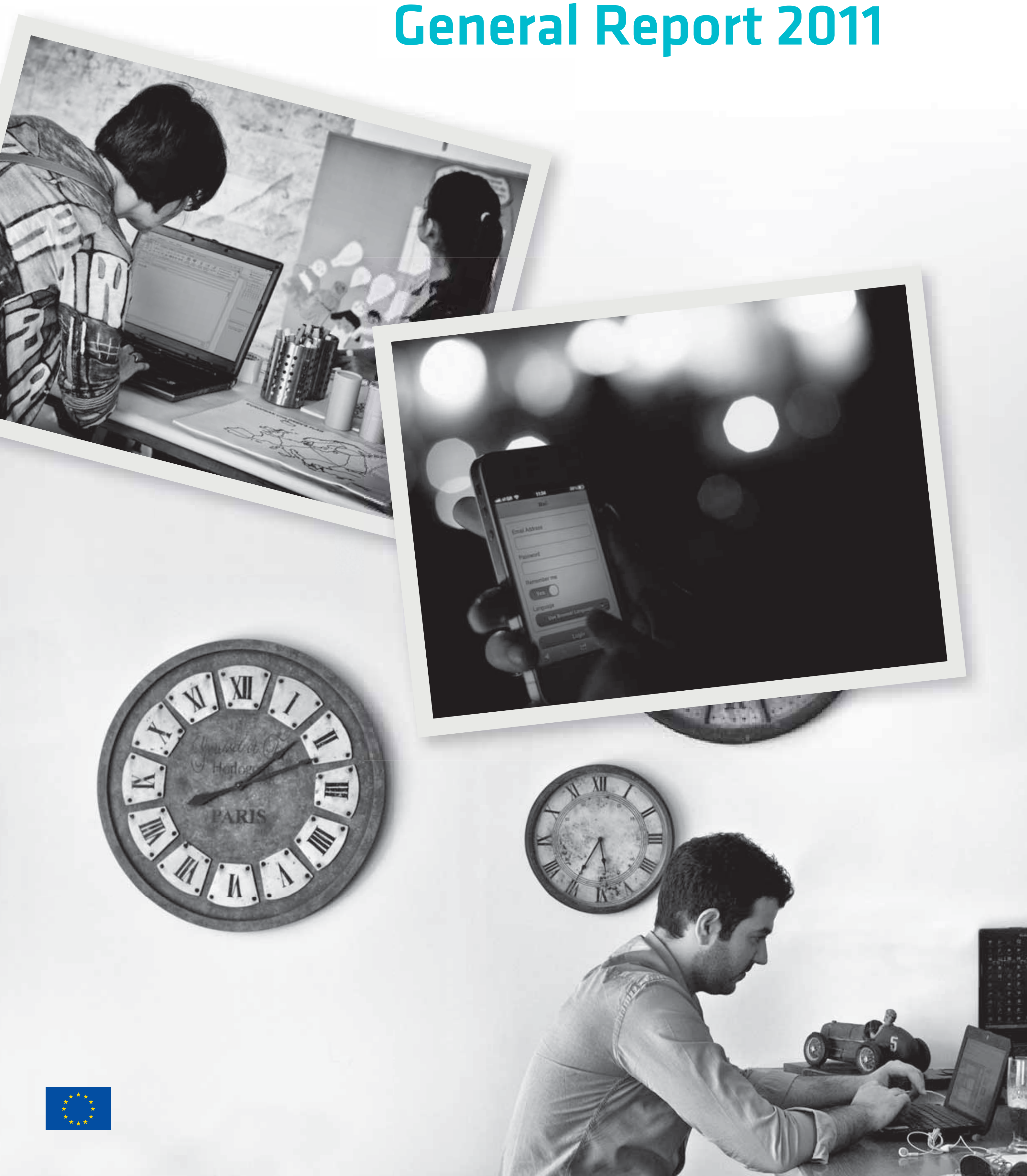
enisa
European Network
and Information
Security Agency

SECURING EUROPE'S INFORMATION SOCIETY
General Report 2011



A MESSAGE FROM THE EXECUTIVE DIRECTOR

This has been a year full of developments and new challenges for ENISA. Looking toward a new Regulation for the Agency, we received many positive comments and much positive feedback in 2011. This brings closer the realisation of the modernised ENISA as foreseen in the Digital Agenda for Europe.[1] The key role of Computer Emergency Response Teams (CERTs) has been strengthened over the course of this year, with for example, close collaboration with Malta and Ireland, where ENISA helped to set up new CERTs. The Agency is also represented in the expert team that is working to create a CERT for the EU institutions.

Along with an increasing call for assistance with CERTs, 2011 also saw a rise in the number of Member States' other requests for assistance. In recognition of this, on 12 August, ENISA set up a new Mobile Assistance Team within the Technical Competence Department. This is one of a number of organisational changes that are enabling ENISA to work more efficiently and focus its resources to best effect.

ENISA's work throughout 2011 continued to deal with emerging fields, such as cloud computing and applications for mobile phones. These were addressed in our reports, amongst many other thought-provoking topics. Another area that has attracted interest is Data Breach Notification. Dealing with how security is addressed from the legislative dimension is a growing area of work, alongside more technical issues.

Throughout 2011, ENISA continued to support EP3R, the European Public-Private Partnership for Resilience. The Agency's role was to further develop working groups, drive the agenda and discussions, and collect the feedback of participants. This input will help form the basis for EP3R Position Papers, to be published in early 2012. The topics covered include definitions of critical infrastructure, baseline security requirements, and responses to large-scale disruptions, in, for example, the fields of botnets, mutual aid agreements and cyber security exercises.

The global nature of risks is apparent, as attacks have no physical borders; in the light of this, a major exercise, Cyber Atlantic 2011, was held between the EU, the US Department of Homeland Security and EU Member States. The exercise, facilitated by ENISA, took place in Brussels and was marked by excellent cooperation among all actors.

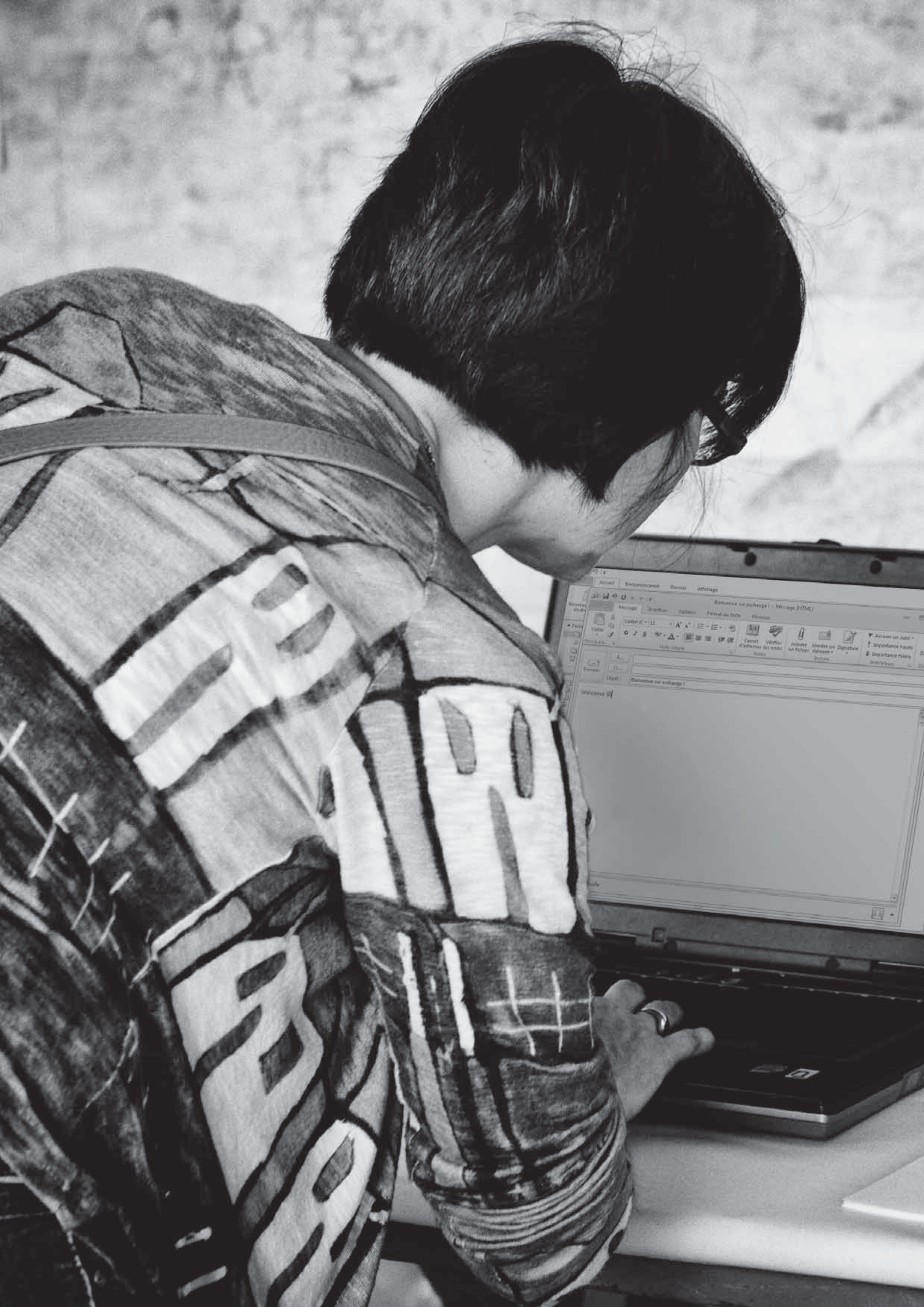
Amidst the reality of global challenges and opportunities, we need strong international cooperation as shown in Cyber Atlantic 2011 and all of ENISA's work. This includes cooperation throughout Europe as well as worldwide in both the public and private sectors. A shared commitment at international level will result in a completely new and mutual understanding of cyber security implementation, thereby ensuring reliable cross-border mechanisms for a safe and solid European digital society.

Udo Helmbrecht
Executive Director

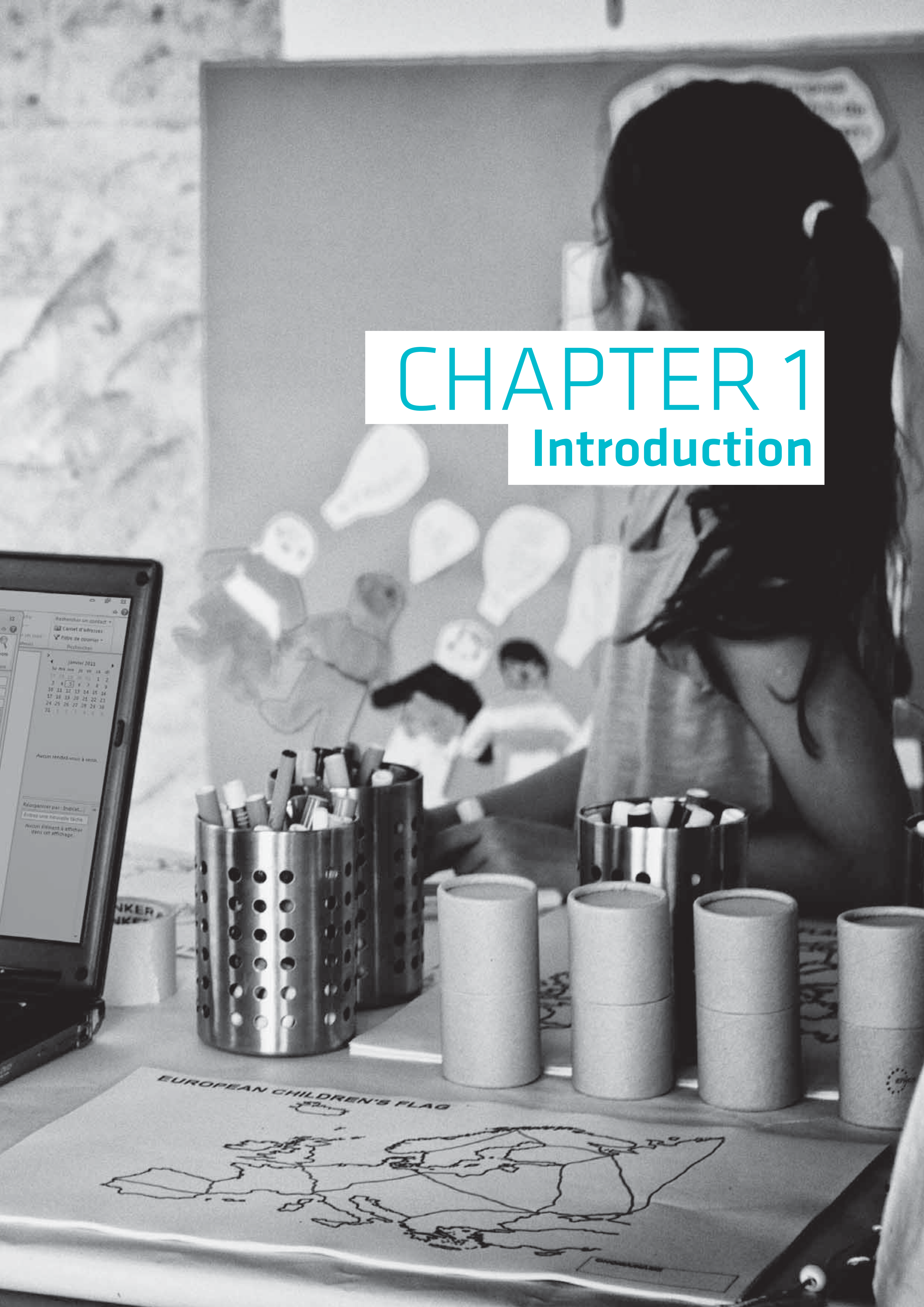
[1] A Digital Agenda for Europe, Key Action 6, *The Commission will*: Key Action 6: Present in 2010 measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as a modernised European Network and Information Security Agency (ENISA).

enisa
Securing Europe's information society
Cultivating trust and confidence in the use of ICT
Securing inform
infrastructure
moting information
security standards,
guidelines and
certification sche
pporting the fight
ainst cyber crime
Educating the wider
public about ICT

TABLE OF CONTENTS



CHAPTER 1
Introduction



NETWORK AND INFORMATION SECURITY IN EUROPE

Information and Communication Technologies (ICT) have provided innumerable benefits to citizens, businesses and governments, and have transformed Europe's society and economy. In the future, however, these technologies could provide even greater benefits. Thus, European Commission Vice President Neelie Kroes has put forward the Digital Agenda for Europe. The objective of the Agenda is to apply ICT to improve the quality of life for European citizens. Better healthcare, safer and more efficient transport solutions, a cleaner environment, new media opportunities and easier access to public services and cultural content are just a few examples of the areas that could be positively impacted by ICT.[1]

The Evolving threat landscape

> "Society is continuously evolving and new technologies and business models are emerging at a feverish pace. New business models push existing concepts and regulation to their limits."

While the vision of a Digital Society is compelling, robust Network Information Security (NIS) will be needed to get there. In the area of NIS, we face an entirely new set of challenges. Society is continuously evolving and new technologies and business models are emerging at a feverish pace. New business models push existing concepts and regulation to their limits. Cloud computing, and other technologies where data is de-centralised and spread over virtual and physical locations, is a prime example. Our concepts of data, data protection and data sharing are often difficult to apply in these settings, and this can be problematic given the rate of uptake of these new technologies.

Meanwhile, new threats are emerging from unexpected places. Not only are new technologies and business models continuously being introduced, the use of old technologies is being extended in ways that were never envisaged when they were first developed. A good example of this is the supervisory control and data acquisition (SCADA) industrial control systems that control power plants, transportation systems and other key infrastructure. SCADA systems were initially designed to be independent without connectivity to other systems, but are now increasingly being connected to the Internet. This makes them potential targets of malware or other cyber threats, such as the Stuxnet worm that was used to attack the SCADA systems of nuclear facilities.

In general, cyber threats have become more sophisticated, more sinister and more common. ICT is increasingly used in crime and politically motivated attacks. Germany, for example, saw an increase of 8.1% in criminal acts associated with the Internet during 2010.[2] Moreover, nowadays attacks may benefit from the backing of rogue states or organised crime. Apart from their potential to cause disruption, cyber threats complicate the deployment of ICT solutions used by citizens in their day-to-day lives, such as online payment systems and e-government services.

To achieve the full potential for improvement made possible by ICT, therefore, citizens, businesses, governments and critical infrastructure need to be better protected from criminals. This is recognised in both the Digital Agenda and the EU Internal Security Strategy.[3] The protection of critical infrastructure and the applications that run on top of it is not just about cyber security – it is closely connected to the EU's competitiveness and prosperity.

[1] COM(2010) 245 final/2.

[2] http://www.dw-world.de/dw/article/0,,15093336,00.html.

[3] COM(2010) 673 final.

Mitigating threats – a fragmented approach

Unfortunately, while great strides have been made over the past several years, our approach to mitigating threats remains overly fragmented. Different approaches to securing information and systems are developed independently in different Member States and in different communities. In such an environment, the principle of the weakest link applies; for example, weaknesses in one Member State could easily be used to compromise security in other Member States. In a global networked environment, issues that transcend national boundaries must be managed and controlled correctly. Without a coordinated global approach to major incidents on the Internet, for example, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are beyond their control.

Ensuring a coherent pan-European approach

> “Any future approach to securing Europe’s ICT systems must be coherent across geographical borders and pursued with consistency over time.”

Instead of fragmentation, what is needed is a holistic approach to cyber security, including cybercrime, on a pan-European level. Any future approach to securing Europe’s ICT systems must be coherent across geographical borders and pursued with consistency over time. The entry into force of the Lisbon Treaty is an opportunity to improve the level of dialogue between communities in the area of NIS. The EU institutions should provide the support and the framework for Member States to achieve a coordinated global approach. These efforts to improve NIS must involve the private sector, as users of ICTs, as implementers of ICT-based business models, as producers of the technologies and as operators of services and infrastructure, as well as citizens.

ENISA’s role

ENISA is working together with the Member States to secure Europe’s information society. A significant part of this effort involves protecting infrastructure and applications, and ensuring that Europe is prepared for incidents when they do happen by reinforcing incident response capabilities across the EU. The focus of ENISA is on cross-border issues, helping Member States to identify dependencies and to decide on the most appropriate way to deal with them. In an increasingly connected and global world, the Agency is a key asset in ensuring the overall security of Europe’s network and information systems. As ENISA’s Regulation states: “The Agency should have the task of contributing to a high level of network and information security within the Community and of developing a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union, thus contributing to the smooth functioning of the internal market.”[4]

[4] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance).

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 de-centralised 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. Promote information security standards, guidelines and certification schemes
3. Educate the wider public on ICT

In 2011, ENISA published numerous reports and studies on a range of NIS issues, including:

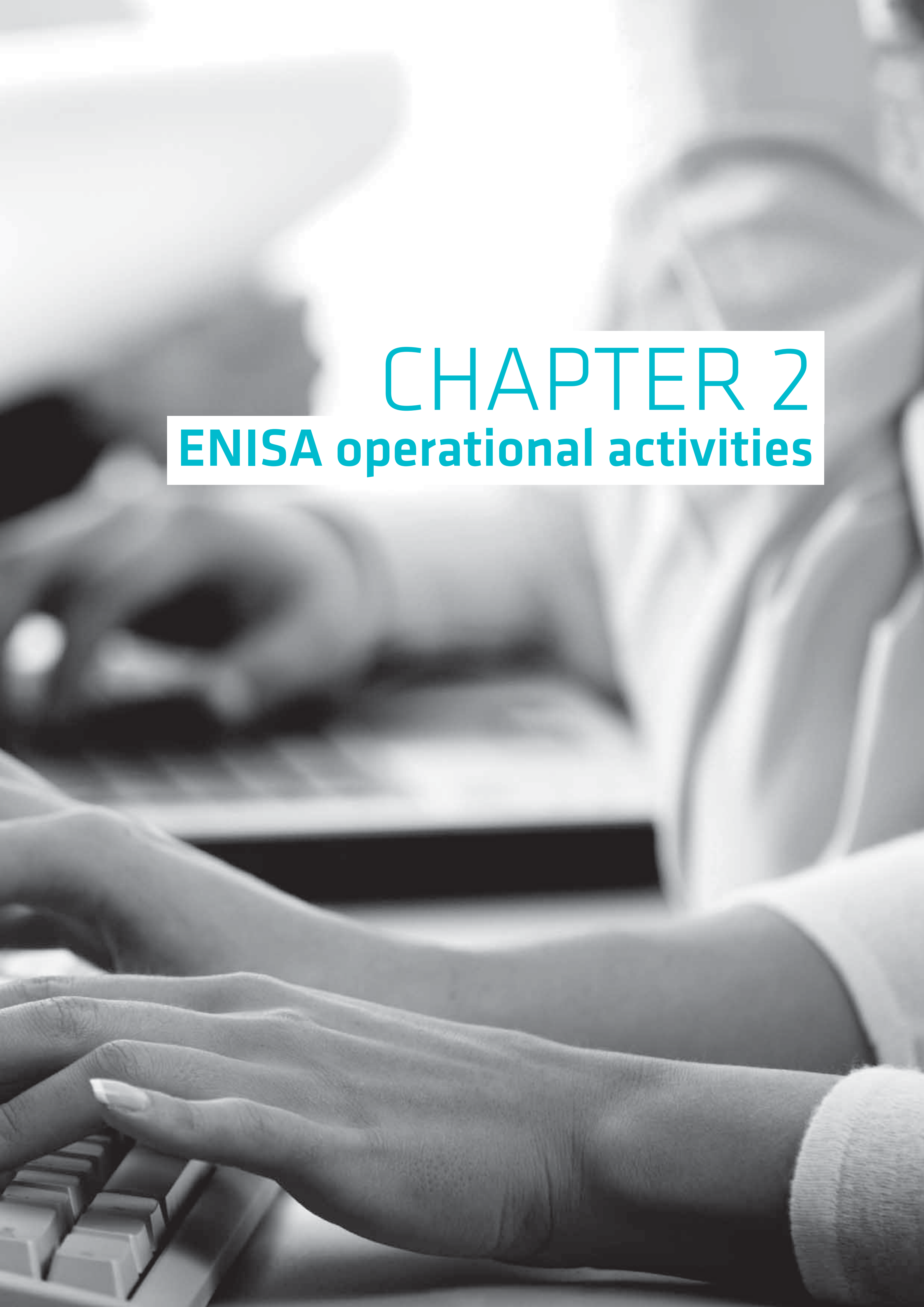
- smart phone and appstore security
- smart grids
- the resilience of the Internet interconnection ecosystem
- protecting Industrial Control Systems (ICS)
- an ontology and taxonomies of resilience
- the use of cryptographic techniques in Europe
- spam
- social networking
- botnets
- standards
- risk assessment
- risk management
- business continuity
- 'digital fire brigades'
- next generation web standards
- supply chain integrity
- the monetization of privacy

The Agency also conducted a feasibility study for a European-wide Information Sharing and Alert System (EISAS). ENISA co-organises conferences, runs workshops and publishes position papers.

As a European agency, ENISA is uniquely positioned to bring together a wide range of key players in network and information security, by acting as a neutral and independent adviser. With its technical expertise, its central position and its independence, the Agency is well placed to provide expert advice on current issues, as well as 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 set up to help implement EU policies more efficiently, and to respond to particular needs identified by the EU institutions and Member States. They provide 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

RESILIENCE AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

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

Reliable communications networks and services are now critical to public welfare and economic stability. Attacks on the Internet, disruptions due to physical phenomena, software and hardware failures, and human error all affect the proper functioning of public e-communications networks. Such disruptions reveal the increased dependence of our society on these networks and their services. Moreover, experience has shown that neither single providers nor a country alone can effectively detect, prevent and respond to threats.

Recent official Communications from the European Commission have highlighted the importance of network and information security and resilience for the creation of a single European information space. They have stressed the importance of dialogue, partnership and the empowerment of all stakeholders to properly address these threats.

Fully recognizing this need, ENISA is engaged in several activities with the ultimate objective of collectively evaluating and improving the resilience of public e-communication networks and services in Europe.

For 2011, the Resilience activities and tasks were defined within the ENISA Work Programme 2011 – Securing Europe's Information Society. The Resilience activities were included within Work Stream (WS) 1: ENISA as a facilitator for improving cooperation and WS 2: ENISA as a competence centre for securing future technology. The work packages dedicated to Resilience were Work Package (WPK) 1.1: Supporting Member States in implementing article 13a; WPK 1.2: Preparing the next pan-European exercise and WPK 2.2: Interdependencies and interconnection.

Incident reporting and the implementation of Article 13a

A new European Directive on telecommunications requires operators to report security incidents. Article 13a of the new legislation defines these requirements, and also states that they must take measures to enable secure and uninterrupted delivery of communication services.

In 2010, ENISA and the European Commission set up a working group of experts, from telecommunication regulatory authorities in the EU, to discuss the technical aspects of implementing Article 13a.

Continuing this work in 2011, ENISA organised discussions with the working group in face-to-face workshops and teleconferences. These meetings led to a consensus on two technical guidelines:

- Technical guideline on incident reporting, http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting
- Technical guideline for minimum security measures, http://www.enisa.europa.eu/act/res/reporting-incidents/minimum-security-requirements

The working group will continue to meet in 2012 to develop further guidelines, if needed.

Towards a pan-European Public-Private Partnership for Resilience (EP3R)

Increasing the resilience of Critical Information Infrastructures (CIIs) is fundamental within Member States. Several national Public-Private Partnerships (PPPs) have already been established to enhance preparedness for and response to disasters or failures, by coordinating the efforts of telecom operators. Initially, cross-border mechanisms were set up on an ad hoc basis. However, the need to respond to both existing and emerging threats at a European level soon became apparent. In March 2009, therefore, the European Commission adopted a policy initiative to address this challenge, and soon a European Public-Private Partnership for Resilience (EP3R) was established to support such coordination. The objectives of the EP3R are to:

1. Encourage information sharing and take stock of good policy and industrial practices that foster common understanding
2. Discuss public policy priorities, objectives and measures
3. Improve the coherence and coordination of policies for security and resilience in Europe
4. Identify and promote the adoption of good baseline practices for security and resilience

ENISA has supported the EP3R process, facilitating the establishment of three working groups (WGs) to address:

- Identification of key assets, resources and functions for the continuous and secure provisioning of e-communications across Member States
- Baseline requirements for the security and resilience of e-communications – this includes the coordination and cooperation needed to prevent and respond to large-scale disruptions affecting electronic communications
- Coordination and cooperation needs and mechanisms to prepare for and respond to large-scale disruptions affecting electronic communications. This area initially covers two important topics, namely Botnets and Cyber-Exercises.

The working groups have produced four position papers containing recommendations covering the four different areas of EP3R. A number of the recommendations aim at establishing the foundations for the harmonised and enhanced resilience and security of critical ICT.

Good practice guide on how to build successful Public Private Partnerships

Within the EP3R project, ENISA conducted a Study on Cooperative models for effective Public Private Partnerships (PPPs). The aim of the study was to consolidate and validate a taxonomy revealing the main components required to create and maintain a PPP. ENISA also published a Good Practice Guide that sets out the principles underpinning Public Private Partnerships and reviews the range of partnership options available. It describes some of the ways in which partnerships can be used, and gives advice on the issues that need to be addressed when implementing them. The Good Practice Guide is designed to help and support stakeholders in choosing options that will add value when they set up and run a PPP. To this end, a set of recommendations for good practice has been included in the guide.

The report is available at: https://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps

Security of Industrial Control Systems

> "With the rapidly increasing interconnection of Industrial Control Systems with corporate networks and the Internet, and the growing use of commercial off-the-shelf components, in the last decade ICS have become highly vulnerable to computer network-based attacks…"

Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. These systems monitor and control a variety of processes and operations, such as gas and electricity distribution, water treatment, oil refining and rail transport. With the rapidly increasing interconnection of Industrial Control Systems with corporate networks and the Internet, and the growing use of commercial off-the-shelf components, in the last decade ICS have become highly vulnerable to computer network-based attacks and have faced a notable number of incidents. Recognising the importance of the problem, ENISA launched a series of activities that aim to bring together the relevant stakeholders and engage them in an open discussion on ICS protection. The primary goals of this open dialogue were to identify the main concerns regarding ICS security, and to recognize and support national, pan-European and international initiatives in this area.

Based on the discussions described above, ENISA published Protecting Industrial Control Systems, recommendations for Europe and Member States, a report that contains a set of recommendations for the public and private sector. These recommendations provide useful and practical advice for improving current initiatives, enhancing co-operation, developing new measures and good practices, and reducing barriers to information sharing. The recommendations call for the creation of national and pan-European ICS security strategies, the development of a Good practices guide on ICS security, fostering awareness and education as well as research activities or the establishment of a common test bed, and the development of ICS-computer emergency response capabilities.

Protecting Industrial Control Systems, recommendations for Europe and Member States https://www.enisa.europa.eu/act/res/other-areas/ics-scada/protecting-ics-report

Seminars for cyber exercises

Cyber exercises are an important tool for assessing the preparedness of a community in case of cyber attacks, natural disasters, technology failures or emergency situations. Throughout the year, ENISA experts delivered seminars, and shared information and knowledge on how to plan, design, organise and conduct national cyber exercises. Since 2010, ENISA has delivered twelve seminars on planning, conducting and evaluating CIIP exercises. In 2011, ENISA continued to build its capacity in cyber exercise organisation by preparing a more in depth analysis of the cyber exercise scenario development process. The study resulted in a handbook on cyber exercise development, which together with a good practice guide on national exercises will be part of the ENISA offering on planning and designing cyber exercises.

Table 1 ENISA Seminars on Cyber Exercises in 2010-11

	Country	Date
	Belgium	09/05/2011
	Bulgaria	10/11/2011
	Czech Republic	08/06/2011
	Greece	16/05/2011
	Iceland	19/04/2011
	Italy	09/06/2011
	Latvia	24/05/2011
	Lithuania	25/05/2011
	Luxembourg	09/05/2011
	Portugal	10/11/2010
	Romania	14/05/2011
	Slovak Republic	08/06/2011

Cyber Europe

After the success in 2010 of the first ever pan-European cyber exercise, Cyber Europe 2010, the exercise evaluation report was published in 2011.

One of the key findings was that Member States' information technology bodies communicate in a wide variety of ways and the ease with which the relevant points of contact within organisations can be found varies. The main recommendations were:

- Europe should continue to hold exercises in Critical Information Infrastructure Protection (CIIP)
- The private sector should provide value in future exercises by increasing the levels of realism
- 'Lessons learned' should be exchanged with those holding other (national or international) exercises

Following up on the recommendations, ENISA has already started the organisation and planning process for the next pan-European cyber exercise, Cyber Europe 2012.

Cyber Atlantic 2011

Cooperation work during the exercise

Following an EU-US commitment to foster greater efforts and cooperation on cyber security, the first joint cyber security exercise between the EU and US was held in November 2011, with the support of ENISA and the US Department of Homeland Security (DHS). More than twenty EU Member States were involved, including sixteen that actively participated. The objectives of the exercise were to:

- Explore and identify issues in order to improve the way in which EU Member States and the US engage with each other during cyber crisis management activities
- Exchange good practices regarding approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration

The exercise had a two-fold scenario. The first scenario revolved around a cyber incident that affected the EU, the second scenario involved cyber incidents in the US. The main recommendations from Cyber Atlantic 2011 were to:

- Further develop and raise awareness of the European Standard Operating Procedures (SOPs) for co-operation during a cyber crisis
- Develop and implement initiatives to improve the understanding of structures and mechanisms available for international cooperation
- Identify the resource requirements for effective cooperation

Cyber Atlantic 2011 was a major event that attracted the attention of the mainstream media.

For further information:
https://www.enisa.europa.eu/act/res

National Cyber Contingency Plans

When all countries prepare, deploy and test National Cyber Contingency Plans (NCPs), there is a major benefit for the resilience of Critical ICT Infrastructures (CIIs) The main problem, however, is that there has been no clear definition of what an NCP is, the main elements that it should include and how it should be developed and deployed. To close the information gap, ENISA is preparing a good practice guide that will facilitate the development of National Contingency Plans (NCP) and their lifecycle.

For further information:
https://www.enisa.europa.eu/act/res

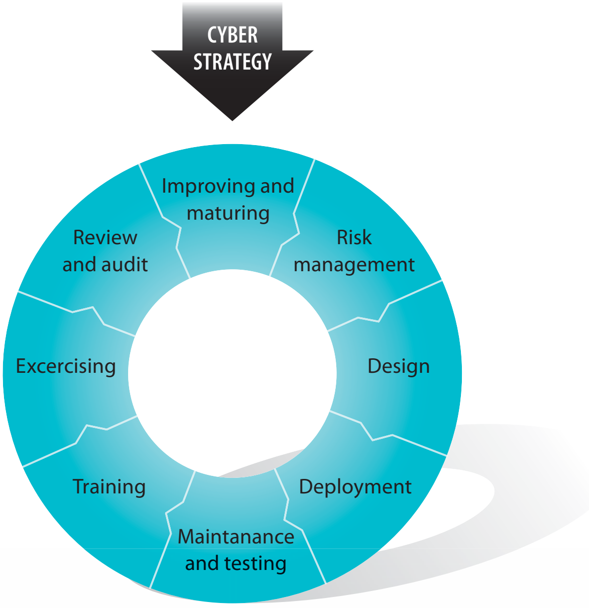
The elements of a national contingency plan typically have been identified as:

Figure 1: Elements of a National Contingency Plan

Elements	Description
1. Introduction	Explaining the purpose and scope of the NCP as well as the relation with other documents
2. Key definitions & Activation criteria	Stating what is considered to be a (cyber) crisis requiring national coordination by means of activation criteria
3. Roles, structures and responsabilites	Explaining the responsabilities and roles of the most important actors and providing an overview of the response coordination structure
4. Processes and actions	Giving insight in the activities performed in the emergency response process

ENISA has also identified the lifecycle for the development and maintenance of NCPs. By following the steps within the cycle, a country is guided through the process of developing and continuously improving the contingency plan. As described in the guide, the steps are:

1. Understand the scenarios and threats for which to prepare
2. Design the objectives, structure, roles and responsibilities of the response
3. Deploy the NCP with planning, resources and processes
4. Maintain processes and procedures
5. Test the plan's underlying technology, tools and infrastructure
6. Train the people involved
7. Perform exercises
8. Organise review and auditing, and continuously improve the plan



Resilience of the Internet interconnection ecosystem

Network operators provide their customers with connectivity to the Internet. There are different interconnection and peering policies used by operators. It is a complex ecosystem.

ENISA prepared the first study on the subject: Inter-X: resilience of the Internet interconnection ecosystem, and published it in April 2011. This study helps to provide a better understanding of what is needed for a more secure and resilient interconnected network environment. The Agency has explored the resilience of the system of interconnections between Internet networks, focusing not only on the actual interconnections, but also on the arrangements, agreements, contracts and incentives that underpin them. Together all of this is referred to as the ecosystem.

The study identified a number of concerns, including a striking lack of information on the size and shape of the Internet infrastructure. It recommended the investigation of incidents by an independent body, in order to understand the nature of successes and failures.

Inter-X: resilience of the Internet interconnection ecosystem

https://www.enisa.europa.eu/act/res/other-areas/inter-x/report/interx-report

As a follow up, ENISA launched a project on Good practices for resilient Internet interconnections. The aim of this study is to assess technical issues (e.g. logical, physical, application layers, replication and diversity of services and data, data centres), peering and transit issues (e.g. service level agreements), and market, policy and regulatory issues. The final result of this project, to

Cyber security is crucial for the maritime sector be published in early 2012, will be an exhaustive analysis of areas such as:

- Known good measures, practices, standards and policies to highlight the interconnections
- National and international initiatives, structures and strategies used for interconnection (including information exchanges and public-private partnerships)
- Challenges in the area of inter-domain routing and traffic re-direction
- Emerging issues and research issues and topics

Analysis of the cyber security aspects of smart grids

> "Improved operations and services will come at the cost of exposing the entire electricity network to new challenges, particularly regarding the security of communication networks and information systems."

Smart grids could be described as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering, and monitoring systems have been added. Based on recent experiences, smart grids will substantially improve control over electricity consumption and distribution to the benefit of consumers, electricity suppliers and grid operators. Nevertheless, improved operations and services will come at the cost of exposing the entire electricity network to new challenges, particularly regarding the security of communication networks and information systems.

In order to help public stakeholders gain deeper insight into the issue, ENISA produced a research study on the topic. Furthermore, ENISA would like to pave the way for future actions and studies by compiling a list of recommendations to different stakeholders.

The objective of the 2011 ENISA study on *Analysis of the Cyber Security Aspects of Smart Grids* was to take stock of the risks and challenges related to the cyber security aspects of these systems. Through a dedicated survey and a series of interviews with key subject matter experts, ENISA analysed the cyber security controls deployed in the various smart grid architectures. The analysis resulted in recommendations for all stakeholders. These recommendations will help to improve the security, safety and resilience of future smart grid deployments.

Cyber security aspects in the maritime sector

The maritime sector is of vital importance to European society. Securing its critical infrastructure is a major area of concern, as it sustains essential services and the movement of foodstuffs and other vital goods and materials. Delays in the supply chain can cause massive economic and social dislocation. Therefore, adequate cyber security for maritime activities is crucial. In 2011, ENISA published a study *Analysis of Cyber Security Aspects in The Maritime Sector* that analyses cyber security in the maritime sector and identifies key insights and considerations. It also touches on the policy context at the European level and situates the topic in the context of the global protection of ICT infrastructure.

Analysis of Cyber Security Aspects in The Maritime Sector

http://www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector

Mutual Aid Agreements

The topic of Mutual Aid Agreements appeared for a first time as a recommendation in the 2007 EU Commission-sponsored report, *Availability and robustness of electronic communications infrastructure (ARECI)*. Mutual Aid Agreements are an advanced means of emergency preparedness.

This years' ENISA report on *Mutual Aid for Resilient Infrastructure in Europe (MARIE) Phase 1* presents twelve key observations about Mutual Aid Agreements and in so doing lays the foundation for actionable recommendations which are planned for the MARIE Phase 2 report (expected in 2012).

Critical services

The Secure Applications and Services (SAS) group at ENISA addresses the security of services and applications, ranging from cloud-based services and web applications to smartphones and smartphone apps.

Procure secure

This project covers security aspects over the complete lifecycle from Request for Proposal (RfP) to monitoring of contract fulfilment in public IT procurement. The objective of the project is to provide tools to minimise information security risk for potential cloud customers and teams managing outsourced projects (not necessarily cloud related). The customers could be IT officers, IT security officers or procurement officers.

Smartphone developer guidelines

Smartphones will outnumber PCs by 2013 and they will be the most common devices for accessing the Internet. ENISA's report, *Smartphone developer guidelines*, looks at ways to ensure security for this important technology. A key feature of smartphones is the use of appstores: managed repositories of third party software. Apple's appstore and Google's Android Market have hundreds of thousands of apps, and claim billions of app downloads. Whereas in the past, mobile phone users could only perform simple actions such as changing their ringtone or wallpaper, the new apps turn the smartphone into the digital equivalent of a Swiss army knife, offering everything from sonic mosquito repellent to point-of-sale credit card payment.

Smartphone developer guidelines

http://www.enisa.europa.eu/media/news-items/top-ten-smartphone-security-controls-for-developers

App-stores – the five lines of defence

Apps and app-stores have not escaped the attention of cyber attackers. In 2010, diallerware was found in app-stores for Windows Mobile phones and in 2011 malware was disguised as a popular app on the Android app-store infecting thousands of smartphones. Still, the number of malware attacks on smartphones pales in comparison to the number of attacks on PCs. The large market share of PCs plays a role, but ENISA believes that security design choices have also been instrumental in preventing smartphone malware attacks. To consolidate this head start, ENISA's *App-stores – the five lines of defence*, analysed malware threats in app ecosystems and identified five lines of defence that protect end-users from malware and non-secure apps.

App-stores – the five lines of defence

http://www.enisa.europa.eu/act/application-security/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware

A Security analysis of next generation web standards

The web browser is arguably the most security-critical component in our information infrastructure. It has become the channel through which most of our information passes. In its *Security analysis of next generation web standards*, ENISA made detailed recommendations for improvements to browser security. The recommendations were made before standards became fixed (the last W3C standard deadline for comments was in August 2011). After this point, improvements become "non-negotiable". The standards that govern browsers are currently undergoing a major upgrade. This includes HTML5, cross-origin communication standards such as Cross Origin Resource Sharing (CORS) and standards for access to local data such as geo-location. In total, 51 security threats and issues have been identified and detailed in this report.

Security analysis of next generation web standards

http://www.enisa.europa.eu/act/application-security/web-security/a-security-analysis-of-next-generation-web-standards

SECURE SERVICES AND PROJECT SUPPORT

In its proposal for a European Digital Agenda, the European Commission aims to build people's trust in using the Internet, thereby creating the conditions for the Internet ecosystem to flourish. This can be achieved on two fronts: by safeguarding the integrity of information, protecting the source of information and personal data, and protecting the privacy of individuals; and by protecting the network infrastructure and support services underlying the Internet. These efforts are in alignment with the associated regulatory framework in the EU, in particular Directive 2002/58 on Privacy and Electronic Communications (also known as the ePrivacy Directive) and the Telecommunications Package Reform.

On-line services, applications and transactions are expected to bring about considerable benefits for European citizens and provide competitive advantage for the European economy. However, this can only be achieved if the economic stimuli for developing and using such applications are present and barriers are carefully controlled. Unfortunately, as of today, there is little data at the pan-European level describing such barriers and incentives.

The work of Secure Services and Project Support covers two areas: secure architectures and technologies, and privacy and trust.

Secure architectures and technologies were previously included in the ENISA resilience programme. Starting in 2008, the Agency produced a number of publications in this area, mainly covering the current and emerging technologies that enhanced resilience. The publications also provided guidelines and recommendations for future work and research. In 2011, in order to capture the existing knowledge and basing its work on it, ENISA developed an ontology and taxonomies for resilience. These were intended for use in all resilience-related activities. ENISA also extended and updated its studies on technologies and techniques for ensuring resilience.

Pilot projects in the area of privacy and trust started in 2010 and were well received by many stakeholders. Thus, work was continued on this topic in 2011. The Agency performed several studies on trust and reputation models, and ways of assessing the value of privacy. At the same time, ENISA continued its work on the implementation of the data breach notification obligation in the EU, becoming a centre of expertise in this area.

For 2011, the Secure Services and Project Support activities and tasks were defined in the ENISA Work Programme 2011 – *Securing Europe's Information Society*. The activities were included within Work Stream (WS) 2: *ENISA as a competence centre for securing future technology* and WS3: *ENISA as promoter of privacy & trust*. The work packages dedicated to Secure Services and Project Support were Work Package WPK 2.3: *Secure architectures and technologies;* WPK 3.2: *Deploying privacy & trust in operational environments*; and WP 3.3: *Supporting the implementation of the ePrivacy Directive.*

Secure architectures and technologies

Ontology and taxonomies for resilience

In 2011, ENISA developed an ontology of resilience that embeds a taxonomy of resilience. The proposed ontology introduces tools for understanding resilience as a network design target and the output of those tools when applied to resilience. The tools are classification using taxonomy, and relationship modelling using ontology, with taxonomy at its core. The ontology presented is an open, interoperable and scalable framework that is intended to lead to further developments in standardization. Ontology and taxonomy were addressed as methods that extend the role of standards in complex areas. They do so by allowing more complex scenarios to be addressed than are normally considered by standardisation. Resilience falls into this class of complex scenarios as it covers many different technologies and strategies compared with many other simpler – though still complex – protocols.

Ontology and taxonomies for resilience
http://www.enisa.europa.eu/act/it/technology-for-resilience/ontology

> "While the importance of the privacy by design principle is widely accepted, lax data protection practices are a reality among many online service providers."

Technologies with the potential to improve the security of the Internet's infrastructure

The Internet's architecture can be divided into GAN (Global Area Network), WAN (Wide Area Network), LAN (Local Area Network) and SAN (Storage Area Network) networks. Between 2008 and 2010, ENISA studied the potential of several technologies (mainly used in GAN) to improve the resilience characteristics of the Internet's infrastructure and enhance how this potential was perceived by network operators, based on their deployment status. During 2011, ENISA examined the deployment status of these technologies, and identified four others with the most relevant characteristics. The following redundancy technologies employed in these parts of the Internet were selected for the survey: IS-IS (WAN), VRRP (LAN/WAN), RSTP (LAN), Fibre Channel). These were described in detail and research was conducted on their deployment status. Conclusions were drawn and guidelines were proposed.

Review of technologies enhancing resilience and their status of deployment
http://www.enisa.europa.eu/act/it/technology-for-resilience/tech

Supply chain integrity

Supply chain integrity in the ICT industry is a topic that receives attention from both the public and private sectors. Currently, it is addressed differently in different industries. Important solutions have been developed in various areas of ICT, which have led to considerable progress and highlighted the need for a comprehensive research study dealing with supply chain integrity. ENISA launched a study on good practices among various industry segments, investigating the feasibility of bridging the gaps in developing common guidelines.

Use of advanced cryptographic techniques in Europe

The increasing use of e-government services has led to significant growth in the amount of citizens' sensitive data being transmitted over public networks (e.g. the Internet) and stored within applications that are accessible from anywhere on the Internet. The study performed by ENISA surveyed cryptographic guidelines and requirements, as well as specifications defined and used by the Member States. It was based on answers received from 13 Member States, covering almost 75% of the European Union's population. ENISA has found that many cryptographic specifications or recommendations prepared and used for e-government services recommend good practice encryption algorithms. However, according to the IT industry, many of the cryptographic solutions that they audit and test are poorly deployed; in many cases, the deployment teams for

systems or services handling unclassified information lack cryptographic expertise.

Use of advanced cryptographic techniques in Europe http://www.enisa.europa.eu/act/it/library/the-use-of-cryptographic-techniques-in-europe

Deploying privacy & trust in operational environments

Trust and reputation models

Reputation systems are a key success factor for many websites, enabling users and customers to have a better understanding of the information, products and services being provided. However, by using reputation systems, citizens of the European Union place themselves at additional risk. A study carried out by ENISA in 2011 revealed that there is a significant difference between the real-life implementation of reputation systems and the academic research that is currently being conducted. The reputation systems currently being deployed primarily facilitate and promote business transactions. They appear not to take into account or further develop academic research into privacy and trust solutions; they do not embed the research in operational systems. ENISA also identified conclusions in five core areas that covered the following points:

- Risks to users of reputation systems and the trustworthiness of risk assessment scores
- Customer communications regarding reputation systems
- Lack of clarity regarding governing legislation

Trust and reputation models http://www.enisa.europa.eu/act/it/library/trust-and-reputation-models

Study on data collection and storage in the EU

While the importance of the privacy by design principle is widely accepted, lax data protection practices are a reality among many online service providers. In view of this state of affairs, the aim of this study was to present an analysis of the legal framework applied by Member States. The framework is based on the principles of minimal disclosure and the storage of personal data for the shortest possible duration. The study does not delve deeply into the legal complexities of data protection legislation. Instead it focuses on a limited number of actual cases. It then documents how the aforementioned principles were applied in concrete legal or regulatory provisions, and how they were observed in practice.

Study on data collection and storage in the EU http://www.enisa.europa.eu/act/it/library/deliverables/data-collection

Monetizing privacy

Privacy is a fundamental human right; yet nowadays, personal data is traded like other commodities in the market place. The authors of this report consider an economic analysis of privacy as complementary to a legal analysis as it improves our understanding of human decision-making with respect to personal data. Our understanding of the cost-benefit trade-off individuals enter into when conducting purchases on the

Internet is far from complete. In a 2011 Eurobarometer Survey, 74% of Europeans stated that they see disclosing personal data as part of modern life and 43% said that they have been asked for more information than necessary when using a service or trying to access it. Understanding the economic issues concerning online privacy is a step toward defending the individual's rights. ENISA's analysis of the monetization of privacy examined the consumer's decision about disclosure or non-disclosure of personal data within a transaction to obtain a good. The results were based upon theoretical and experimental insights. The findings rely on research results that use a new economic model. ENISA gave advice for the general public and for experts, and provided research background and the theoretical modelling.

Supporting the implementation of the e-Privacy Directive (2002/58/EC)

Workshop on data breach notifications

A Data breach notifications workshop organised by ENISA had two goals – to disseminate a study on data breach notifications performed under the umbrella of the Agency Work Programme, and to gather opinions on ENISA's future work in this field. The workshop was very successful and attracted over 80 participants from all over Europe.

Workshop webpage: http://www.enisa.europa.eu/act/it/risks-and-data-breaches/data-breach-notification

Technical recommendations for the implementation of Art. 4

Building on its established capabilities, ENISA has continued to work in the area of data breach notification. In 2011, the Agency developed specific technical recommendations for the implementation of Article 4 of the e-Privacy Directive, including a practical and usable definition of a "data breach", and in particular its relationship to the definition of an "information security incident". ENISA also developed criteria for:

- Determining when a data breach has occurred
- Identifying and assessing security controls that help determine when a breach has occurred
- Identifying and assessing the risks regarding data breaches
- Developing procedures for notification when data breaches occur, in either the private or public sectors

The work also addressed the online processing of data breaches, the definition of "undue delay", and other issues. The expert group that helped ENISA in this task was composed of representatives from the EU institutions, the Art. 29 Working Party, national Data Protection Authorities and industry. The work constituted ENISA's input to the consultations on new European data protection rules.

ASSISTING MEMBER STATES WITH OPERATIONAL SECURITY ISSUES

Network and Information Security (NIS) is a public good; it requires large-scale collaboration, coordination and investment. Investment by a single organisation is not enough, because no organisation can afford to finance the required effort on its own. For this reason, governments must develop strategic plans and policies, and then compel all relevant actors to take an active part in their implementation. This can be achieved through several strategies:

1. Establish a commonly agreed upon approach to risk analysis as well as management strategies to highlight all the components or risk: risk for the organisation, risk for its direct environment (customers, personnel, etc.) and risk to European society (citizens, SMEs, etc.).
2. Develop a methodology based on the analysis of risk that ensures a positive return on security investment, if not for the organisation itself, then for society as a whole.
3. Legislation and regulation at both EU and Member State levels is necessary. Without the pressure of law, sometimes the managers of organisations neglect their responsibilities completely or else fail to give adequate priority to establishing security measures on time. Regulation and standardisation also provide guidelines for implementers of NIS. The guidelines help implementers make more efficient and focused investment efforts.
4. Training the members of communities responsible for the implementation of security mechanisms and countering threats in the cyber-space: CERTs (Computer Emergency Response Teams), CSIRT (Computer Security Incident Response Team) and SOC (Security Operational Centre), EUROPOL/CEPOL (Law enforcement authorities).

The first two strategies have been addressed through Work Stream (WS) 1: *ENISA as a facilitator for improving cooperation* of Work Programme 2011 – Securing Europe's Information Society and the other two by the activities under WS 3: *ENISA as a promoter of privacy, trust and awareness*.

ENISA has also deployed awareness raising activities to make easier the dissemination of the guidelines and research results by all the teams in the Agency, as well as to facilitate the interchange of information and networking between security experts and policy makers of different MS.

"Network and Information Security (NIS) is a public good; it requires large-scale collaboration, coordination and investment."

The most relevant achievements of ENISA during 2011 in those areas are briefly described in the following sections. Many links are provided to allow the reader to retrieve further information on the related documents, or the documents themselves.

ENISA CERT related activities

In the area of Computer Emergency Response Teams (CERTs), ENISA aims to support the EU Member States in ensuring that their respective national or governmental CERTs act as key components of their national capability for preparedness, information sharing, sustainable coordination and response. This is done by defining, together with the relevant stakeholders, baseline capabilities, and by providing the necessary means to achieve them.

Work related to CERTs / CSIRTs

"National/governmental CERTs have been created all across the EU, many of them with the support of ENISA's CERT team."

ENISA works to achieve results that are of direct use to the EU Member States and other stakeholders. Examples include good practice guides and pilot projects. However, the Agency also does more strategic work, both to prepare its own activities and to support those of others. National/governmental CERTs have been created all across the EU, for example, many of them with the support of ENISA's CERT team. More information about ENISA's strategic work is provided below.

EISAS - European Information Sharing and Alert System

In 2006 ENISA was asked by the European Commission to carry out a Feasibility study for a European-wide Information Sharing and Alert System (EISAS). More information is available at: http://www.enisa.europa.eu/act/cert/other-work/eisas.

CERT operational gaps and overlaps report

In 2011, ENISA published a report on current *CERT operational gaps and overlaps*. The report analyses the operational gaps and overlaps of national and governmental CERTs and provides some recommendations.

CERT operational gaps and overlaps

http://www.enisa.europa.eu/act/cert/other-work/gaps-overlaps-report

Secure communication with CERTs and other stakeholders

This report, delivered by ENISA in 2011, aims to give an overview of the work that was done in Work Package 1.3 of ENISA's Work Programme 2011. This identified ways to improve communication with the CERTs and other stakeholders.

Secure Communication with CERTs & Other Stakeholders

http://www.enisa.europa.eu/act/cert/other-work/secure-communication

Background information on CERTs and CSIRTs

"ENISA has been continuously producing training material to improve the operational capabilities of the CERT community."

ENISA has been continuously producing training material to improve the operational capabilities of the CERT community.

- **CERT factsheet**

A brochure that provides an overview of ENISA's work. http://www.enisa.europa.eu/act/cert/background/cert-factsheet

- **Inventory of CERT activities in Europe**

A continuously updated overview of known CERTs and their activities, in Europe and beyond.

http://www.enisa.europa.eu/act/cert/background/inv

- **An insight into CERT cooperation**

A detailed report about past and present cooperation among CERTs, and how it could be further enhanced.

http://www.enisa.europa.eu/act/cert/background/coop

The Economics of security

> "ENISA has analysed economic drivers and barriers, and has identified potential areas that have a significant impact on the economics of security."

This area of ENISA work encompasses a number of activities around the economics of security, ranging from information on risk management and risk assessment to the economic implications of managerial decisions on the implementation of security measures and tools. ENISA also collects and disseminates information about activities and events in this area.

ENISA has analysed economic drivers and barriers, and has identified potential areas (legal, policy, technical and educational) that have a significant impact on the economics of security. The Agency will identify potential areas of improvement that can boost security and resilience in public systems and networks, as well as related products and services. The work conducted also elaborates on economic issues (e.g. behavioural economics, return on investment, risk management, the economics of resilience, etc.) arising from the fulfilment of such requirements. In this way, this work package contributes to the points announced in the Digital Agenda for Europe, such as boosting Europe's economic performance and the introduction of measures to reinforce the benefits of the Single Market.

Computer Emergency Response Teams

In the area of the economics of security, ENISA has produced two deliverables:

- *Economics of Security: Facing the Challenges*

https://www.enisa.europa.eu/act/rm/EoS/EoS

- Ec*onomic Efficiency of Security Breach Notification Schemes*

https://www.enisa.europa.eu/act/rm/EoS/call-for-contributions

The target group is users, both experts and non-experts, who are interested in learning more about Risk Management, in keeping abreast of current developments and trends in that area, or in applying existing Risk Management practices to their organisation.

Risk Management

The issues in the area of Risk Management that have been addressed in 2011 include results achieved in the area of emerging risks and have been delivered in the reporting period. In particular:

- *"To log or not to log?"*: ENISA is looking ahead to 2014 to predict positive and negative effects of online, «life-logging» on citizens and society. In a new report, the risks and benefits of emerging life-logging technologies have been assessed. The Agency uses a fictional family's day-to-day lives to examine the impact on their privacy, the "family wallet", psychology, and other issues, as they put ever more personal information online. The report includes recommendations for addressing security and privacy risks.
  It examines both the advantages and risks of people's increasing use of online applications. To enjoy the benefits of life-logging technologies, people need to upload personal information – be it personal thoughts, videos, or financial data – to Internet locations over which they have little control. For individuals, that implies threats to privacy, loss of personal data control, harm to one's reputation and the possibility of psychological damage from exclusion or the feeling of constant surveillance. For commercial organisations, there is the risk of breaching data protection laws, resulting in legal sanctions and irreversible damage to the organisation's reputation. Governments may suffer the loss of public confidence if they are perceived not to be properly protecting their citizens' personal information.

  «*To log or not to log?*» Risks and benefits of emerging life-logging applications

  http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/life-logging-risk-assessment/

- *Cyber bullying & online grooming*: the report identifies the top emerging risks and makes 18 non-technical recommendations for their mitigation. Digital devices and the Internet now play a significant role in children's lives. Today's young people live their online lives in both private and educational settings. This is an environment radically different from that of their parents, during their childhood years. Risks in a child's online environment can be detrimental to their physical development and social skills, argues the ENISA Expert Group on Internet risks.

The report details a scenario of 13-year old Kristie's changed behaviour, poor grades and negative attitudes due to abuse in her online life. Many parents lose control, as they lack the knowledge and tools to support their children, the report argues. The Agency thus issues 18 recommendations to mitigate identified risks.

Cyber bullying & online grooming

http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/at_download/full-Report

In the area of Risk Management some horizontal support has been provided. In particular ENISA has supported the European Maritime Security Agency (EMSA) in a risk assessment and risk mitigation activity leading to a security policy for a maritime application. In a similar manner, ENISA has supported a Member State in setting up their National IT Security strategy by transferring knowledge in the area of National Risk Management Preparedness.

Awareness Raising

ENISA supported public and private organisations in their efforts to raise information security awareness among their employees and/or customers by providing attractive, ready-to-use sets of materials such as posters, illustrations, screensavers and video clips. This material is available for download and use in any information security training programme or awareness activity and can be uploaded to a company's own websites. ENISA also supported organisations by providing customised material and by identifying key awareness messages and areas where information security awareness should be raised.

For more information visit:

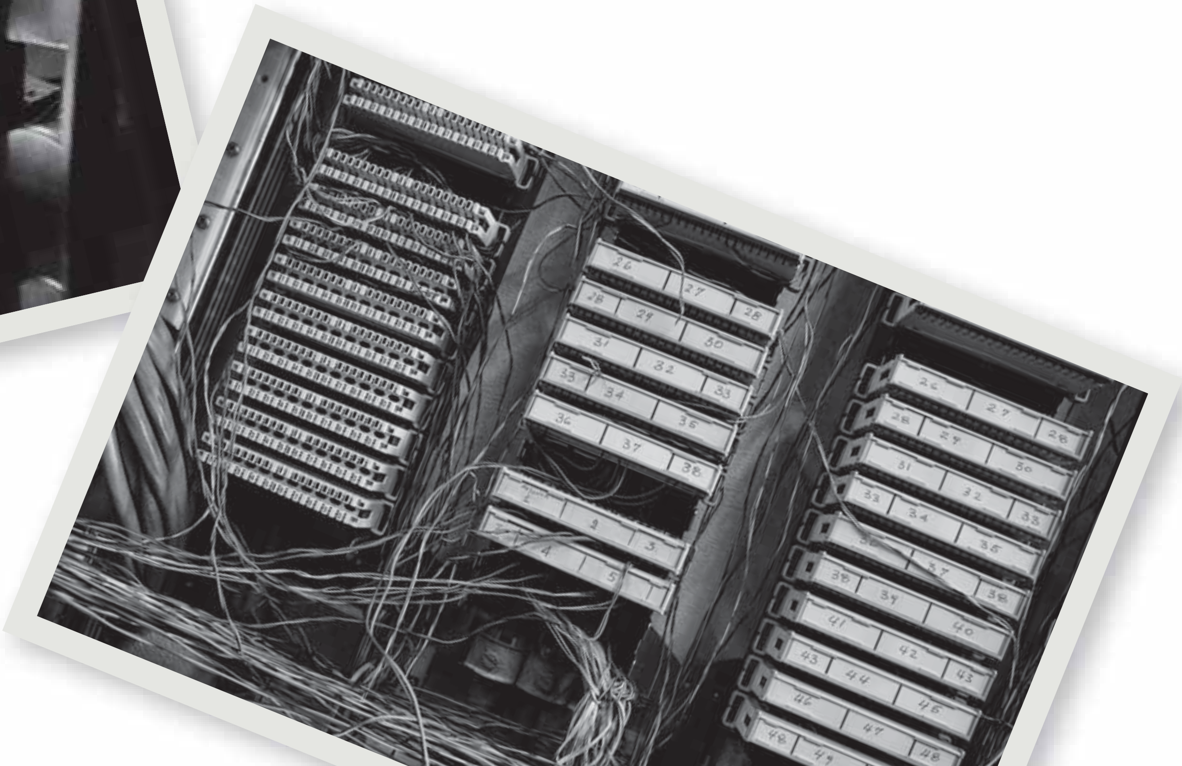
https://www.enisa.europa.eu/act/ar/achievements/achievements

European Month of Network and Information Security for All

In 2011, ENISA was asked to explore and assess various options on how a "European Month of Network and Information Security for All" could become an effective instrument for raising awareness about NIS challenges

The concept was inspired by similar campaigns that have been implemented successfully in other regions of the world for some time now. One of the key success factors for this activity would be to develop an effective structure and coordination scheme.

To this end, ENISA was asked to carry out a feasibility study by examining the possible implementation of such a campaign in addition to an overview of the prevailing elements of security days/weeks organised at the national level across Europe.



ENISA has been promoting cyber education for children

This project was in line with the Awareness Raising work stream of the EU-US Working Group on Cyber-security and Cyber-crime. The working group was established in the context of the EU-US summit of 20 November 2010 held in Lisbon.

For more information:

European Month of Network and Information Security for All

http://www.enisa.europa.eu/act/ar/deliverables/2011/europeansecuritymonth) by examining

National Cyber Security Awareness Month

http://www.enisa.europa.eu/act/ar/security_month/NCSA

National Cyber-security Awareness Campaign – "Stop. Think. Connect" (organised in the US)

www.dhs.gov/files/events/stop-think-connect.shtm

National Cyber Security Awareness Week (organised in Australia)

http://www.enisa.europa.eu/act/ar/security_month/staysmartonline

NIS in Education

The Agency has delivered a consolidated ENISA report on *Network Information Security in Education*. The report provides young digital citizens and stakeholders with an overview and highlights of good practices on how to become educated to feel and behave safer online.

The Report on Network Information Security (NIS) in Education comes at a time when education and ICT are more interrelated and interconnected than ever. The challenge of the digitally active citizen is to remain informed about the news coming from the dynamic field of ICT and of Information Security in particular.

Long life learning, formal, non-formal and informal education are all on the agenda of policymakers. Children, youth and their peers, parents and educators are all part of the discussion and ENISA recommends that they cooperate and get involved as much as possible. The material available is facilitates the easy transfer of knowledge between stakeholders. This material is a contribution towards the objective of the Digital Agenda for Europe, which states: "Youth engagement will make the Digital Agenda a reality."

ENISA's intention is to start the knowledge transfer process between all involved actors in order to achieve sustainable results that have a real impact on the Euro-

pean digital citizen. One way to achieve this is by disseminating the work done in the last few years by ENISA using a language that can be understood by the target group. The Agency, therefore, has summarised the findings of ENISA reports in the form of short summaries. Interested parties can read and use this material and, if necessary, look for further details in the full documents. The selection of the reports was done in order to deliver content that can be directly used for educational purposes.

The information in this consolidated report helps all stakeholders to be better informed, better educated and better involved in the area of Network and Information Security.

Network Information Security in Education

http://www.enisa.europa.eu/NISinEducation.pdf

ENISA maps good practice in Europe

In 2011 ENISA launched online an updated edition of its *Country Reports* on Network and Information Security (NIS) in the Member States and other European countries.

The level of preparedness for dealing with cybercrime, network attacks and network resilience varies widely across European countries. *Country Reports* features an overview and detailed, separate reports on 30 European countries, including information on stakeholders and trends.

For more information:

http://www.enisa.europa.eu/act/sr/country-reports

A **key finding** of this edition of *Country Reports* is that no pattern exists in the observed countries with respect to national NIS strategies. However, many countries are enhancing their efforts and making progress in this area. Information exchange mechanisms and cooperation amongst key stakeholders also vary from country to country. Successful NIS initiatives are outlined as blueprints for others to consider. Areas examined include security incident management and reporting, risk management and emerging risks, network resilience, privacy and trust, and awareness raising.

Country Reports offers a unique overview of the current NIS landscape in the 27 EU Member States and the three European Economic Area countries (EEA: Iceland, Lichtenstein and Norway), without comparing them individually with each other, given the different historical origins of NIS structures in these states.

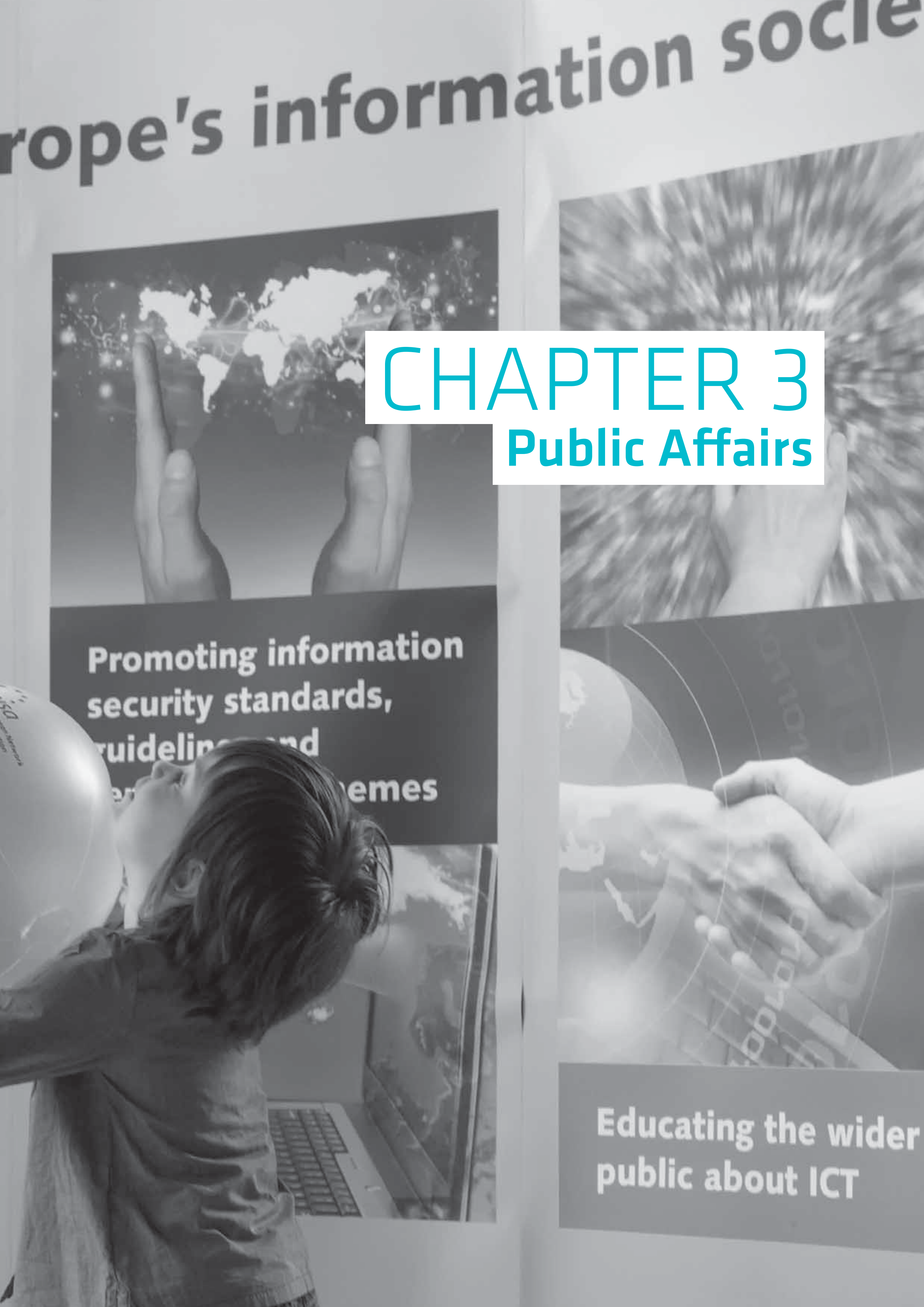
Each national report outlines: the individual country's NIS strategy, regulatory framework and major policy measures; key stakeholders and their mandate, role and responsibilities. The reports provide an overview of the main NIS activities, stakeholders' interactions, information exchange mechanisms, co-operation platforms, and country-specific facts, trends, and good practice case studies.

Country Reports are available for download at:

http://www.enisa.europa.eu/act/sr/country-reports

enisa
European Network and Information Security Agency
Securing Eu
Cultivating trust and confidence in the use of ICT
curing information
rastructure
g the fight
er crime
Love

CHAPTER 3
Public Affairs


rope's information socie
Promoting information security standards, uidelin nd emes
Educating the wider public about ICT

COMMUNICATING CYBER SECURITY

Throughout 2011, ENISA's communications activities focused on providing stakeholders with accurate, well-targeted information, precisely when it was needed and in easily accessible formats. The Agency's Public Affairs Unit (PAU) kept ENISA in the spotlight by managing and updating the ENISA website, and by creating wider public awareness of ENISA's reports and other work via the media and special events. In addition, PAU achieved synergies with other EU bodies at shared events, such as an Agencies Day in Brussels, and a Digital Agenda 'Going Local' event on Crete. The latter event highlighted the benefits of information communication technology for all of Europe's citizens.

Major Public Affairs achievements in 2011 included gaining Europe-wide coverage for *Cyber Atlantic 2011* – the first ever joint EU-US cyber security exercise, and a high level event in Brussels. This brought together representatives of industry, the European Parliament, the European Commission, and Europol.

At the start of the year, the structure of the Public Affairs Unit was changed, under the direction of a new Head of Unit, to strengthen in particular the team's planning, delivery and evaluation capabilities.

Achieving impact across Europe and locally

Communicating the results of ENISA's operational work is crucial for the development of a stronger cyber-security culture, supporting a safe and sustainable digital society. Outreach channels used by ENISA's Public Affairs Unit include public relations campaigns, digital communications, internal communications, and media activity and events conducted across the EU. A strong ENISA 'corporate brand' runs through all of these, and helps the Agency to deliver consistent and coherent messages in all of its communications.

This year saw the EU 2020 'Going Local' initiative bring ENISA closer to the Region of Crete, where the Agency's headquarters are located. Working with the Directorate General for the Information Society (DG Infso) team ENISA presented information on the importance of IT security for Europe's citizens. The Agency also strengthened its ties with local authorities and media. Acknowledging the importance of Agencies in the European regions, ENISA has worked with local authorities and Chambers of Commerce, and in addition schools have participated in open door sessions. ENISA is also distributing information through a new *Europe Direct Info Point* that has opened its doors in Heraklion.

Coherence and consistency – communication planning

Corporate communications are fully aligned with ENISA's operational and policy development work. All communications activities fall within the scope of six planned areas of Public Affairs activity in ENISA's work programme. This ensures that information forms part of a coherent and consistent narrative that supports the Agency's work.

To ensure continued consistency in Agency communications, in 2011 a contract was awarded for the creation of a new ENISA brand identity that will be unveiled in

2012. In addition, contracts were signed to provide the Agency with comprehensive editorial, graphic design and printing services, to enhance the quality and consistency of ENISA's communications.

Media outreach

ENISA's media programme gives the Agency an opportunity to reach many more people than it can through direct means. In 2011, the Agency issued 24 media releases, and ran 60 individual news items on its website. As part of ENISA's work to make its messages accessible to stakeholders across Europe, the Agency routinely issues media releases in five EU languages, to press, radio, television and web-based news organisations. These include the mainstream media, as well as specialist NIS publications and websites. Evaluation of the Agency's media output shows that in 2011, this work generated several stories in European news media, News stories on the ENISA website received more than 90,000 direct hits in 2011.

A major media event was the Cyber Atlantic 2011 security exercise and the subsequent media briefing in Brussels. Cyber Atlantic was the first ever joint cyber security exercise between the EU and the US, and required a fully coordinated communication strategy, drawn up by ENISA in close collaboration with the Commission, Member States and the US Department of Homeland Security. The media coverage of the successful exercise generated a high impact, as illustrated in ENISA's media monitoring and in web statistics.

Other media outreach work included press conferences targeted both at media in specific countries, and centred around NIS special interest areas. For example, in November, the German Permanent Representation to the EU hosted an ENISA conference for Brussels-based German language media, generating extensive coverage.

The Agency continued its awareness advertising throughout 2011, running campaigns in Brussels-based publications as well as in the Greek media, as part of its local community outreach work.

Web communications

ENISA's website continues to be the Agency's principal communications channel, and in 2011 development work was carried out to enhance its structure, appearance and ease of use. The focus was on user accessibility, but 'behind-the-scenes' developments included a greater ability for the Agency to gather and analyse statistics on which web pages and reports are most popular, and search engine optimisation to help users find ENISA information more easily. The tagging of ENISA's reports was also revised to improve search results.

Technical improvements in 2011 included the migration of ENISA's website and all portals to Version 4 of the Plone content management system, and the application of all security patches to the Zope application and PHP scripting used by the ENISA site.

A dedicated web portal for ENISA's Management Board (MB) was further developed and enhanced. It now incorporates a "collaboration area" where the MB members can have online discussions and exchange ideas. A video-wiki was also added to enhance the user experience.

In addition to incremental improvements made throughout 2011, a full website restructuring is being planned. This will focus on developing a new, modern and more functional and intuitive look and feel.

Publications and brand identity

ENISA strives to communicate with a broad audience of people interested in its work. These range from European citizens to expert stakeholders of the Agency. In 2011, ENISA focused on long-term communication, and launched a new set of corporate publications, all available on the Agency's website. The *General Report 2011* is published in both hard copy and digital versions and disseminated on CD-ROM as well as the Agency's website. The goal is to reach out to as many recipients as possible. A new newsletter for our Management Board was created, and work is continuing on a brand new ENISA newsletter in early 2012. Brand material has regularly been produced and distributed both during corporate events and to visitors. In addition, a poster campaign for children's safety online was initiated in 2011, and is being rolled out to MS in 2012.

Work commenced in 2011 on a new brand image for ENISA, as well as a revamping of the corporate identity communicated through all Agency channels. The new brand positioning is to be put in place during 2012.

Internal communication

A sound, two-way flow of internal communication is essential for consistent and credible external communication. The activities revolving around internal communication shape ENISA's culture, which is developed through staff meetings and events, as well as through an in-house intranet and staff interviews. During 2011, internal surveys and team-building events took place to reinforce common goals for all staff and encourage consistent interaction. Regular staff meetings as well as unit and department meetings are held to guarantee a clear vision of our role as European ambassadors in the field of cyber security. In 2011, the broader use of ENISA's intranet offered common ground for all staff to easily manage administrative procedures, as well as participate in leisure events and general planning. In conjunction with the Technical Competence Department, in 2011 the Public affairs Unit also re-launched ENISA's Management Board Newsletter, with a focus on "bite sized" pieces of information, hyperlinked to in-depth information. The format has proved successful, and a more general ENISA newsletter is set to launch in 2012.

Europe Day celebrations

Conferences and joint events

ENISA was involved in numerous high-level European conferences in 2011. These included ENISA's own events, as well as joint conferences and speaking events. During 2011, ENISA participated in or co-ordinated 52 events and conferences throughout Europe and further afield.

One of the key events during the year was ENISA's High-Level Panel Discussion, which took place in October in Brussels. The panel discussion dealt with future challenges in network and information security. It brought together experts from the European Commission, Parliament, Council, Member States and industry. An audience made up of people from the worlds of network and information security, government and politics had the opportunity to watch the debate and put questions to the panel.

In addition to these events, the Public Affairs Unit provided support to the Executive Director for his participation in events across Europe. These included the European Parliament Hearing on the proposed ENISA mandate in May, as well as the Council Working Group in September, where the Executive Director made the presentation, 'ENISA today and in the future'.

IRELAND
DUBLIN
LONDON
PARIS
FRANCE
Marseille
MADRID
SPAIN
PORTUGAL
LISBOA
Gibraltar

CHAPTER 4
Relations with ENISA stakeholders

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 Stakeholders Group (composed of multiple stakeholders), as well as the Agency's informal networks and expert working parties, give ENISA unparalleled insights and access to public and private sector Network and Information Security (NIS) experts. This in turn enables ENISA to identify emerging risks and gain new insights in order to help Member States and private sector organisations better prepare themselves for challenges in a proactive and professional manner, as well as 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. It must ensure consistency between the Agency's work and activities conducted by Member States as well as at EU 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 EU's legislative and policy priorities for Network and Information Security. Lastly, the Management Board also adopts the Agency's budget.

The full Management Board met twice in 2011: in March (Budapest, Hungary) and October (Athens, Greece).

The preparation and subsequent adoption of the Work Programme for 2012, the (amended) 2011 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 July 2011 in Greece. The meeting focused on setting the priorities and themes of the Work Programme 2012. In addition, an informal Management Board meeting on strategic guidance for Work Programme 2013 was held in Athens in November 2011.

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

For a list of members of the Management Boards, 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 2010.

The PSG met formally twice in 2011, in April and November. An informal joint meeting with the Management Board was also held in July. The purpose of that meeting was to continue discussing ENISA's Work Programme 2012.

A meeting between the PSG and National Liaison Officers (NLOs) was held in November in Athens. The discussion focused on ways to improve the dissemination of results.

Responding to requests for assistance from Member States

In 2011, ENISA received eight requests for assistance from Member States – a marked increase over the two received in 2010. These requests, made under Article 10 of the ENISA Regulation, often require the provision of highly technical support at short notice to the Member State concerned. In response to this need, ENISA established a Mobile Assistance Team (MAT) in 2011. The MAT works from the Agency's branch office in Athens.

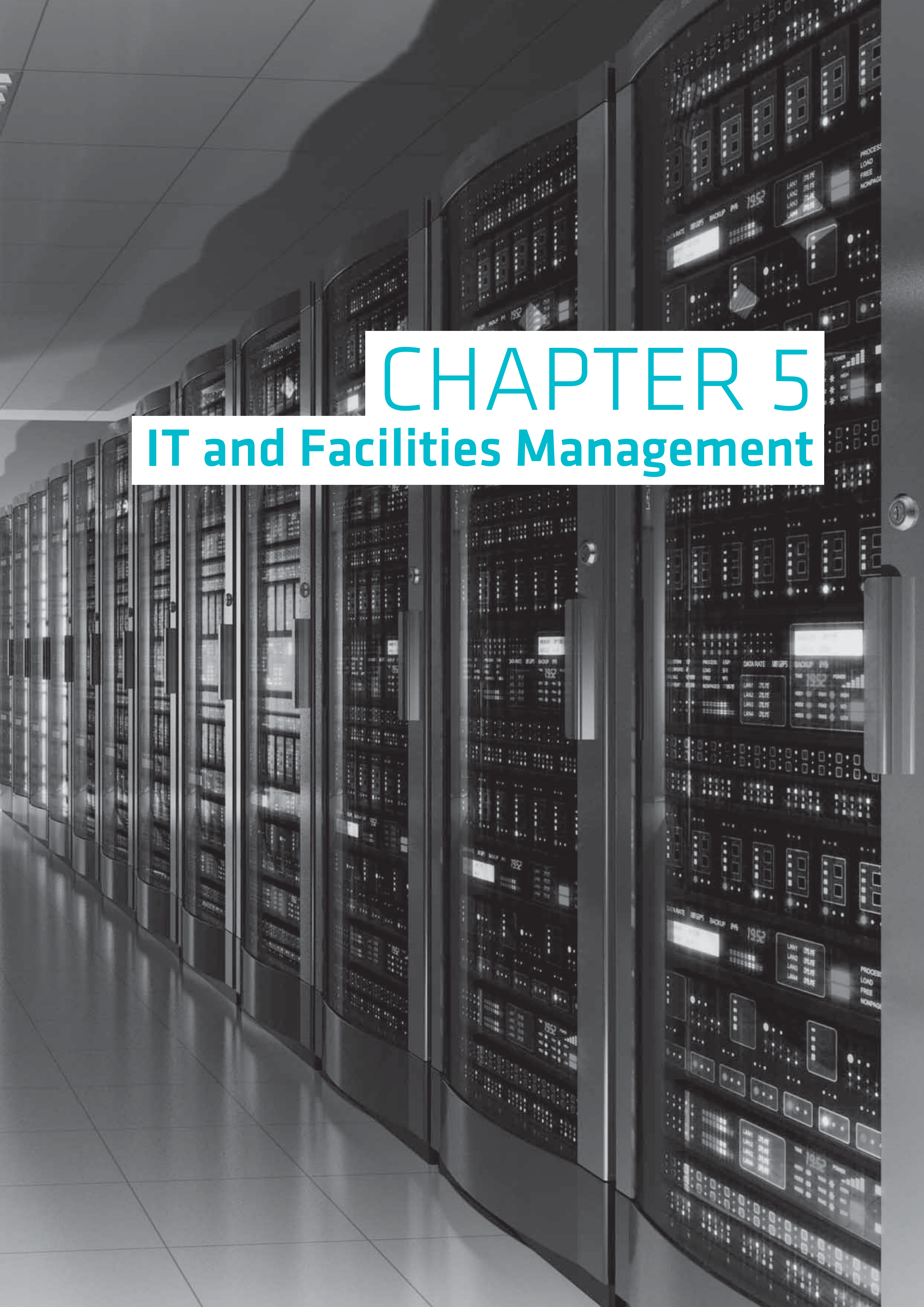
National Liaison Officer (NLO) network

ENISA's network of National Liaison Officers (NLOs) continued to play a vital role in disseminating the Agency's work and gathering feedback to help ensure that communications are reaching their target audiences. The NLOs are members of staff in Member State government departments who perform their ENISA role as an additional responsibility. Given their positions, the NLOs are uniquely placed to act as a link between ENISA and Member States. The Agency greatly appreciates the work its NLOs perform, and the 2011 joint meeting between the NLOs and ENISA's Permanent Stakeholder Group (PSG) provided an opportunity to find synergies between these two important groups of ENISA "ambassadors".

Management Board members at the Budapest meeting

Joint meeting of PSG members and NLOs

BACKUP
1952
DATA RATE



CHAPTER 5
IT and Facilities Management

Infrastructure

In early 2011 a new, centralised system for managing software on computers was rolled out in preparation for the replacement of all user computers, screens and keyboards. The new computers run Windows 7 and have Office 2010. The roll out went very smoothly. The new computing environment has led to an improvement of the end-user experience. Larger screens have also helped to improve the work experience while the smaller size of the computers, with speakers built into their screens, means that this equipment takes up less space on desktops.

Another project, the outsourcing of hosting and development related to the ENISA website and portals, went ahead as planned and was successfully concluded. Responsibility for the websites was transferred to the Public Affairs Unit. A further project was the rollout of a new system to automate flexi-time, which had previously been paper-based.

In preparation for a planned outsourcing of email to the Cloud, the email system was migrated to the latest version of Exchange and extensive testing commenced of Office 365 Cloud services. These services not only cover email, but also include Lync, a communication tool offering instant messaging, online meetings, desktop and application sharing, and presence. A tool like Lync has become a requirement given the high degree of workforce mobility. The technical evaluation of Office 365 was concluded at the end of the year with the plan to roll it out to users in phases in early 2012, following further analysis of such aspects as privacy and data protection.

ENISA hosts heads of IT from EU agencies

Following a request from other EU agencies, ENISA IT Services successfully hosted the bi-annual two-day meeting of the heads of IT of the various EU agencies. Given the high degree of interest in cloud computing as well as CERT activities, and more generally IT Security, various ENISA experts gave presentations and were available to offer advice and information to the more than forty delegates who attended.

A new work management system, Matrix, was tested and put into operation in December. This system, which contains several different modules, will allow ENISA to better manage its Work Programmes, projects, resources, and procurements and tenders. It has been in operation since 1st January 2012.

IT Risk Assessment conducted by Internal Audit Services (IAS)

A preliminary IT Risk Assessment was conducted by the Internal Audit Services (IAS) of the European Commission. ENISA performed well overall. The only significant weakness identified was the updating and testing of the Business Continuity Plan (BCP). The testing of the BCP has been planned for the second half of 2012, following the Agency's move to its new building.

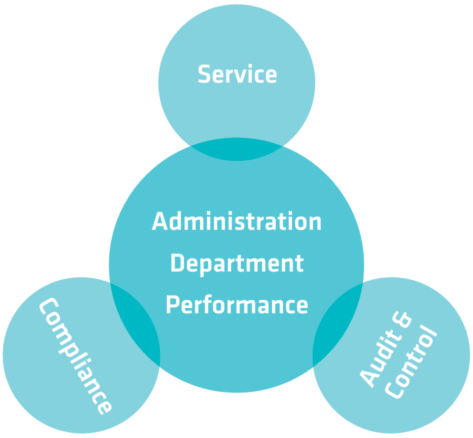
IT and Facilities Management Unit (ITFMU) created

In November, responsibility for ENISA's physical security and facilities management, and the two staff members covering these areas, was transferred to the Head of IT, resulting in the creation of the IT and Facilities Management Unit (ITFMU). This enables a more efficient use of Agency resources and will bring benefits when ENISA moves to the new building. The move is currently scheduled to take place after May 2012. ENISA has been working closely with the Foundation for Research and Technology Hellas (FORTH) to ensure that ENISA's requirements are adequately taken into consideration. This project will be a big challenge in 2012!

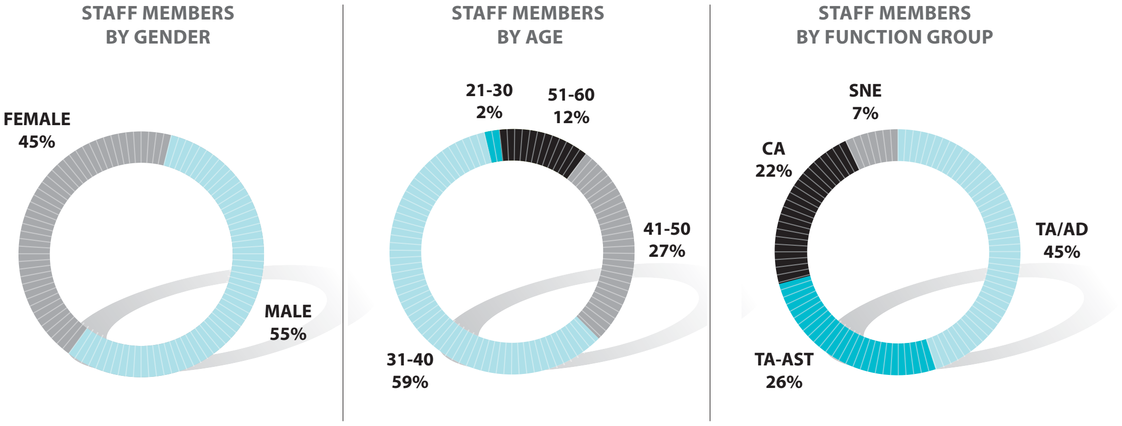
ENISA's new building under construction

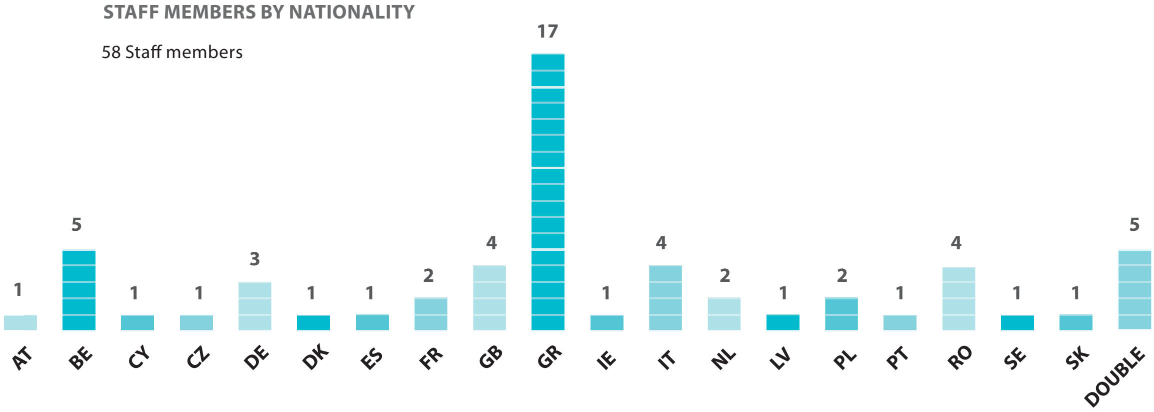
CHAPTER 6
Administration

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 tasks of the department are represented 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. As an EU Agency, ENISA benefits from having a diverse multi-national workforce. Some statistics regarding personnel at ENISA are presented below:[1]





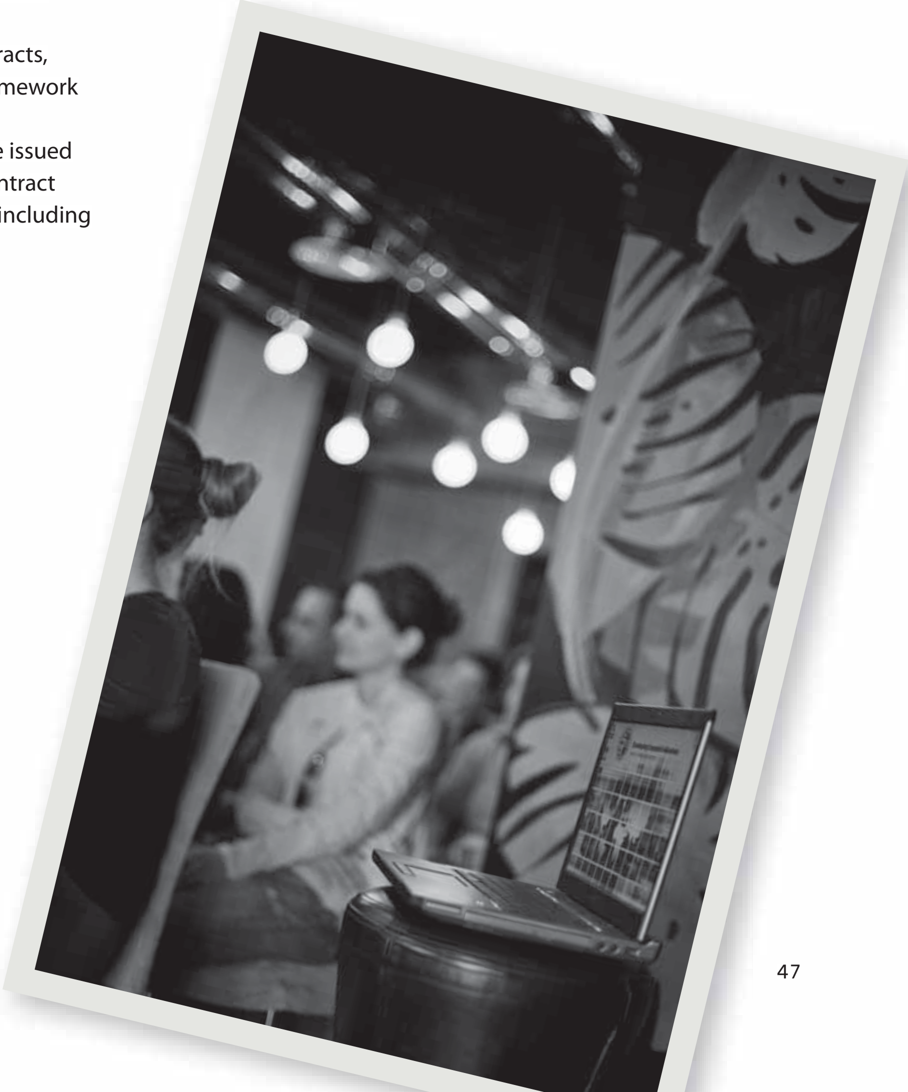
[1] Last update: 31 December 2011.

In 2011, the Agency committed its appropriations at a rate of 100% (99.95% in 2010) in order to carry out its operational activities specified in the Work Programme 2011, as well as administrative tasks that are necessary to ensure compliance and services made available by the Agency. Payments reached the level of 85.82% (75.46% in 2010, a jump of 10% compared to last year) of the total appropriations managed. Both commitment and payment rates are historical highs for the Agency, and demonstrate an increased capacity utilisation of the Budget. An overview of the year's performance follows below:

Budget Title	Description	Budget	Committed	%	Paid	%
		('000 EUR)	('000 EUR)		('000 EUR)	
Title 1	Staff expenditure	5,021	5,021	100%	4,887	97%
Title 2	Administrative expenditure	677	677	100%	446	66%
Title 3	Operating expenditure	2,405	2,405	100%	1.621	67%
Total		**8,103**	**8,103**	**100%**	**6.954**	**86%**

The outturn of contracts awarded as a result of procurement procedures contracted in 2011, is as follows:

- Contracts: 32, including 24 service contracts, 2 framework service contracts and 1 framework supply contract.
- Purchase orders: 218, 111 of which were issued under an existing framework service contract
- Procurement procedures launched: 31, including 10 open procedures



FINANCIAL REPORTING

Balance Sheet

	Notes	31.12.2011	31.12.2010
I. Non Current Assets		**252.222**	**300.782**
Intangible fixed assets	1	14.658	19.232
Tangible fixed assets	1	237.564	281.550
II. Current Assets		**1.565.971**	**3.184.067**
Short-term receivables	2	81.347	66.686
Cash and cash equivalents	3	1.484.624	3.117.381
Total Assets		**1.818.193**	**3.484.849**
III. Non Current Liabilities		**0**	**0**
Long-term provision for risk and charges	4	0	0
IV. Current Liabilities		**1.105.268**	**2.076.973**
EC Pre-financing Received	5	129.295	774.858
EC Interest Payable	5	42.877	83.506
Accounts payable	5	220.792	498.817
Accrued Liabilities	6	562.400	669.792
Short-term provision for risk and charges	7	149.904	50.000
Total Liabilities		**1.105.268**	**2.076.973**
V. Net Assets			
Accumulated result		1.407.876	1.200.233
Result for the year		-694.950	207.643
Total Net Assets		**712.925**	**1.407.876**
VI. Contingent assets and liabilities			
Contingent assets	8	42.884	0
Contingent liabilities	8	676.804	1.253.158
Total Contingent assets and liabilities		**719.688**	**1.253.158**

Economic Outturn Account

	Notes	2011	2010
Revenue from the Community Subsidy	9	7.973.626	8.021.504
Other revenue	10	424	0
Total Operating Revenue		**7.974.050**	**8.021.504**
Administrative expenses		-6.186.440	-5.553.227
Staff expenses		-4.780.987	-4.448.485
Fixed asset related expenses		-165.303	-155.919
Other administrative expenses		-1.240.150	-948.823
Operational expenses		-2.479.880	-2.257.823
Total Operating Expenses	11	**-8.666.320**	**-7.811.050**
Surplus/(Deficit) from Operating Activities		-692.270	210.454
Financial expenses		-1.297	-1.158
Exchange rate loss		-1.383	-1.653
Surplus/(Deficit) from Ordinary Activities		**-694.950**	**207.643**
Economic Result for the Year		**-694.950**	**207.643**

Cash Flow Statement

	2011	2010
Surplus/(deficit) from ordinary activities	-694.950	207.643
Operating activities		
Amortization (intangible fixed assets)	14.591	15.419
Depreciation (tangible fixed assets)	150.712	**140.500**
Increase/(decrease) in Provisions for liabilities	99.904	-13.441
(Increase)/decrease in Short term Receivables	-14.661	102.698
Increase/(decrease) in value reduction for doubtful debts	0	0
Increase/(decrease) in Accounts Payable	-1.071.609	-543.526
Gains on sales of Property, Plant and Equipment	0	0
Net cash Flow from operating activities	**-1.516.013**	**-90.707**
Cash Flows from investing activities		
Purchase of tangible and intangible fixed assets	-116.744	-60.120
Proceeds from tangible and intangible assets	0	0
Net cash flow from investing activities	**-116.744**	**-60.120**
Net Increase/(decrease) in cash and cash equivalents	-1.632.757	-150.827
Cash at the beginning of the period	3.117.381	3.268.209
Cash at the end of the period	**1.484.624**	**3.117.381**

Statement of Changes in Capital

	Reserves	Accumulated Surplus / Deficit	Economic result of the year	Capital
Balance as of 1 January 2011	0	1.200.233	207.643	1.407.876
Allocation of the Economic Result of Previous year		207.643	-207.643	0
Economic result of the year			-694.950	-694.950
Balance as of 31 December 2011	**0**	**1.407.876**	**-694.950**	**712.925**

enis
Securing inf
infrastructu

APPENDIX

sa
uropean Network
d Information
rity Agency
Securing Europe's information socie
Cultivating trust and confidence in the use of ICT
forma
re
upporting the fight
gainst cyber crime
omoting information
ecurity standards,
guidelines and
certification sche
Educating the wide
public about ICT
Love

APPENDIX 1: MEMBERS OF THE MANAGEMENT BOARD

As of 13 February 2012

ENISA's Management Board includes one representative of each EU Member State and three representatives appointed by the European Commission. There are also three non-voting members, proposed by the Commission and appointed by the Council, who represent respectively:

- The Information and Communication Technology industry
- Consumer groups
- Academic experts in Network and Information Security

Finally, the Management Board also includes three observers from the European Economic Area (EEA) Member States – Liechtenstein, Norway and Iceland. The Management Board is chaired by Mari Herranen (Finland).

LIST OF ENISA MANAGEMENT BOARD REPRESENTATIVES AND ALTERNATES

COMMISSION REPRESENTATIVES

Representative	Alternate
Robert MADELIN *Director-General DG Communications Networks, Content and Technology* tel: +32 229 63338 robert.madelin@ec.europa.eu	**Giuseppe ABBAMONTE** *Head of the Unit in charge of Trust and Security DG Communications Networks, Content and Technology* giuseppe.abbamonte@ec.europa.eu
Paul TIMMERS *Director in charge for Sustainable and Secure Society DG Communications Networks, Content and Technology* paul.timmers@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 STATES REPRESENTATIVES

Member State	Representative	Alternate
Austria	**Reinhard POSCH** *Chief Information Officer* tel: +43-1-53115/6152 reinhard.posch@cio.gv.at	**Herbert LEITOLD** *A-SIT, Secure Information Technology Center - Austria Institute for Applied Information Processing and Communication, IAIK Graz* tel: +43-316-873-5521 herbert.leitold@iaik.at
Belgium	**Daniel LETECHEUR** *Information Security Analyst* *Fedict* daniel.letecheur@fedict.belgium.be	**Dr. Stéphane VAN ROY** *Engineer-Advisor* *BIPT* Stephane.Van.Roy@bipt.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	**Jiří PRŮŠA** *Director of Department of the Main Architect of eGoverment* *Ministry of Interior of the Czech Republic* jiri.prusa@mvcr.cz	**Marie SVOBODOVÁ** *Department of the Main Architect of eGoverment* *Ministry of Interior of the Czech Republic* tel: +420 974 817 544 marie.svobodova@mvcr.cz
Denmark	**Flemming FABER** *Senior Adviser* *Ministry of Defence Project Office for Cyber Security Danish GovCERT* tel: +45 3545 0364 ff@itst.dk	**Thomas KRISTMAR** *Head of Danish GovCERT* *Ministry of Defence Project Office for Cyber Security Danish GovCERT* tel: +45 3337 9104 tkr@itst.dk
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** *CHAIR OF ENISA MANAGEMENT BOARD* *Senior Adviser* *Ministry of Transport and Communications, Communications Policy Department* tel: +358.9.160 28305 fax: +358.40.720 1693 mari.herranen@lvm.fi	**Pauli PULLINEN** *Senior Officer* *Ministry of Transport and Communications* *Communications Policy Department* pauli.pullinen@lvm.fi
France	**Patrick PAILLOUX** *Director General of ANSSI* *(French Network and Information Security Agency)* tel: +33 1 71 758401 patrick.pailloux@ssi.gouv.fr	**Jean-Baptiste DEMAISON** *ANSSI, International Relations* rit.sr.eu@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

Member State	Representative	Alternate
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* *International Representative National Cybersecurity Center* tel: +36 1 301 2030 fax: +36 1 353 1937 Ferenc.Suba@cert-hungary.hu	
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 of Instituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI), Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, Department of Communications, 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	**Saulius STAROLIS** *Head of Electronic Communications Unit* *The Ministry of Transport and Communications of the Republic of Lithuania* saulius.starolis@sumin.lt	**Dr. Rytis RAINYS** *Head of Network and Information Security Department of the Communication Regulatory Authority of Lithuania* rytis.rainys@rrt.lt
Luxembourg	**François THILL** *Accréditation, notification et surveillance des PSC* tel: +352 478 4165 francois.thill@eco.etat.lu	**Pascal STEICHEN** *Ministry of the Economy and Foreign Trade* *Department for electronic commerce and information security* tel: +352 478 4179 fax: +352 478 4311 pascal.steichen@eco.etat.lu
Malta	**George ZAMMIT** *Assistant Director* *Cabinet Office, Office of the Prime Minister* george.v.zammit@gov.mt	**Rodney NAUDI** *Malta Information Technology Agency (MITA)* tel: +356 2599 2621 / +356 7947 4747 fax: +356 2123 4701 rodney.naudi@gov.mt
Netherlands	**Edgar DE LANGE** *Senior policy adviser Ministry of Economic Affairs, Agriculture and Innovation* *Dir.-Gen. for Energy, Telecommunications and Markets* 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

Member State	Representative	Alternate
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	**José TORRES SOBRAL** *DiretorGeral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança* jtsobral@netcabo.pt	**Paulo MATEUS** *Professor Associado do Departamento de Matemática do Instituto Superior Técnico e Coordenador do "Security and Quantum Information Group" (SQIG) do Instituto de Telecomunicações* pmat@math.ist.utl.pt
Romania	**Victor VEVERA** *Director General CERT Romania* victor.vevera@cert-ro.eu	**Bogdan POPESCU** *Deputy Director General CERT Romania* *bogdan*.popescu@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** *Director 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
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** *Senior Adviser* *Office of Director-General Swedish Post and Telecom Agency (PTS)* anders.johanson@pts.se
United Kingdom	**Giles SMITH** *Information Economy - Security and Resilience, Department for Business, Innovation and Skills* giles.smith@bis.gsi.gov.uk	**Robert PRITSCHARD** RobertP@csoc.gsi.gov.uk

MEMBER STATES 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** *Chair of the CEPIS Legal and Security Issues Network/Chair of Mobile Business & Multilateral Security, Council of European Professional Informatics Societies/ Goethe University Frankfurt* tel: +49 69 798 34701 kai.rannenberg@cepis.org	**Niko SCHLAMBERGER** *President Slovenian Society INFORMATIKA Statistical Office of the Republic of Slovenia, Secretary* tel: + 386 1 2415 295 niko.schlamberger@gmail.com

MEMBER STATES REPRESENTATIVES

Group	Representative	Alternate
Iceland	**Björn GEIRSSON** *Director of Legal Divison 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	**Christine HAFSKJOLD** *Senior Adviser* *Norwegian ministry of government administration, reform and church affairs Department of ICT policy and public sector reform* christine.hafskjold@fad.dep.no

APPENDIX 2: THE PERMANENT STAKEHOLDERS GROUP (PSG)

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 expressions of interest. Each PSG member has proven abilities and expertise in fields relevant to the PSG mandate and has the capacity to contribute to ENISA's activities and 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, and different user and consumer communities.

THE PERMANENT STAKEHOLDERS'GROUP 2010-2012

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	Chief Product Security Officer	SAPAG	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	Qualys Inc.	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: ACRONYMS AND ABBREVIATIONS

ARECI	Availability and robustness of electronic communications infrastructure
BCP	Business Continuity Plan
CEPOL	European Police College
CIIP	Critical Information Infrastructure Protection
CIIs	Critical Information Infrastructures
CORS	Cross Origin Resource Sharing
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
EP3R	European Public-Private Partnership for Resilience
EISAS	European-wide Information Sharing and Alert System
FORTH	Foundation for Research and Technology Hellas
IAS	Internal Audit Services
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
MARIE	Mutual Aid for Resilient Infrastructure in Europe
MS	Member State
NCPs	National Cyber Contingency Plans
NIS	Network Information Security
NLOs	National Liaison Officers
PPPs	Public-Private Partnerships
PSG	Permanent Stakeholder Group
SAS	Secure Applications and Services group
SCADA	Supervisory Control and Data Acquisition (industrial control systems)
SOC	Security Operational Centre
SOPs,	Standard Operating Procedures
W3C	World Wide Web Consortium

APPENDIX 4: ENISA DELIVERABLES

Deliverables Produced by ENISA during 2011	WPK
Technical Guideline on Reporting Incidents http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting	1.1
Technical Guideline for Minimum Security Measures http://www.enisa.europa.eu/act/res/reporting-incidents/minimum-security-requirements	1.1
Exercise Scenario Development Handbook (available upon request please contact Panagiotis.Trimintzios@enisa.europa.eu)	1.2
Status of CYBER EUROPE 2012 – the ExPlan (Exercise Plan) (https://resilience.enisa.europa.eu/eu-exercises/)	1.2
Cyber Exercise Seminars Report in 2011 (available upon request please contact Panagiotis.Trimintzios@enisa.europa.eu)	1.2
Proactive detection of network security incidents report : http://www.enisa.europa.eu/act/cert/support/proactive-detection	1.3
Updated ENISA inventory of CERTS in Europe: http://www.enisa.europa.eu/act/cert/background/inv	1.3
Two TRANSITS training courses were supported by ENISA during Q4 2011.	1.3
Secure communication with the certs & the other stakeholders: http://www.enisa.europa.eu/act/cert/other-work	1.3
A flair for sharing - encouraging information exchange between CERTs – A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe : http://www.enisa.europa.eu/act/cert/support/legal-information-sharing	1.4
CERT operational gaps and overlaps report: http://www.enisa.europa.eu/act/cert/other-work	1.4
6th CERT Workshop on cybercrime, 3-4/10/2011, Prague, Czech Republic: http://www.enisa.europa.eu/act/cert/events/6th-workshop-cybercrime	1.5
Participation and contribution to work program of the High-Level IoT expert group (done).	2.1
Conference on cloud assurance	2.1
Survey and analysis of security parameters in cloud SLAs across the European public sector (http://www.enisa.europa.eu/act/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector	2.1
Top Ten Smartphone Controls for Developers (http://www.enisa.europa.eu/media/news-items/top-ten-smartphone-security-controls-for-developers)	2.1
Interdependencies of ICT on Maritime Sector (www.enisa.europa.eu/act/res/other-areas/cyber-security-aspects-in-the-maritime-sector)	2.2
Ecting Industrial Control Systems. Recommendations for Europe and Member States: https://www.enisa.europa.eu/act/Resilience%20and%20CIIP/critical-infrastructure-and-interdependencies/scada-industrial-control-systems	2.2
Good practices on mutual aid assistance and co-ordinated response and recovery measures : www.enisa.europa.eu/act/res/other-areas/mutual-aid-agreements)	2.2

Deliverables Produced by ENISA during 2011	WPK
Review of technologies enhancing resilience and their status of deployment : http://www.enisa.europa.eu/act/it/technology-for-resilience/tech	2.3
Use of advanced cryptographic techniques in Europe: http://www.enisa.europa.eu/act/it/library/the-use-of-cryptographic-techniques-in-europe	2.3
EISAS roadmap: http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas	2.4
EISAS basic toolset report: http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas	2.4
EISAS 'enhanced' report: http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas	2.4
Economics of Security: Facing the Challenges - A multidisciplinary assessment : http://www.enisa.europa.eu/act/rm/Economics-of-Security	3.1
Trust and reputation models : http://www.enisa.europa.eu/act/it/library/trust-and-reputation-models	3.2
Workshop on data breach notification : http://www.enisa.europa.eu/act/it/risks-and-data-breaches/data-breach-notification/data-breach-notifications-in-europe-2013-the-way-forward	3.3
Technical recommendations for the implementation of the Art.4 of ePrivacy Directive : http://www.enisa.europa.eu/act/it/risks-and-data-breaches/dbn	3.3
European month of network and information security for all – A feasibility study : http://www.enisa.europa.eu/act/ar/deliverables/2011/europeansecuritymonth	3.4

Deliverables Produced by ENISA during 2011 and published during 2012	WPK
Good practice guide on national contingency plans	1.2
Report on Cyber Atlantic 2011	1.2
First version of a good practice collection on CERTs and law enforcement	1.5
Good practices on interconnected networks	2.2
Study on smart grids	2.2
Economic efficiency of security breach notification	3.1
Study on monetizing privacy	3.2
Report on minimal disclosure and other principles supporting privacy and security requirements	3.2
Study on supply chain integrity – challenges and guidelines	3.3
Technical implementation guidelines on Article 4 implementation	3.3

European Commission

General Report 2011
European Network and Information Security Agency

Editing and design by De Visu Digital Document Design, BE
Published in August 2012

Luxembourg: Publications Office of the European Union, 2012
64 pp. – 29.7cm x 21cm
ISBN: 978-92-9204-061-1
ISSN: 1830-981X
Catalogue no.: TP-AB-12-001-EN-C
doi 10.2824/24282

TP-AB-12-001-EN-C

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

Publications Office

ISBN 978-92-9204-061-1
9 789292 040611