *Ministry of Transport and Communications of the Republic of Latvia* tel: +371 67028262 fax: +371 67217180 maris.andzans@sam.gov.lv
Lithuania	**Valdas KIŠONAS** *Director of Information Society Development Committee under the Ministry of Transport and Communications of the Republic of Lithuania* tel: +370 5 2665160 valdas.kisonas@ivpk.lt	**Tomas BARAKAUSKAS** *Director of the National Regulatory Authority of the Republic of Lithuania* tel: + 370 5 210 216 1564 tbarakauskas@rrt.lt
Luxembourg	**François THILL** *Accréditation, notification et surveillance des PSC* tel: +352 478 4165 francois.thill@eco.etat.lu	**Pascal STEICHEN** *Ministère de l'Economie et du Commerce extérieur Direction des Communications CASES* tel: +352 478 4179 fax: +352 478 4311 pascal.steichen@eco.etat.lu
Malta	**Francis BORG** *Deputy Cabinet Secretary* *Office of the Prime Minister* tel: +356 22001260 fax: +356 2200 1262 francis.a.borg@gov.mt	**Rodney NAUDI** *Malta Information Technology Agency (MITA)* tel: +356 2599 2621 / +356 7947 4747 fax: +356 2123 4701 rodney.naudi@gov.mt

Member State	Representative	Alternate
The Netherlands	**Mr. Edgar DE LANGE** *Ministry of Economic Affairs, Agriculture and Innovation* *Directorate-General for Energy, Telecommunications and Markets* P.O. Box 20101, 2500 EC The Hague, The Netherlands tel: + 31 70 379 8153 fax + 31 70 379 8266 e.r.delange@minez.nl	**Peter HONDEBRINK** *Ministry of Economic Affairs, Agriculture and Innovation* *Dir.-Gen. for Energy, Telecommunications and Markets* tel: +31 70 379 6474 j.p.hondebrink@minez.nl
Poland	**Krzysztof SILICKI** *Technical Director* *Research and Academic Computer Network (NASK)* tel: +48 22 5231315 fax: +48 22 5231201 krzysztof.silicki@nask.pl	**Piotr DURBAJŁO** *Deputy Director of the IT Security Department* *The Internal Security Agency* tel: +48 22 5858857 fax: +48 22 5858232 pdurbajlo@abw.gov.pl
Portugal	**Pedro Manuel BARBOSA VEIGA** *Presidente da Fundação para a Computação Cientifica Nacional (FCCN)* tel: +351 21 844 01 00 +351 21 847 21 67 pedro.veiga@fccn.pt	**Manuel Filipe PEDROSA DE BARROS** *Director de Tecnologias e Equipamentos da Autoridade Nacional das Comunicações (ANACOM)* tel: +351 21 434 86 00 +351 21 434 85 02 manuel.barros@anacom.pt
Romania	**Mireille RADOI** *Chief of staff* *Ministry of Communications and Information Society* tel: +40 21 312 00 21 fax: +40 21 311 41 31 mireille.radoi@cert-ro.eu	**Andreea STOICIU** *Councillor* *Ministry of Communications and Information Society* andreea.stoiciu@cert-ro.eu
Slovakia	**Peter BIRO** *Information Society Division* *Ministry of Finance of the Slovak Republic* tel.: + 421 2 5958 3222 fax: +421 2 5958 3048 peter.biro@mfsr.sk	**Ján HOCHMANN** *Information Society Division* *Ministry of Finance of the Slovak Republic* tel.: + 421 2 5958 3223 fax: +421 2 5958 3048 jan.hochmann@mfsr.sk
Slovenia	**Gorazd BOZIC** *Head* *ARNES SI-CERT* tel: +386 1 479 8922 gorazd.bozic@arnes.si	**Denis TRCEK** *Laboratory of e-media, Head* *Faculty of Computer and Information Science University of Ljubljana* tel: +386 1 4768 918 fax: +386 1 4264 647 denis.trcek@fri.uni-lj.si

Member State	Representative	Alternate
Spain	**Salvador SORIANO MALDONADO** *Deputy Director – Information Society Services* *Secretariat of State for Telecommunications and Information Society* tel: +34 91 346 15 97 fax: +34 91 346 15 77 slsoriano@mityc.es	**Juan LLORENS** *Adviser* *General Direction for the Development of the Information Society* *Ministry Of Industry, Tourism and Trade* tel: +34 91 346 22 86 fax: + 34 91 349 15 77 jdllorens@mityc.es
Sweden	**Jörgen SAMUELSSON** *Deputy Director Division for Information Technology Policy Ministry of Enterprise, Energy and Communications* tel: +46 405 82 18 fax: +46 8 543 560 80 jorgen.samuelsson@enterprise.ministry.se	**Anders JOHANSON** *Director* *National Post and Telecom Agency* anders.johanson@pts.se
United Kingdom	**Geoff SMITH** *Head of Information Security Policy, Information Security Policy Team* tel: +44 20 7215 2940 Geoff.Smith@bis.gsi.gov.uk	**Andrew POWELL** *Centre for the Protection of National Infrastructure* andrewp@cpni.gsi.gov.uk

STAKEHOLDER REPRESENTATIVES

Group	Representative	Alternate
Information and communication technologies industry	**Mark MACGANN** mmacgann@webershandwick.com	**Berit SVENDSEN** *Executive Vice President Technology / CTO of Telenor ASA and chairman of Telenor R&D* tel: +47 678 90 000 berit.svendsen@telenor.com
Consumer groups	**Markus BAUTSCH** *Stiftung Warentest, Deputy Head of Department* tel: +49 30 2631 22 50 m.bautsch@stiftung-warentest.de	
Academic experts in network and information security	**Kai RANNENBERG** *T-Mobile Chair of Mobile Business & Multilateral Security Dept. of Business Information and Communication Systems, Goethe University, Frankfurt, Council of European Professional Informatics Societies (CEPIS)* tel: +49 69 798 34701 kai.rannenberg@cepis.org	**Niko SCHLAMBERGER** *Statistical Office of the Republic of Slovenia, Secretary* tel: + 386 1 2415 295 niko.schlamberger@gmail.com

EEA-COUNTRY REPRESENTATIVES (OBSERVERS)

Group	Representative	Alternate
Iceland	**Björn GEIRSSON** *Legal Counsel* *Post and Telecom Administration in Iceland* tel: +354 510 1500 fax: +354 510 1509 bjorng@pta.is	
Liechtenstein	**Kurt BÜHLER** *Director* *Office for Communications* tel: +423 236 6480 Kurt.buehler@ak.llv.li	
Norway	**Jörn RINGLUND** *Deputy Director General* *Ministry of Transport and Communications* *Department of Civil Aviation, Postal Services and Telecommunications* tel: +47 22 24 82 02 jorn.ringlund@sd.dep.no	**Eivind JAHREN** *Deputy Director General, Department of IT Policy* *Ministry of Modernisation* tel: +47 22 24 03 20 eja@fad.dep.no

APPENDIX 2:
MEMBERS OF THE PERMANENT STAKEHOLDERS' GROUP

The Permanent Stakeholders' Group (PSG) comprises 30 independent experts who are appointed ad personam (i.e. selected on personal merit rather than representing either a country or a company) for a Term of Office of 2½ years following an Open Call for Expression. Each PSG member has proven abilities and expertise in fields relevant to the PSG mandate and has the capacity to contribute to ENISA activities and to advise the Executive Director.

PSG Members represent a broad range of stakeholders including the Information and Communication Technology industry, research and academia in the field of Network and Information Security, as well as representatives from different user and consumer communities.

Name	Job Title	Organisation	Nationality	Sector
Prof. Fred Piper	Professor of IT and Mathematics	Royal Holloway, University of London	British	Academia
Prof. Janusz Gorski	Professor of Software Engineering	Gdansk University of Technology	Polish	Academia
Mr. Ioannis Askoxylakis	Head of FORTHcert	FORTH	Greek	Academia
Dr. Matthew Robshaw	Senior Cryptographic Expert	Orange Labs	British	Academia
Mr. Peter Hoath	CSO	BT Global Services	British	Industry
Mr. Paul King	Senior Security Advisor	Cisco Systems	British	Industry
Mr. Nick Coleman	Consultant	Consultant	British	Industry
Dr. Claire Vishik	Security Policy/Technology Manager	Intel	American	Industry
Mr. Gerold Hübner	Government Security Director	Microsoft	German	Industry
Mr. Mika Lauhde	Director	Nokia	Finnish	Industry
Mr. Martin Boyle	Senior Policy Advisor	Nominet	British	Industry
Mr. Ilias Chantzos	Director of Government Relations	Symantec	Greek	Industry
Dr. Ingo Stürmer	Executive Director	DsiN	German	Industry
Mr. Maarten Botterman	Consultant/Director	GNKS Consult/PIR	Dutch	Industry
Mr. Sven Karge	Head of Department	eco	German	Industry
Mr. Urho Ilmonen	Lawyer	FACT Law	Finnish	Industry
Dr. Rainer Baumgart	CEO	secunet, Security Networks	German	Industry
Mr. Christian Wernberg-Tougaard	Chair	Board for Greater IT-Security	Danish	Industry
Mr. Paul Theron	Resilience Engineering Expert	Thales Sec. Solutions & Services	French	Industry
Mr. Casimiro Juanes	Head of IT Security	Ericsson	Spanish	Industry
Mr. Corrado Giustozzi	Head of Security Solutions Division	Capgemini	Italian	Industry
Mr. Raoul Chiesa	Manager Strategic Alliances	Mediaservice.net	Italian	Industry
Mr. Tom Daniewski	Information Security Manager	BSkyB	Polish	Users
Mr. Gianluca D'Antonio	CISO	FCC Group	Italian	Users
Mr. Andrew Cormack	Chief Regulatory Advisor	JANET(UK)	British	Users
Mr. Francois Gratiolet	CISO	Groupe La Poste	French	Users
Dr. Wim Hafkamp	Head Info Sec. Strategies & Policies	Rabobank	Dutch	Users
Mr. Rik Froyen	Senior IT Expert-IT Management	European Central Bank	Belgian	Users
Mr. Liam Lynch	Chief Security Strategist	eBay	Canadian	Users
Mr. Marcos Gomez-Hidalgo	Security/e-Trust Deputy Manager	INTECO	Spanish	Users

APPENDIX 3:
NATIONAL LIAISON OFFICERS*

Member State	National Liaison Officer
Austria	**Mr. Gerald TROST** *Bundeskanzleramt* *Büro der Informationssicherheitskommission* Tel: + 43 1 53115/2749 Fax: + 43 1 2697861 gerald.trost@bka.gv.at
Belgium	**Mr. Rudi SMET** *Belgian Institute for postal services and telecommunications* Tel: + 32 2 226 87 56 Fax: + 32 2 226 88 04 rudi.smet@bipt.be
Bulgaria	**Ms. Tsvetanka KIRILOVA** *Head of the Interoperability and Information Security Department* *Ministry of Transport, Information Technologies and Communications* Tel: + 359 2 949 20 60 tskirilova@mtitc.government.bg
Cyprus	**Mr. Neophytos PAPADOPOULOS** *Director of the Commissioners Office for the control of the Telecommunications and Postal services* Tel: + 357 22 69 31 06 neophytos.papadopoulos@ocecpr.org.cy **Mr. Antonis ANTONIADES** *Senior Officer of the Commissioners Office for the control of the Telecommunications and Postal services* Tel: + 357 22 69 31 15 antonis.antoniades@ocecpr.org.cy
Czech Republic	**Ms. Marie SVOBODOVÁ** *Communication Infrastructure Department* *Ministry of Interior of the Czech Republic* Tel:+ 420 974 817 544 marie.svobodova@mvcr.cz

Member State	National Liaison Officer
Denmark	**Mr. Flemming FABER** *Senior Advisor* *IT-Security Division* *National IT and Telecom Agency* Tel: +45 3545 0364 ff@itst.dk
Estonia	**Mr. Toomas VIIRA** *Estonian Informatics Centre* *Riigi Infosüsteemide Arenduskeskus* Tel: + 372 6630243 toomas.viira@ria.ee
Finland	**Ms. Mirka MERES-WUORI** *Senior Officer* *Communications Networks Unit* *Ministry of Transport and Communications* Tel: +358 9 160 28532 mirka.meres-wuori@lvm.fi
France	**Mr. Sylvain LEROY** *Central Directorate for Information Systems Security* *Direction centrale de la sécurité des systèmes d'information* *Secrétariat général de la défense nationale* Tel: +331 71 75 82 64 Fax: +331 71 75 82 60 sylvain.leroy@sgdn.gouv.fr
Germany	**Mr. Martin BIERWIRTH** *Federal Office for Information Security (BSI)* *International Relations* Godesberger Allee 185 -189 53175 Bonn Tel: +49 (0)228 99 9582 5119 Fax: +49 (0)228 99 10 9582 5119 SIB@bsi.bund.de

*As of 17 August 2010

Member State	National Liaison Officer
Greece	**Mr. Panagiotis PAPASPILIOPOULOS** *General Directorate of Communications* *Ministry of Transport and Communications* Tel: +30 210 6508538 Fax: +30 210 6508550 p.papaspil@yme.gov.gr
Hungary	**Mr. Ferenc SUBA** *Chairman of the Board of CERT-Hungary* Tel:+36 1 301 2080 Fax: +36 1 353 1937 ferenc.suba@cert-hungary.hu
Ireland	**Mr. John MOORE** *Communications business & technology division* *Department of communications* John.Moore@dcenr.gov.ie
Italy	**Ms Rita FORSI** *Director General* *Ministry of Economic Development* Tel: +39 6 54442360 Fax: +39 6 54442020 Rita.forsi@sviluppoeconomico.gov.it
Latvia	**Mr. Maris ANDZANS** *Head of Transport and Communications Security Division* *Ministry of Transport and Communications of the Republic of Latvia* Tel: +371 67028262 Fax: +371 67217180 maris.andzans@sam.gov.lv
Lithuania	**Mr. Rytis RAINYS** *Head of Network and Information Security Division* *Communications Regulatory Authority* Tel: +370 5 2105676 Fax: +370 5 2161564 rrainys@rrt.lt

Member State	National Liaison Officer
Luxembourg	**Mr. Manuel SILVOSO** *Ministry of the Economy and Foreign Trade - Department for e-commerce and information security* Tel: + 352 247 88429 Fax: + 352 247 84311 manuel.silvoso@eco.etat.lu
Malta	**Mr. Steve AGIUS** *Chief Information Officer* *Malta Communications Authority* Tel: + 356 21 33 6840 sagius@mca.org.mt
The Netherlands	**Mr. Edgar DE LANGE** *Ministry of Economic Affairs, Agriculture and Innovation* *Directorate-General for Energy, Telecommunications and Markets* P.O. Box 20101, 2500 EC The Hague, The Netherlands Tel: + 31 70 379 8153 Fax + 31 70 379 8266 e.r.delange@minez.nl
Poland	**Krzysztof SILICKI** *Technical Director* *Research and Academic Computer Network (NASK)* Tel: +48 22 5231315 Fax: +48 22 5231201 Krzysztof.silicki@nask.pl
Portugal	**Mr. Lino SANTOS** *CERT.PT/FCCN,* *Director of security and users services* Tel: +351218440100 Fax: +351218472167 lino@fccn.pt
Romania	**Mr. Razvan GAVRILA** *CERT-RO* *Expert* Tel: +40 21 316 12 59 razvan.gavrila@cert-ro.eu

Member State	National Liaison Officer
Slovakia	**Mr. Rastislav MACHEL** *CISSP* Tel: + 421-905-622435 Rastislav.Machel@machel-cs.eu
Slovenia	**Mr. Radovan PAJNTAR** *Ministry of Higher Education, Science and Technology, Directorat Information Society Directorate Trg* Tel: + 386-1-478-46-47 Fax: + 386-1-478-46-65 radovan.pajntar@gov.si
Spain	**Mr. Oscar MARTINEZ DE LA TORRE** *Head of Unit for eSignature & eSecurity - Directorate for Information Society services.* *Ministry for Industry - Secretary of State for Telecommunications and for Information Society - Ministry for Industry, Tourism and Commerce - Kingdom of Spain* Tel: +34.91.346.1558, +34.91.346.2748, +34.91.246.2268 Fax: +34.91.346.1577 OMartinez@MITyC.ES
Sweden	**Mr. Björn SCHARIN** *Adviser* *National Post and Telecom Agency* *Network Security Department* Tel: + 46-8-678 55 98 Bjorn.Scharin@pts.se
United Kingdom	**Ms. Alice REEVES** *Communications Security and Resilience, BIS* alice.reeves@bis.gsi.gov.uk Tel: +44 20 7215 3093 alice.reeves@bis.gsi.gov.uk

EEA	National Liaison Officer
Iceland	**Mr. Björn GEIRSSON Legal Counsel** Tel: + 354 510 1500 Fax: + 354 510 1509 bjorng@pta.is
Liechtenstein	**Mr. Kurt BUEHLER** *Director* *Office for Communications* Tel: + 423 236 6488 Fax: + 423 236 6489 kurt.buehler@ak.llv.li
Norway	**Ms. Heidi KARLSEN** *Adviser Ministry of Transport and Communications* Tel: + 47 22 24 81 48 Fax: + 47 22 24 56 09 heidi.karlsen@sd.dep.no

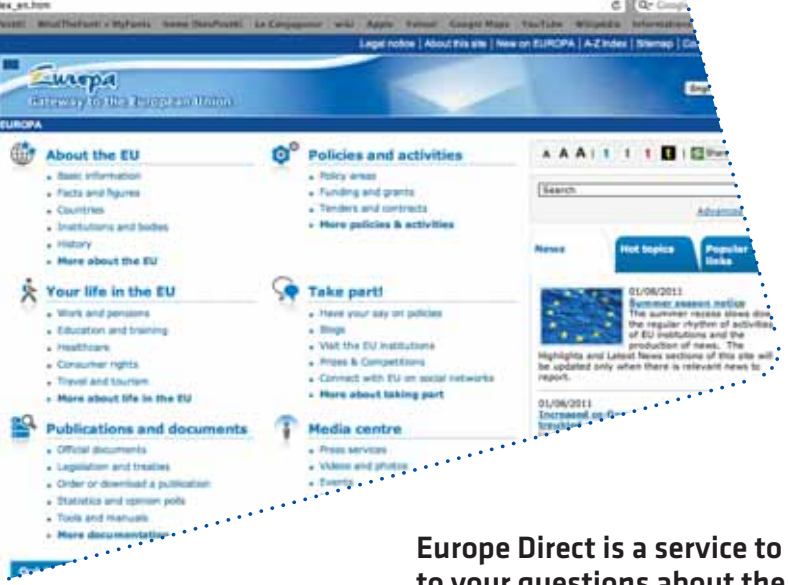
European Commission Liaison	
European Commission	**Mr. Rogier HOLLA** *Policy Officer, Policy Developer ENISA* Tel: + 32 2 2967066 Tel: + 32 2 2991111 Rogier.Holla@ec.europa.eu

Council Liaison	
Council of the European Union	**Mr. Anastassios PAPADOPOULOS** *Council of the European Union - General Secretariat* anastassios.papadopoulos@consilium.europa.eu

APPENDIX 4:
ACRONYMS AND ABBREVIATIONS

AR	Awareness Raising
CERT/ CSIRT	Computer Emergency Response Team/Computer Security Incident Response Team
CIIP	Critical IT Infrastructure Protection
DG INFSO	Directorate General Information Society and Media
EC	European Commission
EEA	European Economic Area
EFMS	European Forum for Member States
EFR	Emerging and Future Risk
EFTA	European Free Trade Association
eIDM	electronic identity management
EISAS	European Information Sharing and Alert System
EP3R	EU Public Private Partnership for Resilience
EQR	ENISA Quarterly Review
EU	European Union
FAQ	Frequently Asked Questions
FIA	Future Internet Assembly
FI-ISAC	Financial Institutions – Information Sharing and Analysis Centre
FORTH	Foundation for Research and Technology – Hellas
GPG	Good Practice Guide
ICT	Information and Communication Technology
IE	Information Exchange

AR	Awareness Raising
ISAC	Information Sharing and Analysis Centre
ITU-D	International Telecommunication Union Telecommunication Development Group
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JRC	Joint Research Centre
MB	Management Board
MEP	Member of the European Parliament
MTP	ENISA Multi-annual Thematic Programme
NIS	Network and Information Security
NLO	National Liaison Officer
NRM	National Risk Management
OECD	Organisation for Economic Co-operation and Development
PA	ENISA Preparatory Action
PA	Public Administrations
PIA	Privacy (and data protection) impact assessments
PSG	ENISA Permanent Stakeholders' Group
RFID	Radio Frequency Identification
SME	Small and Medium Enterprise
SNS	Social Networking Site
WARP	Warning Advice and Reporting Point
WPISP	Working Party on Information Security and Privacy
WPK	ENISA Work Package



Europe Direct is a service to help you find answers to your questions about the European Union

FREEPHONE NUMBER*:

00 800 6 7 8 9 10 11

*Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

How to obtain EU publications

Free publications

- via EU Bookshop (http://bookshop.europa.eu);
- at the European Commission's representations or delegations. You can obtain their contact details by linking http://ec.europa.eu or by sending a fax to +352 2929-42758.

Publications for sale

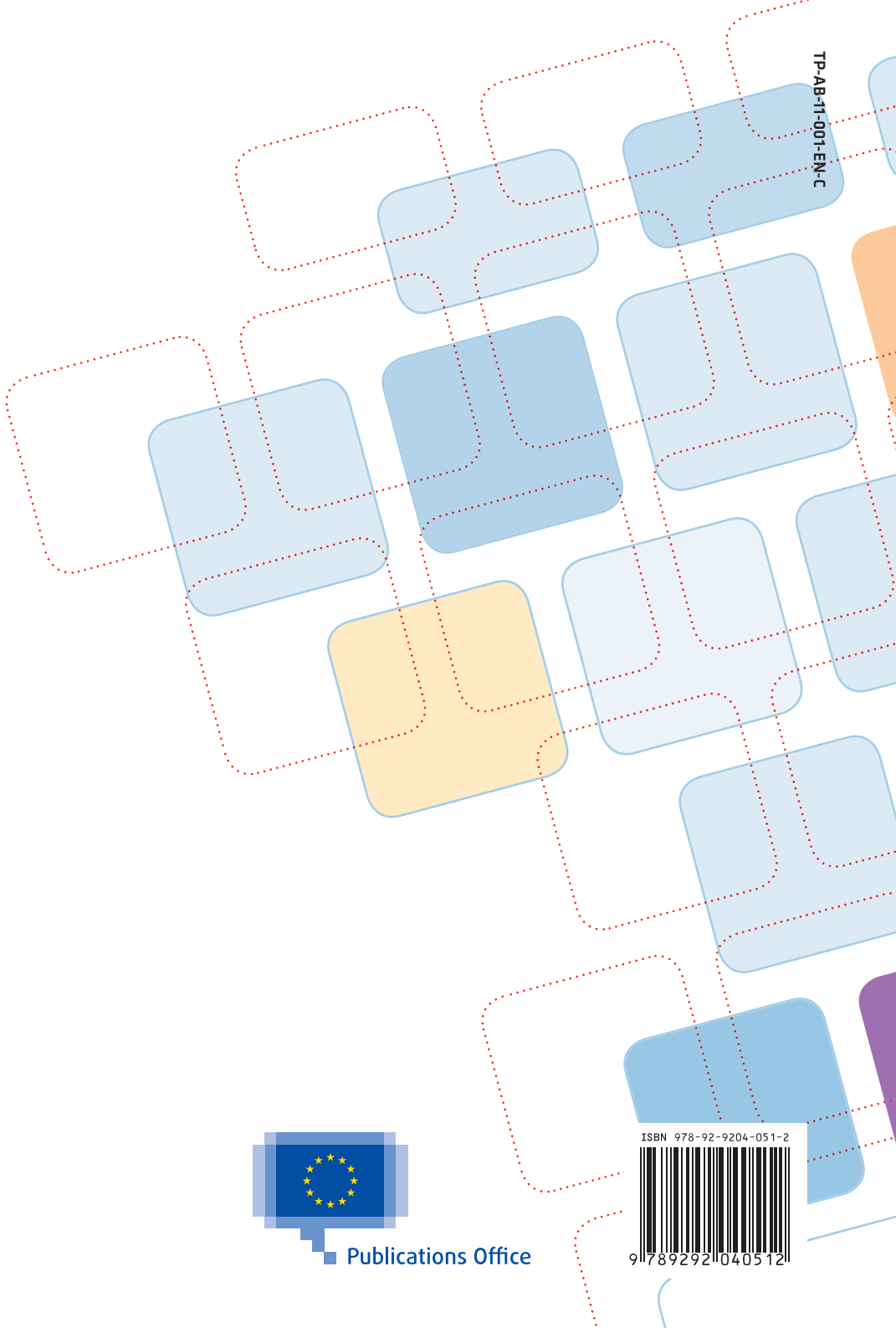
- via EU Bookshop (http://bookshop.europa.eu);
- Priced subscriptions (Official Journal of the European Union, legal cases of the Court of Justice as well as certain periodicals edited bythe European Commission) can be ordered from one of our sales agents. You can obtain their contact details by linking http://ec.europa.eu or by sending a fax to +352 2929-42758.

European Commission

General Report 2010
European Network and Information Security Agency

Editing and design by De Visu Digital Document Design, BE
Published in August 2011

Luxembourg: Publications Office of the European Union, 2011
64 pp. – 29.7cm x 21cm
ISBN: 978-92-9204-051-2
ISSN: 1830-981X
Catalogue no.: TP-AB-11-001-EN-C
doi 10.2824/21096



TP-AB-11-001-EN-C

ISBN 978-92-9204-051-2

Publications Office

enisa
European Network and Information Security Agency

ENISA – European Network and Information Security Agency
PO Box 1309, 710 01, Heraklion, Greece
Tel: +30 2810 39 12 80, Fax: +30 2810 39 14 10
www.enisa.europa.eu