enisa
European Network
and Information
Security Agency

ENISA GENERAL REPORT 2012

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

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2013

ISBN 978-92-9204-065-9

doi:10.2824/16829

Printed in Belgium

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

A MESSAGE FROM THE EXECUTIVE DIRECTOR

Cyber Cooperation and future directions

The year 2012 has been ENISA's most successful to date, with all areas of our Work Programme completed on time, and a level of financial performance achieved that has surpassed our excellent performance in 2011. For an agency that deals with the ever-changing world of cyber security, however, success will always be determined by how we manage future challenges, rather than how we performed in the past.

Information technology now supports every aspect of our modern lives, and the borders between the virtual and real worlds are dissolving, as new technologies, services and business models push existing concepts and regulation to their limits. The organisational structures and physical barriers that ensured security in the past are now being tested, and in some cases, breached by cyber threats that are continually evolving. Dealing with these challenges requires cooperation between everyone involved with the cyber world – the IT industry, policy makers, politicians and, not least, citizens. In 2012, ENISA focused on ways to strengthen cyber cooperation across all sectors. This cooperation includes coordination throughout Europe as well as worldwide in both the public and private sectors.

Our starting point was to ask ourselves: what are the next steps for building stronger bridges and establishing common ground amidst the ever-evolving cyber scenarios? In responding to destructive digital attacks, what are the new challenges for EU institutions, the private sector and citizens?

Providing answers to these questions in 2012 has been challenging yet rewarding. One of the highlights in 2012 was ENISA's successful management of Europe's biggest ever cyber security exercise, Cyber Europe 2012. The exercise involved all EU Member States and countries from the European Free Trade Area (EFTA) as well as private sector organisations (a first for Europe). We also responded swiftly and professionally to Member States' requests for assistance, through ENISA's Athens-based mobile team.

In terms of the development of ENISA's activities, the Agency took up a formal role in Europe's Cyber Incident Reporting framework, under Article 13a of the EU's Telecommunications Framework Regulation, and assisted with the setup of new Computer Emergency Response Teams (CERTs) in Malta, Romania, Cyprus and Ireland, while providing ongoing support to established teams. ENISA was also closely involved in the CERT-EU pre-configuration team, and, in cooperation with the European Commission, organised the pilot for the first ever European Cyber Security Month, with activities across eight European countries throughout October. In addition, the agency continued to strengthen its collaboration with Europol, part of which has included having a member on the board of the new European Cybercrime Centre (EC3) in The Hague.

This year has also seen the new ENISA Regulation progressing towards the final stages of approval within the European Parliament and the Council of Ministers. We look forward to a new mandate for ENISA, so that the Agency can proactively and efficiently support the Member States.

Although there is still a significant amount of work to be done to achieve the vision of a harmonised approach to cyber security across the EU, it is clear that great progress has been made in collaborating across communities and across national boundaries.

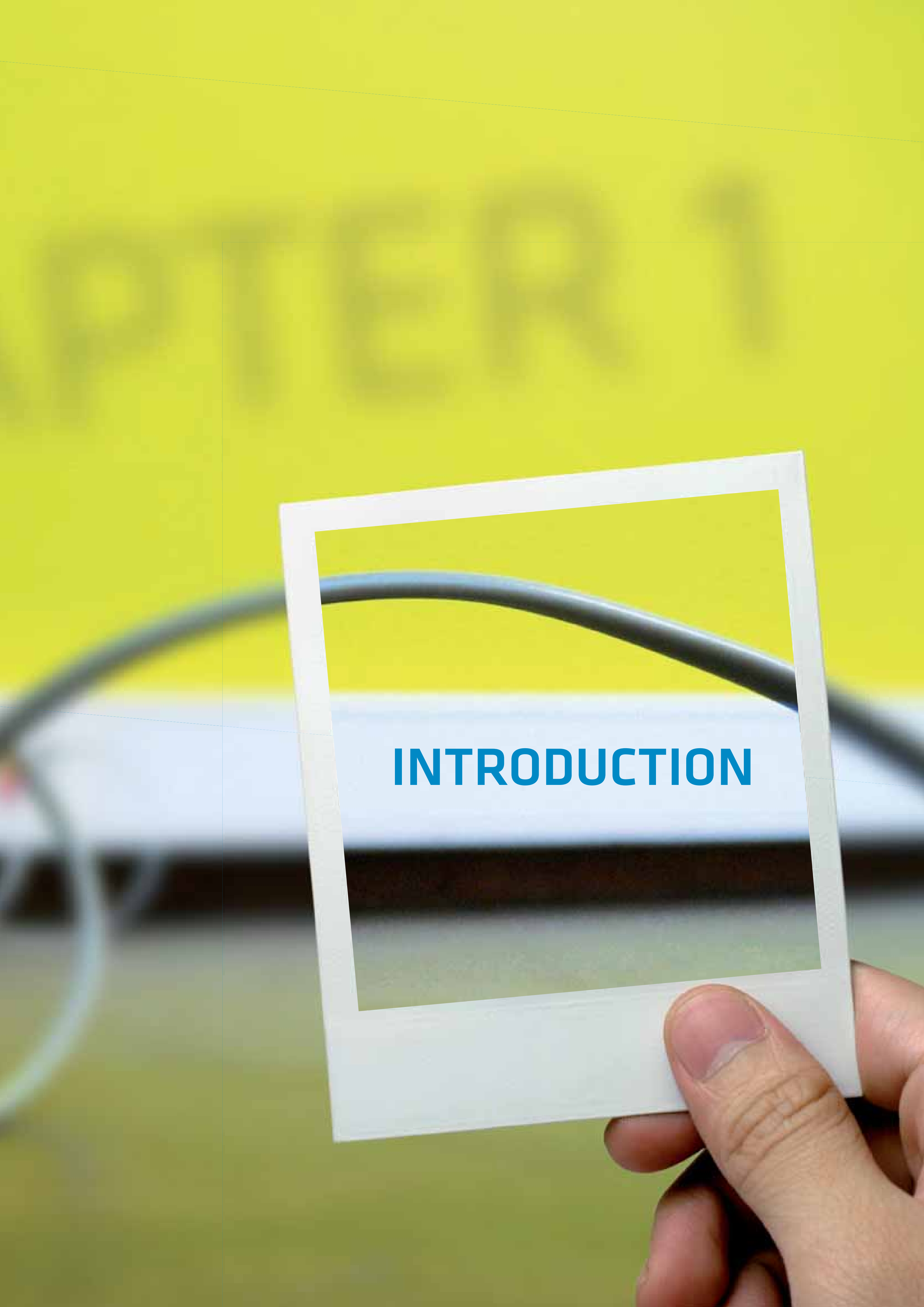
In this new inter-dependent world we must act as one, and develop a cohesive online ethos: the next chapters of cyber security depend on it. It is crucial that the Internet is safeguarded as an arena for commercial, governmental, cultural and leisure activity. Therefore all efforts and strategies dedicated to securing Europe's cyber cooperation must remain coherent, consistent and unified.

I hope that you find our 2012 General Report useful and informative.

Udo Helmbrecht
Executive Director

TABLE OF CONTENTS

CHA



INTRODUCTION

INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT): A "DOUBLE-EDGED SWORD"

Information and Communication Technologies (ICT) have provided countless benefits to citizens, businesses and governments, and have become the backbone of Europe's society and economy. Such technologies present us, however, with a double-edged sword: greater benefits invariably come with new threats. All of us depend inextricably on cyber-space, yet very few of us are in a position to fully appreciate the magnitude of damaging activity that occurs online every day.

The number and sophistication of cyber-attacks affecting public and private information systems has increased dramatically over the past year, and is expected to continue to grow at a fast pace. Moreover, in today's world, geographically separated societies are interconnected by information technology – and are irreversibly dependent on it. New threats thus reflect the global nature of the systems they target and their mitigation often requires international collaboration. The propagation and implications of threats such as malware (and botnets in particular) mean they are no longer just an issue for individuals, but are increasingly a social and civic responsibility that affects all sectors of our digital society.

"The organisational structures and physical barriers that have stood for centuries are being severely put to the test by cyber threats that are continually evolving."

VIRTUAL VS. REAL: BORDERS BLUR

The borders between virtual and real worlds are dissolving. New technologies, services and business models push existing concepts and regulation to their limits. The organisational structures and physical barriers that have stood for centuries are being severely put to the test by cyber threats that are continually evolving. Even national borders may hinder us more than protect us against challenges which are global in nature and which require responses that are coordinated across sectors, organisations and national borders. The leading role that information technologies play in modern society has made cyber security essential to the worldwide economy. Moreover, the EU's competitiveness and prosperity are closely connected to the safety and security of critical infrastructures. Hence, we need to cooperate closely in order to ensure that the EU as a whole is equipped with appropriate protection and defence mechanisms, including an overview of major cyber incidents.

THE DIGITAL AGENDA

European Commission Vice President Neelie Kroes has put forward the Digital Agenda for Europe, with the objective of improving citizens' quality of life through, for example, better healthcare, safer and more efficient transport solutions, a cleaner environment, new media opportunities and easier access to public services and cultural content.[1] This is a major step towards the creation of the Digital Society. Cyber-attacks, however, complicate the deployment of ICT solutions used by citizens in their day-to-day lives, such as online payment and e-government services. According to the Special Eurobarometer 390 on Cyber Security (published in July 2012), 29% of EU citizens do not feel confident in using the Internet for banking or purchases and 12% said they had already fallen victim to online fraud.[2] Moreover, the Special Eurobarometer 371 on Internal Security found that eight out of ten Europeans consider cybercrime to be an important challenge to EU security.[3]

THE IMPORTANCE OF CROSS-BORDER COOPERATION

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and pursued with consistency over time. This is not yet the case, as approaches vary in different Member States and communities. Without a coordinated global strategy for combatting major incidents on the Internet, Member States could find themselves in a situation where local systems cannot function effectively because of issues that are beyond their control. The EU institutions and bodies play an important role in improving cyber security by providing support for collaboration and a policy framework for Member States to achieve a coordinated global approach.

ENISA'S ROLE

Since its launch in 2004, ENISA has endeavoured to build bridges between communities by promoting cooperation across the EU and beyond. The Agency has successfully done so through activities such as supporting the CERT community (including the newly formed EU CERT), organising the Cyber Europe and Cyber Atlantic exercises, assisting the Member States in implementing the requirements of security breach notification legislation, responding quickly and efficiently to Member States' requests for Assistance through ENISA's Athens-based Mobile Assistance Team (MAT) and in helping to establish new Computer Emergency Response Teams (CERTs) in Malta, Romania, Cyprus and Ireland. ENISA aims to support communities that are striving to improve the level of EU cyber security, by improving the resilience of critical information infrastructures and services, in both the public and private sectors.

There are a number of areas where the current approach to improving cyber security in the EU could sensibly be extended. For example, there is a clear need to collect and analyse data relating to information security in a cross-border context which could reveal trends that are not visible at present. This is already under way with cyber incident reporting under Article 13a of the EU's Telecommunications directive[4], but there is scope for this to be done across more areas. In addition, a new ENISA Regulation is progressing towards its final stages within the European Parliament and the Council of Ministers. The coming into force of the Lisbon Treaty offers an unparalleled opportunity to improve the level of dialogue between communities in the area of Network and Information Security. A proactive approach to building these new cross-border communities will bring great benefits, both in terms of effectiveness of approach and efficiency in the use of resources.

At a time in which the importance of cyber security is recognised by all, it is important that efforts to protect and facilitate the development and prosperity of the European Information Society do not lose momentum. We need to prepare for a range of security-related incidents that threaten large-scale disruption. ENISA is assisting the Commission and the Member States in identifying and preparing for such incidents and is

[1] 1 COM(2010) 245 final/2
[2] http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
[3] http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf
[4] Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive) http://www.enisa.europa.eu/media/news-items/agency-initiative-to-implement-art.-13-of-telecom-package

actively collaborating with a wide-range of stakeholder communities as part of this effort. It is important that ENISA is fully supported and further developed so that the Agency can continue to respond to these challenges and provide support and expertise to stakeholders across Europe.

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 with a branch office in Athens.

ENISA's objectives are to:

- Secure Europe's information infrastructure
- Promote information security standards, guidelines and certification schemes
- Educate the wider public on ICT

The main contributions of ENISA to enhancing cyber security are in the following areas:

- Identification and analysis of emerging trends and threats
- Awareness of network and information security risks and challenges
- Early warning and response
- Critical information infrastructure protection
- Adequate and consistent policy implementation
- Supporting other community actors in actions against cybercrime
- International cooperation
- Information exchange
- Building communities

In 2012, ENISA published numerous reports and studies on a range of NIS issues, including:

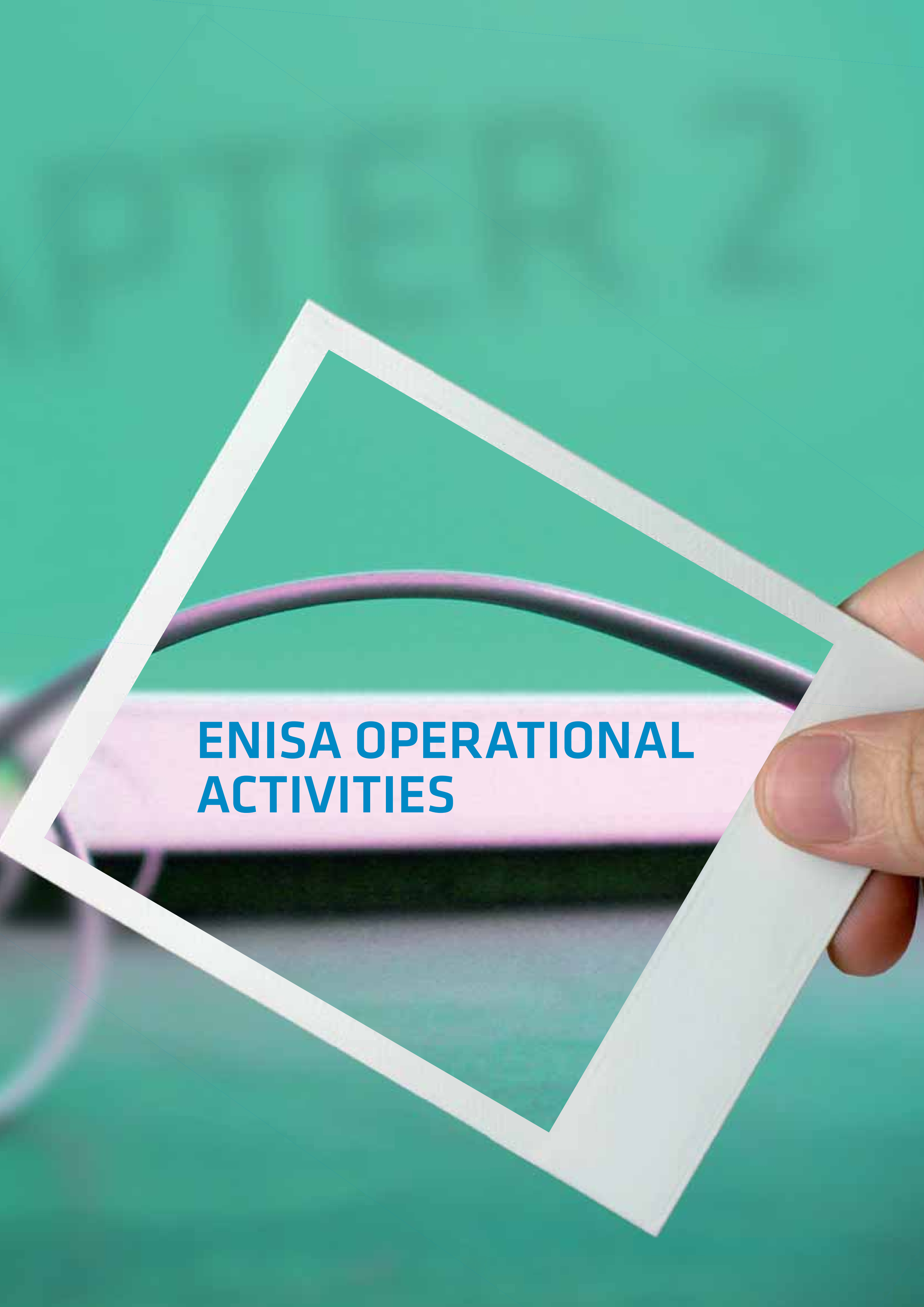
- Minimum security measures and reporting incidents
- Cyber incident reporting in the EU
- Assessing cloud computing security risks
- Minimum security requirements for smart grids
- Protecting Industrial Control Systems
- National cyber security strategies
- Incentives and barriers in the cyber insurance market in Europe
- National and international cyber security exercises
- Good practice for national cyber contingency plans
- Cyber exercise scenario modelling
- Cooperation between n/g CERTs and other stakeholders
- Proactive detection of security incidents using honeypots
- The right to be forgotten
- Privacy considerations of online behavioural tracking
- ICT supply chain risks and challenges
- Electronic identification and trusted services for electronic transactions
- Consumerization of IT
- Involving intermediaries in cyber security awareness raising
- Collaborative solutions for Network Information Security in education

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.



ENISA OPERATIONAL ACTIVITIES

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP) AND RESILIENCE

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. 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 recognising 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 2012, the Resilience activities and tasks were defined within the ENISA Work Programme 2012 – Improving Information Security Through Collaboration. The Resilience activities were included within Work Stream (WS) 2: Improving Pan-European CIIP & Resilience and Work Stream (WS) 3: Supporting the CERT and other Operational Communities. The work packages dedicated to Resilience were Work Package (WPK) 2.1: Further Securing EU's Critical Information Infrastructure and Services; Work Package (WPK) 2.2: Cyber Exercises; Work Package (WPK) 2.3: European Public Private Partnership for Resilience (EP3R); and Work Package (WPK) 2.4: Implementing article 13a.

Article 13a: Incident reporting and security measures in the electronic communications sector

The 2009 reform of the EU Regulatory Framework for electronic communications added Article 13a to the Framework Directive. Article 13a requires operators to take technical and organisational measures to manage the risks posed to the security of networks and services, as well as to report security incidents to competent National Regulatory Authorities (NRAs). Article 13a asks NRAs in turn to send an annual report to the European Commission and ENISA that summarises the reported incidents.

In 2010, ENISA formed a working group to work together with NRAs to achieve a harmonised implementation of Article 13a across the EU and to establish a process for reporting incidents to the European Commission and ENISA. In 2011, the Article 13a Working Group agreed on two technical guidelines, a Technical Guideline for Minimum Security Measures and a Technical Guideline on Reporting Incidents.

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

In 2012, NRAs reported on the 2011 security incidents to the European Commission and ENISA, and later that year ENISA published a summary and aggregate analysis of the incidents in 2011 that were reported to regulators across the EU. This marked the first time that security incidents from across the EU were collected and analysed. ENISA also took a snapshot of existing and future EU legislation on security measures and incident reporting. In its findings, published in Cyber Incident Reporting in the EU, ENISA underlined the important steps that have been taken, but also pointed out gaps and the fact that most security incidents fall outside the scope of incident reporting legislation and are not reported to authorities. ENISA is currently completing the creation of an online incident reporting tool for reporting security incidents.

The Annual Incident Reports 2011 is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011

The report Cyber Incident Reporting in the EU is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

The Technical Guideline for Minimum Security Measures is available at:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures

The Technical Guideline on Reporting Incidents is available at:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting

Cloud computing: from individual contracts to EU governance

In 2009, when cloud computing was still a relatively new concept, ENISA published Cloud Computing Security Risk Assessment, an assessment of the risks and opportunities for SMEs considering adopting cloud computing. The risk assessment became one of the most widely quoted papers on cloud computing security. In the paper, ENISA stressed the enormous potential of cloud computing, particularly in terms of security. Cloud computing allows different customers to join forces and in this way, with little investment, get access to state-of-the-art technology and resources, such as a 24/7 security team, a thorough software development process with extensive security testing, or geographically redundant data centres.

In a cloud computing environment, the work of the organisation's IT officer changes as well: instead of setting up hardware and installing software, IT officers in a cloud computing environment have to manage service contracts with IT service providers. In December 2011, ENISA surveyed IT officers across the EU's public sector to analyse security parameters in cloud Service Level Agreements (SLAs). The cloud SLA survey showed that many key aspects of service delivery are not adequately monitored by customers and that as a result customers may find out about issues too late. To remedy this situation, in 2012 ENISA published a guide on monitoring key security parameters in cloud service contracts.

With many private and public sector organisations switching to cloud computing, IT resources are no longer distributed across a large number of remote locations but instead concentrated in a few large data centres. From a security perspective this concentration is a 'double edged sword'. On the plus side, large cloud providers can deploy state of the art security and business continuity measures and spread the associated costs across many customers. On the minus side, if an outage or a security breach occurs then the consequences could be more widespread, affecting a large amount of data, many organisations and a large number of citizens. In 2012, ENISA finalised an analysis of the key security issues to consider from a national and CIIP perspective regarding the uptake of cloud computing. That year, ENISA also examined cloud computing from a national CIIP perspective and began work on an update of the 2009 cloud computing risk assessment for small and medium-sized enterprises (SMEs). Both documents are open for consultation and they are currently being validated by a working group of cloud computing experts from industry and the public sector.

> "From a security perspective, the concentration of IT resources in a few large data centres is a 'double edged sword'."

Towards the end of 2012 the European Commission worked on two initiatives which will have an important bearing on ENISA's future work in the area of cloud computing. First of all, the Commission issued a cloud computing strategy that would have ENISA work with the European Telecommunications Standards Institute (ETSI). The two institutions would map the standards relevant to the security and privacy of cloud computing services, and take stock of existing security governance and auditing schemes that could be used for governing cloud computing services. Secondly, the European Commission is working on a cyber security strategy that will focus on critical services including cloud services.

The report Cloud Computing Security Risk Assessment is available at:

http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

The report Procure Secure: A guide to monitoring of security service levels in cloud contracts is available at:

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

Emergency Communications

Crisis events like the terrorist attacks in New York, London, Madrid, and Mumbai, industrial accidents like the ones that happened in Enschede or Toulouse, and natural disasters such as the Elbe floods in Saxony, the Tsunamis in the Indian Ocean and Japan, and the Katrina and Sandy storms in the US, have highlighted the importance of maintaining communications during emergencies. Crisis managers need to maintain an accurate picture of the current situation, efficiently deploy and command the available resources and relay important information to the public.

A common observation in the analyses made after some of the above disasters is that communications were often a weakness in the response operations. In many cases, communications networks failed or were overloaded. One of the needs identified during the studies covering technical and economic aspects of the underlying communications infrastructure in 2010 (Inter-X: Resilience of the Internet Interconnection Ecosystem) and 2011 (Resilience of Interconnections) was the need for a broad understanding of current communication practices used during a crisis.

ENISA addressed this key topic in 2012 by taking stock of existing practices in this area. The goal was to understand the mechanisms, policies and legal frameworks used in Europe and in selected third countries to facilitate emergency communication including voice and data (wireless, wired, and satellite) during a crisis. The study used a comprehensive methodology of primary research and interviews with relevant stakeholders in the regulatory, service provision and crisis response sectors. On the basis of the report findings, three key objectives were identified:

- Develop improved inter-agency crisis communications technology and procedures
- Define standards in crisis communications technology and procedures
- Encourage the uptake of data services in emergency communications, particularly in the area of public interaction

A series of recommendations have been made to Member State Governments, Competent Authorities, Service Providers and the Institutions of the European Union.

Securing European Smart Grids

The smart grid can be defined as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added. Smart grids will be able to efficiently integrate the behaviour and actions of all users connected to them — generators, consumers and those that do both — in order to ensure an economically efficient, sustainable power system with low losses and a supply that is safe, secure and of high quality. Information and Communication Technologies (ICT) are the platform underpinning smart grids.

Achieving a secure smart grid will not be an easy task. Assessing risks, securing processes as well as identifying technological gaps and organisational problems are some of the main challenges that the smart grid will face in the years to come. Recognising the importance of Smart Grids for the functioning of the EU economy and society, ENISA has launched a series of new activities or actively participated in existing ones.

The Agency has published two relevant studies and is conducting another one on the *Minimum security requirements for smart grids*. The studies recommend that the European Commission and Member States take measures such as bolstering research in smart grid cyber security, improving the regulatory and policy framework, fostering awareness raising, training and test bed initiatives and promoting the development of security certification schemes for the components and products of smart grid infrastructure.

Apart from these activities, ENISA has taken the first steps towards defining a common model for the security and resilience of smart grids. Such a model would be used by regulators and operators, or by other stakeholders.

The report on Protecting Industrial Control Systems is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.

The report on Smart Grid Security Recommendations is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations.

National Cyber Security Strategies: Practical Guide on development and execution

Cooperation at the pan-European level is necessary to effectively prepare for and respond to cyber-attacks. Comprehensive national cyber security strategies are the first step in this direction. In 2012, ENISA published a practical guide that identifies the most common elements and practices of National Cyber Security Strategies (NCSS), in the EU and non-EU countries. The guide also proposes a national cyber security strategy lifecycle, with a special emphasis on the development and execution phase. For each component of the strategy a list of possible KPIs is described. The report includes specific recommendations for policymakers.

The report on National Cyber Security Strategies is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

Incentives and barriers in the cyber insurance market in Europe

Cyber-insurance has captured the imagination of many involved in cyber-security at the policy and research level as a means of transferring cyber security-related financial risks to third parties. The coverage in traditional insurance policies may not fully address the risks faced by an organisation that is part of the digital economy. To address this gap, ENISA has conducted a study to identify what may be inhibiting the cyber-insurance market and ways to kick start its development.

The report on Incentives and barriers of the cyber insurance market in Europe is available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe

Cyber crises exercises and cooperation

Cyber Europe 2012

On 4 October 2012, nearly 600 cyber-security professionals across Europe participated in Cyber Europe 2012, the second pan-European Cyber Exercise. The exercise built on extensive activities at both the national and European level to improve the resilience of critical information infrastructures. Cyber Europe 2012 was a milestone in the efforts to strengthen cyber-crisis cooperation, preparedness and response across Europe.

Cyber Europe 2012 had three objectives:

1. Test the effectiveness and scalability of mechanisms, procedures and information flow for public authorities' cooperation in Europe.
2. Explore the cooperation between public and private stakeholders in Europe.
3. Identify gaps and challenges to see how large-scale cyber-incidents can be handled more effectively in Europe.

Twenty-nine EU Member States and EFTA countries were involved in the exercise of which 25 countries participated actively in the exercise, while four countries were involved as observers. Overall, 571 individuals from 339 organisations – including several EU institutions – participated. Following up on a key recommendation of Cyber Europe 2010, the private sector took part in this exercise. Cooperation between public and private players took place at the national level, while public authorities also cooperated across borders.

In 2013, ENISA plans to initiate discussions with the EU Member States on the future objectives and scope of the upcoming Pan-European Cyber Exercise, Cyber Europe 2014.

The exercise report is available upon request.

Status report on national and international CIIP Exercises

Cyber exercises are an important tool for assessing the preparedness of a community against cyber crises, technology failures and critical information infrastructure incidents. ENISA supports the stakeholders involved in EU cyber exercises.

This report aims to support European and international bodies involved in cyber exercises with lessons learned from cyber exercises. The report presents the results of research and analysis conducted by ENISA in 2012. ENISA examined 85 exercises covering the period between 2002 and 2012. In total, 84 countries worldwide participated in the multinational exercises analysed in this report. A total of 22 European countries have conducted national cyber-exercises over the past several years. In 2013, ENISA will follow-up with a 2nd International Conference on Cyber Crisis Exercises and Cooperation.

The report on National and International Cyber Security Exercises: Survey, Analysis and Recommendations is available at:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercises/exercise-survey2012

Cyber exercises in Europe

The results of several cyber exercises in Europe – Cyber Europe 2010 and 2012, and Cyber Atlantic 2011[5] – have confirmed the need for and significance of cyber-crisis cooperation.[6] Other efforts such as the European Cyber Crisis Cooperation Framework (ECCCF) and the European Standard Operating Procedures for cross-country cyber-crisis mitigation (EU-SOPs)[7] are currently under development by Member States. This ENISA report covers current and past efforts in the area of cyber exercises. It provides an overview of the role and objectives of cyber exercises, potential stakeholders, international and regional cooperation and a summary of the exercises themselves. It complements the results and recommendations of the recently published ENISA report on over 80 cyber exercises.[8]

The document is available upon request.

ENISA Report on National Contingency Plans for Critical Information Infrastructures

National Cyber Contingency Plans (NCPs) are the interim structures and measures needed to respond and recover services following major incidents that involve Critical Information Infrastructures (CIIs). CIIs, used synonymously with 'cyber' hereafter, are the Information and Communication Technology systems, services, networks and other infrastructures, such as embedded processors and controllers in critical industries, which form a vital part of the European economy and society. An NCP helps a nation make its CII more resilient by establishing a response framework before incidents occur.

ENISA's Good Practice Guide on National Cyber Contingency Plans shows how a nation can plan, develop, test, improve and maintain a good and well-functioning NCP for Critical Information Infrastructures. In 2013, ENISA will follow-up this work with a project that focuses on a single element of the NCP lifecycle, National Risk Assessment for Critical Information Infrastructures.

The Good Practice Guide on National Cyber Contingency Plans is available upon request.

Regional cyber security exercises: EuroSOPEx 1 & 2

In 2012, ENISA organised two distributed table-top regional exercises, called EuroSOPEx, in order to familiarise Member States with the EU Standard Operating Procedures (EU-SOPs)[9], as part of preparing for Cyber Europe 2012. The first EuroSOPEx exercise was organised on 30 May 2012 with Cyprus, Estonia, Greece, Iceland and Malta. The second EuroSOPEx exercise was organised on 6 June 2012 with Belgium, Denmark, Ireland, Italy, Netherlands, Romania, and Spain. In 2013, ENISA will continue to foster and facilitate regional cyber exercises by organising two similar EuroSOPEx exercises based on the specific findings of the Cyber Europe 2012 report.

[5] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011.

[6] Cyber Europe 2010 Final Report (2010), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report

[7] The ECCCF report and the draft EU-SOPs are both available at ENISA's resilience portal at: https://resilience.enisa.europa.eu/eu-exercises/sops

[8] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercises/exercise-survey2012.

[9] Available at ENISA's resilience portal: https://resilience.enisa.europa.eu

The EuroSOPEx 1&2 exercise report is available upon request.

Cyber Exercise Scenario Modelling (CESMO)

The aim of this work was to identify a model that can help designers of cyber exercises to develop and model their scenarios. The report defines the basic blocks that make up cyber incidents such as the type of actor that initiates and carries out the event, the threats that exist, or the outcome of a cyber-incident. These basic building blocks are then connected together in a logical fashion that clarifies the dependencies that exist between them. For example, an incident affects a resource; an actor has a motive. At a high-level, the model represents cyber-incident scenarios as a sequence of events that can be combined to form any type of scenario. At a low-level, the model focuses on two major concepts, incidents and impact. Incidents may be either intentional, such as a malicious attack, or unintentional, such as a natural disaster. Impact comes as the result of an incident and may have virtual consequences, like loss of data or privacy, as well as physical consequences, such as loss of money or life.

To validate the effectiveness of the model and modelling process, six sample scenarios involving cyber incidents were modelled. In each scenario, the parameters of that scenario were mapped onto the model, to demonstrate its flexibility and capability in representing cyber incidents. Guidance is given on how the model and modelling process may be instantiated using a simple data base system.

Based on the findings of this report, ENISA has developed a pilot application for creating cyber exercise scenarios. In 2013, ENISA experts will work on a more advanced project that will use the existing CESMO prototype as a starting point.

The report on Cyber Exercise Scenario Modelling is available upon request.

EP3R - European Public-Private Partnership for Resilience

The European Public-Private Partnership for Resilience (EP3R) was continued in 2012, to address the three main areas established by the EP3R Non-Paper (the memorandum that defines the initial establishment of EP3R) in June 2010:

- **Area 1**: Key assets, resources and functions for the continuous and secure provisioning of electronic communications across countries.[10]
- **Area 2**: Baseline requirements for the security and resilience of electronic communications.[11]
- **Area 3**: Coordination and cooperation needs and mechanisms to prepare for and respond to large-scale disruptions affecting electronic communications.[12]

Four working groups were established to address these areas with area 3 divided specifically between exercises and botnets. Each working group reached a number of conclusions in June 2012, and prepared for the new cycle beginning in 2013. In 2012, ENISA also developed an agile working model together with an enhanced governance proposal for EP3R, and established task forces. Task forces are smaller groups of 5-6 experts that focus solely on 1-2 work packages. Each task force will deliver their initial conclusions before the end of May 2013, and in June 2013, an EP3R plenary will vote on each recommendation issued by the task forces.

All the work of EP3R experts (whether working groups or task forces) is documented on the EP3R web portal[13], along with the EP3R publications to be delivered by the end of December 2012.

[10] http://ec.europa.eu/information_society/policy/nis/docs/ep3r_docs/ep3r_tor_area1.pdf

[11] http://ec.europa.eu/information_society/policy/nis/docs/ep3r_docs/ep3r_tor_area2.pdf

[12] http://ec.europa.eu/information_society/policy/nis/docs/ep3r_docs/ep3r_tor_area3.pdf

[13] https://resilience.enisa.europa.eu/ep3r/ (a login is requested to see this content)

SUPPORTING CERTS AND OTHER NIS COMMUNITIES

National/governmental Computer Emergency Response Teams (CERTs) are responsible for supporting the management of security incidents for systems and networks within their country's borders, as well as for the protection of critical information infrastructure. They act as an official national point of contact for their counterparts in other Member States.

From the very beginning of ENISA's existence, the Agency has provided intensive support to this group of stakeholders. Our aim is to continuously support the establishment and operations of CERT teams, as they are considered by Member States to be an indispensable means for ensuring the resilience and stability of vital ICT infrastructure.

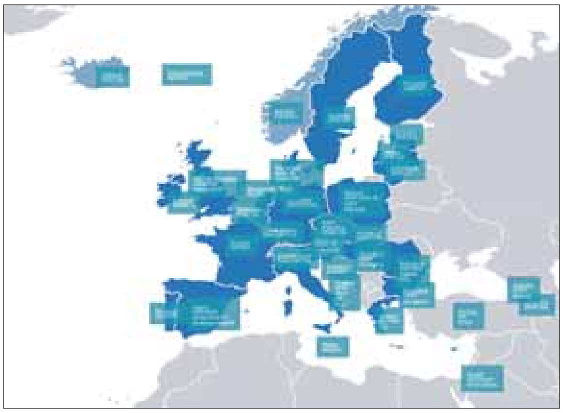


Figure 1: national/governmental CERTs in Europe 2012

National/governmental CERTs – Situation in Europe in 2012

The 2011 Progress Report on the CIIP Action Plan[14] noted that a minimum set of baseline capabilities and related policy recommendations for a well-functioning network of national/governmental Computer Emergency Response Teams (n/g CERTs) in all Member States has been developed. These developments encompass preparedness, information sharing, co-ordination and response. ENISA addressed this topic in detail and presented a status report in 2012 on the deployment of baseline capabilities for n/g CERTs in Europe.

The report describes the current situation in Europe regarding n/g CERTs' capabilities, and how they are deployed. The current situation was assessed according to four baseline capabilities previously defined by ENISA and accepted by the CERT community.[15] As the report notes, the role of n/g CERTs is usually supported by an official mandate. There are many variations concerning the hosting organisations of n/g CERTs, however. Several Member States have followed the trend in creating national cyber-security centres. These will ultimately be responsible for the implementation of cyber-security strategies that integrate the functionality of n/g CERTs. Key constituents such as governmental bodies receive the complete menu of services, while a subset of services is available for other constituents, including end-users. More than 80% of n/g CERTs employ 6–8 or more full-time equivalents, which is the minimal staffing level considered necessary to provide an acceptable level of service.

For more information: http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

> "Our aim is to continuously support the establishment and operations of CERT teams, as they are considered by Member States to be an indispensable means for ensuring the resilience and stability of vital ICT infrastructure."

[14] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[15] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

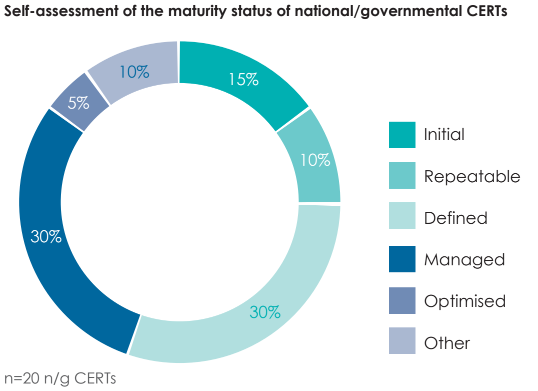


Figure 2: Years of operation of national/governmental CERTs

ENISA response to CERT-related requests from the Member States

The mission of ENISA is to work together with the EU institutions and the Member States to develop a culture of Network and Information Security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union. In particular, based on our experience to date, we have assisted several Member States with the process of setting up an n/g CERT. Our proactive attitude towards brokering relationships between those Member States with a particular requirement and those willing to share their experience helped with this process in Ireland and Romania this year.

Ireland

The Irish National Cyber Security Centre (INCSC) built on existing emergency planning in Ireland and is focusing on protecting the energy, communications and finance sectors. INCSC is itself divided into three sections covering computer security (CSG), critical national infrastructure (CNIPF), and incident response (CSIRT-IE). CSIRT-IE focuses on helping government departments to protect their ICT infrastructure and data against attack and misuse.

Romania

CERT-RO[16] was established in response to the EU action calling for n/g CERTs to be established in all Member States, and was created by a law passed by the Romanian Parliament in May 2011. The goals of CERT-RO are to analyse and respond to cyber-security incidents in Romania, and to develop national IT security policies and strategies in conjunction with other public bodies. It also acts as a national contact point for the international community.

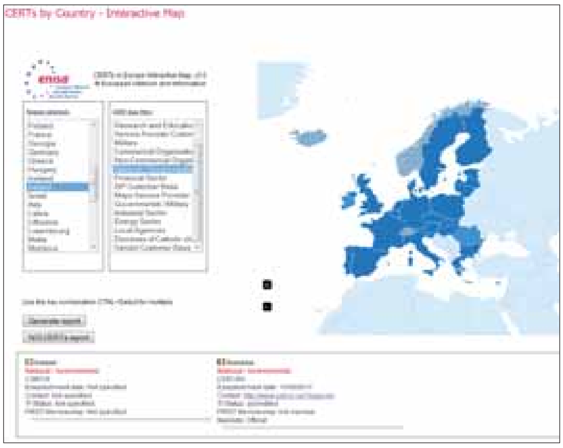


Figure 3: CERTs by Country – n/g CERTs in Ireland and Romania

ENISA's updated recommendations on gaps in the baseline capabilities of national/governmental CERTs

Despite progress in the deployment of baseline capabilities by n/g CERTs across Europe, there are still several challenges which need to be addressed by interested parties such as legislators, CERT teams themselves, cooperation partners, international initiatives and – last but not least – ordinary citizens. That is why in 2012 ENISA presented an updated set of recommendations on n/g CERTs' baseline capabilities.

The gaps identified and addressed in the report are mainly legal and political. There are a number of actions that need to be taken by policymakers in the Member States to support n/g CERTs in their work, especially regarding the protection of critical information infrastructure and the coordination of incident handling. This will require the clarification of n/g CERTs' mandates, as well as incorporating the provisions on n/g CERTs into national cyber-security strategies. More concretely, the n/g CERTs should be empowered to require the exchange of information with telecommunication operators, Internet service providers and law enforcement authorities.

Although the n/g CERTs cannot influence many of the above-mentioned items on their own, they can take action. For example, in a time of economic crisis and with a perceived lack of funding for their activities, n/g CERTs should actively look for additional resources such as EU funds, consulting engagements with the private

[16] http://www.cert-ro.eu/index.php?lang=en

sector, and research projects. It is also crucial that they increase their transparency and visibility by publishing general statistics on incidents and other activities or by raising awareness of their actions among their constituencies.

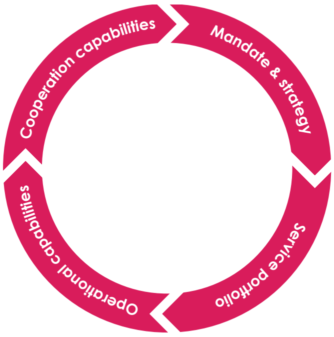


Figure 4: Four baseline capabilities of national/governmental CERTs

ENISA's goal is to continuously support the Member States in enhancing and strengthening the cooperation among n/g CERTs in order to ensure a powerful incident response when it is needed.

Seventh annual CERT workshop "CERTs in Europe"

Part I: Technical training for national/governmental CERTs

Every year ENISA organises the workshop "CERTs in Europe" for national and governmental CERTs in Europe. The workshop is one of the most efficient and indispensable tools ENISA has for supporting CERT teams in their daily work and for continuously improving their capabilities.

The 7th annual workshop (Part I) took place on 14-15 June 2012 in Valletta, Malta. Last year the workshop focused on addressing NIS aspects of cybercrime, particularly the operational and technical aspects of the collaboration between national/governmental CERTs and the Law Enforcement Authorities (LEAs) in the EU Member States. This year, the first part of the workshop focused on hands-on technical training for national/governmental CERTs in Europe. ENISA enhanced CERTs' capabilities in the EU Member States by providing information on good operational practice and facilitating suitable training and exercises. Hands-on training for CERT team members on operational topics is essential for improving the capabilities of the team as a whole. ENISA, supported by the well-known Internet security research firm Team Cymru, offered two days of deep technical information on topics like botnets and mobile malware. The workshop was hosted by the University of Malta.

Part II: ENISA and EUROPOL joint forces on fight against cybercrime

ENISA and Europol jointly organised the 7th annual CERT Workshop, Part II, as a follow up event to the very successful 6th Annual CERT workshop held last year in Prague, Czech Republic. This year the workshop was held at the Europol premises in The Hague, The Netherlands on 16-17 October 2012. The focus remained on cooperation between national/governmental CERTs (n/g CERTs) in Europe and their national Law Enforcement Authority counterparts (LEAs). Out of a total number of 44 participants 15 represented n/g CERTs and 12 represented national LEAs (usually the high tech crime units). The other participants were experts from industry as well as from international organisations. Belgium, Czech Republic, France, Germany, Greece, Hungary, Ireland, Luxembourg, Netherlands, Slovenia, Spain, United Kingdom were the EU Member States that participated along with non-EU countries Norway and Switzerland. Emphasis was placed on how to increase the exchange of information on cybercrime threats as well as cooperation between the n/g CERT and LEA communities on a practical working level, both nationally and across borders. There is an urgent need for these two communities to collaborate because of their complementary responsibilities. Currently, however, in many cases this collaboration is very limited and sometimes even non-existent. The workshop aimed to identify synergies and gaps and practically address these obstacles to cooperation. It was also a forum for discussing the next steps that need to be taken in order to improve collaboration in the short-term.

The fight against cybercrime

One of the key elements in the fight against cybercrime is cooperation between different actors involved in this fight. While a lot of work has been done in this area in some Member States, there is still room for improvement. ENISA, therefore, has focused on the cooperation between n/g CERTs and their LEA counterparts.

ENISA started its support for operational collaboration between CERTs and LEAs in 2010. Various activities, including the workshops mentioned above, have since been launched. In addition, in 2012 ENISA published a Good Practice Guide concerning cooperation between n/g CERTs and other stakeholders, primarily LEAs within Europe. The guide provides a snapshot of ENISAs support for CERTs and LEAs, and includes good practices and recommendations for both communities. Fostering collaboration between CERTs and LEAs is, however, a process of trust building, tackling obstacles together, discussion and finally working together which will need time and the active, continuous support of ENISA.

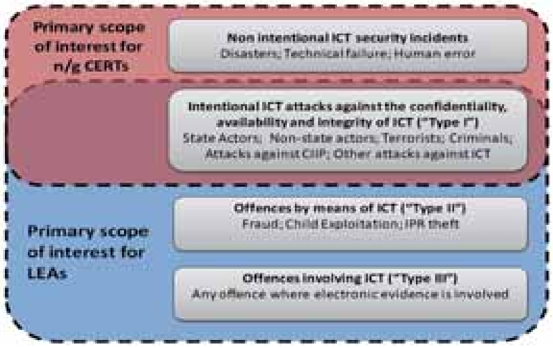

Primary scope of interest for n/g CERTs
Non intentional ICT security incidents
Disasters; Technical failure; Human error
Intentional ICT attacks against the confidentiality, availability and integrity of ICT ("Type I")
State Actors; Non-state actors; Terrorists; Criminals; Attacks against CIIP; Other attacks against ICT
Offences by means of ICT ("Type II")
Fraud; Child Exploitation; IPR theft
Primary scope of interest for LEAs
Offences involving ICT ("Type III")
Any offence where electronic evidence is involved

Figure 5: CERT / LEA interests[17]

CERT exercises – learning by doing

ENISA CERT exercises and training material were introduced in 2008. In 2012 these were complemented with new exercise scenarios containing essential material for success in the CERT community and in the field of information security. ENISA CERT exercise material consists of a handbook for teachers, a toolset for students and a virtual image to support hands-on training sessions. The complete set of material can be found at: https://www.enisa.europa.eu/activities/cert/support/exercise

The exercise and training material have been prepared in great detail so that teachers can, with minimal effort, prepare and conduct high quality training sessions that are enjoyable for both teachers and students.

The exercise material covers operational, organisational, and technical areas in the field of CERT activities, and supports the economically efficient training of CERT teams or any relevant and interested target audience. The training suite, for example, challenges students to identify a malware infection inside a mobile device or in a Supervisory Control and Data Acquisition (SCADA) network and proposes the most efficient methodologies for mitigating the incidents. From the management point of view it offers a solution for calculating the cost of information security incidents that have occurred within an organisation. It also suggests an economically efficient method for mitigating the identified risks using calculations explained in the exercise "Cost of ICT incident"

Those who are more interested in understanding the organisational aspects of running a CERT might be attracted to exercises that improve and develop the communication skills and critical thinking in a CERT team. Exercises such as "Cooperation with Law Enforcement agencies" and "Assessing and Testing Communication Channels with CERTs and all their stakeholders" develop and improve such skills.

The whole exercise suite consists of 23 exercises, ranging from technical hands-on training to training on organisational aspects. The exercises meet the needs of target audiences with different skills and expectations.

The exercises available for immediate use are:

- Triage and basic incident handling
- Incident handling procedure testing
- Recruitment of CERT staff
- Developing CERT infrastructure
- Vulnerability handling
- Writing security advisories
- Network forensics
- Establishing external contacts
- Large-scale incident handling
- Automation in incident handling
- Incident handling in live role playing
- Cooperation with Law Enforcement Agencies
- Incident handling during an attack on Critical Information Infrastructure
- Proactive incident detection
- Cost of ICT incident calculation
- Mobile incident handling

[17] Adapted from presentation given at the Octopus Conference of the Council of Europe Convention Against Cybercrime 21-23 November 2011, Strasbourg

- Incident handling in the cloud
- Advanced persistent threat incident handling
- CERT participation in incident handling related to the Article 13a obligations
- CERT participation in incident handling related to Article 4 obligations
- Assessing and testing communication channels between CERTs and all their stakeholders
- Social networks used as an attack vector for targeted attacks
- Honeypots

Investing in training and exercises leads to a win-win situation in which the CERT team's skills are improved and developed further. It may also indicate the gaps where further training may be needed for improvement of overall awareness and the security posture.

Settings
1 process and 0 services 12MB

Trusteer Rapport
1 process and 1 service 3.2MB 28:36

Google Services
1 process and 1 service 5.8MB 32:48

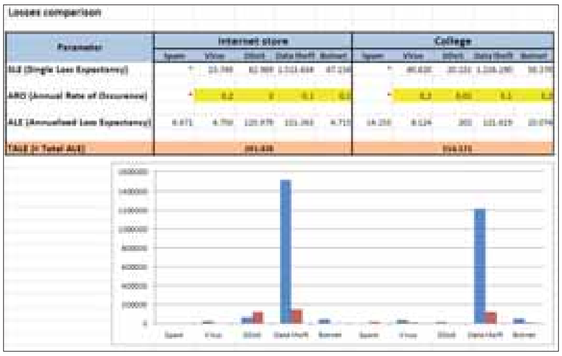
Android keyboard 4.9MB

```
import os

from abusehelper.core.config import relative_path
from abusehelper.core.startup import Bot

xmpp_jid = 'abusehel@localhost'
xmpp_password = 'exercise'
service_room = 'abusehelper'
enable_mailer = True

def basic(name, *args, **attrs):
    template = Bot.template(
        xmpp_jid=xmpp_jid,
        xmpp_password=xmpp_password,
        service_room=service_room,
        xmpp_ignore_cert = True,
        ## Uncomment the following lines, and the bots
        ## persistent state and log to files, respectiv
        bot_state_file=relative_path("state", name + "
        log_file = relative_path("log", name + ".log")
    )
    return template(name, *args, **attrs)
```



Losses comparison

Parameter	Internet store					College				
	Spam	Virus	DDoS	Data theft	Botnet	Spam	Virus	DDoS	Data theft	Botnet
SLE (Single Loss Expectancy)	-	23.749	62.989	1.511.614	47.150	-	40.620	20.220	1.226.290	50.270
ARO (Annual Rate of Occurrence)	-	0.2	0	0.1	0.1	-	0.2	0.01	0.1	0.2
ALE (Annualised Loss Expectancy)	4.671	4.750	125.979	151.161	4.715	14.250	8.124	202	122.619	20.074
TALE (= Total ALE)	291.436					194.171				

Honeypots – powerful tools for the detection of incidents

In order to cope with the increasing number of complex cyber-attacks, CERTs, the digital fire brigades, need to improve their operational capabilities in the proactive detection of attacks.

The most common approach used by CERTs to handle security incidents, is to wait for incoming incident reports, then try to 'treat' the effects of the attacks but not necessarily the 'cause'. In such cases the incident has already occurred and potentially had an impact on production environments.

Another approach is possible, however, when dealing with security incidents, and that is to be proactive in detecting attacks by using honeypots to collect attack information. This 'threat intelligence' includes information such as the attack source and attack technique. It may be used to block further attacks.

Honeypots are 'digital traps'. They can be a service, an application, a system or a piece of information whose sole task is to be probed, attacked, compromised, used or accessed in any unauthorized way. Honeypots are core components of Early Warning Systems used in attack detection.

The *Proactive detection of security incidents: Honeypots* study that ENISA ran in 2012 was initiated to investigate

'digital traps', or honeypot technologies, in-depth. The goal was to identify technologies that can be used by CERTs in general and national/governmental (n/g) CERTs in particular to proactively detect and capture network attacks directed at their constituencies. The core of the document is an investigation of existing honeypot and related technologies, with a focus on open-source solutions, including online honeypots and sandboxes, and other early warning systems or initiatives. One of the study's findings was that while honeypots are recognised by CERTs as useful tools that can be utilised to detect and study attacks, their usage in the CERT community is not as widespread as would be expected. This implies that barriers exist to their deployment.

The *Proactive detection of security incidents: Honeypots* study is available at:

http://www.enisa.europa.eu/activities/cert/support/proactive-detection-of-security-incidents-II-honeypots

EISAS Pilot: a collaborative approach to reach out to EU citizens and small and medium-sized enterprises (SMEs)

No firewall or security policy can efficiently protect users if they are not sufficiently aware of the risks they are facing. As European Commissioner Neelie Kroes has said, "Cyber security is also about ensuring ordinary computer users are 'Web Wise'".

Introduced by the European Commission in 2006, EISAS, the European Information Sharing and Alert System, aims to enhance the cooperation of Member States in reaching out to citizens and small and medium-sized enterprises (SMEs) with relevant security information. This year ENISA ran the EISAS Pilot project. National/governmental CERTs and other communities in Germany, Hungary, Portugal, Norway, Spain and Poland participated in a collaborative cross-border awareness raising effort. Innovative awareness raising materials were obtained from major public and private actors at a national level. An international team was set up to process and adapt the materials to the particularities of each stakeholder's population. These materials were then disseminated to EU citizens and SMEs through social networks and other communication channels.

In due course, this large-scale pilot reached more than 1,700 people. Citizens and SMEs across Europe were empowered with security knowledge to protect themselves against some of today's most critical cyber threats. However, the achievement of this pilot project goes beyond raising citizens' awareness; it also shows that European collaboration in awareness raising works and offers a cost-effective solution to better prepare EU citizens facing ever-evolving cyber threats.

SECURE SERVICES

The work performed within the framework of Secure Services includes areas of privacy and trust, security governance and electronic identities/trust services.

Projects in the area of privacy and trust started in 2010 and were very well received by many stakeholders, which led to the extension of this topic in the following years. The Agency performed numerous studies on topics such as trustmarks, the right to be forgotten, and behavioural tracking. 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 2012, the Secure Services activities and tasks are defined within the ENISA Work Programme 2012 – *Improving Information Security Through Collaboration*. The activities are included within Work Stream (WS) 4: *Securing the Digital Economy*. The work packages dedicated to Secure Services are Work Package WPK 4.2: *Secure governance*; and WP 4.3: *Supporting the development of secure, interoperable services*.

Privacy and trust

Trustmarks

As online users, we increasingly face the decision of whether or not to trust specific applications or services. One way we deal with this situation is by taking decisions based on recommendations made by our family, friends, colleagues or other trusted sources. In addition, an increasing number of trust indicators, such as trustmarks and seals, are becoming available to assist us in our decision-making. These labels are issued by national, international or commercial bodies, most of which use standardised methodologies for assessing and certifying products, processes, or persons. The EU data protection legislation framework is also under revision and further work is being carried out in the area of privacy seals by bodies such as the European Commission's Directorate General for Justice (DG JUST) and the Joint Research Centre (JRC). This work complements that of other initiatives and provides a good starting point for further work by other stakeholders.

Deliverable: Developing recommendations for an EU approach on certification schemes. Identifying criteria and certification levels for trustmarks – delayed, due to postponement of the EC project on seals.

The right to be forgotten

The right to be forgotten is included in the proposed Regulation on data protection published by the European Commission in January 2012. The Regulation remains to be adopted by the European Parliament before entering into force. The different legal aspects of the right to be forgotten, such as the right to erasure or the right to oblivion, have been debated in different contexts and are beyond the scope of this paper. Instead, with this paper we focus on the technical means to enforce or support the right to be forgotten in information systems. The paper shows that there are technical limitations as well as the need to clearly define terminology and legal aspects.

The report *The Right to be forgotten* - between expectations and practice is available at:

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten

Privacy considerations of online behavioural tracking

Internet users are being increasingly tracked and profiled and their personal data are used extensively as currency in exchange for services. It is important that this new reality is better understood by all stakeholders in order to support and respect the right to privacy.

The report Privacy considerations of online behavioural tracking is available at:

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking

Annual Privacy Forum 2012

Privacy is an area that is multidisciplinary by its nature. Regulations, legal frameworks, technology, user adoption, and economic considerations are all necessary for elevating privacy to the status of an accepted societal norm. A crucial element of individual protection and autonomy is also individuals' ability to understand and act on their context, assisted by appropriate and intuitive tools.

Against this backdrop, the first Annual Privacy Forum (APF'12) was held in Limassol, Cyprus from 10-11 October 2012. The Forum was co-organised by ENISA and the European Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT), with the support of the Department of Computer Science of the University of Cyprus. APF'12 was endorsed as an official event of the Cyprus Presidency of the Council of the European Union. At the Forum, 20 papers were presented and four technical sessions and three panel sessions were held. In addition, keynote speakers representing the Council Presidency, the European Commission, industry and research participated in the event. APF'2012 was attended by 71 researchers, academics, industry representatives and policy makers from 12 countries (including several non-EU countries), exceeding the objectives set. Moreover, the Forum website has had more than 1,000 visitors, over 1,700 visits and over 5,500 page views.

The main objective of the Commission and ENISA is for the Forum to evolve into an annual event that will foster dialogue between the policy, research and industrial communities, thus "closing the loop from research to policy".

The report of the Annual Privacy Forum is available at:

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/report-on-annual-privacy-forum-2012

Security governance

Supply chain integrity

Supply Chain Integrity (SCI) in the ICT industry is a topic receiving attention from both the public and private sectors – including vendors, infrastructure owners, operators, and others – as part of a wider review of supply chain management. Understanding supply chains is critical to business success and thus to the economy of nation states. ENISA focused on supply chain integrity in 2012 with a view to providing guidance to EU Member States. One of the many aims of this work was to identify what SCI means in the ICT context and to propose means for ensuring SCI, primarily by taking the telecommunications sub-sector as a model for ICT in general.

The report An overview of the ICT supply chain risks and challenges, and vision for the way forward is available at:

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/sci

Methodology for severity assessment of data breaches

In 2011, the Agency developed specific technical recommendations for the implementation of Article 4 of the e-Privacy Directive, these included:

- 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 sector

As a continuation of this work, in 2012 ENISA collaborated very closely with the national Data Protection Authorities participating in the Technology Subgroup of the Art. 29 Working Party on developing a specific methodology for assessing the severity of data breaches. In view of the need for extensive discussions among multiple national Data Protection Authorities, this work was not finalised in 2012 and will continue in the first quarter of 2013.

Electronic identities and trust services

Notifications of security breaches at trust service providers

E-Government services have significant potential to make public services more efficient for the benefit of citizens and businesses in terms of time and money, and while these benefits are increasingly being realised at the national level, e-Government services still face administrative and legal barriers at the cross-border level. In order to remove existing barriers to cross-border e-ID based services, the European Commission has proposed a draft Regulation on electronic identification and trust services for electronic transactions in the internal market, which will replace the existing Electronic Signature Directive 1999/93/EC. Article 15 of the proposed Regulation requires that trust service providers undertake extensive security measures and notify competent bodies of any breach of security and loss of integrity that could have a significant impact on the trust service provided and on the personal data maintained therein. ENISA has reviewed the feasibility of implementing this article and provided guidelines for such implementation.

The report Implementation of article 15 of the draft Regulation on electronic identification and trusted services for electronic transactions in the internal market is available at:

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/implementation-of-article-15

IDENTIFYING AND RESPONDING TO THE EVOLVING THREAT ENVIRONMENT

Information Security is about managing risks and threats linked to the security of information and information systems. ENISA's objective in this work is to provide stakeholders with information on how risks and threats are evolving. More specifically, the aim is to link particular trends to particular stakeholder communities, thereby helping such communities to recognise and respond to changes in the threat landscape that are particularly relevant to their activities. In addition, suitable mitigation strategies have been proposed and recommendations and implementation options for dealing with the identified risks have been identified. The emphasis is on the provision of non-technical information regarding all the components of risks.

ENISA emerging threat landscape

As with information security, the ability to respond to the evolving cyber-threat environment is a journey rather than a destination. There is and will always be an "arms race" in cyber space between attackers and defenders. The bad news is that currently attackers are one step ahead. In this race, it is impossible to know your opponents without understanding their methods of attack. Hence, analysing threats is essential for protecting cyber assets. It needs to be within the focus of information security professionals.

The ENISA Threat Landscape is based on publicly available data and provides an independent view on threats, threat agents and threat trends observed. The current top cyber threats have been identified. In addition, current threat trends have been derived by comparing current threat information with that from previous years. Finally, a number of threat trends for emerging areas of information technology have been identified. The emerging areas taken into account were: Mobile Computing, Social Technology, Critical Infrastructures, Trust Infrastructures, Cloud Computing and Big Data. An overview of the ENISA Threat Landscape is shown in Table 1.

The ENISA Threat Landscape is available at:

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

Given the specific trends towards Mobile Computing, shown in Table 1, ENISA has delivered detailed assessments in the areas of "Consumerization of IT" and "Bring Your Own Device". This work covers risks as well as opportunities emerging from mobile computing. A set of security policies for the mitigation of these risks has been developed.

The report Consumerization of IT: Risk Assessment and Risk Mitigation Strategies and Good Practices is available at:

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Risk_Mitigation_Strategies

The ENISA Threat Landscape is a contribution towards understanding the 'cyber enemy'. Many steps need to follow, however, to collect the intelligence and knowledge needed to defeat cyber-attacks. Some of those steps are:

- Collect and develop better evidence about attack vectors
- Collect and develop better evidence about impact achieved by adversaries
- Collect and maintain more qualitative information about threat agents
- Use common terminology within threat reports
- Include the user perspective
- Develop use cases for threat landscapes
- Collect security intelligence that covers incidents in an end-to-end manner
- Perform a shift in security controls to accommodate emerging threat trends

Key findings regarding the threat landscape

Top Threats	Current Trends	Top Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Trends of the ENISA Landscape

Consumerization of IT and Bring Your Own Device

The risk environment is evolving rapidly, yet we lack of an overall knowledge base for mitigating risks in the areas of Consumerization of IT (COIT) and Bring Your Own Device (BYOD). To address this issue, ENISA conducted an assessment. The assessment provides guidance on developing effective strategies and policies for mitigating the underlying risks. The analysis examines three areas of mitigation that should be considered in concert: technical considerations, governance aspects and the prevailing regulatory environment. Each organisation should create an effective blend of the three areas in their mitigation strategies.

The analysis also identifies relevant security controls that could facilitate the efforts of stakeholders to develop and implement a combination of controls in their risk mitigation plans. While there is no "one size fits all" solution, a combination of controls can be chosen which suits a stakeholder's particular operational setting, strategy and policy requirements.

Identifying Consumerization of IT (COIT) risks

It is important to identify which COIT risks need to be mitigated within your organisation while the window of opportunity still remains open (see opportunity assessment in Consumerization of IT: Top Risks and Opportunities, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/consumerization-of-it-top-risks-and-opportunities/at_download/fullReport)

5 key messages for decision makers

Five key messages for decision makers, such as Chief Information Officers and Chief Executives, have been derived from this report:

- Ensure that governance aspects are derived from business processes and protection requirements and are defined before dealing with technology.
- End-user involvement can effectively mitigate risks. Awareness raising on COIT programmes is highly effective for the enforcement of security policies.
- Periodic risk assessment on COIT programmes should be undertaken to ensure that security policies remain compatible with evolving technologies.
- Keep in mind that encryption complements, but does not replace, strategic risk management within a COIT programme.
- Perform small steps initially and proceed with more complex policies when sufficient experience has been gained.

European Cyber Security Month (ECSM)

Citizens are increasingly relying on the Internet in their everyday lives for banking, shopping, education and a number of other services. It is, therefore, important that they are able to use the Internet in a secure and confident manner.

Making the Internet a better place for all citizens is a shared responsibility, at both the European and global level. The EU Cyber Security Strategy, due for release in the near future, will set out just how important this is, with concrete proposals to improve digital security. Moreover, the European Union has been working with the US, and at last year's EU-US Summit, several steps were agreed upon to help make the online world secure, on both sides of the Atlantic.

For the first time, last October, a European Cyber Security Month (ECSM) took place as a pilot project across Europe. The ECSM campaign raised awareness about Network and Information Security (NIS). It was planned in the EU-US Summit final report and in the roadmap produced by the awareness-raising sub-group of the EU-US Working Group on Cyber-security and Cyber-crime in December 2011. The project was supported by ENISA and the European Commission.

The main objectives of the European Cyber Security Month were to:

- Generate general awareness about Network and Information Security
- Promote safer use of the Internet for all users
- Build a strong track record to raise awareness through the ECSM
- Involve relevant stakeholders
- Increase national media interest through the European and international dimension of the project
- Enhance attention and interest with regard to information security through political and media coordination

This year, eight countries participated in the first European Cyber Security Month: the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain and the United Kingdom. These countries replied positively either to a call for expressions of interest to organise 'Security week' pilot projects sent to all members of the awareness-raising sub-group of the EU-US Working Group on Cyber-security and Cyber-crime, or to a communication campaign on the project initiated by ENISA.

Latvia, together with the Council of the European Union, officially supported the project. Each pilot country decided upon the scope and number of activities and events to be organised.

Over the course of the month of October, a range of local activities and events were held across Europe to raise the security awareness of different target groups. These included, among others:

- Conferences and workshops in Norway, Portugal and Spain
- Media and social media campaigns in Norway and Slovenia
- Non-governmental organisation (NGO) round tables in the Czech Republic
- Competitions and quizzes in Luxembourg, Norway and Slovenia
- Roadshows in the United Kingdom

Each country built on its own existing activities and experience for maximum impact. The private sector was involved in almost all pilot countries. The proportion of campaigns encompassing general users versus those targeting business users was almost the same. A wide variety of key messages were promoted across the different European countries by using a variety of techniques that were fun, exciting and motivating. The wide variety of delivery channels used made it possible to match different messages to different media and opportunities across all sectors and countries.

ENISA supported the organisation of the European Cyber Security Month pilot projects in various ways. The Agency coordinated the organisation of the 2012 ECSM, acting as the hub for all pilot countries by providing suggestions, replying to enquiries and generating synergies between countries when possible. For example, the interaction between Luxembourg and Norway and that between the United Kingdom and Slovenia, along with Norway, demonstrated how successful synergies could be. ENISA provided guidance on how to organise information security campaigns using its methodology on how to prepare and implement awareness campaigns. In addition, the Agency developed a series of common messages and material to help Member States prepare their cyber security education and awareness campaigns in similar ways. This material was recognised by all countries as an important tool in reaching people and getting them to change their behaviour, or for reinforcing good behaviour. The first European Cyber Security Month pilot project was successful, especially because of the engagement, existing good practices and experience of the participating countries.

ACTIVITIES FOR AWARENESS RAISING AMONG END USERS

Involving intermediaries in cyber security awareness raising

ENISA and the European Commission have been co-operating with the US Department of Homeland Security on “Involving Intermediaries in Cyber Security Awareness Raising’’. The project developed mechanisms for cross-border cooperation as well as for public-private cooperation and information exchange. Forty-five EU and US representatives from the private and public sectors gathered in Brussels to discuss the topic of “Involving Intermediaries in Cyber Security Awareness Raising’’.

Key conclusions:

- Make companies aware that awareness raising will help them to create business opportunities and make money by burnishing their brand image.
- Cyber security is a matter of cultural challenge and behavioural change.
- Remember not to scare users and to encourage them to get online, but in a safe way. Do not start technical. This is about communication. Therefore, messages have to resonate with the target audiences.

The report Involving intermediaries in cyber security awareness raising is available at:

http://www.enisa.europa.eu/activities/cert/security-month/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/involving-intermediaries-in-cyber-security-awareness-raising

Collaborative solutions for Network Information Security in education

Collaborative Solutions for Network Information Security in Education intends to bring the reader more useful information that should be immediately applicable in practice. Together with the information we hope to also introduce the reader to the 'can do' attitude that should be deployed by educators and their students of different age groups. The report addresses educators, such as trainers, teachers, and peers involved in formal education and non-formal education, including lifelong learning.

The report consists of three parts, each of which is equally important:

- Results of the survey and consultations with stakeholders involved at different levels in Germany, Romania, The Netherlands, Estonia, Italy, Greece, Ireland and Poland as well as bodies like the Open Web Application Security Project (OWASP)
- ENISA recommendations from 2012 deliverables
- Case studies from Austria, Luxembourg and Denmark

Some of the most important recommendations from the report are:

- Cyber-security strategies should include a subsection on education and research as part of the overall strategy
- There is a need to promote awareness of personal information security and regarding legal advice on misbehaviour
- A new didactic approach and 'textbook-atlas-concept' should be used for NIS manuals
- Using pseudonyms and aliases on the Internet is the first step to protecting your personal data

The report Collaborative solutions for Network Information Security in education is available at:

http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/collaborative-solutions-for-network-information-security-in-education

CH

PUBLIC AFFAIRS

COMMUNICATING CYBERSECURITY RESULTS

ENISA's Public Affairs Unit (PAU) continued to keep the Agency and its mission in the spotlight during 2012. Notable achievements included the redesign of ENISA's web site and the addition of social media to the Agency's communications channels. The year also saw closer cooperation with local and national media, resulting in TV coverage, editorials in the press and articles published in online news portals. PAU gained Europe-wide coverage for Cyber Europe 2012 – the second, and to date, largest, pan-European cyber security exercise.

Broadly speaking, the Public Affairs Unit focused on six areas during 2012:

1. Deepening and broadening audience impact across Europe and locally
2. Gaining increased media coverage
3. Enhancing the use of digital media
4. Ensuring coherence and consistency – communication planning
5. Strengthening the ENISA brand
6. Internal communication

DEEPENING AND BROADENING AUDIENCE IMPACT ACROSS EUROPE AND LOCALLY

As the cyber security information hub, PAU's focus is on communicating the results of ENISA's operational work to diverse audiences through the appropriate channels. This is a key element of ENISA's mandated mission to develop a cyber-security culture that will result in a safe and sound digital society. ENISA's Public Affairs Unit outreach channels include public relations campaigns, digital communications, both external and internal communications, and media activity and events across the EU.

Deepening and broadening communication with various audiences was a major thrust of PAU's work in 2012. To do so, the unit organised or participated in joint events with other EU bodies, such as the high-level cyber event in Brussels that brought ENISA together with representatives of the European Parliament, the European Commission and industry. The Agency also engaged in outreach work, particularly with the local community, such as organising a Europe Day celebration event on Crete to highlight the benefits of information and communication technology for all of Europe's children. The Public Affairs team has also worked to further strengthen ties with Greece's government, which hosts the Agency in Heraklion and Athens. Moreover, in 2012, ENISA engaged in collaborations with the Regional Governor of Crete and the Heraklion local authorities.

GAINING INCREASED MEDIA COVERAGE

ENISA's impact, outreach and media programme provides the Agency with an opportunity to reach many more of its stakeholders than it can through direct means. In 2012, the Agency adopted a new media outreach distribution and media monitoring process to enhance the targeting and reach of its media work. Major accomplishments include:

- Produced and issued 25 media releases.
- Posted more than 80 individual news items on the ENISA web site.
- Many media releases and news items simultaneously published in the Agency's social media channels.

Multi-lingual approach

As a fundamental part of ENISA's work is to make its messages accessible to stakeholders across Europe, the Agency issues media releases in five EU languages: English, German, French, Spanish and Greek, to press, radio, television and web-based news organisations. It also maintains online landing pages in German, French and Greek. ENISA media releases are distributed to both general media, and specialised ICT/Network and Information Security publications and web sites. Media monitoring analysis and in depth-evaluation of the Agency's media output shows that in 2012, this work generated more than 2,000 stories in European news media, and that stories appeared in all 23 EU languages.

Cross-media impact

Figures show a clear correlation between peaks in web visitors and the distribution of media releases in multiple channels, thus demonstrating the beneficial effect of media activity. Overall, ENISA reached a combined potential audience of several million readers, listeners and viewers. Directly, news stories on the ENISA web site received more than 171,000 unique page views in 2012.

Cyber Europe 2012

A major media focus during the autumn was the Cyber Europe 2012 security exercise. This was the second pan-European cyber security exercise, following on from Cyber Europe 2010, and from the first ever EU-US exercise, Cyber Europe 2011. The 2012 exercise was Europe's biggest to date, involving around 400 individual participants. In addition to involvement from all EU Member States, the exercise included the private sector for the first time, with telecommunications, banking, and Internet Service Providers (ISPs) taking part. This major event required a fully coordinated Communication Strategy, drawn up by the Public Affairs Unit, in close collaboration with the Commission, and the Member States. The exercise's 'media footprint' included more than 225 individual stories across Europe and globally. More than 100 of these were on the day of the exercise itself, and included live interviews.

With regard to ENISA's wider work, the Public Affairs Unit organised two special media briefings in Brussels – one in relation to a European Parliament hearing. Other media outreach work included a high-level event examining European cooperation in cyber security. The event involved key EU policy makers, stakeholders, and research and industry participants.

Other media outreach activities

Other press conferences and briefings were targeted at media in specific countries or around Network Information Security special interest areas. As part of its media activities, the Agency also produced a Crisis Communication Strategy and Scenario Plan in 2012, which it will continue to develop in 2013.

DIGITAL MEDIA

ENISA's website continues to be the Agency's principal communications channel. In 2012, development work was carried out to re-design the website and enhance its interactivity for users. A new template layout was introduced throughout the website and the information structure of the home page and publications was improved. A faceted search for publications was introduced to improve the search function. Three mini-sites in French, German and Greek were also launched.

Social media

The launch of social media channels – Facebook, LinkedIn, Twitter and YouTube – has enabled ENISA to connect with new communities or deepen its ties with existing ones. The channels are accessible through the website's home page.

Website Improvements

Further enhancing the website for users, and helping visitors to navigate with greater ease to find the information they are looking for, is an on-going process. To this end, after the launch of the new design, a web usability project was also carried out in 2012, the results of which will be used in 2013 to augment and improve the information architecture of further sections of the site.

Technical improvements in 2012 included the development of web tools for the Agency's extranets (portals), used by specialist expert communities, and the application of all security patches to the Zope application and PHP scripting used by the ENISA site.

Further enhancements and improvements will be carried out on the website in 2013. These will include an improved content structure, based on the results of the web usability project, and further development of the French, German and Greek mini-sites.

Video

Turning to other digital media, in 2012, the Public Affairs Unit produced videos covering key areas of activity, such as the Cyber Europe 2012 exercise, Incident Reporting and a corporate info film and clip. For 2013, ENISA envisages the production of videos and other digital products such as podcasts and info films that underline the achievements in ENISA's major work-streams.

ENSURING COHERENCE AND CONSISTENCY: COMMUNICATION PLANNING

In 2012, the Public Affairs Unit ensured that ENISA's corporate communications activity was fully aligned with ENISA's operational and policy development goals. Partly this entailed forming close links with the European Parliament, the European Commission, the Council and Member States. All communications activity falls 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 on the Agency's work. In addition, the continuing provision of high quality editorial, graphic design and printing services, through contracts managed by PAU, has helped to ensure quality and consistency in ENISA's communications.

STRENGTHENING THE ENISA BRAND

Branding

Given the nature of ENISA's mission, branding is an important aspect of PAU's work. A strong ENISA brand helps the Agency to achieve consistent and coherent results with all of its communications. It raises awareness and increases understanding regarding Network Information Security issues. The ENISA brand was strengthened in 2012 through several means:

- **Visual identity**: the ENISA brand's visual identity was developed further in 2012 through updated brand guidelines. The new visual identity will be launched in early 2013.
- **Campaigns**: to increase awareness and recognition of the ENISA brand, campaigns were run in Brussels-based publications.
- **Promotional material**: promotional material has been produced on a regular basis and distributed both during corporate events and to visitors. Special focus was given to children this year, notably with the Europe Day celebrations.

An effective brand strategy is the key to connecting effectively with our audiences. Therefore, refreshing the look and feel of ENISA material will create a new chapter in the way the Agency communicates and is perceived.

Publications

Publications are the 'face' of the ENISA brand and an important communication tool given ENISA's mission. Through 2012, ENISA published around 40 publications as Work Programme 'deliverables' and produced around 30 other reports, papers and studies. The Public Affairs Unit assists with the editing and design of these publications, and during 2012, a brand new publication review process was developed, with the close support of the Agency's Quality Control Advisor.

Along with the writing and design of the Agency's General Report, in 2012, the Public Affairs team also produced a special report for the ENISA high-level event in November, EU Cyber cooperation: the digital frontline. The report gave an overview of Europe's cyber security position and examined areas where cooperation can ensure a secure digital environment.

In 2012, the Public Affairs team worked with the Agency's NIS experts to step up the frequency of its special Flash Notes – short expert reports published to provide advice, guidance or commentary on a 'hot topic' in security. Subjects covered included the Flamer cyber attacks on Middle-Eastern oil and gas companies, the 'high roller' automated attacks on bank accounts, and the ease with which customers' passwords can be stolen from some large organisations. The Flash Notes were extremely well received because of their frankness and immediacy, and the Agency will do more in this area in 2013. In early 2013, PAU will also begin publication of a brand new ENISA monthly newsletter.

On a wider front, a poster campaign for child protection online was successfully launched, and will be translated and distributed in every Member State through the EU Representations and Info points.

INTERNAL COMMUNICATION

Employees are ENISA's key ambassadors and reaching them successfully is both challenging and rewarding. Defining common ground between 60 members of staff from 18 different Member States is a continuous challenge. Activities revolving around internal information planning, best practices and resourcing help to shape a culture of cooperation and support within ENISA, a culture which is developed through staff meetings and social events, as well as through an in-house intranet platform. The dynamics of the workplace are changing internal communications, however, as the rapid development of communications-related technology and the rapid expansion of communications channels create opportunities and challenges.

During 2012, employee engagement has been encouraged through follow-up on internal surveys and teambuilding events. Strengthening common goals for all staff and encouraging on-going interaction have also been crucial at a time when the Agency has been reorganised, and greater focus placed on the Agency's Athens-based mobile team. Clear communication is essential during times of change, and the Public Affairs team is closely involved in keeping staff updated on these developments.

CONFERENCES, JOINT EVENTS AND VISITS

The Public Affairs events coordinator organised 60 ENISA conferences and events in 2012. In addition, the Agency took part in numerous external events and high-level European conferences.

One of the key events during the year was ENISA's high-level event, "EU cyber cooperation", which took place in November in Brussels. The event explored how greater cooperation can help to enhance cyber security across Europe, and brought together experts from the European Commission, the European Parliament and industry. An audience made up of people from the worlds of network and information security and politics had the opportunity to watch the debate and put questions to the panel.

In addition to these activities, the Public Affairs Unit provided support to the Executive Director for his participation in events across Europe. These included a round table presentation at the European Parliament, made at the special request of members of the Parliament's Committee for Industry, Research, and Energy (ITRE) Committee. In-house events facilitated by the Public Affairs team included a visit in July by MEPs from the European Parliament's ITRE Committee. The group included Rapporteur, Giles Chichester, Amelia Andersdotter and Ivailo Kaflin.

In September, MEP Jutta Haug, a Vice Chair of the Parliament's Budget Committee, visited the Agency to learn more about its future plans and excellent budgetary performance.

CHA

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 Agency is governed by a **Management Board** (MB), composed of one representative from each EU Member State and EEA country (Iceland, Liechtenstein, and Norway), three representatives from the Commission and three representatives from designated stakeholder groups (the information and communication technology industry, consumer groups; academic experts in network and information security).

In line with established practice, two MB meetings were held as planned during 2012. In addition to several, regular and extraordinary administrative, management and budgetary items, the preparation and subsequent adoption of the Budget and the Work Programme for 2013 were important activities during the year.

Minutes and decisions of the Management Board are available on the ENISA website: http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/minutes-decisions-1

Furthermore, an informal joint meeting between the MB and the Permanent Stakeholders Group took place in February 2012. The meeting focused on setting the priorities and deliverables of the Work Programme 2013. In addition, an informal MB meeting on strategic guidance for Work Programme 2014 was held in November 2012.

For a list of members of the MB, see Appendix: Members of the Management Board

PERMANENT STAKEHOLDERS GROUP

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 advice to the Executive director and input for the annual work programme. The term of office of the PSG is two and a half years. Following the open call for Members in April 2012, a new composition of the PSG was established. The 30 appointed members formally started their term of office on 17 August 2012.

For the list of members of the PSG, see Appendix: Members of the Permanent Stakeholders Group.

The PSG met three times in 2012, in April, September and November. The September meeting was an introductory meeting for the new members, which was followed by the meeting in November to discuss the themes and possible deliverables for the ENISA Work Programme 2014.

RESPONDING TO REQUESTS FOR ASSISTANCE FROM MEMBER STATES

Throughout 2012, ENISA received inquiries as well as a number of requests for advice and assistance according to Article 10 of ENISA's founding Regulation. Altogether, 13 requests according to art. 10 were received by ENISA from various Member States and EU Institutions referring to different areas of NIS-activities.

Please see Appendix 4: Handling of requests for Advice and Assistance in 2012 for more information.

The NLO team

NATIONAL LIAISON OFFICER (NLO) NETWORK

Although not formally based on ENISA's Regulation, the network of National Liaison Officers (NLOs) is very helpful to the Agency, improving the production of deliverables that match stakeholders' expectations and needs. NLOs serve as ENISA's primary contact point within the Member States. They liaise with national bodies and institutions in their respective Member State, and build and maintain a national network of contacts that includes relevant stakeholders in their country.

NLOs are well placed to reinforce the impact of the Agency in the Member States, and to facilitate the exchange of information between ENISA and its stakeholders as well as amongst them. They do this by disseminating ENISA's deliverables, Press Releases, and procurement and vacancy notices, and by providing feedback on the impact of ENISA deliverables and outcomes in their country.

During 2012, ENISA conducted a survey to gather information about the members of the NCO and the means of dissemination used by each respective NLO. The survey showed that most of the Member States have in place adequate dissemination tools in order to reach a relevant number of stakeholders in the EU. The survey also recommended areas for improvement, such as using structured channels of communication to categorise the information and produce targeted messages to stakeholders.

Also during 2012 the Management Board newsletter distribution list was expanded to include NLOs.

For the list of members of the NLOs, see Appendix: Members of the National Liaison Officers network.

The NLO-network met once in November 2012 in Athens, Greece. The primary purpose of this meeting was a discussion on how to enhance collaboration and the reach of ENISA's dissemination activities within the Member States.

INFORMATION TECHNOLOGY, FACILITIES MANAGEMENT AND ADMINISTRATION

The IT and Facilities Management Unit (ITFMU) and the Administration Department play a supportive yet important role in enabling ENISA's operational units to smoothly and securely execute their work.

INFORMATION TECHNOLOGY

As one of the guardians of Network and Information Security (NIS) in Europe, ENISA needs to practice what it preaches. We therefore strive to achieve a high level of security for our own information technology infrastructure. Moreover, to keep abreast of the latest technological developments, we keep our IT infrastructure up-to-date with the most modern technologies. The IT and Facilities Management Unit (ITFMU) is tasked not only with maintaining ENISA's IT infrastructure and facilities, but with ensuring that the Agency follows IT best practise in doing so.

Collaboration and Mobility

In order to enhance user collaboration and communication, as well as offer integrated online meeting services, ENISA implemented Microsoft Lync in 2012. This service enables ENISA staff to be able to reach and collaborate with the rest of the organisation, no matter where they are located. The system will also include IP telephony in 2013, thus offering full Unified Communications.

Given the high mobility of the ENISA workforce, ENISA implemented Direct Access in 2012. This allows staff to securely connect to internal resources in a transparent manner when they are outside the office. The solution supports multiple factor authentication (Kerberos, Machine Digital Certificate, User credentials) and modern network protocols like IPv6 and IPSEC.

Security

To enhance the security of the internal network, ENISA implemented authentication and encryption of the network connections using IPSEC. This not only ensures the privacy of the data exchanged between ENISA clients and servers, but also the ENISA servers themselves are better protected. This was demonstrated in practice by a penetration test that was conducted against our Intranet by EsCert. The results were very favourable results for ENISA.

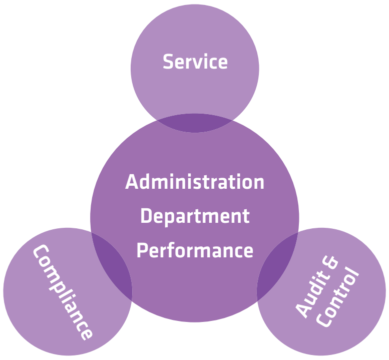
In addition to the above enhancements, ENISA's firewall was upgraded to be fully redundant (hot standby).

FACILITIES MANAGEMENT

Following the agreement to open a branch office in Athens, serious effort was put into the selection of a suitable location. The implementation of Lync telephony as well as Direct Access will allow those staff involved to easily transition to the new office.

ADMINISTRATION

The Administration Department seeks to ensure compliance and deliver services reliably to the ENISA's operational units. It does so by enhancing the functionality of the administrative procedures of the Agency that are mandated by the regulatory framework. The main tasks of the department are represented below:



Human resources

As a knowledge-based organisation, ENISA relies on its personnel to deliver its services to its stakeholders and ensure compliance with the regulatory framework. The Agency also strives to implement modern HR practices such as teleworking and flexitime. As an EU Agency, ENISA benefits from having a diverse multi-national workforce, as demonstrated in the statistics regarding personnel at ENISA presented below:[18]

Staff in service: 58 Staff Members: 42 Temporary Agents (27 TA AD's, 15 TA AST's), 12 CA's, 4 SNE's.

Note: 7 Staff members have double nationality: 2 GR/NL, 1 IT/AU, 1GB/IT, 1 CY/GR, 1 NL/CH, 1 GR/DE.

[18] Last update: 31 December 2012.

Financial resources

In 2012, the Agency committed its appropriations at a rate of 100%, repeating the performance of 2011. This allowed the Agency to carry out its operational activities as specified in the Work Programme 2012, and to make the investments needed to ensure an appropriate operating environment, compliance and the continued provision of services by the Agency. Payments reached the level of 91.45% of the total appropriations managed. This represents a 6% increase over the 85.82% level reached in 2011. Moreover, it demonstrates the strong effort made to finalise administrative and operational activities and deliverables within the financial year and minimise the carry forward of appropriations to the next year. Both commitment and payment rates constitute historical highs for the Agency, and confirm the sustained capacity of the Agency to efficiently utilise its annual budget.

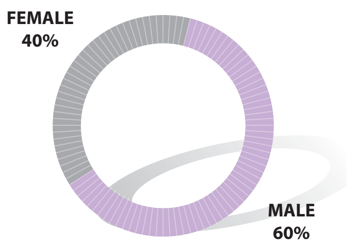
An overview of the year's performance follows below:

Budget Title	Description	Budget ('000 EUR)	Committed ('000 EUR)	%	Paid ('000 EUR)	%
Title 1	Staff expenditure	5,247	5,247	100%	5,088	97%
Title 2	Administrative expenditure	694	694	100%	451	65%
Title 3	Operating expenditure	2,216	2,216	100%	1,921	86%
Total		**8,158**	**8,158**	**100%**	**7,460**	**91%**

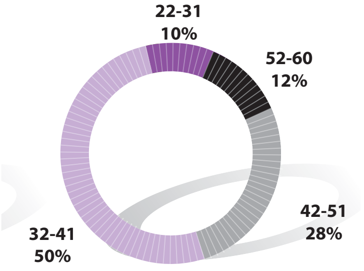
The outturn of contracts awarded as a result of procurement procedures contracted in 2012, is as follows:

- Contracts: 21, including 17 service contracts and 4 framework service contracts.
- Purchase orders: 246, of which 141 were issued under an existing framework service contract.
- Procurement procedures launched: 30, including 9 open procedures consisting of 20 separate Lots.

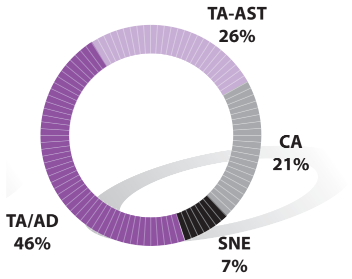
STAFF MEMBERS BY GENDER



STAFF MEMBERS BY AGE

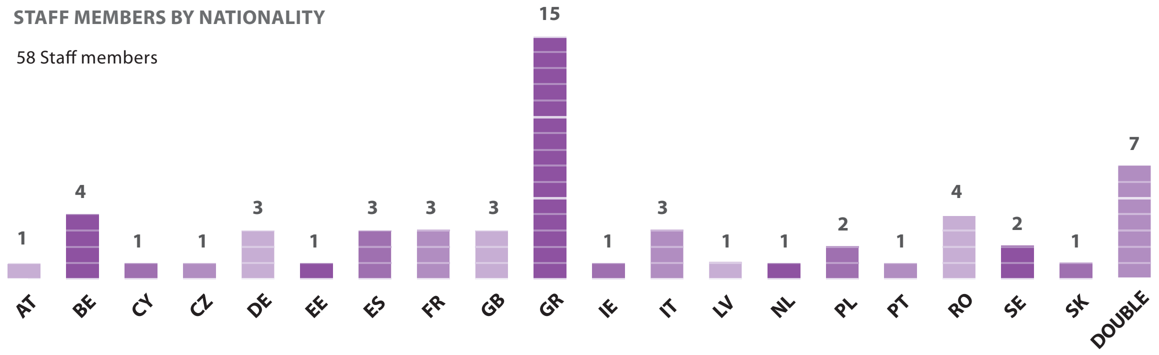


STAFF MEMBERS BY FUNCTION GROUP

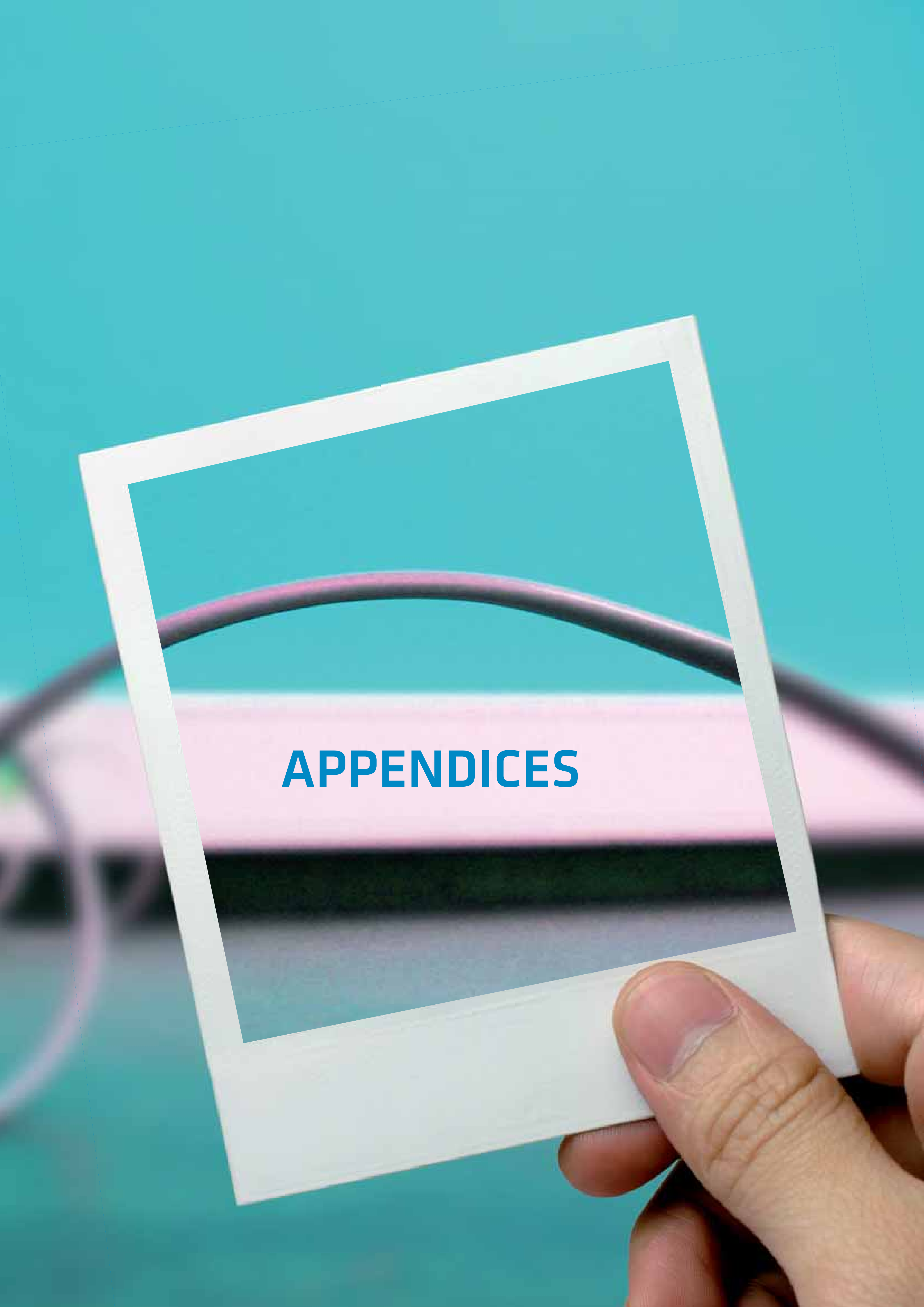


STAFF MEMBERS BY NATIONALITY

58 Staff members



APPENDICES



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 in 2012 was 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* 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 * Replaced Mr. Andrea Servida, alternate, as of 01.07.2012.
Paul TIMMERS *Director in charge for Sustainable and Secure Society* *DG Communications Networks, Content and Technology* paul.timmers@ec.europa.eu * Replaced Mr. Gerard De Graff, member, as of 01.07.2012.	**Jakub BORATYNSKI** *Head of the Unit in charge of the fight against organised crime* *DG Home Affairs* jakub.boratynski@ec.europa.eu
Francisco GARCIA MORÁN *Director-General* *DG Informatics* francisco.garcia-moran@ec.europa.eu	**Marcel JORTAY** *Director in charge of infrastructure services provision* *DG Informatics* marcel.jortay@ec.europa.eu

MEMBER STATES REPRESENTATIVES

Member State	Representative	Alternate
Austria	**Reinhard POSCH** *Chief Information Officer* reinhard.posch@cio.gv.at	**Herbert LEITOLD** *A-SIT, Secure Information Technology Center - Austria Institute for Applied Information Processing and Communication, IAIK Graz* herbert.leitold@iaik.at
Belgium	**Daniel LETECHEUR** *Information Security Analyst* *Fedict* daniel.letecheur@fedict.belgium.be * Replaced Mr. Luc Hindryckx, member, as of 09.07.2012	**Dr. Stéphane VAN ROY** *Engineer-Advisor* *BIPT* Stephane.Van.Roy@bipt.be * Replaced Mr. Charles Cuvelliez, alternate and National Liaison Officer as of 09.07.2012.
Bulgaria	**Valeri BORISSOV** *Director of eGovernance Directorate in the Ministry of Transport, Information Technologies and Communications* vborissov@mtitc.government.bg	**Vasil GRANCHAROV** *Director of Communication and Information Systems Directorate in the Executive Agency 'Electronic Communications Networks and Information Systems'* vgrancharov@esmis.government.bg
Cyprus	**Antonis ANTONIADES** *Senior Officer of Electronic Communications and Postal Regulation* antonis.antoniades@ocecpr.org.cy	**Markellos POTAMITIS** *Officer of Electronic Communications and Postal Regulation* 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* marie.svobodova@mvcr.cz
Denmark	**Flemming FABER** *Senior Adviser* *Ministry of Defence* *Project Office for Cyber Security* *Danish GovCERT* ff@itst.dk	**Thomas KRISTMAR** *Head of Danish GovCERT* *Ministry of Defence* *Project Office for Cyber Security* *Danish GovCERT* tkr@itst.dk
Estonia	**Mait HEIDELBERG** *IT-Counsellor of the Ministry of Economic Affairs and Communications* mait.heidelberg@mkm.ee	**Jaak TEPANDI** *Head of the Chair of Knowledge-Based Systems, Department of Informatics, Tallinn University of Technology* jt@tepinfo.ee
Finland	**Mari HERRANEN** *CHAIR OF ENISA MANAGEMENT BOARD* *Senior Adviser* *Ministry of Transport and Communications, Communications Policy Department* mari.herranen@lvm.fi	**Pauli PULLINEN** *Senior Officer* *Ministry of Transport and Communications* *Communications Policy Department* pauli.pullinen@lvm.fi * Replaced Mr. Mikael Kiviniemi, alternate as of 16.05.2012.
France	**Patrick PAILLOUX** *Director General of ANSSI* *(French Network and Information Security Agency)* 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)* michael.hange@bsi.bund.de	**Roland HARTMANN** *Head of International Relations* *Federal Office for Information Security (BSI)* SIB@bsi.bund.de

Member State	Representative	Alternate
Greece	**Nikos MOURKOGIANNIS** nikos@nikos.com * Replaced Mr. Constantine Stephanidis, member, as of 12.10.2012.	**Theodoros KAROUBALIS** *Hellenic Ministry of Transport and Communications* t.karoubalis@yme.gov.gr
Hungary	**Ferenc SUBA** *VICE-CHAIR OF ENISA MANAGEMENT BOARD* *International Representative* *National Cybersecurity Center* Ferenc.Suba@cert-hungary.hu	
Ireland	**Aidan RYAN** *Telecommunications Adviser* *Department of Communications* Aidan.Ryan@dcmnr.gov.ie	**Paul CONWAY** *Head of Compliance and Operations* *Commission for Communications Regulation* 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* rita.forsi@sviluppoeconomico.gov.it	**Alessandro RIZZI** *Audiovisual and Telecommunications* *Permanent Representation of Italy to the European Union* tlc@rpue.esteri.it
Latvia	**Edmunds BEĻSKIS** *Director of Communications Department* *Ministry of Transport and Communications of the Republic of Latvia* edmunds.belskis@sam.gov.lv	**Maris ANDZANS** *Head of Transport and Communications Security Division* *Ministry of Transport and Communications of the Republic of Latvia* 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* francois.thill@eco.etat.lu	**Pascal STEICHEN** *Ministry of the Economy and Foreign Trade* *Department for electronic commerce and information security* pascal.steichen@eco.etat.lu
Malta	**Charles MIFSUD** *Team Leader* *Computer Security Incident Response Team (CSirt)* charles.h.mifsud@gov.mt * Replaced Mr. George Zammit, member, as of 27.09.2012.	**Rodney NAUDI** *Malta Information Technology Agency (MITA)* 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* e.r.delange@minez.nl	**Peter HONDEBRINK** *Ministry of Economic Affairs, Agriculture and Innovation* *Dir.-Gen. for Energy, Telecommunications and Markets* j.p.hondebrink@minez.nl

Member State	Representative	Alternate
Poland	**Krzysztof SILICKI** *Technical Director* *Research and Academic Computer Network (NASK)* krzysztof.silicki@nask.pl	**Piotr DURBAJŁO** *Deputy Director of the IT Security Department* *The Internal Security Agency* pdurbajlo@abw.gov.pl
Portugal	**José TORRES SOBRAL** *DiretorGeral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança* jtsobral@netcabo.pt * Replaced Mr. Pedro Manuel Barbosa Veiga, member, as of 02.07.2012.	**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 * Replaced Mr. Manuel Filipe Pedrosa De Barros, alternate, as of 02.07.2012.
Romania	**Liviu NICOLESCU** *Director General* *CERT Romania* liviu.nicolescu@cert-ro.eu * Replaced Mr. Victor Vevera, member, as of 06.09.2012.	**Dan TOFAN** *Technical Director* *CERT Romania* dan.tofan@cert-ro.eu * Replaced Mr. Bogdan Popescu, alternate, as of 06.09.2012.
Slovakia	**Peter BIRO** *Information Society Division* *Ministry of Finance of the Slovak Republic* peter.biro@mfsr.sk	**Ján HOCHMANN** *Director* *Information Society Division* *Ministry of Finance of the Slovak Republic* jan.hochmann@mfsr.sk
Slovenia	**Gorazd BOZIC** *Head* *ARNES SI-CERT* gorazd.bozic@cert.si gorazd.bozic@arnes.si	**Denis TRCEK** *Laboratory of e-media,* *Head Faculty of Computer and Information Science* *University of Ljubljana* denis.trcek@fri.uni-lj.si
Spain	**Manuel ESCALANTE GARCIA** *Director General* *Instituto Nacional de Tecnologias de la Communication (INTECO)* manuel.escalante@inteco.es * Replaced Mr. Salvador Soriano Maldonado, member, as of 21.09.2012.	**Ignacio GONZALEZ UBIERNA** *Deputy director for Corporate Development* *Instituto Nacional de Tecnologias de la Communication (INTECO)* Ignacio.gonzalez@inteco.es * Replaced Mr. Juan Llorens, alternate, as of 21.09.2012.
Sweden	**Jörgen SAMUELSSON** *Deputy Director Division for Information Technology Policy Ministry of Enterprise, Energy and Communications* jorgen.samuelsson@gov.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	**Colin WHORLOW** *Head of International Relations* *CESG* colin.whorlow@cesg.gsi.gov.uk

STAKEHOLDERS' REPRESENTATIVES

Group	Representative	Alternate
Information and communication technologies industry	**Mark MACGANN** *Senior Vice President, Head of Government Affairs and Public Advocacy* *Member of the European Management Team* *NYSE Euronext* mmacgann@nyx.com mailto:mark.macgann@eicta.org	**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* 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* kai.rannenberg@cepis.org	**Niko SCHLAMBERGER** *President* *Slovenian Society INFORMATIKA* *Statistical Office of the Republic of Slovenia, Secretary* niko.schlamberger@gmail.com

EEA-COUNTRY REPRESENTATIVES (OBSERVERS)

Group	Representative	Alternate
Iceland	**Björn GEIRSSON** *Director of Legal Divison* *Post and Telecom Administration in Iceland* bjorn@pfs.is	
Liechtenstein	**Kurt BÜHLER** *Director* *Office for Communications* Kurt.buehler@ak.llv.li	
Norway	**Jörn RINGLUND** *Deputy Director General* *Ministry of Transport and Communications* *Department of Civil Aviation, Postal Services and Telecommunications* 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 * Replaced Mr. Eivind Jahren, alternate, as of 16.05.2012.

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 2012-2015

Name		Job Title	Organisation	Nationality	Sector
Constance	**Bommelaer**	Director	Internet Society (ISOC)	French	Users
Martin	**Boyle**	Senior Policy Advisor	Nominet	British	Industry
Ilias	**Chantzos**	Director of Government Relations	Symantec	Greek	Industry
Raoul	**Chiesa**	Principal	Cyberdefcon Ltd	Italian	Industry
Nick	**Coleman**	Global Cloud Security Leader	IBM	British	Industry
Andrew	**Cormack**	Chief Security Adviser	JANET(UK)	British	Users
Gianluca	**D'Antonio**	CISO	FCC Group	Italian	Users
Harald	**Deppeler**	Information Security Manager	Google Switzerland GmbH	Swiss	Industry
Christos	**Dimitriadis**	Head of Information Security	INTRALOT Group	Greek	Users
Serge	**Droz**	Head of SWITCH Security	SWITCH	Swiss	Industry
Stefan	**Fenz**	Senior Researcher	Vienna University of Technology	Austrian	Academia
Patrick	**Froyen**	Senior IT Expert	European Central Bank	Belgian	Users
Denis	**Gardin**	Senior Vice president	CASSIDIAN SAS	French	Industry
Corrado	**Giustozzi**	lecturer	Università Campus Biomedico	Italian	Academia
Marcos	**Gómez-Hidalgo**	Security/e-Trust Deputy Manager	INTECO	Spanish	Users
Janusz	**Gorski**	Professor of Software Engineering	Gdansk University of Technology	Polish	Academia
François	**Gratiolet**	CSO	Qualys, Inc.	French	Industry
Dimitris	**Gritzalis**	Professor of ICT Security	Athens University of Economics and Business	Greek	Academia
Bruno	**Halopeau**	Information Assurance & Cyber Defence First Officer	Europol	French	Users
Stamatis	**Karnouskos**	Senior Researcher/ Research Expert	SAP	Greek, German	Industry
Cornelia	**Kutterer**	Director	Microsoft	German	Industry
Mika	**Lauhde**	Director	Nokia	Finnish	Industry
Jean-Pierre	**Mennella**	Cyber Security Manager	Alstom Grid Power Electronic and Automation	French	Industry
Katerina	**Mitrokotsa**	Senior Researcher	Ecole Polytechnique Federale de Lausanne	Greek	Academia
Rain	**Ottis**	Scientist / Senior Analyst	NATO Cooperative Cyber Defence Centre of Excellence	Estonian	Industry
Bart	**Preneel**	Professor	Katholieke Universiteit Leuven	Belgian	Academia
Alfredo	**Reino**	Security Solutions Architect	Verizon	Spanish	Industry
Volker	**Schneider**	Senior Business Development Manager	secunet Security Networks	German	Industry
Marc	**Vael**	Chief Audit Executive	SMALS vzw	Belgian	Industry
Claire	**Vishik**	Security Policy/ Technology Manager	Intel	USA	Industry

APPENDIX 3: ENISA NATIONAL LIAISON OFFICERS

(Status: 31.12.2012)

Member State	National Liaison Officer
Austria	**Mr. Timo MISCHITZ** *Austrian Federal Chancellery* *Federal ICT Strategy* *Cyber Security Coordinator* Tel.: + 43 1 53115 2545 timo.mischitz@bka.gv.at
Belgium	**Mr. Stéphane VAN ROY** *Belgian Institute for postal services and telecommunications Advisor* Tel.: + 32 2 226 87 68 stephane.van.roy@IBPT.BE
Bulgaria	**Ms. Tsvetanka KIRILOVA** Head of the Interoperability and Information Security Department *Ministry of Transport, Information Technologies and Communications* Tel.: + 359 2 949 20 60 tskirilova@mtitc.government.bg
Cyprus	**Mr. Neophytos PAPADOPOULOS** *Director of the Commissioners Office for the control of the Telecommunications and Postal services* Tel.: + 357 22 69 31 06 neophytos.papadopoulos@ocecpr.org.cy **Mr. Antonis ANTONIADES** *Senior Officer of the Commissioners Office for the control of the Telecommunications and Postal services* Tel.: + 357 22 69 31 15 antonis.antoniades@ocecpr.org.cy
Czech Republic	**Ms. Marie SVOBODOVÁ** *Communication Infrastructure Department* *Ministry of Interior of the Czech Republic* Tel.:+ 420 974 817 544 marie.svobodova@mvcr.cz
Denmark	**Mr. Flemming FABER** *Head of Division of the IT-Security Division* *National IT and Telecom Agency* Tel.+45 3545 0364 ff@itst.dk
Estonia	**Mr. Toomas VIIRA** *Head of CIIP Department* *Estonian Information System's Authority* Tel.: + 372 6630243 toomas.viira@ria.ee
Finland	**Mr. Pauli PULLINEN** *Policy Department Senior Officer* *Ministry of Transport and Communications* Tel: + 358 295 342 680 pauli.pullinen@LVM.FI
France	**Mr. Jean-Baptiste DEMAISON** *ANSSI, International Relations* Tel.: + 33 1 71 75 82 63 rit.sr.eu@ssi.gouv.fr
Germany	**Ms. Fabienne MIDDEKE** *Federal Office for Information Security* *International Relations* Tel.: + 49 228 99 9582-5818 SIB@bsi.bund.de
Greece	**Mr. Panagiotis PAPASPILIOPOULOS** *General Directorate of Communications* *Ministry of Transport and Communications* Tel.: +30 210 6508538 p.papaspil@yme.gov.gr
Hungary	**Mr. Ferenc SUBA** *Chairman of the Board of CERT-Hungary* Tel.:+36 1 301 2080 ferenc.suba@cert-hungary.hu
Ireland	**Mr. John MOORE** *Communications business & technology division* *Department of communications* John.Moore@dcenr.gov.ie
Italy	**Ms. Rita FORSI** *Director General* *Ministry of Economic Development* Tel.: +39 6 54442360 rita.forsi@sviluppoeconomico.gov.it
Latvia	**Mr. Viktors LIPENITS** *Transport and Communications Security Division, Senior Expert* *Ministry of Transport and Communications* Tel.: + 371 670 28 227 Viktors.Lipenits@SAM.GOV.LV
Lithuania	**Mr. Vaidotas RAMONAS** *Chief Specialist of Internet Surveillance Division* *Communications Regulatory Authority* Tel.: +85 210 5676 vramonas @ rrt.lt

Member State	National Liaison Officer
Luxembourg	**Mr. Manuel SILVOSO** *Ministry of the Economy and Foreign Trade - Department for e-commerce and information security* Tel.: + 352 247 88429 Fax: + 352 247 84311 manuel.silvoso@eco.etat.lu
Malta	**Mr. Martin CAMILLERI** *INFOSEC Authority, Cabinet Office, Office of the Prime Minister* Tel.: +356 2200 1285 martin.d.camilleri@gov.mt
The Netherlands	**Mr. Edgar DE LANGE** *Ministry of Economic Affairs* *Directorate-General for Energy and Telecommunications* *ALP C/334* Tel.: + 31 70 379 8153 e.r.delange@minez.nl
Poland	**Mr. Krzysztof SILICKI** *Technical Director* *Research and Academic Computer Network NASK* Tel.: + 48 22 5231315 krzysztof.silicki@nask.pl
Portugal	**Mr. Lino SANTOS** CERT.PT/FCCN, *Director of security and users services* Tel.: +351218440100 lino@fccn.pt
Romania	**Mr. Dan TOFAN** *CERT-RO* Tel.: + 752188854 dan.tofan@CERT-RO.EU
Slovakia	**Mr. Rastislav MACHEL** *CISSP* Tel.: + 421-905-622435 Rastislav.Machel@machel-cs.eu
Slovenia	**Mr. Radovan PAJNTAR** *Ministry of Higher Education, Science and Technology, Directorat Information Society Directorate Trg* Tel.: + 386-1-478-46-47 Fax: + 386-1-478-46-65 radovan.pajntar@gov.si
Spain	**Mr. Ignacio GONZÁLEZ UBIERNA** *Deputy Director for Corporate Development* *Instituto Nacional de Tecnologías de la Comunicación (InTeCo)* Tel.: + 34 987 877 189 ignacio.gonzalez@inteco.es

Member State	National Liaison Officer
Sweden	**Mr. Björn SCHARIN** *Adviser* *National Post and Telecom Agency* *Network Security Department* Tel. + 46-8-678 55 98 Bjorn.Scharin@pts.se
United Kingdom	**Mr. Giles SMITH** *Information Economy - Security and Resilience* *Department for Business, Innovation and Skills* Tel.: +44 20 7215 5757 giles.smith@bis.gsi.gov.uk

EEA	National Liaison Officer
Iceland	**Mr. Thorleifur JONASSON** *Director of Technical Division Post and Telecom Administration* Tel.: + 354 510 1500 thorleifur@pfs.is
Liechtenstein	**Mr. Kurt BUEHLER** *Director* *Office for Communications* Tel.: + 423 236 6488 Fax: + 423 236 6489 kurt.buehler@ak.llv.li
Norway	**Mr. Hans Einar NERHUS** *Postal Services and Telecommunications Senior Advise* *Ministry of Transport and Communications Department of Civil Aviation* Tel.: + 47 2224 8156 Hen@sd.dep.no

European Commission	**Mr. Ivan BRINCAT** *Policy Officer* Tel.: + 32 2 2965311 Ivan.Brincat@ec.europa.eu

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

APPENDIX 4: HANDLING OF REQUESTS FOR ADVICE AND ASSISTANCE IN 2012

1. Background

This document provides a short summary of the requests for advice and assistance that ENISA has dealt with in 2012.

ENISA is handling requests in line with the following legal framework:

- Art. 10 of the Regulation[19];
- the implementing decision of the Management Board[20]; and
- its internal procedure[21].

In the course of developing its internal procedure and policy document, ENISA has built up an intranet platform for responding to art. 10 requests as well as to inquiries in the most efficient way.

2. Scope of Art. 10 requests

Requests for advice and assistance and stated as "requests" in this document and by ENISA are "Article 10-requests". For a request to be classified as an Article 10 request, the following conditions must be satisfied:

- The request for advice and assistance must be made directly to the Executive Director (art. 10.1).
- The request must be made by a qualified entity, being the European Parliament, the Commission, any competent body appointed by a MS such as an NRA as per art. 2 of Directive 02/21/EC (art. 10.2)
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF
- The request for advice and assistance must fall directly within the Agency's scope, objectives and tasks (art. 10.1).
- The request must be accompanied by sufficient background information in order to assess its relevance (art. 10.1).

All other queries that do not fulfil all the requirements of art. 10 of the Regulation as mentioned above are referred to as "inquiries". They are followed up by ENISA while at the same time taking into account its resources and priorities in line with the Work Programme.[22]

[19] According to Art. 10 of 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; as follows "the Regulation".
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[20] Decision of the Management Board of 6 March 2006 on practical arrangements concerning requests to the ENISA.

[21] Internal procedure "Handling Of Requests For Advice and Assistance (art. 10 requests)", Version 1.0 final, 29 May 2012

[22] Please note that the new ENISA Regulation, which is currently being negotiated by the European Parliament and the Council of the EU, provides for more flexible criteria as regards the definition of "requests". They will actually be "Art. 14 Requests", as the new regulation enters into force.

3. Requests for advice and assistance received by ENISA

In 2012 up to today, 13 requests have been received by ENISA. This table shows the requests ENISA has received and replied to during 2012. It names both the requestor and the area of activity the specific request refers to.

Nb.	Requestor	Area of NIS activity	Status
1.	Commission, DG INFSO (A3)	Security of the supply chain request for contribution of ENISA	completed
2.	Hellenic Republic, Ministry of Administrative Reform and e-Government	Implementation of eGov services in Greece	completed
3.	Commission, DG INFSO (D4)	PIA Framework follow-up	completed
4.	Commission, DG INFSO (A3)	Legislative Work Programme 2012	completed
5.	Romania	Supporting CERT RO in becoming fully operational	completed
6.	Ireland	Setting up of national CERT	60% (status "reporting and feedback")
7.	Hellenic Data Protection Authority	Implementation of Art4 of the ePrivacy Directive	completed
8.	National CSIRT of Czech Republic	ENISA feedback to draft of Czech Cyber Security Bill	completed
9.	Romania-CERT	CIP Workshop	completed
10.	BSI Germany	Support of DFS (Air Traffic Germany)	60% (status "reporting and feedback")
11.	Commission, DG HOME	Data Security in Data retention reform	25% (project definition and start-up)
12	Poland	ENISA involvement in Polish exercise	Completed
13.	Commission	Sec. Gen. Business continuity corporate exercise	Completed

4.Summary of requests

4.1. Commission, DG INFSO (A3)

DG INFSO requested ENISA for support on the "security in the supply chain" as one of the proposed areas of action for the European Public-Private Partnership for Resilience (EP3R).

ENISA actions: creation of a group of experts, preparation of a document covering the state-of-the-art in the area taking into account of a survey to a selected number of EU National Security Agencies

4.2. Hellenic Republic, Ministry of Administrative Reform and e-Government

The Hellenic Republic requested assistance of ENISA in various areas of ICT.

ENISA actions: Meetings (Hellenic DPA, S. Katsikas, Vice Minister Voloudakis-ED) took place; ENISA provided an overview mapping of eID and the approaches followed within the EU by other MS regarding the following points: how a citizen's id is confirmed, which dbases are used, how as well as how many, their interconnection, how privacy is handled, what they use (cards, mobile apps, etc.); a workshop was held at the ministry of administrative reform and eGov.

4.3. Commission, DG INFSO (D4)

In order to achieve an efficient, effective and truly European implementation of the PIA-Framework, the European Commission monitors the current developments in the Member States and creates conditions for facilitating the emergence of a common European approach. A first milestone in this respect was a conference in Brussels (in CCAB) on 8th February 2012.

ENISA actions: meetings, ENISA participation in EC PIA conference on RFID PIA Framework.

4.4. Commission, DG INFSO (A3)

In Nov2011 the Commission adopted the Commission Legislative Work programme for 2012:

http://ec.europa.eu/atwork/programmes/index_en.htm. In annex I, two initiatives on a "Pan European framework for electronic identification, authentication and signature" and a "European Strategy for Internet Security" were announced. The EC invited ENISA to respond on how the Agency could support the EC in shaping up these initiatives on which we have already started working.

ENISA actions: The following options were found for ENISA to assist the EC in particular:

- the promotion of security standards in public procurement of new/innovative technologies/systems
- the definition of the scope and provisions of the legal measure the EC intends to propose (with Art 114 as legal basis). An element of this measure would be the extension of the applicability of the "security breach notification" model and mechanism of Art 13.a of the FD beyond the electronic communication market, thus covering the information society service (as set in the e-commerce Directive) as well as other sectors. In this regard, the work planned by ENISA on security breach notification for the cloud would be extremely relevant. Another element to reflect upon (wrt the scope) would be how to embrace and/or articulate the link/relation with obligations for critical infrastructure provides.
- Another component of the legal measure, on which ENISA may have already some ideas and provide some support on how to shape the legal provisions, relates to supporting the cooperation and information exchange/communication between National Competent bodies.

4.5. Romania

ENISA received a request to support CERT RO in becoming fully operational, in the areas of

- Incidents response procedures;
- Technical expertise;
- Training;
- Help in development of Romanian early warning system, interconnected with other National systems;
- Help in developing of a national contingency plan.

ENISA actions: Workshop was delivered, request was completed.

4.6. Ireland

ENISA received a request for support in setting a national CERT.

ENISA actions: meetings, support in the national/ governmetal CERT, participation in the TRANSITS I training in Portugal, Porto, information on CERT communities was provided.

4.7. Hellenic Data Protection Authority

The Hellenic Data Protection Authority requested ENISAs collaboration.

ENISA actions: following the invitation of art. 29 Technology Subgroup to ENISA to collaborate in the implementation of pilots regarding the art. 4 publication in 2 MS, it was decided to carry out the first two pilots in collaboration with the DPAs of Greece and Poland; meetings took place; Hellenic DPA participated in the pilots (tests) of severity assessment methodology, workshop in Athens took place.

4.8. National CSIRT of Czech Republic

The Czech Republic requested ENISA's feedback to the draft of the Czech Cyber Security Bill.

ENISA actions: ENISA provided comments on the document contributing to the preparation of the drafting of the bill on cyber security in the Czech Republic.

4.9. Romania CERT

Romania CERT requested ENISA's help in the organisation of a CIIP workshop/exercise.

ENISA actions: The CIIP workshop took place.

4.10. BSI Germany

The BSI Germany requested ENISAs support of DFS (Air Traffic Germany).

ENISA actions: The Deutsche Flugsicherung GmbH (DFS) is working on a norming effort of CEN TC 377 (Air Traffic Management committee) with the subject of security in ATM. Coordination with ENISA on this issue has taken place, i.e. the interoperability of risk assessments performed by the different stakeholders.

4.11. Commission (DG HOME)

The request by DG HOME for support consisted of two elements:

- On the one hand, ENISA was requested to provide input and comments on the benefits, main impacts and possible means of enforcement of new data security measures in the reform of the EU legal framework for data retention.
- ENISA was also requested to assess the current implementation of data security measures for data retention in selected MS that can be considered as "best practice" in this respect.

ENISA actions: Due to the results of an internal assessment in DG Home, and the identified dependencies with ePrivacy directive, the reform is delayed and as such the request for finalizing this request was shifted to the second part of 2013. ENISA will start working in March with the new contractors for the survey and also for the state-of-the art recommendations for data security.

4.12. Poland

Poland asked for ENISA's assistance with their national cyber exercise.

ENISA actions: Advice was provided, organisation of a seminar.

4.13. Commission, SG

The Commission's Secretariat General asked for ENISA's assistance regarding the Business Continuity Corporate Exercise 2012.

ENISA actions: providing of a seminar to relevant Commission staff on organising/planning cyber exercises, providing a skeleton cyber scenario using Cyber Europe's 2012 basic scenario adapted to the needs of the Commission, participation in a workshop.

Fulfilment of SMART goals and KPIs

Below SMART goals and KPIs regarding requests for advice and assistance have been successfully achieved:

SMART Goal	KPI	Achieved
In 2012, at least 3 request will result in a suitable policy update of the requesting party	Number of requests Number of policy updates	6
In 2012 at least 5 requests will be received by ENISA	Number of requests received	14
In 2012 at least 3 requests will be responded to by ENISA	Number of responses to requests	14
Drafting a reply to a request should not exceed 50 person days per request	Time	Fulfilled
Overall time for accepting/rejecting a request should not exceed 10 working days (from registration to reply to Sender)	Time	Fulfilled

Inquiries

In 2012, ENISA has also dealt with a number of queries that do not qualify as requests according to art. 10 Regulation because they do not fulfil all requirements as laid down in art.10. These queries are referred to as “inquiries”, they are not foreseen in ENISA’s annual Work Programme but the Agency handles them anyway, if workload and resources allow so.

Therefore in 2012, ENISA has received a number of inquiries. This list provides a short overview of these inquiries:

Nb.	Requestor	Area of NIS activity	Status
1.	Italy	Support in setting up of national CERT	20% (status “reporting and feedback”)
2.	Lithuania	internet networks infrastructure, resilience and monitoring projects	completed
3.	Telecommunications Administration in China	Visit to ENISA	completed - visit postponed
4.	Bosnia and Herzegovina	Support in setting up of CERT through TAIEX program	completed
5.	Interpol	ENISA’s participation as observer at @tomic 2012	completed
6.	Ireland	Setting up of national CERT	60% (status “reporting and feedback”)
7.	Malta	Cross-border cooperation for national Csirts	completed
8.	Croatia	RACVIAC Cyber Security Roundtable	completed
9.	Bulgaria	E-government project	completed

APPENDIX 5: ACRONYMS AND ABBREVIATIONS

APF	Annual Privacy Forum
BYOD	Bring Your Own Device
CERT	Computer Emergency Response Team
CERT-RO	Computer Emergency Response Team-Romania
CIIP	Critical Information Infrastructure Protection
CIIs	Critical Information Infrastructures
COIT	Consumerization of IT
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG JUST	Directorate-General for Justice
EC	European Commission
EC3	European Cyber Crime Centre
ECCCF	European Cyber Crisis Cooperation Framework
ECSM	European Cyber Security Month
EEA	European Economic Area
EFTA	European Free Trade Area
EP3R	European Public-Private Partnership for Resilience
EISAS	European-wide Information Sharing and Alert System
ETSI	European Telecommunications Standards Institute
EU-SOPs	European Standard Operating Procedures
EuroSOPEx	European Standard Operating Procedures Exercises
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
INCSC	Irish National Cyber Security Centre
ISP	Internet Service Provider
ITFMU	Information Technology and Facilities Management Unit
ITRE	Industry, Research, and Energy Committee
JRC	Joint Research Centre
LEAs	Law Enforcement Authorities
MAT	Mobile Assistance Team
MB	Management Board
NCPs	National Cyber Contingency Plans
NCSS	National Cyber Security Strategies
NGO	Non-Governmental Organisation
NIS	Network Information Security
NLOs	National Liaison Officers
OWASP	Open Web Application Security Project
PAU	Public Affairs Unit
PPPs	Public-Private Partnerships
PSG	Permanent Stakeholder Group
SCADA	Supervisory Control and Data Acquisition
SCI	Supply Chain Integrity
SLAs	Service Level Agreements
SMEs	Small- and Medium-sized Enterprises
SOPs	Standard Operating Procedures
WPK	Work Package
WS	Work Stream

APPENDIX 6: ENISA DELIVERABLES

The following table contains links to the formal WP2012 deliverables:

WS/WPK/Deliverable	**Status**
WS1: Identifying & Responding to the Evolving Threat Environment	
WPK1.1 Emerging Opportunities & Risks	
D1: Security threat landscape in Europe based on aggregated data collected from stakeholders	Published
D2: Consumerisation of IT (assessment plan)	Published
D3: Cloud Computing Security Risk Assessment	Published
WPK1.2 Mitigation & Implementation Strategies.	
D1: Consumerisation of IT (implementation/mitigation plan)	Published
D2: Procure Secure	Published
WPK1.3 Knowledgebase	
D1: Knowledge Base and associated procedures	Done–no physical deliverable
D2: Stakeholder Requirements (Q4-2012)	Published–internal deliverable only
WS2: Improving Pan-European CIIP & Resilience	
WPK2.1 Further Securing EU's Critical Information Infrastructures and Services	
D1: Cyber Security Risks and Challenges of Smart Grids	Published
D2: Cloud Computing and Critical Services – Cloud Depend encies and Failures	Published
D3: Analysis and Recommendations on Emergency Communications	Published
WPK2.2 Cyber Crisis Cooperation and Exercises	
D1: Report of Cyber Europe 2012	Restricted Access
D2: Status Report on National and International CIIP Exercises	Published
D3: Roadmap on Exercising for CIIP beyond 2012	Restricted Access
WPK2.3 European Public Private Partnership for Resilience (EP3R)	
D1: Dissemination Actions	Done–no physical deliverable
D2: Management of EP3R Working Groups	Done–no physical deliverable
D3: Good practice guide on cybersecurity strategies	Published
D4: EP3R Activity Report & Position Papers	Published
WPK2.4 Implementing Article 13a	
D1: Three Article13a workshops (Q1-Q42012) – Lisbon, Luxembourg, Mainz	Done–no physical deliverable
D2: Frame work for Collecting Annual National Reports of Security Breaches (Architecture and Implementation of Cyber incident reporting and analysis system-CIRAS)	Available upon request
D3: Technical Guidelines on Incident Reporting v2.0	Published

WS/WPK/Deliverable	Status
WS3: Supporting the CERT and other Operational Communities	
WPK3.1 Support and enhance CERTs operational capabilities	
D1: An updated version of the "Baseline capabilities for national/governmentalCERTs".	Published
D2: A status report on level of deployment of current set of baseline capabilities of national/governmental CERTs in the MS).	Published
D3: An updated and (where appropriate) extended set of CERT exercise material; a new scenario on "Early Warning".	Published
D4: A roadmap on how to enhance the roll-out of ENISA exercise material to the CERT communities.	Published
D5: Updated "ENISA Inventory of CERTs in Europe".	Published
D6: Complete update of Inventory document and map.	Published
WPK3.2 Application of good practice	
D1: support at least two TRANISTS basic courses,and in additionon eTRANISTS enhanced (TRANSITS2) course.	Done (no physical deliverable)
WPK3.3 Support and enhance (co)operation between CERTs, and with other communities	
D1: Pilot of the EISAS activity in one Member State, with the help of ENISA and support by at least one other Member State (Q4-2012).	Published
D2: Updated good practice material for addressing NIS aspects of cybercrime.	Published
D3: Findings/conclusions from the 7th annual CERT workshop (full report, to be shared only among workshopparticipants; public report available via web.)	Published
WS4: Securing the Digital Economy	
WPK4.1 Economics of Security	
D1: Cost of Security Incidents	Published
WPK4.2 Security governance	
D1: Survey on current practices in supply chain integrity.	Published
D2: Contributing in extending and implementing the provisions of Article4 of ePrivacy Directive (Data Breach Notification).	Delayed by agreement with Article29TS
WPK4.3 Supporting the development of secure, interoperable services	
D1: Developing recommendations for an EU approach on certification schemes. Identifying criteria and levels of certifications for trust marks.	Cancelled by DGJUST
D2: (renamed)The right to be forgotten – between expectations and practice	Published
D2: Privacy considerations of online behavioural tracking	Published
D3: Annual workshop on Privacy, Accountability and Trust in the Future Internet	organised on 10th-11th October
D4: EU Developments in the area of eIdentity and eSignature (Article15)	Published
PS1: AwarenessRaisingActivities	
D1.Implementation of 2011 recommendations on the European Month of Network & Information Security for all (Q4–2012).	Published
D2: Transfer of experience in implementing NIS with in the school curriculum (Q4–2012).	Published

European Commission

General Report 2012
European Network and Information Security Agency

Luxembourg: Publications Office of the European Union
2013 - II, 64 pp. – 21 x 29.7 cm
ISBN 978-92-9204-065-9
doi:10.2824/16829

TP-AB-13-001-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 2810391280, Fax: +30 2810391410
http://www.enisa.europa.eu

Publications Office

ISBN 978-92-9204-065-9

9 789292 040659