enisa

10 YEARS OF CYBER SECURITY FOR EUROPE 2004-2014

December 2014

Management Board News

Welcome!

Dear reader, welcome to our December Management Board newsletter.

I am pleased to present the December issue of the MB Newsletter. This issue presents media coverage of the Cyber Exercise 2014, the list of ENISA deliverables to be launched to implement Work Programme 2014, as well as tenders launched to start the implementation of the next year's Work Programme. As ever, in 2015, ENISA will continue to publish quarterly newsletters. This way we are able to provide you with important dates as well as other relevant information. Meanwhile, the ENISA staff wish all of you and your families a safe and very happy holiday season!

With best wishes,
Udo Helmbrecht, Executive Director, ENISA

The largest Cyber-Security Exercise

More than 200 organisations and 400 cyber-security professionals from 29 European countries tested their readiness to counter cyber-attacks in a day-long simulation, organised by ENISA on 29th- 31st October, 2014.

Continued on page 2...

CYBER EUROPE 2014 CYBER EUROPE

DATES FOR YOUR DIARY

2015 STATUTORY MEETS

The dates and locations of scheduled meetings are listed below:

19 February
Brussels, Belgium
MB Ad hoc group meeting on Strategy and international cooperation

12 March
Athens, Greece
The EB Meeting

TBD June
Athens, Greece
Informal MB Editorial meeting on WP 2016

21 October
Athens, Greece
The EB Meeting

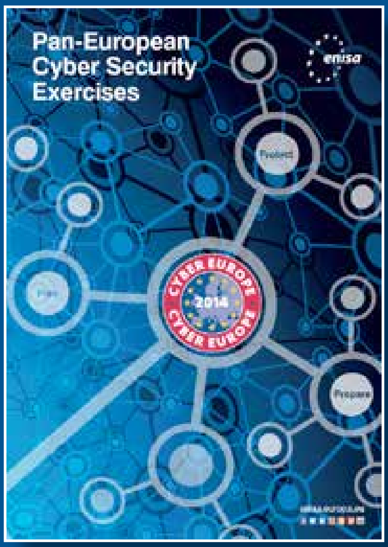
22 October
Athens, Greece
The MB Ordinary meeting

Continued from cover

The heart of European cyber security.
Securing Europe's cyber future
CYBER EUROPE 2014 CYBER EUROPE

The biggest ever Cyber-Security Exercise

EU cyber-crisis cooperation – pan European exercises
enisa
CYBER EUROPE 2014 CYBER EUROPE
enisa.europa.eu


Pan-European Cyber Security Exercises
enisa
Protect
CYBER EUROPE 2014 CYBER EUROPE
Prepare

Following the first phase of CE2014 in April this year, participants joined forces in the operational phase of the exercise to identify collaboration strengths and weaknesses on cybersecurity issues between European countries. This year's exercise focused on targeted attacks on energy infrastructures.

CE2014 Objectives

- **Test cross-country cooperation procedures EU-SOPs (EU-level)**
- **Test national-level capabilities (national-level)**
- **Explore cooperation between private-public and private-private players**
- **Explore the escalation and de-escalation processes (technical-operational-strategic)**
- **Explore the public affairs issues**

Interim results

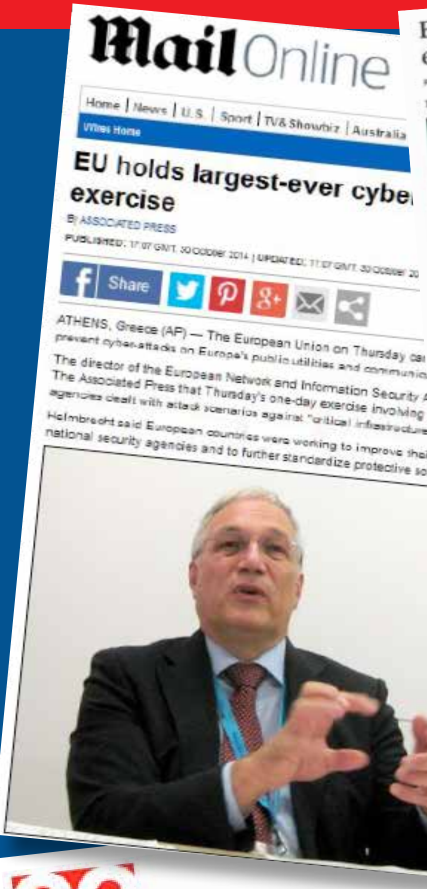
Primary results demonstrate cooperation and standard operating procedures at a national and EU level worked well, with many opportunities for information exchange and collaboration. Further improvement can be achieved and "lessons learnt" have been recorded. As the crisis escalated it was clear that a response is needed at a political level.

Next Steps

A report on the CE2014 - OLEx evaluation will be made publically available in the next months. Additionally, a final after action report will be distributed to participants only (2nd Quarter 2015).

CE2014 Material

Relevant material to the CE2014 exercise with footage, photos, background information and briefing pack can be found on the ENISA website: https://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today



MailOnline

Home | News | U.S. | Sport | TV&Showbiz | Australia

Wires Home

EU holds largest-ever cyber exercise

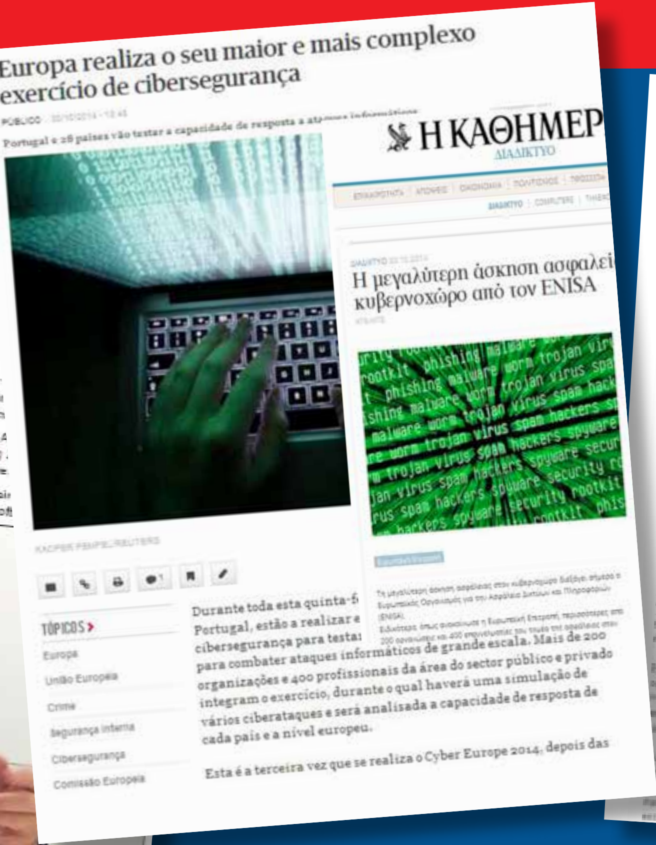
By ASSOCIATED PRESS

PUBLISHED: 17:07 GMT, 30 October 2014 | UPDATED: 17:07 GMT, 30 October 20

ATHENS, Greece (AP) — The European Union on Thursday car prevent cyber-attacks on Europe's public utilities and communic

The director of the European Network and Information Security A The Associated Press that Thursday's one-day exercise involving agencies dealt with attack scenarios against "critical infrastructure

Helmbrecht said European countries were working to improve their national security agencies and to further standardize protective soft



Europa realiza o seu maior e mais complexo exercício de cibersegurança

PÚBLICO · 30/10/2014 - 12:41

Portugal e 28 países vão testar a capacidade de resposta a ataques informáticos

KACPER PEMPEL/REUTERS

TÓPICOS >

Europa

União Europeia

Crime

Segurança interna

Cibersegurança

Comissão Europeia

Durante toda esta quinta-f Portugal, estão a realizar e cibersegurança para testa para combater ataques informáticos de grande escala. Mais de 200 organizações e 400 profissionais da área do sector público e privado integram o exercício, durante o qual haverá uma simulação de vários ciberataques e será analisada a capacidade de resposta de cada país e a nível europeu.

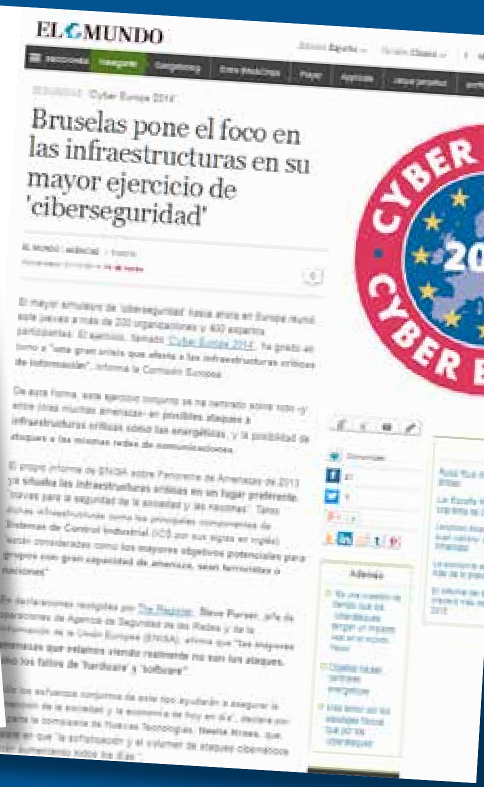
Esta é a terceira vez que se realiza o Cyber Europe 2014, depois das

Η ΚΑΘΗΜΕΡ

ΔΙΑΔΙΚΤΥΟ

Η μεγαλύτερη άσκηση ασφαλεί κυβερνοχώρο από τον ENISA

phishing malware worm trojan virus spam hackers spyware security rootkit



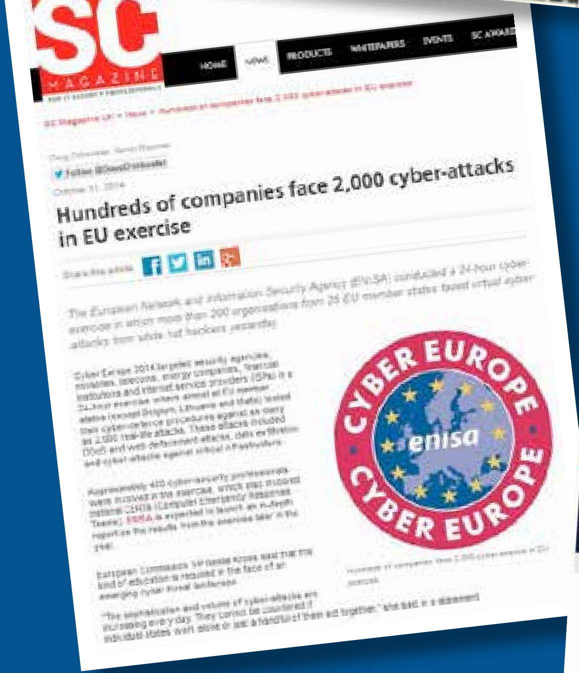
EL MUNDO

'Cyber Europe 2014'

Bruselas pone el foco en las infraestructuras en su mayor ejercicio de 'ciberseguridad'

El mayor simulacro de 'ciberseguridad' hasta ahora en Europa reunió este jueves a más de 200 organizaciones y 400 expertos participantes. El ejercicio, llamado 'Cyber Europe 2014', ha girado en torno a "una gran crisis que afecta a las infraestructuras críticas de información", informa la Comisión Europea.

[illegible]



SC MAGAZINE

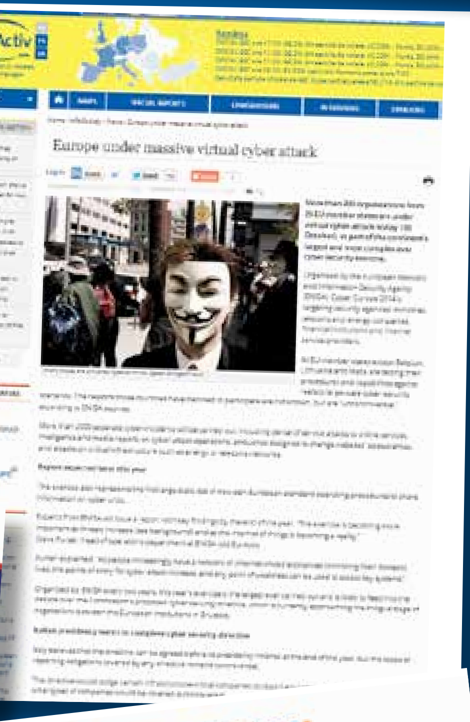
Hundreds of companies face 2,000 cyber-attacks in EU exercise

The European Network and Information Security Agency (ENISA) conducted a 24-hour cyber-exercise in which more than 200 organisations from 26 EU member states faced virtual cyber attacks from white hat hackers yesterday.

[illegible]

Media Coverage

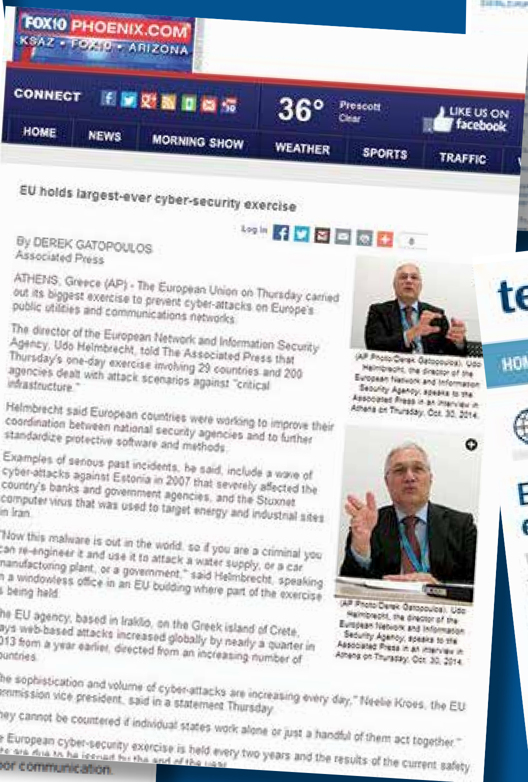
On the day of the launch a total of 400 articles were published, while it is estimated that 800M online users read the news on CE2014. ENISA featured on all major EU and International media outlets. A detailed overview can be found here: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/cyber-europe-2014-media-coverage/view



EurActiv

Europe under massive virtual cyber attack

[illegible]



FOX10 PHOENIX.COM
KSAZ • FOX10 • ARIZONA

EU holds largest-ever cyber-security exercise

By DEREK GATOPOULOS
Associated Press

ATHENS, Greece (AP) - The European Union on Thursday carried out its biggest exercise to prevent cyber-attacks on Europe's public utilities and communications networks.

The director of the European Network and Information Security Agency, Udo Helmbrecht, told The Associated Press that Thursday's one-day exercise involving 29 countries and 200 agencies dealt with attack scenarios against "critical infrastructure."

Helmbrecht said European countries were working to improve their coordination between national security agencies and to further standardize protective software and methods.

Examples of serious past incidents, he said, include a wave of cyber-attacks against Estonia in 2007 that severely affected the country's banks and government agencies, and the Stuxnet computer virus that was used to target energy and industrial sites in Iran.

"Now this malware is out in the world, so if you are a criminal you can re-engineer it and use it to attack a water supply, or a car manufacturing plant, or a government," said Helmbrecht, speaking in a windowless office in an EU building where part of the exercise is being held.

The EU agency, based in Iraklio, on the Greek island of Crete, says web-based attacks increased globally by nearly a quarter in 2013 from a year earlier, directed from an increasing number of countries.

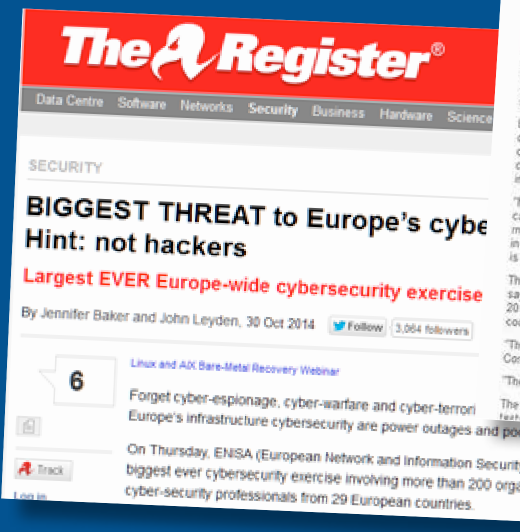
"The sophistication and volume of cyber-attacks are increasing every day," Neelie Kroes, the EU Commission vice president, said in a statement Thursday.

"They cannot be countered if individual states work alone or just a handful of them act together."

The European cyber-security exercise is held every two years and the results of the current safety tests are due to be issued by the end of the year.

(AP Photo/Derek Gatopoulos). Udo Helmbrecht, the director of the European Network and Information Security Agency, speaks to the Associated Press in an interview in Athens on Thursday, Oct. 30, 2014.

(AP Photo/Derek Gatopoulos). Udo Helmbrecht, the director of the European Network and Information Security Agency, speaks to the Associated Press in an interview in Athens on Thursday, Oct. 30, 2014.



The Register®

SECURITY

BIGGEST THREAT to Europe's cybe Hint: not hackers

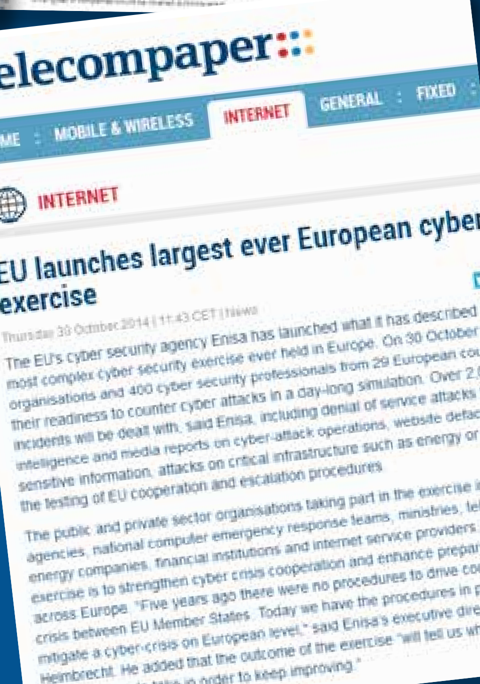
Largest EVER Europe-wide cybersecurity exercise

By Jennifer Baker and John Leyden, 30 Oct 2014

Linux and AIX Bare-Metal Recovery Webinar

Forget cyber-espionage, cyber-warfare and cyber-terrori Europe's infrastructure cybersecurity are power outages and poor communication.

On Thursday, ENISA (European Network and Information Security Agency) held its biggest ever cybersecurity exercise involving more than 200 organisations and 400 cyber-security professionals from 29 European countries.



telecompaper

INTERNET

EU launches largest ever European cyber exercise

Thursday 30 October 2014 | 11:43 CET | News

The EU's cyber security agency Enisa has launched what it has described most complex cyber security exercise ever held in Europe. On 30 October organisations and 400 cyber security professionals from 29 European cou their readiness to counter cyber attacks in a day-long simulation. Over 2, incidents will be dealt with, said Enisa, including denial of service attacks intelligence and media reports on cyber-attack operations, website defac sensitive information, attacks on critical infrastructure such as energy or the testing of EU cooperation and escalation procedures.

The public and private sector organisations taking part in the exercise i agencies, national computer emergency response teams, ministries, te energy companies, financial institutions and internet service providers exercise is to strengthen cyber crisis cooperation and enhance prepar across Europe. "Five years ago there were no procedures to drive co crisis between EU Member States. Today we have the procedures in p mitigate a cyber-crisis on European level," said Enisa's executive dire Helmbrecht. He added that the outcome of the exercise "will tell us wh in order to keep improving."

ENISA launched tenders to start implementation of the Work Programme 2015

In 2014 Q4 the Agency launched tenders for two types of contracts: **Framework contracts** for 3 year period and **Service contracts** for 2015 only. Please see the information below:

Supporting Critical Information Infrastructures Protection and ICS-SCADA security activities

Framework Contracts with ‘Re-opening of Competition’ - maximum budget €280,000 over 2 years

Deadline:
Jan 13, 2015

ENISA seeks to contract the services of a minimum of two (2) and maximum of four (4) service providers which can provide support in the field of Critical Information Infrastructures Protection and ICS-SCADA security. The successful bidders should be able to demonstrate significant experience and skills in the area of CIIP and ICS-SCADA security, with emphasis on the aspects dealt with in the annual ENISA Work Programme.

Supporting Smart Infrastructures activities

Framework Contracts with ‘Re-opening of Competition’ - maximum budget €280,000 over 2 years

Deadline:
Jan 19, 2015

ENISA seeks to contract the services of a minimum of two (2) and maximum of four (4) service providers which can provide support in the field of Smart Infrastructures Technologies. The successful bidders should be able to demonstrate significant experience and skills in this area, with emphasis on the aspects dealt with in the annual ENISA Work Programme. Due to the diverse nature of the services requested, collaboration with other entities via subcontracting and/or consortium/ad-hoc groupings is encouraged.

Supporting Critical Information Infrastructures Protection and ICS-SCADA security activities

Framework Contracts with 'Re-opening of Competition' - maximum budget €250,000 over 2 years

Deadline:
Jan 13, 2015

ENISA seeks to contract the services of a minimum of two (2) and maximum of four (4) service providers which can provide support in the field of security in the electronic communications sector. The successful bidders should be able to demonstrate significant experience and skills in this area, with emphasis on the aspects dealt with in the annual ENISA Work Programme. Due to the diverse nature of the services requested, collaboration with other entities via subcontracting and/or consortium/ad-hoc groupings is encouraged

Security and resilience in eHealth Infrastructures and services

Service contract with maximum budget of €45.000,00

Deadline:
Jan 26, 2015

In the context of this project on eHealth we define all systems and infrastructures that are related to healthcare practice supported by ICTs offered to health professionals and health consumers i.e. tele-medicine, e-pharmacy, e-hospitals. The scope of this study is to identify the security and privacy challenges in these systems and infrastructures; this will be covered under the term cyber security.

A list of ENISA's 2014 work programme publications

The following table presents links to the ENISA Work Programme 2014 deliverables

	Deliverable	Status
WS 1 – Support EU Policy Building		
WPK 1.1 – Identifying technological evolution, risks and challenges		
D1	Annual EU CyberSecurity Threats Landscape	"ENISA Threat Landscape 2014" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2014
D2	Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors)	1) "Threat Landscape and good practice guide for smart home and converged media" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/threat-landscape-for-smart-home-and-media-convergence/ 2) "Threat Landscape and good practice guide for internet infrastructures" Publication expected by 15.12.2014. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl
WPK 1.2 – Contributing to EU policy initiatives		
D1	Engaging Cloud Computing Stakeholders in the EU's Cloud Computing Strategy and Partnership (workshops, contributions to Commission's SIG and ECP work, Q2-Q4 2014)	ENISA, together with Cloud Security Alliance (CSA) and Fraunhofer-FOKUS, organised SecureCloud, a European conference with a specific focus on cloud computing security, on 1-2.04.2014. Contributions EU Cloud Strategy (WG Certification, WG SLAs).
D2	Engaging with stakeholders for the secure implementation of EU's Smart Grids policies (workshops, contributions to COM' EG 2 and MS actions, Q2-Q4 2014)	Dissemination workshop for the EG2 deliverable on "Security measures for smart grids" organised on 02.04.2014. Participated in Smart Grid Task Force – Expert Group 2 (managed by EC DG ENER) and provided contributions to the group.
D3	Algorithms and parameters for secure services (study, Q4)	"Algorithms, key size and parameters report 2014" Published on 21.11.2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014 "Study on cryptographic protocols" Published on 21.11.2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols
D4	Best practice guide for Privacy and Security by Design and Default for the prevention of data leakage and appropriate controls for the access of data (report, Q4)	"Best practice guide for Privacy and Security by Design and Default" Publication expected by 15.12.2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/
D5	Auditing framework for trust services: Technical guidelines for independent auditing bodies and supervisory authorities on the implementation of audit schemes for trust service providers in MS. (Report, Q3 2014)	"Auditing framework for trust services" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp-auditing-framework/
D6	Annual Privacy forum 2014 (APF'2014) (Workshop, report, Q2-Q4 2014)	Forum took place in Athens on 20-21.05.2014. Report: "Privacy Technologies and Policy" http://privacyforum.eu/news/proceedings-apf14-privacy-technologies-and-policy http://2014.privacyforum.eu/programme
WPK1.3 – Supporting the EU in education, research & standardisation		
D1	Inventory of standardisation activities in NIS and Privacy (Workshops, report, Q1-Q4, 2014)	"Inventory of standardisation activities in NIS and Privacy" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standards-eidas

D2	Roadmap for the implementation of the "NIS Driving license"	"Cybersecurity competitions — the status in Europe" Published on 19.11.2014. https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/cybersecurity-competitions-2014-the-status-in-europe "Roadmap for NIS education programmes in Europe" Published on 31.10.2014. https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe Extra mile: "Public Private Partnerships in Network and Information Security Education" Published on 06.10.2014. https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education
WS2 – Support Capacity Building		
WPK2.1 – Support Member States' capacity building		
D1	Assisting MS in building capabilities on NCSS (workshops, Q1-Q4)	Workshop on Cyber Security Strategies organised on 27.11.2014. https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop
D2	White Paper – How to Evaluate a National Cyber Security Strategy (report, Q3 2014)	"An evaluation framework for Cyber Security Strategies" Published on 27.11.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies
D3	Good practice guide on training methodologies, etc. for operational teams and communities like CERTs ("Train the trainers handbook") derived from experiences from delivering suitable CERT training (Q4 2014)	"Good Practice Guide on Training Methodologies" Published on 12.11.2014. https://www.enisa.europa.eu/activities/cert/support/exercise/good-practice-guide-on-training-methodologies
D4	Regular update of "Baseline capabilities" definition and status and conclusions for new training material (Q4, 2014)	""Baseline Capabilities" definition and status" Publication expected 18.12.2014. https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/
D5	New set of CERT exercise material with at least five new scenarios from the four areas of the "Baseline capabilities", including the topic of processing of actionable operational information (Q4 2014)	1) Developing countermeasures; 2) Common framework for artifact analyses activities; 3) Advanced artifact handling; 4) Processing and storing artifacts; 5) Building artifact handling and analyses environment. Publication expected by 15.12.2014. All available here: http://www.enisa.europa.eu/activities/cert/training/training-resources
D6	Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area (Q4 2014)	"Impact Assessment and Roadmap" Published on 01.12.2014. https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap
D7	Assisting MS in building capabilities on national PPPs (workshops, Q1-Q4)	Panel on PPPs during the National Cyber Security Strategies workshop, 27.11.2014 https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop
WPK2.2 – Support private sector capacity building		
D1	Support the Working Groups of the NIS Platform (workshops, contributions, technical support, Q1 – Q4, 2014)	1) NIS Platform: - Support DG CNECT - H4 for project Management & coordination of WGs and rapporteurs - Support to DG CNECT - H4 in the organization of the plenary meetings of the 30 April 2014 and the 25th November 2014 - User management, mailing lists, online collaboration and content management on the Resilience portal 2)Report "EP3R 2009-2013 future of NIS Private public cooperation" Publication date 17.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013

D2	White Paper on the Certification of Smart Grids (report, Q3, 2014)	"Smart grid security certification in Europe" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification Validation workshop for "Smart Grid Components Certification" reports organised on 30.09.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components
D3	White Paper on the Certification of Cyber Security Skills of ICS SCADA experts (report, Q3 2014)	"Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals Validation workshop for the "CERTIFICATION OF CYBER SECURITY SKILLS OF ICS SCADA EXPERTS" report organised on 30.09.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components
D4	Harmonised Minimum Security Measures for ISPs (report, Q4 2014)	"Technical guidelines on security measures for Art.4 and Art.13a" https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/
D5	Minimum Security Measures for Cloud Computing (report, Q4, 2014)	"Cloud Certification Schemes Meta Framework" Published on 15.11.2014 (in the resilience portal) https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework
D6	White Paper - Procurement Guidelines for Secure Cloud Computing Deployment (report, Q4, 2014)	"Security Framework for Governmental Clouds" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/govenmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds
D7	Guidelines for the identification of critical services, assets and links in Electronic Communication Networks (report, Q4, 2014)	"Methodologies for the identification of critical information infrastructure assets and services" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis
D8	Guidelines for Secure Inter-Banking Communications and Transactions (report, Q4, 2014)	"Network and Information Security in the Finance Sector - Regulatory landscape and Industry priorities" Publication expected by 17.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector/
WPK2.3 – Raising the level of preparedness of EU citizens		
D1	Provide technical guidance and support for European Cyber-Security Month (dissemination material, Q4 2014);	1) The launch of the event organised on 01.10.2014. alongside ENISA's high-level event "10 years of securing Europe's cyber security… and beyond!" 2) Dissemination materials available at https://cybersecuritymonth.eu/ 3) European Cyber Security recommendations for all Published http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014 4) ESCM 2014 Deployment report Publication expected by 12.12.2014 https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014
WS3 – Support Cooperation		
WPK3.1 – Crisis cooperation – exercises		
D1	Cyber Europe 2014: Exercise Plan and Exercise (exercice, Q4 2014)	Exercise organised on 30.10.2014.
D2	Report on Cyber Crisis Cooperation and Exercise Activities and Findings (report, Q4 2014)	"Report on Cyber Crisis Cooperation and Management" Published on 06.11.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study
D3	EU-US Cybersecurity Exercise Plan	Was not carried out

WPK3.2 – Implementation of EU legislation		
D1	Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents (report, Q2/3 2014)	1) "Annual Incidents report 2013" Published on 16.09.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013 2) "Technical Guideline on Incident Reporting V2.1" Published on 24.10.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting 3) "Technical Guideline on Security Measures V2.0" Published on 24.10.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures 4) Secure ICT Procurement in Electronic Communications Published on 11.12.2014 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/secure-ict-procurement-in-electronic-communications 5) Security Guide for ICT Procurement Published on 11.12.2014 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/security-guide-for-ict-procurement 6) "Protection of underground electronic communications infrastructure" Publication expected by 18.12.2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure
D2	Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2014)	Cancelled (Amending WP 2014) First ENISA workshop with national authorities held in Brussels on the 17.11.2014. Minutes available upon request.
D3	Support the implementation of the NIS Directive (workshops, Q2-Q4)	Cancelled (Amending WP 2014)
WPK3.3 – Regular cooperation among NIS communities		
D1	9th ENISA CERT workshop to prepare a roadmap for future work of ENISA in the area of CERT training and CERT cooperation with LEA (in cooperation with EC3)(Q4)	ENISA 9th annual workshop 'CERTs in Europe' – Part I organised on 27-28.05.2014. The ENISA 9th annual workshop 'CERTs in Europe' - Part II organised on 13-14.10.2014.
D2	Good practice guide and / or (where applicable) training and exercise material for the exchange and processing of actionable information by CERTs (Q4 2014)	"Best practice guide on exchange processing of actionable information – exercise material" Publication expected by 18.12.2014 https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf
D3	Draft report "Stocktaking on channels and formats for exchange of operational information"	"Stocktaking of standards formats used in exchange of processing actionable information" Publication expected by 18.12.2014 https://www.enisa.europa.eu/activities/cert/support/ActionableInformationforSecurityIncidentResponse.pdf
D4	Draft report "Scalable and accepted methods for trustbuilding within and among communities"	"Scalable and Accepted Methods for Trust Building in Operational Communities" Published on 27.11.2014. https://www.enisa.europa.eu/activities/cert/support/information-sharing/scalable-and-accepted-methods-for-trust-building
D5	Good practice material for first responders in cooperation with the EC3 (Q4)	"Good practice material for first responders" Publication expected by end of December 2014 https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders/
Flash notes: Flash Note: Heartbleed - A wake-up call Published on 14.04.2014. https://www.enisa.europa.eu/publications/flash-notes/flash-note-heartbleed-a-wake-up-call Flash Note: Large scale UDP attacks - the 2014 trend and how to face it Published on 24.02.2014. https://www.enisa.europa.eu/publications/flash-notes/large-scale-udp-attacks-the-2014-trend-and-how-to-face-it Flash note: Risks of using discontinued software Published on 29.01.2014. https://www.enisa.europa.eu/publications/flash-notes/flash-note-risks-of-using-discontinued-software		