OCTOBER
EUROPEAN CYBER SECURITY MONTH
Online security requires your participation

ECSM final report

Roadmap for European Cyber Security Month

November 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Editors of the report Demosthenes OIKONOMOU and Daria CATALUI.

Contact

For contacting the editors please use StakeholderRelations@enisa.europa.eu

For media enquires about this report, please use press@enisa.europa.eu

Acknowledgements

We would like to express gratitude for the work and support of Ann-Sofie RONNLUND (EC DG CONNECT), Vangelis Stavropoulos (ENISA), Jean-Christophe Pazzaglia (SAP). Furthermore appreciations for the work of all coordinators from the 27 ECSM countries who participated with input: Austria, Belgium, Bulgaria, The Czech Republic, Germany, Estonia, Greece, Spain, Finland, France, Hungary, Ireland, Iceland, Italy, Latvia, Lithuania, Luxembourg, Moldova, The Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Serbia, Sweden and the United Kingdom.

ISBN 978-92-9204-079-6 doi: 10.2824/276

Executive summary

The European Cyber Security Month 2013 took place in October in 27 countries. By consulting this report the reader will be introduced to the context of ECSM deployment, the policy context, the stakeholder model of engagement, the activities that were implemented and the results of the fully fledged EU advocacy campaign on NIS topics. This report presents the model of building together a joint EU advocacy campaign, a campaign on cybersecurity topics of interest for all digital citizens, and at the same time for institutions and Small Medium Enterprises.

The main recommendations regarding future editions of the advocacy campaign are mentioned in the conclusions of the evaluation effort and are structured in three pillars as below.

Develop a stable Model of coordination at European level and MS level:

- Plan in advance all steps and communicate them
- Improve content and participation
- Improve interactivity

Enhance Content of ECSM:

- Continue the development of repository of materials
- Keep encouraging private-public common activities
- Introduce a best practice section on the website

Improve International Cooperation:

- Exploring common webinars and e-learning solutions
- Develop an International training kit for NIS activities
- Advance planning

European Cyber Security Month (ECSM) is an EU advocacy campaign that takes place in October. The main objective of the ECSM is to promote cyber security awareness among citizens, to modify their perception of cyber threats and to provide updated security information through education, good practices and competitions. Coordination efforts were managed by the Commission (DG CONNECT) and ENISA, and a large number of NIS stakeholders participated as a result of the open call published early during 2013[1].

[1] http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-2013-get-involved [accessed in October 2013]

Table of Contents

1 Introduction

In October 2013, the first fully-fledged European Cyber Security Month (ECSM) took place all over Europe with the aim to promote cyber security education and sharing of good practices. Furthermore, synergies were built with Africa[2] and world-wide cyber security efforts were embarked on by a shared release of top 12 Mobile Safety Tips[3].

The Goal of this report is to describe what has been achieved, taking account of the policy context and making reference to country profiles and analytics. Furthermore, a number of recommendations are made and a best practice path is proposed in order to set a roadmap for future deployments.

The Target Audience consists of ECSM country coordinators, public and private stakeholders involved in the campaign, policy makers and all those that participated to ECSM activities.

The document is structured in 3 parts:

- The introduction with general considerations on the context;
- The ECSM 2013 deployment with details on coordination and activities. This section includes annexes with important details on each ECSM country, analytics and a report of the Kick-off event;
- The Roadmap for future deployments;

For the specific purpose of this report, **data** was collected from ECSM coordinators talks, ECSM kick off evaluation meeting, webforms with activity evaluations, reports from stakeholders and team meeting evaluations.

1.1 The general policy context

In this section we describe the general Network Information Security (NIS) **background** and the specific context surrounding the ECSM as a method of raising awareness and empowering the digital user. This concept was piloted and developed in Europe taking into account the experience gathered from worldwide actors that have been implementing it[4]. The work is in line with the Awareness Raising work stream of the EU-U.S. Working Group on Cyber-security and Cyber-crime established in the context of the EU-U.S. Summit of 20 November 2010 held in Lisbon[5]. Additionally, the work benefited from a multiannual planning.

[2] Training sessions in Nigeria http://cybersecuritymonth.eu/ecsm-countries/africa-1 [accessed in October 2013]
[3] Safety tips for mobiles - ENISA supporting world-wide cyber security efforts https://www.enisa.europa.eu/media/news-items/safety-tips-for-mobiles-enisa-supporting-world-wide-cyber-security-efforts [accessed in November 2013]
[4] More on the National Cyber Security Awareness Month and the National Cybersecurity Awareness Campaign -Stop.Think. Connect. - organised in the United States http://www.dhs.gov/stopthinkconnect [accessed October 2013]
[5] EU-US Summit Joint statement http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/er/117928.pdf [accessed in October 2013]

Furthermore, the Cyber Security Strategy for the EU[6] calls for "An Open, Safe and Secure Cyberspace" including the importance of raising awareness as a common responsibility where end users need to be made aware and be empowered, as developed on page 8. This is being put in practice in a yearly Cyber Security Month advocacy campaign deployed currently in 27 countries. The basis being a Feasibility Study conducted in 2011 and an initial Pilot with 8 participating countries in 2012. As an example of the common responsibility practice, more than **60 public and private stakeholders** supported the month, including ENISA, together with the European Commission and vice president Neelie Kroes and the Directorate General CONNECT.

1.2 The context of ECSM 2013

Following the publication of the 2011 Feasibility Study[7] and the 2012's pilot[8] phase, European Cyber Security Month 2013 was deployed to reach to new partners. ECSM is set to promote cybersecurity among citizens of the EU, change their perception of cyber threats, and provide current security information through education and the sharing of good practices.

The ENISA Work Programme for 2013 mentions that work should continue together with the Member States and the Commission to further develop the campaign. The approach was established to widen the number of participating Member States, to ensure sufficient focus on a number of key themes and to profile the event as a joint EU campaign with global outreach. Moreover it is anticipated to increase the involvement of the private sector in this initiative by working through industry representation bodies to make full use of material that has been developed already and to build upon this material when necessary.

The objectives were brought into line with the final recommendations and objectives of the 2012 pilot:

- generate general awareness about cyber security, which is one of the priorities identified in the EU Cyber Security Strategy;
- generate specific awareness on Network and Information Security (NIS), which is addressed in the proposed NIS Directive;
- 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 global dimension of the project;
- enhance attention and interest with regard to information security through political and media coordination.

[6] February 2013 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 [accessed in October 2013] For previous relevant Policy documents please consult CIIP action plan for Europe [2009] and The Digital Agenda for Europe [2010]

[7] ENISA report 2011 http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2011/europeansecuritymonth [accessed in October 2013]

[8] ENISA report 2012 https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2012 [accessed in October 2013]

1.3 The stakeholder model of engagement

At a time when cybersecurity is increasingly important, our challenge is to update the skills of end users, increase the capabilities of SMEs and improve trust in public and private services. All these goals can be achieved by building synergies with EU organizations[9] , professional associations[10] and industry representatives. Following the model of stakeholder involvement depicted in the graph below, the ECSM team acted as an information broker, supporting stakeholder mapping and building public-private partnerships for activities.

Furthermore, the support from the European level contributed to make the work more efficient, and build up a strong NIS community behind the campaign. This role is central in advocacy. Additionally, the concrete activities that bring added value happen most of the time at local level, with public bodies, private stakeholders, professional associations and citizens, all working together for greater cyber security in the digital environment. All these sustained efforts aim to create active involvement in the promotion of cyber security for citizens, placing the topic firmly on the agendas for both citizens and governments. Where can you intervene? Are you interested in getting involved in the European and global effort towards this common challenge? We all should engage and ask these questions since everyday life in a digitally connected society requires better informed users and more aware decision makers.

Be aware, be secure!

[9] E.g. EUROPOL, EESC and Europe Direct Network
[10] E.g ISACA, ISSA

2 The ECSM 2013 deployment

As specified in the stakeholder model of engagement, ECSM2013 had a complex interconnected coordination between European-National-International stakeholders. We consider the multi-stakeholder approach as being the appropriate path to follow also for future years, whilst continuing to refine the level of interactions and permantly searching for tailored solutions that may be requested.

2.1 Participation rate of public-private stakeholders

One of the strong points of the 2013 deployment was the number of stakeholders that were involved in the campaign(a record number of 27 countries, consisting of 23 EU MSs and 4 partner countries).

In order to have a general overview on the level of participation and the type of activities that were organized we summarize below data for the 27 participating countries[11]:

Austria: Security awareness, data protection in enterprises and public campaigns: "Safe Usage of the Internet"

Belgium: Online campaign, Information Security Solutions Conference

Bulgaria: InfoSec and data storage

Czech Republic: Online and outdoor campaigns, workshop for NGOs operating helplines

Germany: Internet Day, Security Fair and Congress, online campaigns: secure surfing, mobile-secure, and shopping-secure; use of social networks, activities for SMEs, journalists and citizen

Estonia: ICT for Business, lectures on cyber security

Greece: Security trends and CIIP workshop for students and young professionals

Spain: Impact of cyber security, security campaigns, university lectures

Finland: Digitour, web and social media, network behaviour education for rural stakeholders

France : Online campaigns «Rester alerte, rester serein: la sécurité informatique se construit avec vous», meetings with students

Hungary: Mysec Talk, Cybersecurity conferences

Ireland: Launch of CyberPsychology Research Centre

Iceland: Insights in InfoSec industry 'Hacker Halted'

Italy: Regulatory Framework on Cyber Security workshop, online fraud, social networks; online child protection

Latvia: Social networks used as a method for targeted attacks, free computer check-ups: removal of computer viruses and malware

Lithuania: Network information security

Luxembourg: Ecommerce, Ebanking and Cyberbullying quizzes

[11] 27 country profiles may be consulted in the annexes

Moldova: Cyber Security in Government Week

Netherlands: Cyber Security Awareness & Integrity Help and Hotline, Alert online, college tour

Norway: Online and outdoor campaigns, security tips

Poland: ICT in education, online quizzes

Portugal: Information Security training, round table discussions, workshops

Romania: Series of technical workshops, online campaign, Cyber Security conference

Serbia: Exhibitions and Cyber Security discussions

Sweden: Advice on the protection of personal information, identity, PC/handheld devices, secure use of Wi-Fi, how to create strong passwords

Slovenia: Online campaign-Safe On the Internet

United Kingdom: Poster competition, awareness week on behaviour, ethical hacking, viruses and malware, using your home computer, social media, emails.

With the occasion of the launch of the campaign the Executive Director of ENISA, professor Udo Helmbrecht commented:

> ***"Cyber security is about the possibility to live your digital life. We encourage you to get involved in the campaign: online security requires your active participation!"***

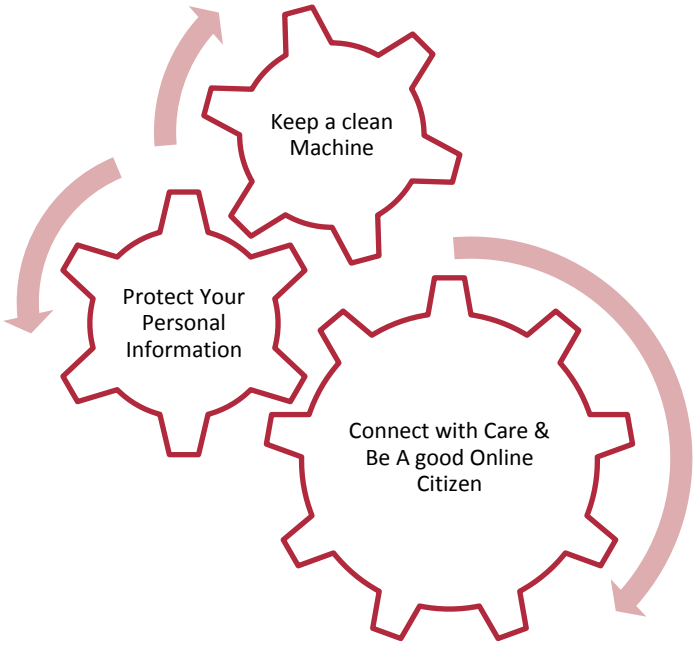
In adition to the data collected we present below the visual presence of ECSM in activities meant to update the citizens on cyber security topics.

2.2 International cooperation

The international cooperation in ECSM had its climax on 29th of October with the coordinated release of 12 Mobile Safety Tips[12] .

ENISA supported the global efforts for achieving improved Network and Information Security for users worldwide, either in their capacities as business users, home users or peers. Together with the National Cyber Security Awareness Month in US, the National Cyber Security Alliance in Singapore and many partner countries the top 12 Mobile Safety Tips were released.

Furthermore, the release was to coincide with European Cyber Security Month 2013, the 10th year of National Cyber Security Awareness Month in the United States and the 4th annual Asia Pacific Economic Cooperation Telecommunications and Information Working Group (APEC-TEL) Cyber Security Awareness Day.



2.3 European level kick-off event

Sharing of experiences and further recommendations for the implementation of the campaign were exchanged in a kick-off event on 11th of October. Here ECSM community members discussed methods for involving the citizens. The main questions asked were in which way may the digital citizen get engaged effectively, how should we measure the impact and which performance indicators to include? We've also learnt that multidisciplinary training in NIS education is emerging in top universities over the world, also that we should be heading towards both technology aware users and user aware technologies. Moreover, as a key message for cyber security advocacy we mention the concept of security by design and user empowerment through better education. All these and more details may be read in the annex where we edited the report of the Kick-Off event.

[12] ENISA release http://www.enisa.europa.eu/media/news-items/safety-tips-for-mobiles-enisa-supporting-world-wide-cyber-security-efforts

2.4 Campaign Analytics and Benefits

In the 2011 Feasibility study we foresaw the benefits associated with a fully fledged campaign. Table 6 and the graphics above from the report mention increased impact and visibility, increased efficiency, potential use of ready-to-use material, reduced costs and investments, all advantages of a coordinated approach.

Table 6: Benefits of the European Month of Network and Information Security for All

Benefits	
	Description
Increase impact and visibility	A European-wide project would create a greater impact and receive more attention from both national and international media
Increase efficiency	The principle of economy of scale would apply
Use of ready-to-use material	Material produced by third parties such as ENISA, the DHS or other Member States could be used across Europe to ensure a consistent message is delivered
Reduce costs/investments	A European-wide project would mean that the very best minds and experience from across the Union could be gathered together, thus reducing cost and required investment from each stakeholder

Once with the implementation of the fully fledged campaign we may add from experience the following advantages reported to us by participants in different occasions:
Strengthening ties with EU bodies

Networking with NIS actors in the country and internationally

Gaining EU visibility for grass root actions e.g. website presence and events participation

Brokerage support from the side of ENISA and from the side of DG CONNECT to EU policy makers

Sharing of best practices

Access to an inventory of **NIS materials** useful for NIS work

Broader outreach and impact towards digital citizens, e-users

According to the country rate of participation [27] and the number of activities[13] organized [more than 50], twitter ECSM community[14] [approx. 1000], website visits [more than 9.500], Media reach [approx. 60 million peak] the 2013 deployment went as planned.

[13] European overview from www.cybersecuritymonth.eu
[14] In permanent increase

Furthermore a detailed overview from meetings, social media, website, rate of involvement of stakeholders may be consulted in annex B.

By participating in ECSM advocacy campaign it did simplify the work and achieved a greater impact …time, effort and resource wise!

3 The Roadmap

Taking into account the multi-annual framework in which the campaign is deployed, we put forward below concrete ideas for the advanced planning of 2014 campaign. It is important to mention that the ideas were inspired from the evaluation meetings, completed evaluation forms and also from the direct interactions with stakehoders. The evaluation work will be the main source for feeding information into the future editions of European Cyber Security Month.

Coordination considerations

- **The team meetings ENISA-CONNECT were essential**. For 2014 they should continue already setting the objectives to mapping stakeholders and building synergies with other stakeholders and other initiatives. ECSM countries may be invited to participate in the EU coordination, rotating over the years.

- **The ECSM coordinators calls/meeting proved to be efficient and appreciated by the coordinators**. The format should be developed further.

- The EU level kick-off event should be organized at the beginning of the month with more ECSM coordinators invited and more materials.

International collaboration

- Advanced planning is needed.
- Exploring common webinars and e-learning solutions.
- Develop an International training kit for NIS activities.

Feedback ideas for implementation

- It would be helpful to produce some small number of ECSM posters, official Factsheets and FAQs about ECSM and have them translated in all official EU languages.
- It should coordinate a common message for the campaign translated in all languages.
- Aim to achieve a stronger collaboration with industry and between bodies at country level.
- Improve interactivity by all means.

In order to further develop a stable model of coordination at European level and MS level the team should firstly plan in advance all steps and communicate them, secondly improve content and participation, thirdly outline action points templates and develop the "Guidelines for stakeholders".

It should be mentioned that resources are scarce, however when budget is not available in kind offers should be agreed.

In order to continue the implementation of ECSM, further ideas should be taken on board to increase the overall impact and start creating an ECSM footprint in the European society.

Enhanced content of ECSM

- Continue the development of repository of materials with:
  1. Most watched NIS videos
  2. Reports and Briefs world wide
- Launching the NIS Driving Licence roadmap in October together with a pilot application for testing basic/advanced NIS knowledge
- Prepare Online templates and few give away materials

Building synergies

- Keep encouraging private-public common activities
- Partnering with more universities in order to reach out to students
- Continue the mapping of NIS initiatives and active stakeholders

Evaluate and scale up the results

- Introduce a best practice section on the website
- Create a basic training kit for NIS multipliers
- Improve the interactions between Participants-coordinators-visitors

ENISA's Executive Director, Professor Udo Helmbrecht commented in regards to ECSM importance: "ENISA is a broker of cyber security knowledge. The European Cyber Security Month campaign makes it possible to share best practices, and to increase the results of the security communities' work. It's about your security, and in your best interest; online security requires your active participation".[15] He added

> "In a time when cyber security is of increasing importance for society and the economy, the challenge is to bring the skills of citizens and SMEs up to speed, to improve the trust in public and private IT services, used in everyday lives."

[15] Press release 10.09.2013 https://www.enisa.europa.eu/media/press-releases/online-security-it2019s-in-your-interest-1st-european-cyber-security-month-coming-up-in-october [accessed in October 2013]

4 Conclusions

To conclude, it should be stresed that the European Cyber Security Month future role is to reach out to increasingly more European citizens and update their knowledge on how to stay safe and secure online. In addition to the feasiblity and pilot the previous years, 2013 was succesful at increasing the level of stakeholder reach and placing the initiative firmly on the agendas of both public and policy–makers. The multi-stakeholder approach will be kept and the dynamic nature of the network and information security topics will be addressed through tailored solutions. Further effort will follow in order to:

Develop a stable Model of coordination at European level and MS level:

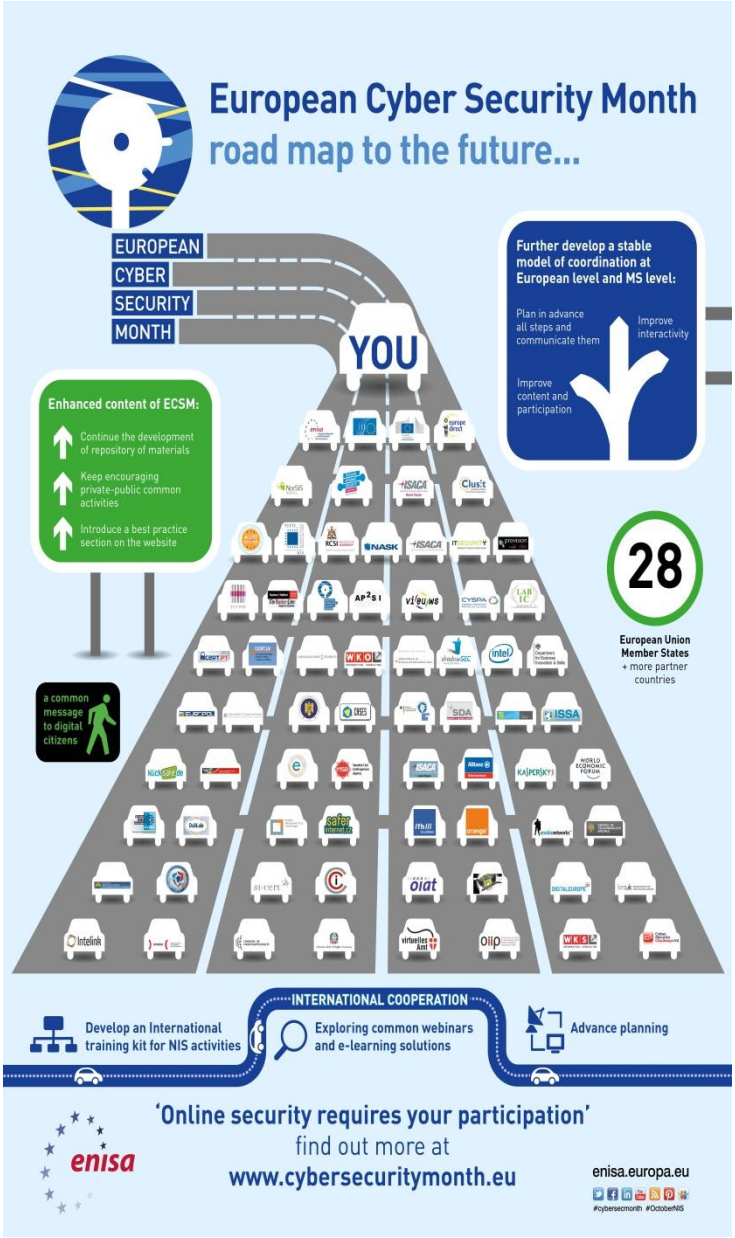
- Plan in advance all steps and communicate them
- Improve content and participation
- Improve interactivity

Enhance Content of ECSM:

- Continue the development of repository of materials
- Keep encouraging private-public common activities
- Introduce a best practice section on the website

Improve International Cooperation:

- Exploring common webinars and e-learning solutions
- Develop an International training kit for NIS activities
- Advance planning



References

[1] European Cyber Security Month www.cybersecuritymonth.eu

[2] ENISA news item Call for ECSM http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-2013-get-involved

[3] Safety tips for mobiles - ENISA supporting world-wide cyber security efforts https://www.enisa.europa.eu/media/news-items/safety-tips-for-mobiles-enisa-supporting-world-wide-cyber-security-efforts

[4] ENISA report 2011 http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2011/europeansecuritymonth

[5] ENISA report 2012 https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2012

[6] ENISA Press release 2013 https://www.enisa.europa.eu/media/press-releases/online-security-it2019s-in-your-interest-1st-european-cyber-security-month-coming-up-in-october

[7] National Cyber Security Awareness Month and the National Cybersecurity Awareness Campaign - Stop.Think. Connect. - organised in the United States http://www.dhs.gov/stopthinkconnect

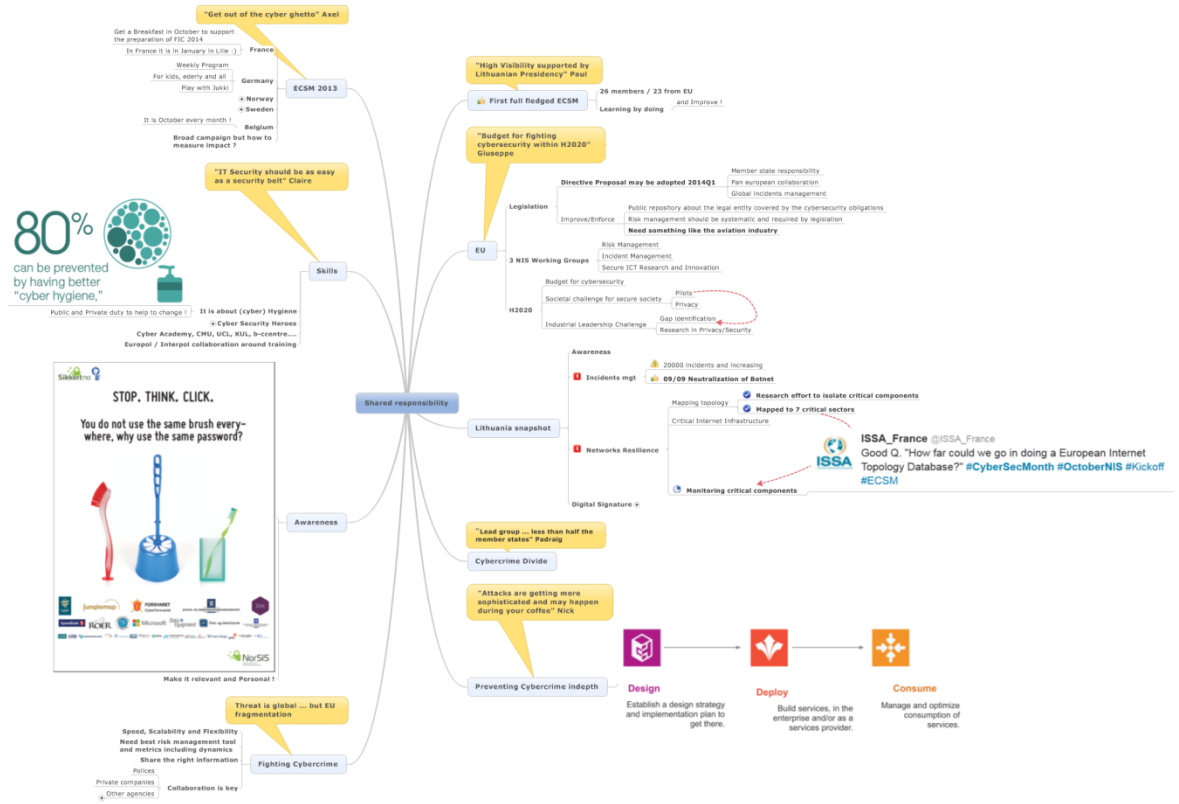
[8] EU Cyber Security Strategy calls for "An Open, Safe and Secure Cyberspace"

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

[9] EU-US Summit Joint statement
http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/er/117928.pdf

Annex A: Report of the ECSM Kick-off event

A.1 The discussion and conclusions[16]



On 11th of October 2013, 67 participants[17] representatives from the private and public sectors gathered in Brussels to the Kick off event of the European Cyber Security Month initiative. Numerous topics were discussed but they all had in common the growing importance of sharing information, knowledge, expertise and responsibility across Europe to improve its resilience to the numerous and worldwide Cyber Security threats. The agenda of the event was balanced between presentations and panels from public bodies with experience in raising network and information security (NIS) awareness and private bodies with initiatives or public–private partnerships (PPPs) in the field. In the opening session, Steve Purser (ENISA) underlined that 2013 was the first fully fledged edition of the European Cyber Security Month and thanked the Lithuanian presidency for its support to promote its visibility. Paul Timmers and Giuseppe Abbamonte (EU DG CONNECT) highlighted the importance of a comprehensive longterm and common strategy for cybersecurity (e.g. ECSM, NIS platform, Directives, eIDAS Regulation, Horizon 2020). Rytis Rainys (RRT- Lithuanian Presidency of the Council of EU) focused on the work already achieved to make the Lithuanian cyberspace more secure. He reiterated their strong support to promote cybersecurity initiatives across EU.

In the keynote, Nick Coleman (IBM) asserted on the need to build a risk aware culture across the different stakeholders.

[16] Rapporteur Jean-Christophe Pazzaglia (SAP, Product Security Research)
[17] 67 in presence/ 44 remotely by web stream

The panel "International Good Practices in Securing the Digital Citizen" highlighted the need of a pan-european collaborative approach and it continued on the need of a paradigm shift for the design and protection of cyber systems. A parallel was established with the common control process of the aviation industry that may be a role model for the cyberspace and that may help to fight against a cyber protection divide within Europe.

The afternoon started with the presentation of some ECSM activities happening within this year edition of the European Cyber Security Month, the campaigns held in Belgium, Germany, Norway, and Sweden complemented with the report on the French “Forum Intenational de la Cybersecurite”.

The last panel “Cyber Security Professional" presented the evolution of the cybersecurity professionals’ skills and their career lifecycle. They supported the existing certifications but also praised the emerging curriculums (e.g. Royal Holloway, Hague University of Applied Sciences, EPITA and ParisTech) in order to equipe Europe with professionals mastering the necessary multidisciplinary scope of technicques to face cybersecurity challenges. The day finished with a visual overview of the main topics addressed during the day done by the rapporteur Jean-Christophe Pazzaglia (SAP). Finally, Steve Purser described the role that ENISA plays for the ECSM and the chosen approach “learning by doing” that may also be used in the new initiatives like the NIS platform. The rest of this report will look into the different sessions one by one.

A.1.1 The difference that ECSM common effort can make

- ECSM 2013 was a considerable increase in stakeholder participation since last year's pilot and DG CONNECT aims to make this an attractive month for all EU countries to participate in 2014. The Cyber security Month initiative exists because of the combined efforts of all of those involved: Governments, businesses, academia, NGOs, professionals in information security, in communications etc. The events illustrate the wealth of knowledge that exists throughout Europe on cyber security.

  We must tap into this collective knowledge to make ourselves more aware of and protect ourselves better against the risks and threats said Paul Timmers. This is where a joint European Cybersecurity Month can make a difference.

- On the Cyber security Month website one can find information and events relating to a wide variety of themes. For instance: information to the workforce, both in public and private sector; information to end-users and citizens; the importance of cyber security to industrial control systems and nuclear installations; the latest malware analysis and cyber forensics.

- We can share experiences and build on awareness raising models that have been proven to work well. We can share messages, re-use them and thereby spare resources. We can instil a sense of joint challenge and enthusiasm. We can make sure that all actors are involved and nobody is left behind.

  And we can discuss how to measure the success of our activities, putting efforts into developing metrics for the Cybersecurity Month.

- EC overview on cyber security:

  - The European Commission, together with the High Representative on Foreign and Security Policy, adopted the EU Cyber security Strategy in February 2013. It has since then been

endorsed by the Council of the European Union in June. The European Parliament in its September resolution welcomed the initiative to organise a European Cyber Security Month.

- DG CONNECT in particular focussing on resilience: How to enhance capabilities and cooperation: NIS Directive; How to identify best practices throughout the value chain: NIS Platform; Funding of new technologies: Horizon 2020; another important on-going activity is the negotiation of the eIDAS Regulation on mutual recognition of electronic identification means and trust services.
- There are more activities that are ongoing in other departments, for instance within DG Home Affairs to fight cybercrime and within the European External Action Service to promote dialogue between civilian and military actors in the EU and to establish international dialogues and norms of behaviour in cyberspace.
- ENISA's mandate was renewed in 2013 as well. This is important because of the central role the Agency has in supporting Member States and the Commission in enhancing cyber security capabilities.

➢ The state of play of the EU Cyber security Strategy, in particular the resilience chapter, and the accompanying legislative proposal on network and information security:

- Growth and jobs agenda depends on the resilience of the ICT systems and networks underpinning the various economic processes of our modern societies. Enhancing the security of the European value chain is of fundamental importance for the Digital Agenda and the completion of the Internal Market.
- The Strategy announced that the Commission would set up a public-private platform – the NIS platform - to identify good cyber security practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. The NIS platform will as a matter of priority aim to identify technologically neutral best practices to enhance cyber security and develop incentives to abide by those best practices and adopt secure ICT solutions. Such best practices will be identified by two Working Groups: the first WG comprises awareness rising, which is of particular interest.
- The Directive will promote a security culture across the value chain so that all players across the chain can reap the benefits of new online services. Users are at the moment hesitating to embrace such services, because of security concerns. Such a security culture should include dynamic risk management, but also participation in the exchange of information on threats and vulnerabilities.
- The EU Cyber security Strategy and R&D: HORIZON 2020, which will be the EU's research and innovation funding programme from 1.01.2014 will fund cyber security research. Cyber security in HORIZON 2020 will be addressed in two pillars: The Societal Challenge of "Secure societies" and Industrial Leadership Challenge of Future Internet (LEIT.

"Priorities for cyber security"

The Lithuanian Presidency was characterized by a heavy agenda due to the end of a political cycle before the European Parliament elections in 2014 and the finalization of the Multiannual Financial Framework 2014-2020. The focus of this presidency was Europe, to restore confidence in EU economy, to boost employment and competitiveness and to strengthen openness and security.

In the area of the telecom and cybersecurity, Lithuania strongly supported different initiatives such as: TEN-TELE - Proposal for a Regulation on guidelines for trans-European telecoms networks; eIDAS - Proposal for a Regulation on electronic identification and trust services in the internal market; NIS- Proposal for a Directive on Network and Information Security; BB Cost Reduction - Proposal for a

Regulation on reducing the costs of broadband infrastructure deployment; WEB Accessibility - Proposal for a Directive on the harmonization measures of the MS related to making Public sector websites available; STM, EC initiative on Single Telecoms Market - Proposal for a Council Decision on the EU Position for the ITRs and EU representation in ITU.

Furthermore, the establishment of the Lithuanian CERT enabled to monitor the incidents, the botnets activity and enable to neutralize a botnet that controlled 5400 bots in September 2013. Proactive measures have been taken to generate automatically alarms for malware, malicious scripts and other anomalies. To assist in the resilience of the Lithuanian internet network infrastructure, research has been conducted to enable:

- Description of the model of the Lithuanian Internet network topology
- Identification of critical network interconnection nodes
- Development of the core of Lithuanian Internet monitoring model

This model was linked with national critical infrastructures and its information systems on the internet for 7 domains (ICT sector, Governmental sector, Finance sector, Energy sector, Health sector, Water and food supply, Transport sector) enabling to monitor with different probes.

"Involving the Citizen"

The landscape for citizens is changing, the adoption of new business models (eg. mobility, social business, outsourcing, SaaS) embracing new technologies (eg. cloud, connected objects, BYOD) is causing an exponential growth of the interconnected digital universe (eg. 30 billions RFID, 1 trillion connected objects). While attacks are becoming more sophisticated and may happen in minutes, cyber hygiene can prevent more than 80% of basic vulnerabilities and may be done quickly (eg. frequent software update).

The landscape for security is changing from a threat and a technology perspective: CISO perceive that External threats are rated as a bigger challenge than internal threats, new technology or compliance; more than one-half say mobile security is their greatest near-term technology concern and 2/3 expect to spend more on security over the next two years.

People are changing the way they connect, and with who they connect.

They frequently exchanged roles as Bank Customer, Online Shopper, Parent, Citizen, Tax Payer, Passenger, Employee, Teacher, Volunteer... within their different roles their needs, their concerns and their behaviours may be extremely different.

To raise citizen awareness the quality of the communication is essential, channel should then be pertinent, the message should be relevant and should enable citizen to identify themselfes.

IT professionals should also rethink their way to design IT solution and put security in the different stages especially in the Cloud/SaaS perspective : Design phase- Establish a design strategy and implementation plan to get there; *Secure by Design* - Focus on building security into the fabric of the cloud; Deploy phase-Build services, in the enterprise and/or as a services provider; *Workload Driven* -Secure resources with innovative features and products; Consume phase- Manage and optimize consumption of services; *Service Enabled*- Govern through ongoing security operations and workflow.

The aim is to create a risk aware-culture where a public private partnership can engage citizen, manage incidents with intelligence and promote automated security hygiene.

Q&A

- The initiative of the Lithuanian authorithy to build an exhaustive map of their internet and to map it against critical services by sector was highly appreciated and commented over twitter.
- The notion of trust and notably trust toward cloud services run by government was debated; What transparency measures and what meaningful certification schemes can enhance their level of security?
- The complexity, the discolsure of vulnerabilities and mismatch between the level of technical skills required to keep device up to date, are all source of concerns and raise the question: who is the CISO of every citizen?
- Quick lifecycle and automated updates are usually good for security, but who is keeping the pace? How many of us are upgrading daily our apps? How can we explain that security policies are mainly technically driven and not informative for the users irrelevant of his/her expertise? Why security related upgrade are not highlighted? Why condition check are not embedded?

A.1.2 Policy panel, "International Good Practices in Securing the Digital Citizen"

- **Figthing cybercrime:** The mission of EC3 is to fight cybercrime, crimes committed by organised groups to generate large criminal profits such as online fraud, crimes which causes serious harm to the victim such as online child sexual exploitation, crimes which affect critical infrastructure and information systems in the European Union. The efficiency relies on the closed pan-european collaborations between police and justice but also involved private companies (e.g. IT/Telco providers) and other agencies targeting cyber security with for example exchanges with ENISA. EC3 invests in R&D to provide a way to gather and process data during crime investigation. EC3 can neither afford to be only reactive and resources are mobilized to identify future trends, to assess future threats and to raise awareness. EC3 however cannot be trigerred by the private citizen as potential crimes should be reported at national level.

  Claire Vishik from INTEL starting by empasing that IT Security should be as easy to use than a security belt.

- **IT security:** due to the growth of data traffic and the interconnection of multiple devices the people may loss the control. Some new services will require to be always connected with no clear path to opt out and that the difference between local and cloud storage will fade out making nearly impossible to track data.
- As of today, too many parameters are necessary to master the secure construction of such applications and a new approach is needed to built in security and privacy mechanisms. These mechanisms should take into account new threats models caused by the multiplicity of use cases, and professionals should tackle them from a multi disciplinary angle. While applications should be secure and respect the right of privacy by default, **users should be aware of the consequence of interacting and sharing information continuously**. This will require education to provide solid technical background. Finally, Thinking Global is necessar

and adherence to standards and interoperability are necessary but not enough to deliver such solutions.

- Current legislation evolution: Thomas McDonogh and Padraig Kenny gave their perspective about the current evolution of the directives and legislation around cybersecurity. If they praised the ongoing effort they also pointed out that the fragmentation of EU is a problem in the fight against cybercrimes and that the foreseen budget decrease may harm it. The fear is that a cyberfighting divide may appear with only half of the EU states in the leading group. They also defended the opinion that the cybercrime regulation should require a systematic risk management for critical services and that a public repository about the legal entity covered by cybersecurity obligations should be established. **This transparency will help the citizen and all stakeholders to better evaluate the effectiveness of the required protection measures**.

Q&A

- The perceived shortage of cybersecurity experts raises the point of dedicated curriculum and asks for better leveraging training initiatives. e.g. Several trainings are emerging in UK, Nederlands, France, and Europol and Interpol started a collaboration to share training material, agencies like ENISA are also key contributors to this area.
- If risk management should be at the root of legislation, the question is to understand if current tools are suitable and if they are able to include the dynamic of changes in technology but also their usage? Similarly if a public repository of critical service exists, what will be its added value for citizen? Which KPIs should be relevant and how should they be disclosed publicly without avoiding risk like generalized mistrust or panic or without being sure to not help cyber criminal looking for vulnerabilities ?

The fragmentation of Europe is perceived as problematic to fight the international threats of cybercrimes, there is a need for collaboration.

A.1.3 Presentations of activities ECSM 2013

- In the perspective of the upcoming 6th edition of the International Forum on Cyber Security[18], the FIC Observatory invited the participants to the event.
- **ECSM activities presented**[19] (e.g. Germany, Norway, Sweden and Belgium): All the activities have in common the use of multiple communication channels (e.g. social network, seminar, traditional press and videos) to address a majority of citizens. Story telling and effective advertisements are used to raise awareness outside the cybersecurity *gettho*. To be more effective, the german strategy was to split the month per week focusing on a particular topic (e.g. password hygiene, social engineering) but also to involve Media to host Q&A sessions with experts. Ederly and kids also deserved a specific treatment with respectively a contest and a dedicated web site using cartoons code. The Norway initiative has choosen the humour to carry the message and to raise awareness. Like the Belgian and German initiatives the campaigns are global and span the whole society with numerous actions including technical vulgarisation but also more advanced lectures. The Swedish ECSM campaign is smaller and it should be understood as a way of gaining experiences for a larger campaign next year. Still the campaign runs in cooperation with the The Swedish Post and Telecom Authority (PTS) and target home users and employees and focus on Secure passwords, Mobile devices, Back up your files, Malicious code and Wireless networks.

[18] http://www.forum-fic.com/2014/en/
[19] Details on the activities here www.cybersecuritymonth.eu

Q&A

- The scope of the intiatives is ambitious and it is both supported by different communication channels and by creative and innovative material. Still the main question remaining is how to measure the impact of the campaigns, how will they affect the daily behaviour of citizens? How many people will change their cyber hygiene, how many will use different passwords? On the other side of the spectrum, how many providers will promote stronger authentication mean, how many of them will restrain to collect data that may be improperly use to harm their customers without an evident immediate added value?

A.1.4 Practice panel, "The Cyber Security Professional"

- The evolution of the cybersecurity professionals' skills and their career lifecycle: analysis "European trends form the 2013 Global Information Security Workforce Study" of the seniority of the cyber security showed a deficit in young talent, one possible explanation coud be the lack of standardized education despite the emergence of dedicated curriculums in Europe and world wide (e.g. Royal Holloway, Hague University of Applied Sciences, EPITA and ParisTech) while one can also argue that (cyber)security professionals are coming from broader initial skills and specialized later.
- In this context professional certifications may be a way to gradually recognize the professional skills acquired by doing security tasks. In order to equip Europe with professionals mastering the necessary broad scope of techniques to face cyber security challenges, intiative like CYSPA maybe a way to match the different stakeholders (e.g. government, agencies, critical sectors and IT provider) expectations and to further define the necessary skills matching specific duties.

Life long learning offer clear career level and paths may also boost the interest of young practitioners.

A.1.5 Summary

Numerous topics were discussed during the day all having in common the growing importance of sharing information, knowledge, expertise and responsibility across Europe to improve its resilience to the numerous and worldwide Cyber Security threats.

"Shared responsibility" was a message carried by all presentations:

- Reponsibility to make the citizen aware of potential risks with continuous and relevant information where this first fully fledged ECSM is key;
- Responsibility to provide the legal framework and research and development tools sustained by the EU with directives, NIS and H2020 program;
- Responsibilty to act today with resourceful national CERTs and to think about proactive measures to lower the risks;
- Responsibility for providers to propose solutions embedding security and privacy by design during the project's lifecycle;
- Responsibility to be cybersecure and fight cybercrime at the EU-wide level by sharing the right information between all stakeholders;
- Responsibility to train highly educated people with the appropriate skillsets.

"ENISA role to brokerage"

A.2 The agenda

8:30-9:00	**Registration EC Conference room**
9:00-10:10	**Welcome address** ▪ "The difference that ECSM common effort can make" Paul Timmers, Director Sustainable & Secure Society (Directorate H) DG CONNECT, EC ▪ "An Open, Safe and Secure Cyberspace" Giuseppe Abbamonte, Head of Unit Trust and Security, DG CONNECT, EC Rytis Rainys -RRT- Lithuanian Presidency of the Council of EU Moderator: Steve Purser, ENISA **European Cyber Security Month (ECSM) is an EU advocacy campaign that takes place in October!**
10:15- 11:00	**Keynotes " Involving the Citizen"** Nick Coleman, Global Cloud Security Leader, IBM **Public-private common activities are welcomed!**
11:00-11:20	**Networking Break** Invited to get more information from the Info desks and poster exhibition organized by ECSM participants & ISSA **Online security requires your participation!**
11:20- 13:00	**Policy panel, "International Good Practices in Securing the Digital Citizen"** ▪ Olivier Burgersdijk, Head of Strategy at the European Cybercrime Centre (EC3) hosted at Europol ▪ Claire Vishik, Security Policy-Technology Manager, INTEL Towards technology-aware users and user-aware technlogies ▪ Cyber Security rapporteur Thomas McDonogh- EESC Employers' Group and Padraig Kenny, ICT consultant from Arup, providing expert services to EESC Panel topics will include: ▪ Best practice examples and policies for citizens ▪ Cooperation and exchange of information ▪ Building top level networks addressing digital risks Moderator: Ann-Sofie Ronnlund, DG CONNECT **Promote cyber security awareness at all levels**
13:00-13:40	**Lunch Break** Invited to visit the poster exhibition organized by ECSM actors & materials on the metrics of the ECSM 2013 advocacy campaign **Online security requires your participation**

13:40-15:30	**Presentations of activities ECSM 2013** ▪ Matthias Gärtner, BSI Germany and Sven Scharioth, Deutschland sicher im Netz ▪ Tore Ordelokkenn, CEO, NorSIS ▪ Kjell Kalmelid, Information Assurance Unit/Swedish Civil Contingencies Agency (MSB) ▪ Axel Dyèvre, Director of CEIS-European Office ▪ Ann Mennens – Manager B-CCENTRE, ICRI KU Leuven – iMinds Moderator: **Philip De Picker, Belgium ISACA chapter** **Building together a joint EU advocacy campaign on NIS topics!**
15:30-15:50	**Networking Break** Invited to visit exhibition space organized by ECSM 2013 & Europe Direct **Online security requires your participation**
15:50-17:00	**Practice panel, "The Cyber Security Professional"** ▪ "Benefits of the CYSPA alliance for users, providers, and public authorities", Véronique Pevtschin, Engineering, CYSPA EU FP7 ▪ John Colley -(ISC)2 Managing Director EMEA, ▪ Sarb Sembhi ,Chair of ISACA Government and Regulatory Advocacy - Europe and Africa ▪ Nigel Payne/Howard Skidmore, e-Skills UK ▪ Steven Bradley, ISSA Brussels European Chapter Panel topics will include: ▪ Career Analysis into Cyber Security: New & Evolving Occupations ▪ Cyber Security Learning Pathways ▪ European trends form the 2013 Global Information Security Workforce Study ▪ Cyber security Career Lifecycle Moderator: Hadi El-Khoury, Board member of the French ISSA Chapter **Equipping Europe with Cyber Security Professionals** **Building together a joint EU advocacy campaign on NIS topics!**
17:00-17:30	**Closing session** ▪ Visualization: Summary of the conference presented by the rapporteur Jean-Christophe Pazzaglia, SAP/ CYSPA project ▪ "ENISA role in NIS community and ECSM example " Steve Purser, Head of Core Operations Department, ENISA Moderator: ENISA **Plan, implement, evaluate!**
From: 19:00 Location: DIGITALEUROPE 14 rue de la Science 1040 Brussels	ECSM talk and Networking ▪ Chris Gow, Chair of Privacy & Security group, DIGITALEUROPE Welcoming remarks ▪ Matthias Gärtner, ECSM country experience-Germany ▪ Zoltan Precsenyi, Presentation on Symantec Cyber Readiness Challenge **Innovate, design, test!**

Home **Registration** **Practical Information**

Annex B: ECSM Analytics

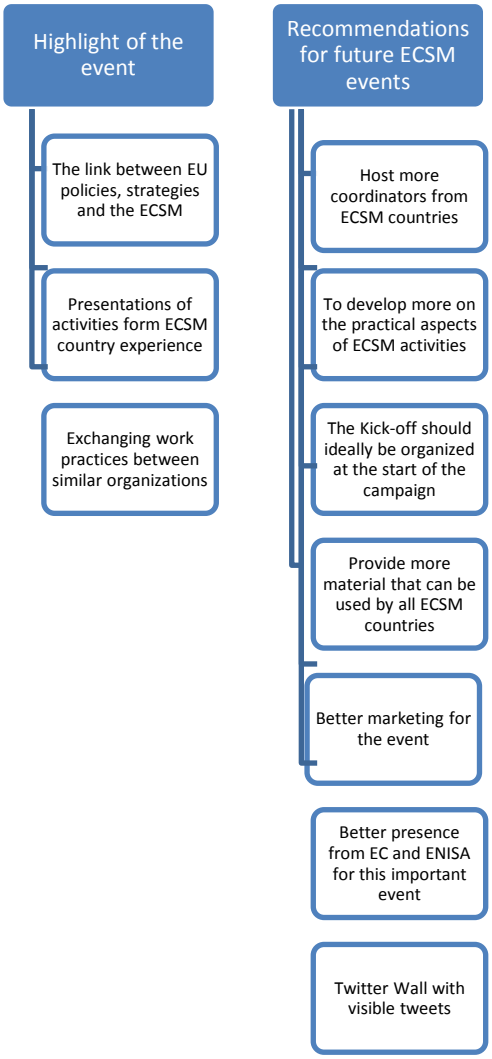
B.1 Coordinators meetings

- The ECSM Coordinators' meeting I took place on the 27th of May in ENISA's Athens office. The Meeting consisted of 19 online/ 5 in presence participants.
- The ECSM Coordinators' meeting II took place on the 30th of July via online channels. The meeting was attended by 7 online participants and 2 in presence participants.
- "ECSM news" sent via e-mail bi monthly;

B.2 Kick off event

- Participation rate: 67 participants in presence/ 44 remotely by web stream;

- Feedback from participants:

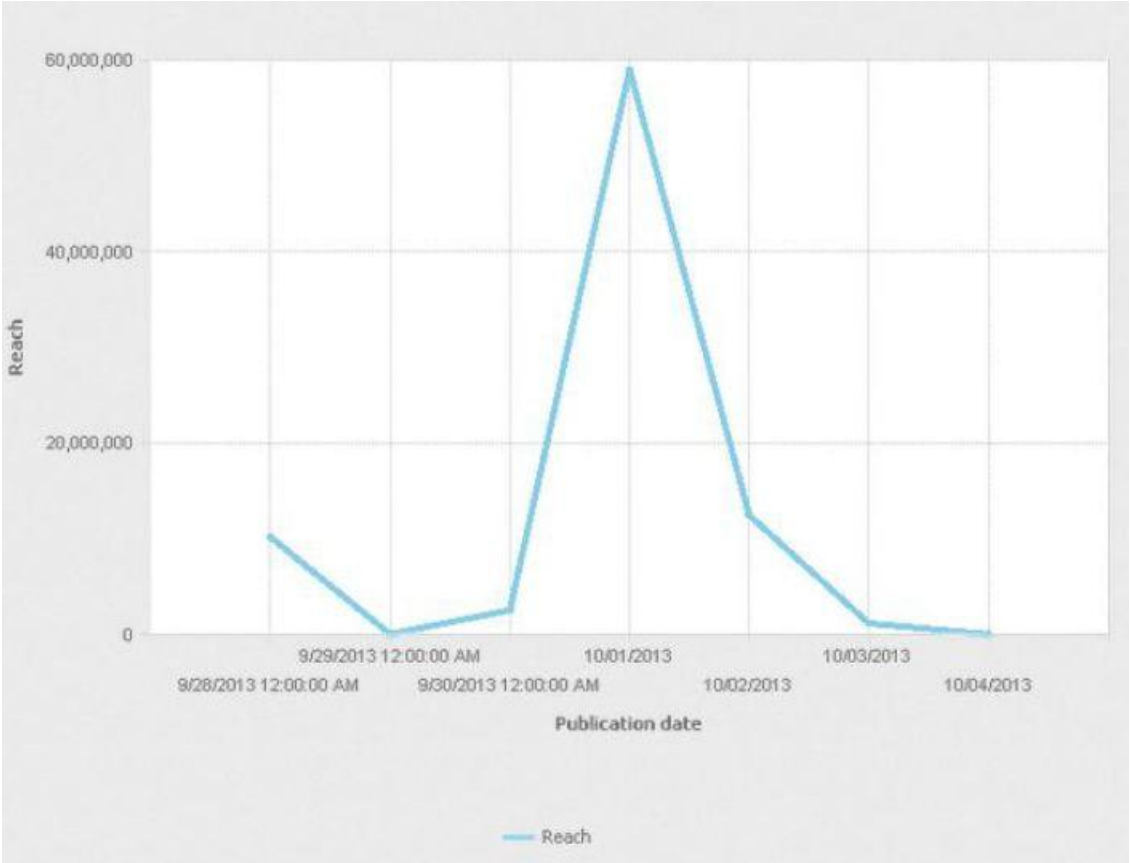


B.3 CyberSecurityMonth.eu Website

- Traffic from 1.09.2013 to 31.10.2103:

B.4 Enisa.europa.eu Website

- PR released on 1.10.2013:



B.5 Social media presence

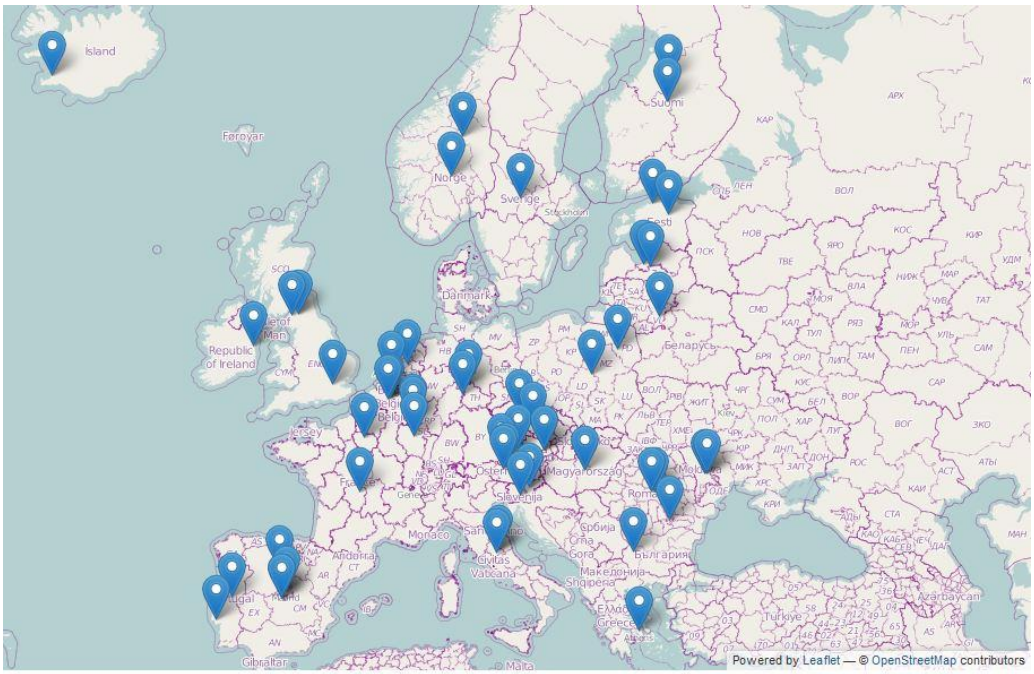
- CyberSecMonth Tag online reach on 2.10.2013:

- Twitter ECSM followers and Tweets activity increased significantly:

B.6 Feedback and ECSM countries

- 27 ECSM countries got involved (e.g 23 EU MSs, 4 EU partners):

- Activities mapping for ECSM 2013:



- International partners for Mobile Safety tips:

B.7 Partners ECSM 2013

More than 60 public and private stakeholders, as below:


Ministero dello Sviluppo Economico


si-cert


RYŠIŲ
REGULIAVIMO
TARNYBA


CASES

BUNDESKANZLERAMT ÖSTERREICH


safer
internet.cz


MSB
Swedish Civil
Contingencies
Agency


EUROPEISKA
INFORMATIONS-
SÄKERHETS-
MÅNADEN


BELGIAN
INTERNET
SECURITY
CONFERENCE


ISACA
Sistemas de información fiables y valiosos
Madrid Chapter


vieuws


RCSI INSTITUTE OF
LEADERSHIP
CyberPsychology Research Centre


ITSECURITY
Sichere Informationssysteme


oiip
Österreichisches Institut für Internationale Politik
Austrian Institute for International Affairs


virtuelles Amt


CYBER SECURITY CHALLENGE
START


oiat


ISACA
Trust in, and value from, information systems


Clusit
Associazione Italiana per la Sicurezza Informatica


DIGITALEUROPE


WKS
INFORMATION · CONSULTING


ISACA
Trust in, and value from, information systems
Latvia Chapter

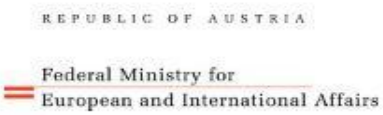

Cyber Security Challenge UK


bm:uk
Bundesministerium für Unterricht, Kunst und Kultur


b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE FOR TRAINING, RESEARCH & EDUCATION


CENTRUL DE
TELECOMUNICAȚII
SPECIALE


fh
st. pölten


REPUBLIC OF AUSTRIA
Federal Ministry for
European and International Affairs


orange


Allianz
Global Assistance


anubisnetworks™


Bundesamt
für Sicherheit in der
Informationstechnik
EUROPÄISCHER
MONAT
DER CYBER-
SICHERHEIT


SDA
SECURITY & DEFENCE AGENDA


FIC
2014
DIGITAL
IDENTITY


KASPERSKY lab


intel


EUROPOL

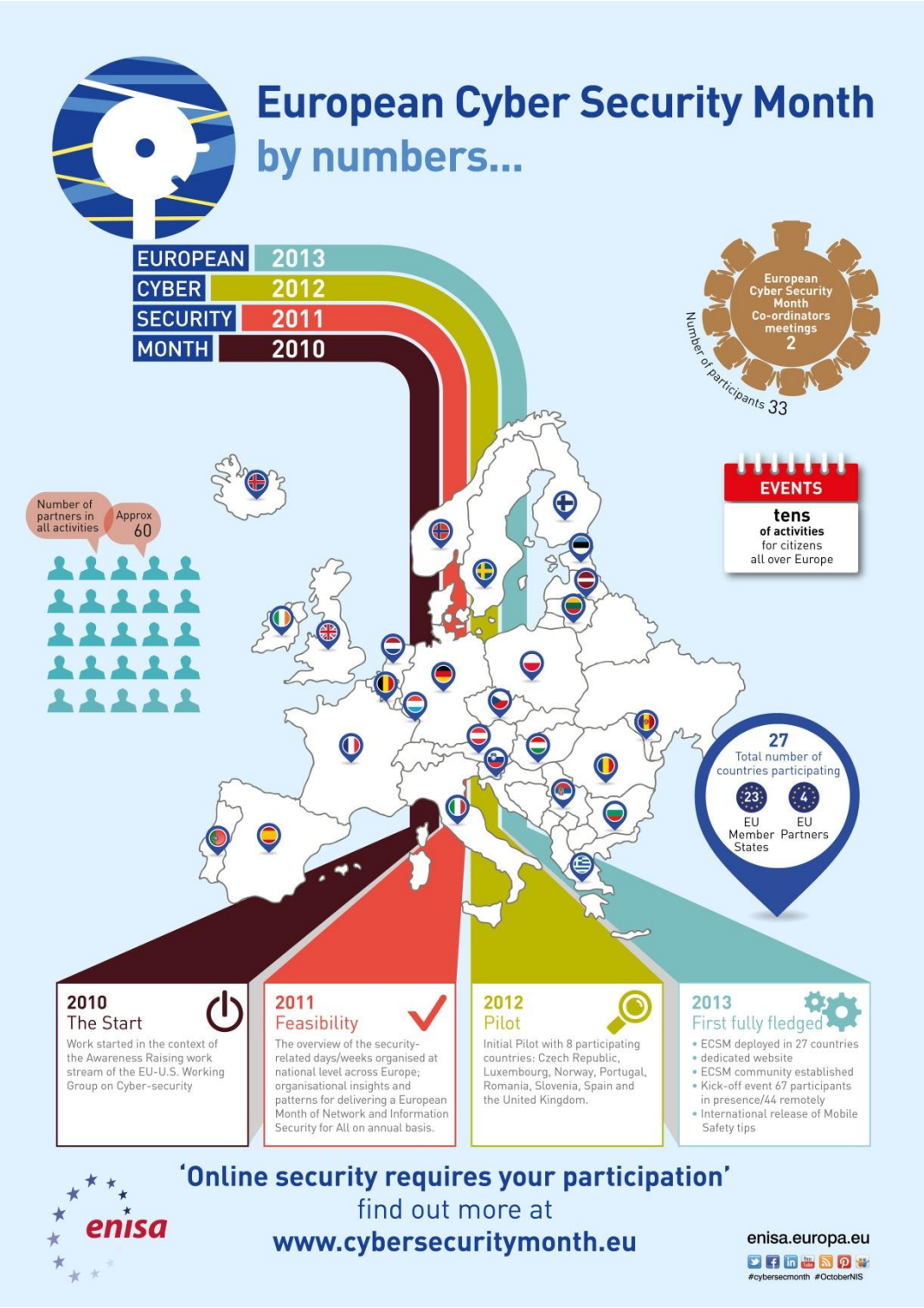

WORLD
ECONOMIC
FORUM


ISSA
Information Systems Security Association

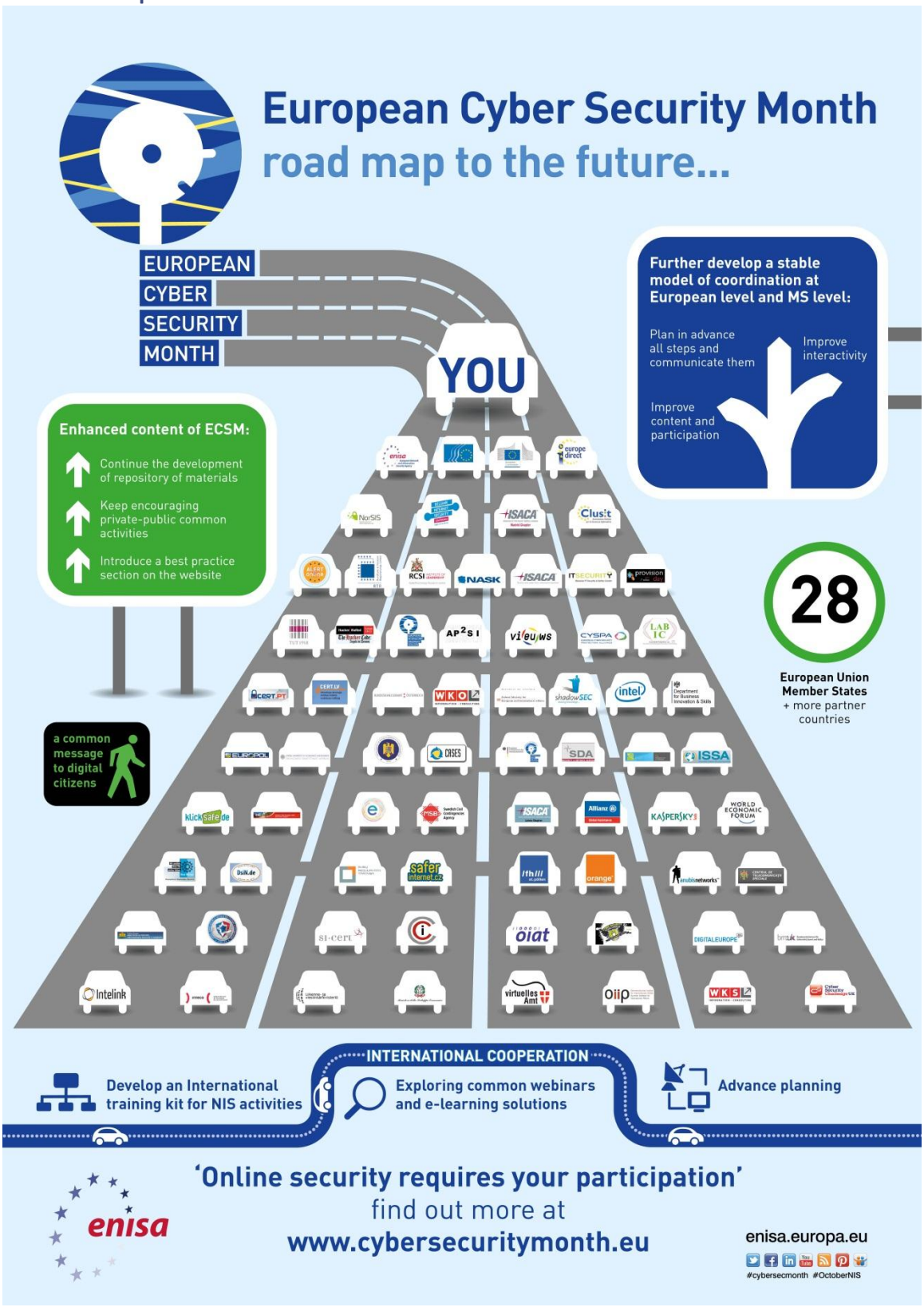

CYSPA
EUROPEAN CYBER SECURITY
PROTECTION ALLIANCE

Annex C: ECSM Info graphics

C.1 Overview on ECSM 2010- 2013



C.2 ECSM roadmap



TP-02-13-786-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu