Funded by the European Commission

Seventh Framework Programme

CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D 7.2 Dissemination Plan and Calendar of Activities

Date of deliverable: 31/5/2015
Actual submission date: 31/5/2015

Start date of the Project: 1st June 2014. Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 0.2

Project funded by the European Commission under the Seventh Framework Programme		
Restriction Level		
PU	Public	✔
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission)	

Revision history

Version	Object	Date	Author(s)
0.1	Creation	10/3/2015	Olga E. Segou, Stelios C.A. Thomopoulos.
0.2	First Draft released for internal review	19/5/2015	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Erik Tews, Peter Kieseberg, Paraskevi Fragopoulou.
0.3	Updated Workshop plan	25/5/2015	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Erik Tews, Peter Kieseberg.
0.4	Second round of review	25/5/2015	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Erik Tews, Peter Kieseberg, Paraskevi Fragopoulou.
0.5	Minor changes	28/5/2015	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Matteo Mauri
0.6	Finalization	18/5/2015	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Matteo Mauri
1.0	Submission	29/5/2015	Fabio Roli, Davide Ariu, Giorgio Giacinto

D7.2
Preliminary Dissemination and Exploitation Report

Responsible

Dr. Stelios C.A. Thomopoulos (NCSRD)
Olga E. Segou (NCSRD)

Contributor(s)

Pr. Fabio Roli (UNICA)
Pr. Giorgio Giacinto (UNICA)
Dr. Davide Ariu (UNICA)
Matteo Mauri (UNICA)
Erik Tews (TUD)
Peter Kieseberg (SBA)
Dr. Paraskevi Fragopoulou (FORTH)

Summary:

The CyberROAD project has been funded under the 7th Framework Programme in order to provide insight on current and future Cyber Crime and Cyber Terrorism research. CyberROAD aims to develop a comprehensive research roadmap, which will enumerate current research gaps and anticipate emerging threats.

CyberROAD devotes Work Package 7 to high-impact dissemination and exploitation activities. This document (D7.2 “Preliminary Dissemination and Exploitation Report”) presents the dissemination and exploitation activities that were undertaken by the consortium towards the effective dissemination and exploitation of key CyberROAD results, within the project’s first year of activities.

This work includes all actions and initiatives undertaken by the partners in order to maximise the visibility of CyberROAD scientific accomplishments, targeting the scientific community, the general public and the relevant stakeholders. It also includes an updated dissemination and exploitation plan for CyberROAD’s second year of activities, as well as updated calendar listings of important dates for dissemination/exploitation activities and WP7 milestones, for the second year of project activities.

Keywords: CyberROAD, Dissemination, Exploitation, Work Package 7, Calendar, Dissemination Plan, Exploitation Plan, Liaison, Public Awareness, Workshop.

TABLE OF CONTENTS

1 Introduction

1.1 Aims of the CyberROAD Project

The CyberROAD project aims to identify current and future issues in the fight against Cyber Crime and Cyber Terrorism, in order to draw a roadmap for cyber security research. Within the two-year lifecycle of the project, a detailed snapshot of the technological, social, economic, political, and legal scenario on which Cyber Crime and Cyber Terrorism do develop will be provided. Cyber Crime and Cyber Terrorism will also be studied, in order to identify priorities and research bottlenecks.

The project relies on a large body of competences, since it has 20 partners, from 11 different countries. The consortium represents all the players and the stakeholders involved in the fight against cyber crime and cyber terrorism: law enforcement, public bodies, universities and reseach centers, as well as companies and industries. The project also relies on a high profile advisory board, made of members of worldwide relevant organizations involved in the fight against cyber crime and cyber terrorism. The wide consortium, as well as the advisory board, will ensure the involvement of all the possible stakeholders, by allowing having a clear and complete picture of the real priorities. Such a large consortium will also allow an adequate dissemination of the project results, fundamental step to foster and to promote research activity toward the directions devised during the project execution. The official project Kick-Off meeting was held in Cagliari, Italy on June 24th-25th, 2014.

1.2 Purpose of this document

This document provides a comprehensive description of dissemination and exploitation conducted within the first year of the project, on par with the dissemination and exploitation strategy within D7.1 (“Dissemination Plan and Calendar of activities”). It also provides an updated plan and calendar for the project’s second year of activities.

Dissemination constitutes a decisive factor for the successful exploitation of the key CyberROAD results, having as its major objective to raise awareness of the activities that will be performed during the project’s lifetime and beyond. Dissemination activities are directed to showcasing CyberROAD project results utilizing all available communication channels. These activities target:

a) **the general public:** Activities will be undertaken to raise awareness on the issue of emerging Cyber Crime and Cyber Terrorism threats. Furthermore, it is the consensus of the CyberROAD consortium that an effective public outreach campaign is necessary as the public should be privy to research results stemming from EC-funded research.

b) **the scientific community:** CyberROAD will reach the scientific community through the publication of research results and the participation of partners to relevant events and gatherings of scientific nature (Workshops, Conferences etc.). Two International Workshops dedicated to promoting cutting-edge research will be organized by CyberROAD to be collocated with high-profile International Conferences.

c) **the potential stakeholders and policy makers:** including Critical Infrastructure operators, Data Protection Authorities etc. The consortium will focus on extensive liaison activities and will organize an additional workshop and a final event, aiming for the widest diffusion of CyberROAD knowledge.

1.3 STRUCTURE OF THIS DOCUMENT

This document is structured as follows:

- **Chapter 1** provides an introduction to the context of Dissemination and Exploitation activities and states the purpose of this document.
- **Chapter 2** provides an overview of activities pertaining the project's digital presence.
- **Chapter 3** provides a report of activities relating to the organization of CyberROAD workshops and dissemination events.
- **Chapter 4** focuses on the scientific dissemination of CyberROAD results, via academic journals and any other means.
- **Chapter 5** lists all other dissemination activities (e.g. production of dissemination material etc.)
- **Chapter 6** focuses on providing examples of exploitation and liaison/networking activities.
- **Chapter 7** provides an updated dissemination and exploitation plan and calendar of WP7 activities for the project's second year.

2 ONLINE PRESENCE

This section details activities related to maintaining a continuous online presence for the project. It includes activities taken up within T7.3 "Establishment of a digital presence". Within the first year, the design and the content of the project website has been updated. Partner FORTH also took up technical maintenance of the main project website. NCSRD maintained the project's social networking accounts. UNICA and the consortium as a whole, contributed necessary additions to the content. Furthermore, it includes information on individual partners' online awareness raising activities within T7.5 "Generalized Awareness and Training Campaign".

2.1 MAIN WEBSITE

The CyberROAD website[1] was launched on September 1, 2014 and reflects one of the main objectives of Task WP7.3 of the project. The project website (Figure 2-1) aims to maximize CyberROAD impact by making all project activities and results visible and accessible to the research community, the stakeholder's community and the public.

The main sections of the website are organized as follows:

- **Home:** the main page of the website which provides an overview of the project,
- **Project:** more detailed information on the project,
- **Partners:** a short profile of all the project partners is provided through this section,
- **Publications:** featuring documents, publications deliverables and presentations,
- **News:** news about the project activities,
- **Events:** events planning, announcements and news,
- **Media:** this section will be used to provide a picture of the media coverage of the project,
- **Twin Projects:** provides information on projects related to the topics of CyberROAD,
- **Contact:** a contact form allowing visitors to contact the project consortium.

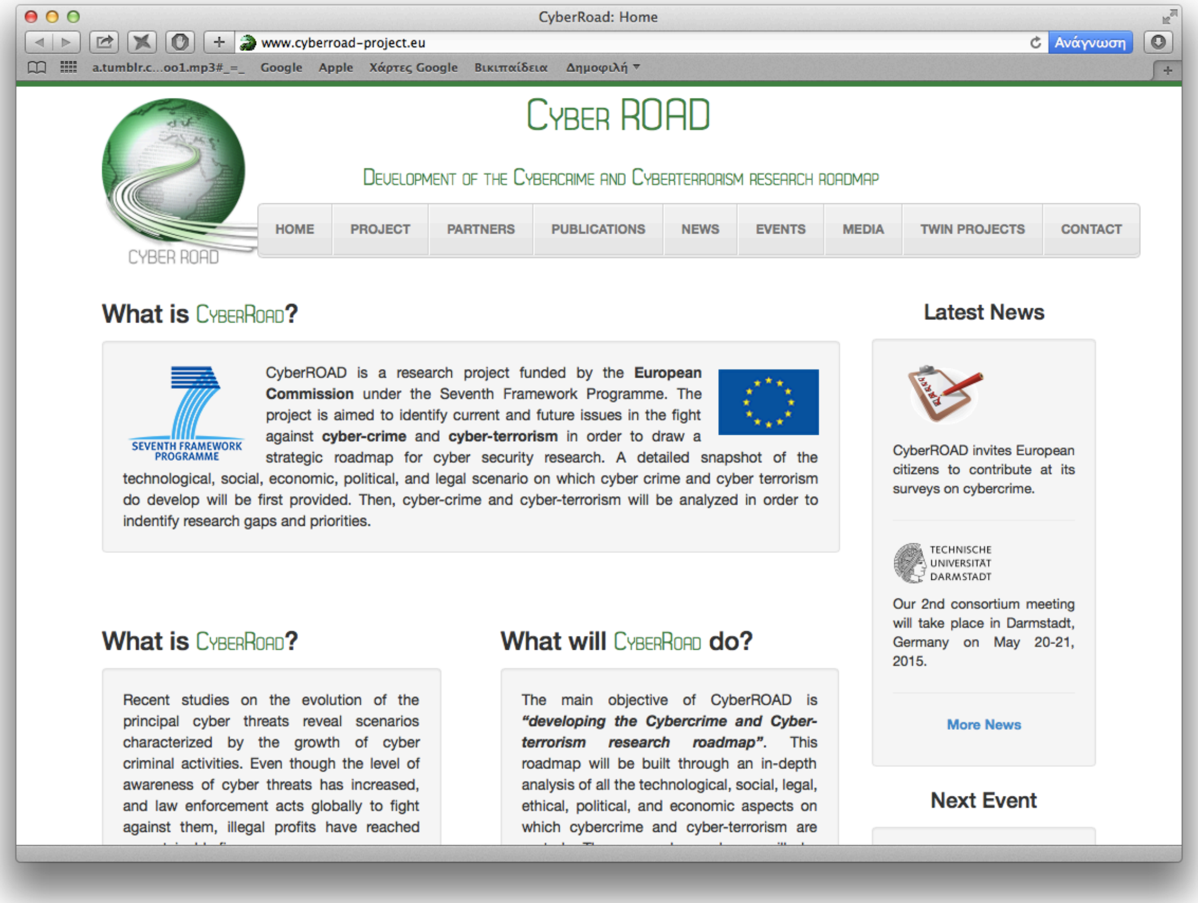
Details on the website design, standards compliance, hosting and data management activities are included in D7.1 ("Dissemination Plan and Calendar of Activities") and report D7.5 ("Project Website and Social Networking accounts").

The website has been registered with Google Analytics by FORTH, in order to measure its impact and effectiveness. This allows FORTH to record and report information such as the number of visitors and sessions within a selected date range, the geographic distribution of visitors and the popularity of various links and sections. Google Analytics can help us to improve our website and learn more about our visitors' experience.

[1] CyberROAD website (Accessed May 2015): http://www.cyberroad-project.eu

The sessions to the CyberROAD website per month during the first eight months of the project can be seen in Figure 2-2. We can see **that a total of 3,696 unique visits** made by mostly new visitors were recorded in this period. This means that we had an approximate of more than 15 sessions per day.

The pages most viewed by the visitors of our website appear in Figure 2-3. Naturally enough, the Front-page of the website and the Partners section dominate the pageviews. It also seems that there is a considerable interest in our Publications section, which hosts deliverables and presentations made by the consortium.



CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBERTERRORISM RESEARCH ROADMAP

What is CyberRoad?

CyberROAD is a research project funded by the **European Commission** under the Seventh Framework Programme. The project is aimed to identify current and future issues in the fight against **cyber-crime** and **cyber-terrorism** in order to draw a strategic roadmap for cyber security research. A detailed snapshot of the technological, social, economic, political, and legal scenario on which cyber crime and cyber terrorism do develop will be first provided. Then, cyber-crime and cyber-terrorism will be analyzed in order to indentify research gaps and priorities.

Latest News

CyberROAD invites European citizens to contribute at its surveys on cybercrime.

Our 2nd consortium meeting will take place in Darmstadt, Germany on May 20-21, 2015.

What is CyberRoad?

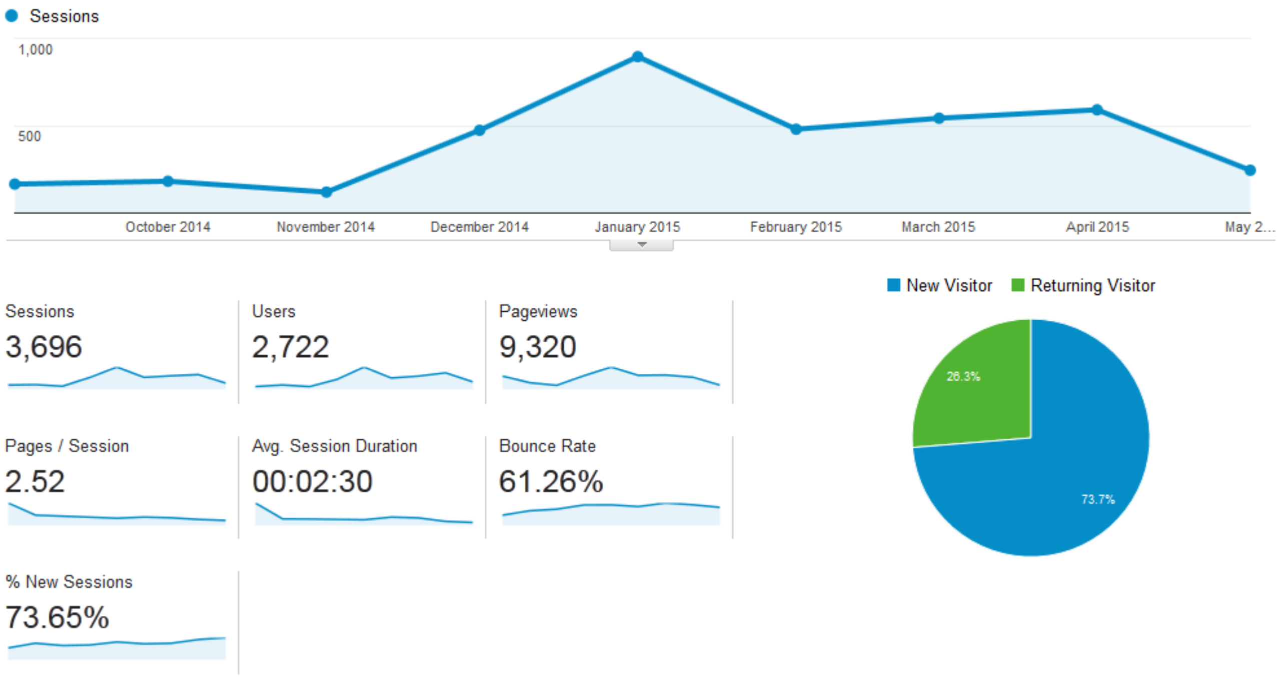
Recent studies on the evolution of the principal cyber threats reveal scenarios characterized by the growth of cyber criminal activities. Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to fight against them, illegal profits have reached

What will CyberRoad do?

The main objective of CyberROAD is ***"developing the Cybercrime and Cyber-terrorism research roadmap"***. This roadmap will be built through an in-depth analysis of all the technological, social, legal, ethical, political, and economic aspects on which cybercrime and cyber-terrorism are

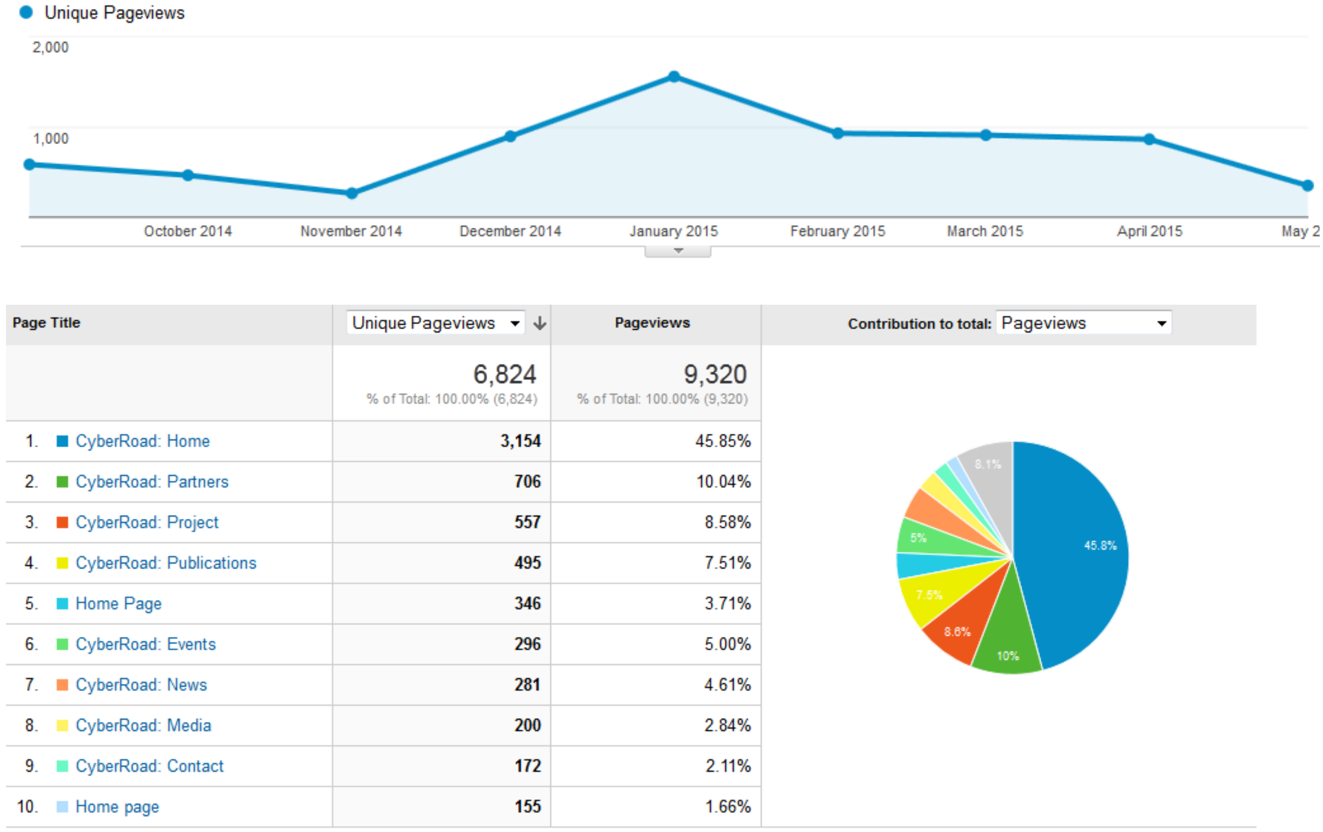
Next Event

Figure 2-1 Main page for the CyberROAD project.



Sessions 3,696	Users 2,722	Pageviews 9,320
Pages / Session 2.52	Avg. Session Duration 00:02:30	Bounce Rate 61.26%
% New Sessions 73.65%		

Figure 2-2 Sessions to the CyberROAD website



Page Title	Unique Pageviews ↓	Pageviews
	6,824 % of Total: 100.00% (6,824)	9,320 % of Total: 100.00% (9,320)
1. 🟦 CyberRoad: Home	3,154	45.85%
2. 🟩 CyberRoad: Partners	706	10.04%
3. 🟥 CyberRoad: Project	557	8.58%
4. 🟨 CyberRoad: Publications	495	7.51%
5. 🟦 Home Page	346	3.71%
6. 🟩 CyberRoad: Events	296	5.00%
7. 🟧 CyberRoad: News	281	4.61%
8. 🟨 CyberRoad: Media	200	2.84%
9. 🟩 CyberRoad: Contact	172	2.11%
10. 🟦 Home page	155	1.66%

Figure 2-3 Unique page views of the website content.

2.2 *Developing a Social Media Strategy*

The project has already established social media accounts on the popular Facebook, Twitter, Google Plus and LinkedIn platforms. An updated social media strategy has been devised and is currently set into place, in order to maximize the project's outreach to stakeholders and the general public. The project's social media strategy can be summarised in the following points:

a) Identification of target audience & improving reach-out:

The target audience for CyberROAD social media is identified as:

- Law Enforcement and other organizations (e.g. the European Defense Agency, NATO Cyber Defense, Europol, Interpol and National Law Enforcement agencies across Europe and globally),
- Professionals and Researchers in IT Security, Criminology, Privacy, etc.
- Privacy and Civil Rights Advocates
- Scientific Communities and Publishers like (IEEE, ACM etc.)
- Mass Media focusing on Technology news (CNET, Financial Times Tech, BBC Tech etc.)
- CERT and CSIRT groups operating in Europe and globally,
- Policy Makers and Legislators across the EU region,
- Other consortia active in Cyber Security Research (e.g. CAMINO, COURAGE, ACDC, UINFC2, Swept, ILLBuster etc.),
- Educators, organizations and initiatives that can reach the general public (e.g. the Cyber Security Month advocacy campaign STOP.THINK. CONNECT. etc.),
- SMEs and Industries active in Cyber Security.

CyberROAD reached out to more than 400 professionals and organizations through the social media, spending more effort in the LinkedIn and Twitter platforms as effective means of communication with professionals and the general public.

b) Sparking discussion in social media:

We envision the CyberROAD social media accounts as channels of two-way communication and not solely as means to promote project activities. Following the reach-out activities, discussions were initiated within the LinkedIn group and Twitter account of the project. These two platforms were identified as more effective means to contact professionals while also maximizing reach-out.

c) Updating social media content:

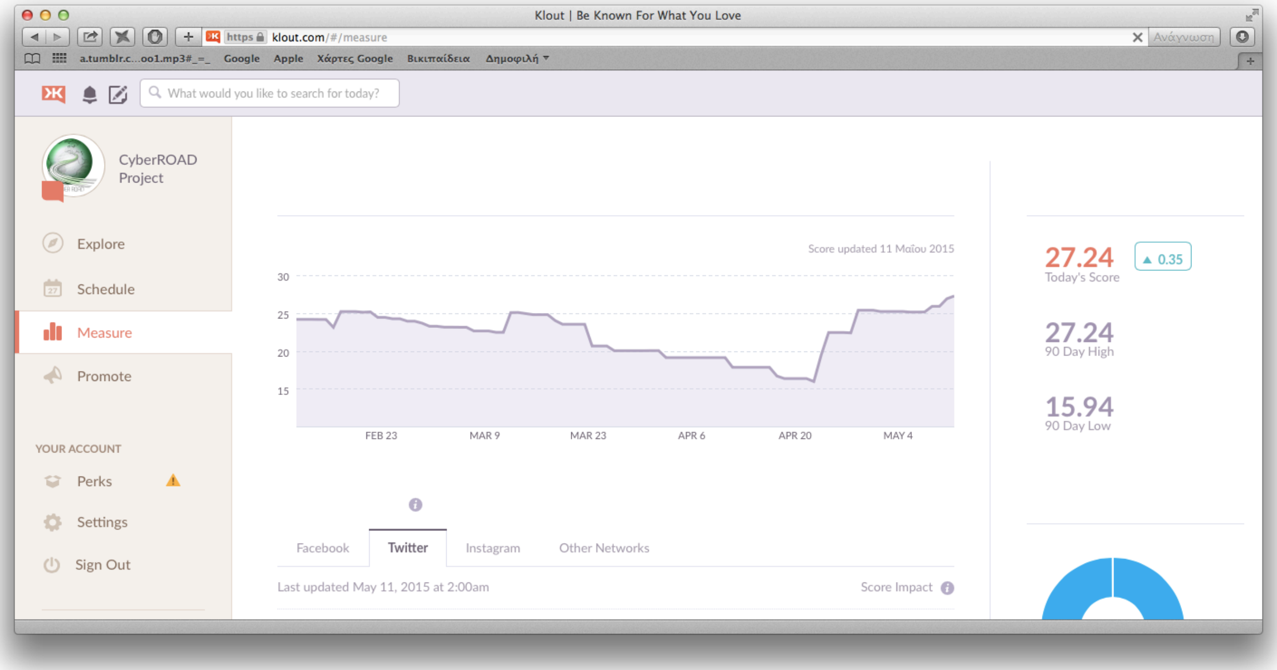
The social media content consists of postings that are relevant to project activities and news articles on Cyber Security, Privacy and Digital Rights. Furthermore, the project survey and FCCT 2015 call for papers were disseminated through our social media.

It is envisioned that CyberROAD Work Packages that have already produced tangible results will contribute appropriate content for public release through the CyberROAD social media, after results have been officially reported to the European Commission.

d) Measuring social impact and re-assessing the current strategy:

The LinkedIn CyberROAD group[2] currently has 70 registered members and has sparked discussions on emerging threats and scenaria among its members. During the second year of activities, discussion will be initiated to discuss CyberROAD results with the professional community of LinkedIn, after related results that can be publicised, have been officially reported with the European Commission. By the end of the project's second year, we estimate that the number of registered members will have increased along with the number of discussions iniated within the group.

The project's Twitter account currently has amassed more than 100 followers among the desired target demographics. The CyberROAD Twitter account was linked to a Klout account (Fig. 2-4) to measure Twitter influence. Klout is a well-known platform used to estimate social impact. Klout[3] uses social media analytics to rank its users according to their online social presense and influence, estimated as the "Klout Score". The Klout Score is represented as a numerical value between 1 and 100. In order to determine the user score Klout *"measures the size of a user's social media network and correlates the content created to measure how other users interact with that content"*. The current score for the CyberROAD online presence ranges from 27-29 (small to medium account) within the first year of project activities, with a target of at least 40 (medium size account) before the project's conclusion and Final Event.



Score updated 11 Μαΐου 2015

27.24 Today's Score ▲ 0.35

27.24 90 Day High

15.94 90 Day Low

Last updated May 11, 2015 at 2:00am

Figure 2-4 The Project's Klout account with the Twitter account activated (May 11, 2015), showing Klout score impact over a 90-day period.

[2] CyberROAD in LinkedIN: https://www.linkedin.com/groups/CyberROAD-8184478/about (Last Access: May 2015)

[3] Klout: https://klout.com (Last Access: May 2015)

2.3 Individual Partner Activities For Public Awareness

CyberROAD partners were encouraged to utilize their existing dissemination capabilities to promote CyberROAD results. Such capabilities include, but are not limited to Partner websites, Blogs, Newsletters, Press Releases, Mass Media, etc.

Table 2-1 Project Information pages, blog and newsletter posts that were created by the consortium, announced the project and promoted the survey activities (Links ccessed May 2015).

Partner	Link
UNICA	*http://pralab.diee.unica.it/en/CyberRoad*
NCSRD	*https://www.iit.demokritos.gr/project/cyberroad*
NCSRD	*https://www.iit.demokritos.gr/newsletter/11.html*
NCSRD	*https://www.iit.demokritos.gr/newsletter/9.html*
NCSRD	*https://www.iit.demokritos.gr/newsletter/7.html*
INDRA	*http://www.indracompany.com/sostenibilidad-e-innovacion/proyectos-innovacion/cyberroad-development-cyber-crime-and-cyber-terrori*
PJ	*http://www.policiajudiciaria.pt/PortalWeb/page/%7B0D3ADE83-BE25-47C7-9EAE-0E39B30004ED%7D*
NASK	*http://www.cert.pl/news/9671/langswitch_lang/en*
SBA	https://www.sba-research.org/research/projects/cyberroad/
SBA	http://www.ares-conference.eu/conference/ares-eu-symposium/fcct-2015/

Table 2-2 Mass Media Activities in the press, online and coverage by TV and Radio (Links accessed May 2015).

Activity	Link
TV coverage in RAI 3 (Italy)	*https://www.youtube.com/watch?v=jGT2g_OFji4*
Press, UNICA News Online (Italy)	*Unica News Online* “CyberRoad, la lotta al crimine e al terrorismo informatico passa dall’università di Cagliari”
Press, La Nuova Sardegna (Italy)	*La Nuova Sardegna* “CyberRoad, la guerra al terrorismo sul web comincia in Sardegna”
Online, HinterlandCagliari (Italy)	*hinterlandcagliari.it* “CyberRoad, la lotta al crimine e al terrorismo informatico passa dall’università di Cagliari.”
Press, Sardegna Oggi (Italy)	*sardegnaoggi.it* “600 mila profili facebook manomessi ogni giorno. Dall’Università di Cagliari lotta al crimine informatico.”
Press, La Provincia del	*http://www.laprovinciadelsulcisiglesiente.com/wordpress/2014/06/cyberroad-la-lotta-al-crimine-e-al-terrorismo-informatico-passa-dalluniversita-*

Activity	**Link**
Sulcis Ingelciente (Italy)	*di-cagliari* "CyberRoad, la lotta al crimine e al terrorismo informatico passa dall'università di Cagliari." *http://www.laprovinciadelsulcisiglesiente.com/* "Gli specialisti di informatica dell'ateneo di Cagliari chiudono un altro anno proficuo per didattica, ricerca e progetti internazionali di alto livello."
Press,Sarda news, (Italy)	*sardanews.it* "CyberRoad, la lotta al crimine e al terrorismo informatico passa dall'università di Cagliari."
Press, Castedduonline, (Italy)	*castedduonline.it* "Hacker e dintorni, a gonfie vele la scuola di sicurezza informatica."
Press, Sardegna Live, (Italy)	*sardegnalive.net* "CyberRoad, la lotta al crimine e al terrorismo informatico passa dall'università di Cagliari."
Press	*latestata.info* "Progetto CyberROAD".
Press and Video, Intelligence Live event	*http://pralab.diee.unica.it/sites/default/files/F.Roli%20Intelligence%20Live%202014.pdf* *https://www.youtube.com/watch?t=1735&v=Z7yK79Js2-4#t=28m45s*
Press	*La Nuova Sardegna* "I servizi segreti a caccia di cervelli: futuri 007 anche dall'isola"
Article in Unica News Online & Newsletter	*http://www.unica.it/pub/7/show.jsp?id=25949&iso=-2&is=7* *http://unica.it/UserFiles/File/Utenti/nuvoli/Unicanews/Unicanews%207 5%20luglio%202014.pdf* "Università e Intelligence, grande opportunità di collaborazione"
Press, Online Article (CERT Polska Annual Report), Poland	*http://www.cert.pl/PDF/Raport_CP_2014.pdf*
GIRPR Newsletter	http://girpr.tk/sites/girpr.tk/files/GIRPRNewsletter_Vol6Num2.pdf Gruppo Italiano Ricercatori in Pattern Recognition Newsletter, Vol.6, No2.
CIPRNet Newsletter	https://www.ciprnet.eu/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1432908784&hash=1c257c0cbf0f304d9f1cede1bf0a0688f0e80fd&file=fileadmin/user_upload/ECN/European_CIIP_Newsletter_Vol_9_No_1__20_.pdf May-June Issue (Vol.9 No.1) of European CIIP Newsletter featuring the FCCT2015 call for papers.
Press	http://www.comunecagliarinews.it/news.php?pagina=12315: "L'Università di Cagliari aderisce al Mese Europeo della Sicurezza Informatica"

3 CYBERROAD WORKSHOPS AND DISSEMINATION EVENTS

Within the first year of the project, a project meeting and workshop took place in TUD premises in Darmstadt. In addition, NCSRD and SBA also took up planning and the organization of two additional events to take place in 2015, on M13 and M15 of the project. This section details these activities and also provides a necessary contingency plan for the organization of the third CyberROAD workshop due to a scheduling conflict, with respect to the ARES 2016 Conference date.

3.1 FIRST CYBERROAD WORKSHOP

The first CyberROAD Workshop was organized and hosted by the Technical University of Darmstadt, on May 20th - 21st 2015 (M12), in Darmstadt, Germany. The Workshop focused on a comprehensive discussion of the roadmapping methodology presented within WP2 ("Scientific Coordination") and receiving feedback from consortium members and external invited advisors. The Workshop explored the links between the work performed within all WPs and their dependencies with the methodologies developed in WP2. In essence, the workshop featured:

- a summarization of the first year of activities within all CyberROAD workpackages and an exploration of the existing links,
- a comprehensive presentation of the CyberROAD roadmapping and risk assessment methodology
- an identification of research gaps and presentation of practical examples,
- the introduction of attending advisory board members,

The participants were then organized in working groups to practice the proposed methodology, by:

- Discussing and building the current state,
- Identifying research gaps in terms of WP3 ("Social, Economical, Political, Legal Scenario"), WP4 ("Technological Scenario"), Wp5 ("Cyber Crime") and WP6 ("Cyber Terrorism"),
- Developing future scenarios and,
- Presenting and consolidating outputs among the working groups.

Results of this activity will be reported within a dedicated deliverable (D7.7) which is expected on M14 (July 2015).

3.2 ORGANIZATION OF FCCT 2015

The second CyberROAD Workshop will be aimed at scientific dissemination and will be collocated with the 2015 International Conference on Availability, Reliability and Security (ARES 2015), taking place in Toulouse, France on 24th-28th August 2015.

The main goal for FCCT (First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism) lies in the development of a **scientific workshop** explicitely targeting the area of cybercrime and cyberterrorism at an academic level. For this, the workshop is collocated with the renowned ARES-conference, a B-rated conference according to CORE[4], which is now in its tenth year. The format of this workshop is the form of a scientific conference – based on a Call-for-Papers (CfP) scientists from all over the world are able to submit original research work. Independent reviewers including members of the consortium, evaluate the papers for their quality and their scientific contribution for enhancing the field of research on cybercrime and cyberterrorism. We enforce a **double-blinded review process**, i.e. neither the reviewers know the name of the authors, nor the other way round. In order to remove any conflicts of interest, the reviewers must possess a different affiliation than the submitting authors. This is checked for by the FCCT-chair together with the organizers if the main conference. Furthermore, all submissions are automatically checked for plagiarism by the organizers of ARES by utilizing state-of-the-art technology. In case of papers submitted by consortium members, independent external reviewers can be invoked. All accepted publications for FCCT will be officially **published with IEEE** Conference Publishing Services[5] in the proceedings of the main conference and are thus legit scientific papers that are available via the IEEE digital library.

All accepted papers must be presented in August at the FCCT in Toulouse by at least one of the authors. Currently, 30 minutes of presentation and discussion with the audience are allocated for each paper. Additionally, Davide Ariu (UNICA) will give a keynote on the principles, aims and preliminary results of the CyberROAD project. Furthermore, we will invite another **external keynote speaker**, most probably on the stakeholder side, to give some more insights into the field from an outside perspective.

The collocation with the ARES conference possesses seveal benefits for the organization of the workshop: First, a big conference is able to draw a **higher number of interested visitors** – all visitors of the ARES conference are also entitled to visit the FCCT as a member of the audience. Second, many of the organizational background, e.g. homepage[6], submission system and dissemination of the CfP, are taken care of the ARES organizers, thus making the organization of FCCT very effective in terms of work time needed to be spent during the CyberROAD project. Third, since the submission rates are very satisfying and the topic considered very important in the future, the organizers strive to **continue** the organization of **FCCT**, together with the members of the CyberROAD consortium, even **after** the **end** of the **CyberROAD** project, thus targeting to establish a long-standing workshop for bringing together research and scientists in these topics. Since the ARES conference moves around Europe to another location every year, also the geographical dimension of such a workshop will be greatly enhanced and allows for the beter inclusion of regional audience and stakeholders.

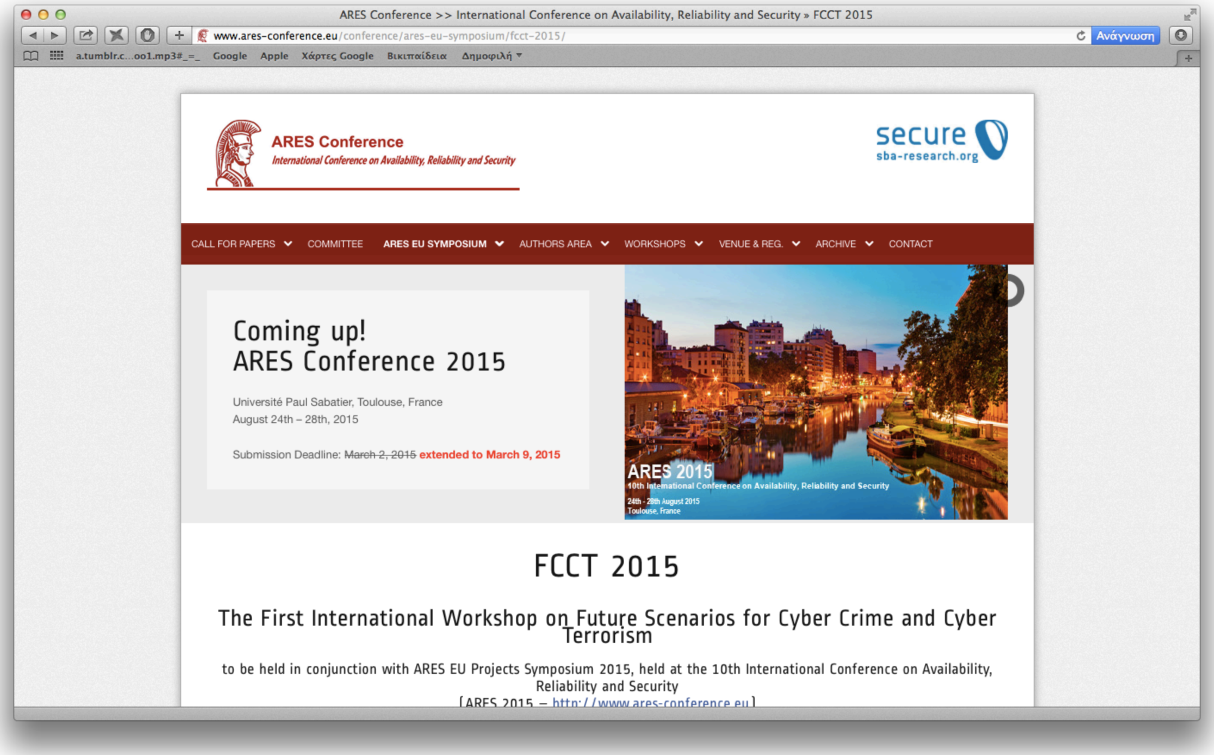
Appendix A includes the FCCT 2015 call for papers, which was disseminated by the partners. The Call for Papers was also available within the European Critical Infrastructure Preparedness and Resilience

[4] CORE Conference Portal listing for ARES : http://103.1.187.206/core/?search=ARES&by=all&source=CORE2014&sort=atitle&page=1 (Accessed May 2015)

[5] IEEE Computer Society main page (Accessed May 2015): http://www.computer.org/web/guest/home

[6] ARES conference main page (Accessed May 2015): http://www.ares-conference.eu/conference/ares-eu-symposium/fcct-2015/

Research Network (CIPRnet) Newsletter (Issue of March 15th - June 15th 2015, Volume 9, Number 1)[7]. Furthermore, the FCCT 2015 event features its own webpage within the ARES conference site[8] (Figure 3-1). The Workshop report for FCCT 2015 will be delivered within one month from the conclusion of FCCT 2015 activities (i.e. September 2015, M16).


ARES Conference >> International Conference on Availability, Reliability and Security » FCCT 2015
www.ares-conference.eu/conference/ares-eu-symposium/fcct-2015/
Ανάγνωση
a.tumblr.c...oo1.mp3#_=_
Google
Apple
Χάρτες Google
Βικιπαίδεια
Δημοφιλή
ARES Conference
International Conference on Availability, Reliability and Security
secure
sba-research.org
CALL FOR PAPERS
COMMITTEE
ARES EU SYMPOSIUM
AUTHORS AREA
WORKSHOPS
VENUE & REG.
ARCHIVE
CONTACT
ARES 2015
10th International Conference on Availability, Reliability and Security
24th - 28th August 2015
Toulouse, France

Coming up!
ARES Conference 2015

Université Paul Sabatier, Toulouse, France
August 24th – 28th, 2015

Submission Deadline: ~~March 2, 2015~~ extended to March 9, 2015

FCCT 2015

The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism

to be held in conjunction with ARES EU Projects Symposium 2015, held at the 10th International Conference on Availability, Reliability and Security
[ARES 2015 – http://www.ares-conference.eu]

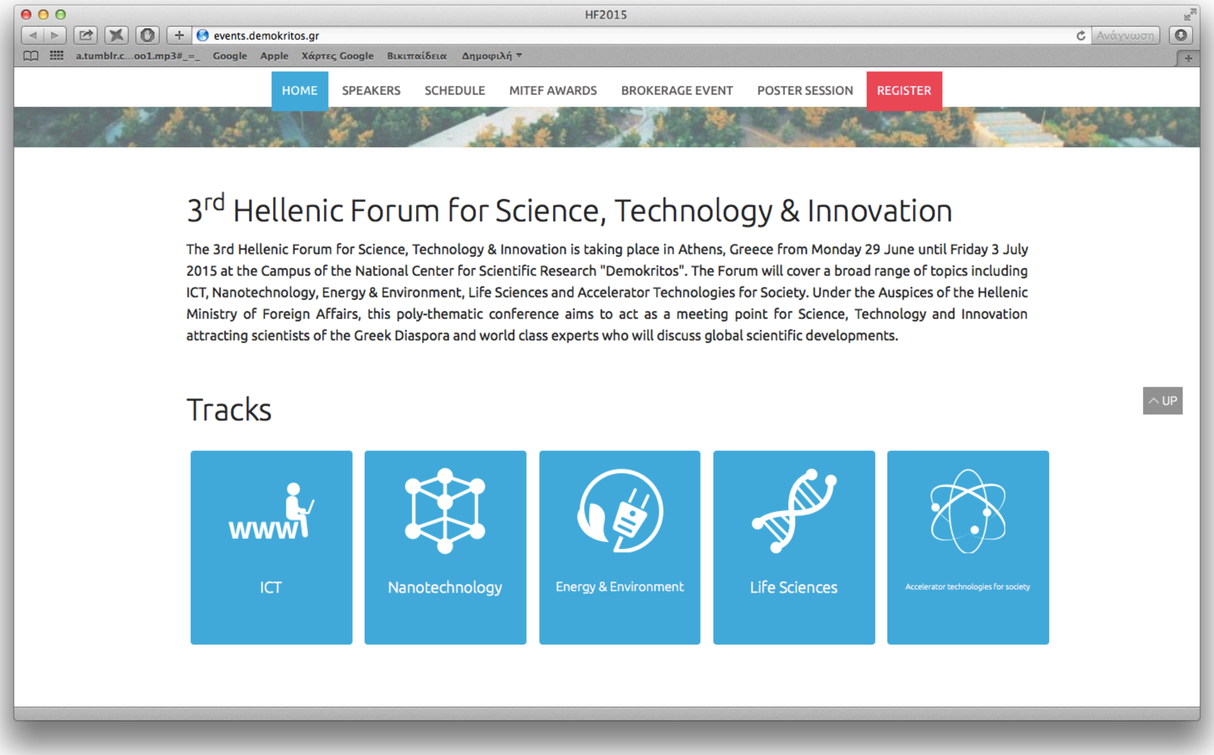
Figure 3-1 Main page for FCCT 2015.

3.3 Organization of the 3rd Hellenic Forum for Science, Technology and Innovation

NCSRD organizes an annual Hellenic Forum for Science, Technology and Innovation. The 3rd Hellenic Forum will take place on NCSRD premises on 29th June-3rd July 2015. Within this event, a free-to-attend public session is organized on “Digital Security, Privacy and Trust” featuring invited speakers across the world. CyberROAD will be represented by NCSRD who will present the project activities and coordinate the session. Representatives of the CAMINO and COURAGE consortia have also been invited to attend the event and present the respective twin projects. The results of this activity will be reported within the D7.7 report, which is expected on July 2015 (M14).

[7] CIPRnet Newsletter issue Available Online at: https://www.ciprnet.eu/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1432908784&hash=1c257c0cbf0f304d9f1cede1bfb0a0688f0e80fd&file=fileadmin/user_upload/ECN/European_CIIP_Newsletter_Vol_9_No_1__20_.pdf (Accessed May 2015).

[8] Main page for FCCT 2015: http://www.ares-conference.eu/conference/ares-eu-symposium/fcct-2015/ (Accessed May 2015).



3rd Hellenic Forum for Science, Technology & Innovation

The 3rd Hellenic Forum for Science, Technology & Innovation is taking place in Athens, Greece from Monday 29 June until Friday 3 July 2015 at the Campus of the National Center for Scientific Research "Demokritos". The Forum will cover a broad range of topics including ICT, Nanotechnology, Energy & Environment, Life Sciences and Accelerator Technologies for Society. Under the Auspices of the Hellenic Ministry of Foreign Affairs, this poly-thematic conference aims to act as a meeting point for Science, Technology and Innovation attracting scientists of the Greek Diaspora and world class experts who will discuss global scientific developments.

Tracks

Figure 3-2 Main page for the 3rd Hellenic Forum.

3.4 RESCHEDULING OF THE THIRD CYBERROAD WORKSHOP

The third CyberROAD workshop will be held in Vienna on February 2016 (M21), hosted by SBA, preceeding the CyberROAD Final Event (on M24). The reason for this rescheduling is the delayed June 2014 start date of the project, in consequence of which was not possible anymore to have two workshops co-located with the ARES conference, which usually takes place in August. Therefore, it was necessary to create a contingency plan wherein the second ARES-collocated Workshop would be replaced by a proposed workshop in Vienna (hosted by SBA) and the Hellenic Forum 2015 (hosted by NCSRD). The Darmstadt workshop, originally planned within the second year of the project, was moved forward to M12 in order to still have a planned workshop within the first year of activities, in accordance with the plan in the description of work. The associated reports have also been rescheduled according to the contingency plan. The report for the Vienna Workshop will be delivered in M22 (March 2016), one month after the conclusion of the workshop activities.

4 ACADEMIC DISSEMINATION OF RESULTS

Academic Dissemination refers to the publication of research results in peer-reviewed scholarly journals or the presentation of results within events such as scientific Conferences, Workshops etc. Deliberable D7.1 ("Dissemination Plan and Calendar of Activities") provides guidelines for the selection of high-impact journals and events. This subsection lists activities related to scientific dissemination within the first year of the project.

4.1 *SCIENTIFIC DISSEMINATION EVENTS*

CYBERDEFCON presented a talk on "Cyber Crime Metrics and Threat Data", during **SECURE 2014, in Warsaw, Poland**. SECURE[9] is a conference *"dedicated entirely to IT security and addressed to administrators, security team members and practitioners in this field. It is recognized as the meeting place for experts involved in the field of network and computer systems security. […] Conference presents state-of-the-art solutions, analysis of the current threats, latest trends in ICT security as well as important legal issues. Participants have an unique opportunity to gain the latest knowledge, improve their qualifications and exchange experience with experts."*

This work acknowledged the CyberROAD project and is particularly relevant to CyberROAD WP3 and WP5 activities. The relevant presentation is available in the project website.

NCSRD delivered a presentation on performance analysis of Location-Based Services that acknowledged the CyberROAD project on **the SPIE Defense, Security and Sensing Conference, which took place in Baltimore, Maryland (US) on April 20th-24th 2015.** SPIE is: *"an international non-profit society that advances emerging technologies through interdisciplinary information exchange, continuing education, publications, patent precedent, and career and professional growth".*

This work acknowledged the CyberROAD project and is particularly relevant to CyberROAD WP4 activities. The relevant presentation is available in the project website.

4.2 *SCIENTIFIC PUBLICATIONS*

CyberROAD was acknowledged in the following scientific article(s):

- Segou, O.E., Thomopoulos S.C.A., (2015). "The Locus Analytical Framework for indoor localization and tracking applications", in Proceedings of the 2015 SPIE Defense, Security and Sensing Conference, Baltimore, Maryland, US.

[9] SECURE 2014: http://www.secure.edu.pl/en/ (Accessed May 2015)

5 OTHER RELEVANT DISSEMINATION ACTIVITIES

This section covers all other events and dissemination activities, such as exhibitions, educational activities etc. with respect to the T7.5 activities for public awareness and the academic exploitation of CyberROAD results.

5.1 *OTHER RELATED EVENTS AND ACTIVITIES*

UNICA presented CyberROAD's goals during a lecture in the International Summer School "Building Trust in the Information Age"[10] 2014, in Cagliari, Italy. The Summer School focuses on "providing a quite accurate overview of the current scenario, and draw future directions for research activities and good practices". The four main themes include: (i) Targeted Attacks Analysis, Threat modeling and Investigation, (ii) Automated detection and characterization of Vulnerable code, Malware, Botnets, (iii) Usable Security, (iv) Privacy in the Era of Internet-based Intelligence.

UNICA presented CyberROAD during the 2014 **European Researchers' Night**, in Nuoro, Sardinia, on September 26, 2014. The European Researchers' Night is a pan-European event that focuses on "Bringing the researchers closer to the general public and increasing awareness of the research and innovation activities with a view to supporting the public recognition of researchers, creating an understanding of the impact of researchers' work on daily life and encouraging young people to embark on scientific careers".

UNICA presented CyberROAD during the "**Verso l'ultima frontiera della Sicurezza Cibernetica**" event that took place in October 9, 2014 in Cagliari, Italy. PRA Lab organized this event within the European Cyber Securoty Month[11] advocacy campaign. ECSM aims to "*promote cyber security among citizens, to change their perception of cyber-threats and provide up to date security information, through education and sharing good practices*". UNICA presented the goals of the project, which was also featured in a poster session.

NASK presented CyberROAD in the **2015 FIRST TC/TF-CIRT Technical Colloquium,** in Las Palmas (Gran Canaria), on January 26th -28th 2015. This event was organized by FIRST, an *"international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs"*. NASK presented the project's goals and general approach within the event. The presentation is available in the CyberROAD website.

[10] International Summer School BTIA 2014: https://comsec.diee.unica.it/summer-school/ (Accessed May 2015)

[11] European Cyber Security Month: https://cybersecuritymonth.eu (Accessed May 2015)

NCSRD presented the project **in the 2015 EXPOSEC Defense World conference, which tool place in Athens, Greece on May 5th-6th 2015.** During the conference, representatives from NCSRD along with delegates from ENISA and major industries took part in a panel discussion on Cyber Security Research including aspects of Privacy and Ethics.

Polícia Judiciária (PJ) presented the project **in the eSPap, on May 5th, 2015.** The eSPap is a leading public corporation, which manages information and services for the Portuguese government. The presentation concerned "Financing innovation at Public Administration" and included a description of the project and its goals.

SBA Research (SBA) presented the project in the poster session at the **annual IMPACT on May 28th at the Austrian Computer Society**. IMPACT is an annual event organized by SBA and presents cutting edge research by local researchers, as well as international highly regarded research units, e.g. (for 2015) Google Switzerland and Gartner. A draft project poster for IMPACT 2015, is available in Appendix B.

UNICA presented the project roadmapping **methodology in the APWG eCrime (Symposium on Electronic Crime Research), on May 28th, 2015, in Barcelona, Spain**. APWG is the "worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors". The talk focused on the scenario analysis and research roadmapping, with the corresponding title: "Anticipate Your Cyber Enemy: From Scenario Analysis to Research Roadmaps for Cybercrime and Cyberterrorism". A presentation was also made in the **2014 eCrime Sync-Up, which took place in NATO school in Oberammergau, Germany on April 1-3, 2014** and is available at the project website**.**

UNICA presented the project at European Electronic Crime Task Force's **Plenary Meeting** (Poste Italiane's headquarters in Rome, Italy. 31 March, 2015), giving the talk "**Hitting the CyberROAD, what to expect in cyber crime by 2020**". The European Electronic Crime Task Force (EECTF) is an information sharing initiative, started in 2009 by an agreement between United States Secret Service, Italian Ministry of Internal Affairs and Poste Italiane, whose mission is to support the analysis and the development of best practices against cybercrime in European countries, through the creation of a strategic alliance between public and private sectors, including Law Enforcement, financial sector, academia, international institutions and ICT security vendors.

5.2 *PRODUCTION OF DISSEMINATION MATERIAL*

NCSRD took up the production of dissemination material in printed and multimedia form. Printed material was available to all consortium members to use for all intents and purposes. Printed material includes (as seen in Appendix B):

- A general broject brochure (A4) available in three colour editions
- A project flyer (folded, A4)

The dissemination material is currently available in English. With the help of CyberROAD partners, promotional material is being translated in multiple languages. CyberROAD material is also currently available on the CyberROAD site.

Additional material covering CyberROAD results and methodologies will be produced within the project's second year, based on public information and results from all CyberROAD Work Packages. This work will be undertaken after the results have been officially reported to the European Commision, at end of the first reporting period.

6 EXPLOITATION & LIAISON ACTIVITIES

This section lists exploitation and liaison activities that were undertaken by the consortium members, aiming to properly utilize CyberROAD results to support their interests in their educational, commercial or research capacities. It also includes liaison activities with othe EC-funded consortia.

6.1 LIAISON AND NETWORKING

CyberROAD dedicates a specific task (T7.2 "Liaison Database") to creating and maintaining channels of communication with researchers, academics, public stakeholders, policy makers, special interest groups etc. and performing targeted dissemination and exploitation activities. Liaison activities that were carried out within the project's first year include interfacing with NATO and the European Defense Agency, as well as maintaining communication with other EU-funded projects.

6.1.1 PARTICIPATION OF HMOD AND NCSRD TO THE MAIN OBSERVATORY OF THE NATO CYBER COALITION 2014 EXERCISE

NATO's largest annual cyber defense exercise, Cyber Coalition Exercise 2014 (CC14) began on 18 November and run until 21 November, with the participation of 26 NATO Nations, as well as five Partner Nations. While this is a cyber defense exercise, the exercise objectives go far beyond items such as malware analysis and other strictly technical challenges to large-scale operational objectives such as ensuring that NATO has the ability to ensure the uninterrupted flow of information in a contested cyber environment. This exercise challenges nations to use collaborative tools to share information in order to overcome technical challenges as rapidly as possible. Exercise objectives for this exercise are to advise decision-making, exercise coordination between NATO bodies and national cyber defense capabilities, including partner nations, information sharing and challenging collective technical capabilities.

A representative from NCSRD participated in Cyber Coalition Exercise as an Industry/Academia Observer in the exercise's main site in Tartu (Estonia) and discussed the project activities with the organizing committee. As a result, representatives of the organizing committee have been invited to attend the 3rd Hellenic Forum and present findings in the "Digital Security, Privacy and Trust" session.

6.1.2 LIAISON AND COOPERATION WITH THE EUROPEAN DEFENSE AGENCY

The Hellenic Ministry of Defense (HMOD) participates in EDA Project Team (PT) for Cyber Defence, which coordinates the cyber security activities across European Union, focused on national defence and on support of EU operations. A national subject matter expert on cyber defence represents each EU Member State. National representatives meet three times a year in order to discuss, analyse, approve and desigh common EU cyber defence activities and related projects. HMOD representative during the 2nd EDA PT meeting presented an overview of the CyberROAD project, which was welcomed by the community as a positive effort towards the collaboration between Defence authorities and the academic and private sectors.

In addition, due to the fact that EDA Research & Technology branch developes its own research agenda, it was agreed that CyberROAD outcomes will be taken into account and affect the decisions on cyber security areas where common efforts between EDA and the project are identified. To that extent, EDA's Project Manager for Cyber Defence, Mr. Wolfgang Roehrig, requested to join the project's External Advisory Board and is thus now officialy affiliated with the project.

6.1.3 LIAISON WITH OTHER CONSORTIA

Communication activities were also undertaken by the consortium members to ensure the liaison with other EC-funded consortia, such as CAMINO, COURAGE and ACDC:

- The CAMINO, COURAGE and ACDC sister projects are acknowledged in the CyberROAD website[12] and Social Networking accounts.
- UNICA, as the project coordinator, participated in multiple joint events (such as the CAMINO workshop in Bern, Switzerland, on September 18th, 2014 as well as the CAMINO/COURAGE joint event on 8th-9th April 2015)
- HMOD, with its subject matter expert, presented the CyberROAD project during the 2nd CAMINO workshop (March 3rd 2015), where most important points regarding the consortium approach to the research agenda were analysed and discussed by the delegates.
- RHUL and CYBERDEFCON will be participating in the EU Cyber Crime Workshop hosted by RHUL and CAMINO in London, June 2015 and will present work performed within CyberROAD WP3 ("Social, Ethical, Political and Legal Scenario") and WP5 ("Cyber Crime"), related to the ethical, social, legal aspects of cyber crime and cyber crime metrics.
- COURAGE and CAMINO were invited to attend the 3rd Hellenic Forum for Science, Technology and Innovation.

[12] Twin projects page on CyberROAD website (Accessed May 2015): http://www.cyberroad-project.eu/en/twin-projects/

7 Updated Work Plan and Calendar of WP7 Activities

This section details the WP7 actions performed within year one of the project and provides an update of anticipated WP7 activities for the second year of the project. Activities listed in Table 7-1 are coded as follows:

- [M], marks Project Milestones,
- [D], marks Delivery dates for WP7 documents etc.,
- [A], marks partner activities,
- [O], marks various other dates of interest.

The Calendar of WP7 activities was updated according to the workshop rescheduling contingency plan presented within Section 3.

Table 7-1 Calendar of WP7 Activities.

Type	Date	Activity	Partners involved	Status
[M]	June 1, 2014 (M1)	Project Kick-Off	All	COMPLETED
[A]	June 24-25, 2014 (M1)	WP Kick-Off meeting	All	COMPLETED
[A]	July 4, 2014 (M2)	Online Dissemination/Exploitation Form	UNICA, NCSRD	COMPLETED
[A]	July 11, 2014 (M2)	Deadline for filling of form details	All	COMPLETED
[D]	July 31st, 2014 (M2)	Expected delivery of D7.1 Dissemination plan and Calendar of Activities	NCSRD, UNICA	COMPLETED
[D]	August 29th, 2014 (M3)	Expected delivery of project Social Networking accounts, Website and Web tools.	FORTH, NCSRD	COMPLETED
[A]	September 1-5, 2014 (M4)	Update for Workshop planning: Start of planning activities, final choice of first scientific Workshop title and venue, start of discussion on the planning activities for the second scientific CyberROAD Workshop, and TUD first CyberROAD Workshop	UNICA, NCSRD, SBA, TUD	COMPLETED
[O]	September 18th, 2014 (M4)	Participation in CAMINO workshop in Bern, Switzerland	Selected delegates.	COMPLETED
[A]	October 13-17, 2014 (M5)	Update for Workshop planning: First Draft of the Call for Papers, identification of Areas of Interest, possible organization of a Panel Discussion, discussion on Liaison activities with other consortia active in Cyber Crime and Cyber Terrorism Research (e.g. CAMINO, COURAGE, CIPHER etc.) and on the presentation of CyberROAD results in the ARES-collocated Workshop.	UNICA, NCSRD, SBA, TUD	COMPLETED

Type	Date	Activity	Partners involved	Status
[A]	December 1-5, 2014 (M7)	Update for Workshop planning: Status of Programme Committee synthesis, start of search for Reviewers, decision on venue/possible dates for the second scientific Workshop.	UNICA, NCSRD, SBA, TUD	COMPLETED
[A]	January 5-9, 2015 (M8)	Update for Workshop planning: Call for papers released and disseminated	UNICA, NCSRD, SBA, TUD	COMPLETED
	3rd March 2015	Participation in CAMINO Workshop	HMOD	COMPLETED
[A]	April 1st, 2015 (M11)	Update for Workshop planning: Status of Reviewer team	UNICA, NCSRD, SBA, TUD	COMPLETED
[O]	8th -9th April 2015 (M10)	Joint CAMINO/COURAGE workshop.	UNICA	COMPLETED
[A]	May 20th-21st 2015 (M12)	TUD Workshop in Darmstadt, Germany	TUD	COMPLETED
[D]	May 31st,, 2015 (M12)	Expected delivery of D7.2 (Preliminary Dissemination and Exploitation Report)	NCSRD, UNICA, HMOD, FORTH, SBA, TUD.	COMPLETED
[M]	May 31st , 2105 (M12)	Conclusion of first year of CyberROAD activities and WP7 periodic reporting	NCSRD, UNICA, all	COMPLETED
[A]	June 1st, 2015 (M13)	Start of Task 7.5 (Generalized Awareness and Training Campaign)	UNICA, NCSRD, all	COMPLETED
[O]	June 15th -16th, 2015 (M13)	Liaison activitiy with CAMINO, at the third CAMINO workshop, in London, UK	RHUL,Cyber Defcon	PENDING
[O]	June 29th-July 3rd 2015, M13-M14	3rd Hellenic Forum for Science, Technology and Innovation, Session on "Digital Security, Privacy and Trust"	NCSRD, possible delegates from CAMINO & COURAGE	PENDING
[D]	July 31st, 2015 (M14)	Delivery of the TUD & Hellenic Forum workshop report (D7.7)	TUD	PENDING
[A]	August 24th-28th,2015 (M15)	FCCT 2015 Workshop (collocated with the ARES 2015 Conference)	SBA, all	PENDING
[D]	September 30th, 2015 (M16)	Delivery of FCCT 2015 Workshop report (First ARES workshop report, D7.6)	SBA, all	PENDING
[A]	TBD, February 2016 (M21)	Second SBA Workshop	SBA, all	PENDING
[D]	TBD, March 2016 (M22)	Delivery of second SBA Workshop report (D7.8)	SBA, all	PENDING

Type	Date	Activity	Partners involved	Status
[A]	TDB, May 2016, (M24)	Final Event	UNICA, all	PENDING
[M]	May 31st, 2016 (M24)	Conclusion of project activities	All	PENDING
[D]	May 31st, 2016 (M24)	Delivery of all remaining WP7 documents and type "Other" deliverables: Delivery of D7.3 (Final Dissemination and Exploitation Report), D7.4 (Liaison Database), D7.10 (Generalized Awareness and Training Campaign), D7.11 (Final Event Report), Year 2 periodic reporting	All	PENDING

8 LIST OF FIGURES

9 LIST OF TABLES

APPENDIX A: FCCT 2015 CALL FOR PAPERS

ARES Conference
The International Dependability Conference

Call for Papers

The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism (FCCT 2015)

To be held in conjunction with the ARES EU Projects Symposium 2015, held at the 10th International Conference on Availability, Reliability and Security (ARES 2015 – http://www.ares-conference.eu) and organized by the FP7 project CyberRoad (http://www.cyberroad-project.eu/),

August 24th – 28th 2015
Université Paul Sabatier
Toulouse, France

With the constant rise of bandwidth available and with more and more services shifting into the connected world, criminals as well as political organizations are increasingly active in the virtual world. While Spam and Phishing, as well as Botnets are of concern on the cybercrime side, recruiting, as well as destructive attacks against critical infrastructures are becoming an increasing threat to our modern societies. Although reactive strategies are useful to mitigate the intensity of cyber-criminal activities, the benefits of proactive strategies aimed to anticipate emerging threats, future crimes, and to devise the corresponding countermeasures are evident.

The aim of **the First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism** is to anticipate the future of cyber-criminal activities, enabling governments, businesses and citizens to prepare themselves for the risks and challenges of the coming years. The first step towards the creation of a strategic *roadmap* for future research on cybercrime and cyberterrorism is the building of *scenarios* on the future transformations of the society, business activities, production of goods, commodities, etc. The aim of FCCT 2015 is to create a forum on *scenario building* and creation of *research roadmaps* for cybercrime and cyberterrorism. The building of future scenarios should allow the identification of the main driving forces and factors that will shape the evolution of cybercrime and cyberterrorism. A principled analysis of the differences between the current state of play and the future scenarios should allow drawing roadmaps and priorities of future research on cybercrime and cyberterrorism.

FCCT 2015 is an international forum for researchers and practitioners from Academia, Industry, Government and Non Governmental Organizations, involved in the investigation of future trends of cybercrime and cyberterrorism.

Contributions are solicited on the building and exploration of future scenarios for cybercrime and cyberterrorism on a realistic time span. Explored scenarios should point out the driving forces and key factors of cybercrime and cyberterrorism, and assess the impact of hypothesised criminal activities. As an example, the following issues should be addressed for the scenario building and the creation of research roadmaps:

Issues related to the Technology & Technology-enabled Services

- Which kind of **technology** will be used in 2020? (Internet of Things, Wearable Sensors, Driverless vehicles, Augmented reality, Remote presence, etc.)
- Which kind of **services** will be used in 2020? How will the current services evolve over the next years? (e.g., Communication service providers, Content service providers, Cloud service providers, Reputation and cyber risk management/insurances).

Issues related to the contextual environment

- How will **citizens** and **social relations** evolve in the foreseen technological scenario? (e.g., roles of individuals and communities, internet governance, identity management)
- How will **the government and political bodies** react on the new challenges posed by new technologies and the related societal transformations? Which **legal** and **law enforcement** transformation can be foreseen?
- How will the **economy** be affected by the technological and societal transformations? (e.g., ubiquitous workforces, use of virtual currencies, personal data selling business models)

SUBMISSIONS AND REGISTRATION

Authors are invited to submit Regular Papers (maximum 8 pages) via ConfDriver, all papers will be reviewed double-blinded by at least three independent reviewers. Papers accepted by the workshop will be published in the Conference Proceedings published by IEEE Computer Society Press. Failure to adhere to the page limit and formatting requirements will be grounds for rejection.

The submission guidelines valid for the FCCT workshop are the same as for the ARES conference. They can be found >>here<<.

Submission of a paper implies that should the paper be accepted, at least one of the authors will register and present the paper in the conference.

A selection of the accepted papers may be invited for publication as an extended version in an edited book.

IMPORTANT DATES

April 10, 2015: Regular Paper Submission
May 10, 2015: Notification Date
June 8, 2015: Camera-Ready Paper Deadline

ORGANIZING COMMITTEE

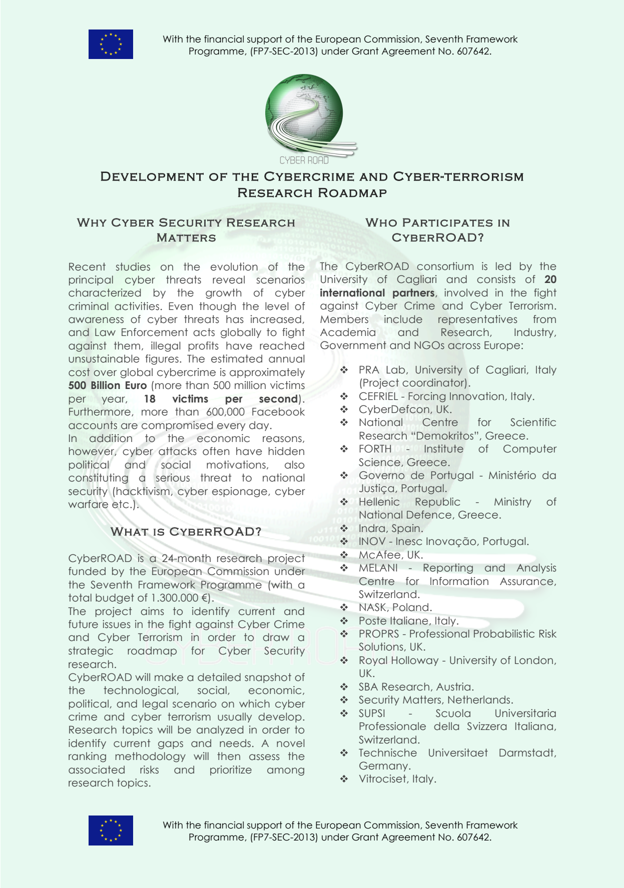
Angelo Consoli (SUPSI)
Giorgio Giacinto (University of Cagliari)
Peter Kieseberg (SBA Research)

ARES Conference
The International Dependability Conference

PROGRAM COMMITTEE
Davide Ariu (University of Cagliari)
Jart Armin (CyberDefcon)
Elias Athanasopoulos (FORTH)
Lorenzo Cavallaro (RHUL)
Luca Didaci (University of Cagliari)
Marina S. Egea (INDRA)
Vivi Fragopoulou (FORTH)
Enrico Frumento (CEFRIEL)
Giorgio Fumera (University of Cagliari)
Jorge L. Hernandez-Ardieta (INDRA)
Evangelos P. Markatos (FORTH)
Javier Martínez-Torres (INDRA)
Manel Medina (UPC)
Fabio Roli (University of Cagliari)
Olga Segou (NCSR Demokritos)
Foy Shiver (APWG)
Erik Tews (TU Darmstadt)
Stelios Thomopoulos (NCSR Demokritos)

CONTACTS
Peter Kieseberg (SBA Research) pkieseberg@sba-research.org

A4 BROCHURE DESIGN (COLOUR)



With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

WHY CYBER SECURITY RESEARCH MATTERS

Recent studies on the evolution of the principal cyber threats reveal scenarios characterized by the growth of cyber criminal activities. Even though the level of awareness of cyber threats has increased, and Law Enforcement acts globally to fight against them, illegal profits have reached unsustainable figures. The estimated annual cost over global cybercrime is approximately **500 Billion Euro** (more than 500 million victims per year, **18 victims per second**). Furthermore, more than 600,000 Facebook accounts are compromised every day.

In addition to the economic reasons, however, cyber attacks often have hidden political and social motivations, also constituting a serious threat to national security (hacktivism, cyber espionage, cyber warfare etc.).

WHAT IS CYBERROAD?

CyberROAD is a 24-month research project funded by the European Commission under the Seventh Framework Programme (with a total budget of 1.300.000 €).

The project aims to identify current and future issues in the fight against Cyber Crime and Cyber Terrorism in order to draw a strategic roadmap for Cyber Security research.

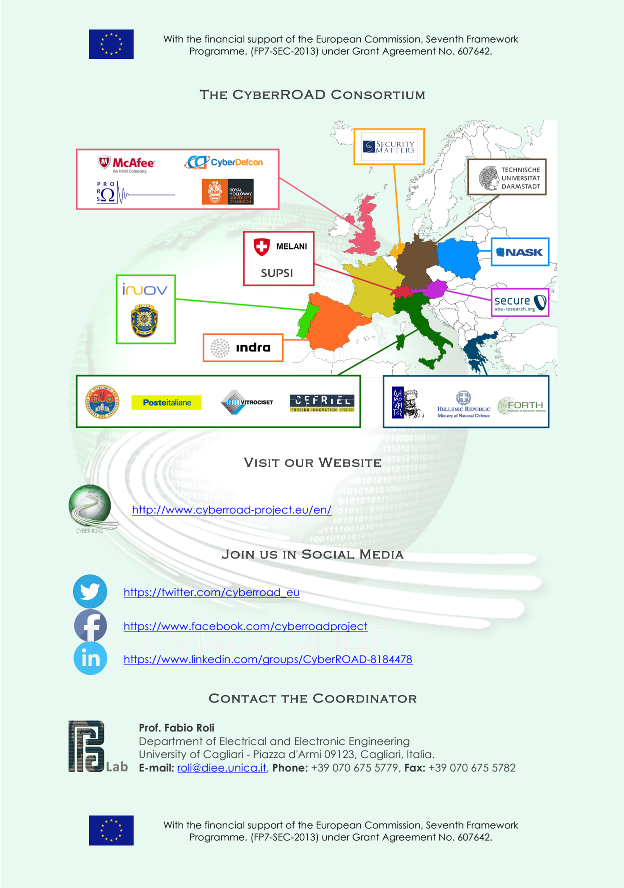
CyberROAD will make a detailed snapshot of the technological, social, economic, political, and legal scenario on which cyber crime and cyber terrorism usually develop. Research topics will be analyzed in order to identify current gaps and needs. A novel ranking methodology will then assess the associated risks and prioritize among research topics.

WHO PARTICIPATES IN CYBERROAD?

The CyberROAD consortium is led by the University of Cagliari and consists of **20 international partners**, involved in the fight against Cyber Crime and Cyber Terrorism. Members include representatives from Academia and Research, Industry, Government and NGOs across Europe:

❖ PRA Lab, University of Cagliari, Italy (Project coordinator).
❖ CEFRIEL - Forcing Innovation, Italy.
❖ CyberDefcon, UK.
❖ National Centre for Scientific Research "Demokritos", Greece.
❖ FORTH - Institute of Computer Science, Greece.
❖ Governo de Portugal - Ministério da Justiça, Portugal.
❖ Hellenic Republic - Ministry of National Defence, Greece.
❖ Indra, Spain.
❖ INOV - Inesc Inovação, Portugal.
❖ McAfee, UK.
❖ MELANI - Reporting and Analysis Centre for Information Assurance, Switzerland.
❖ NASK, Poland.
❖ Poste Italiane, Italy.
❖ PROPRS - Professional Probabilistic Risk Solutions, UK.
❖ Royal Holloway - University of London, UK.
❖ SBA Research, Austria.
❖ Security Matters, Netherlands.
❖ SUPSI - Scuola Universitaria Professionale della Svizzera Italiana, Switzerland.
❖ Technische Universitaet Darmstadt, Germany.
❖ Vitrociset, Italy.

With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.



With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

THE CYBERROAD CONSORTIUM

McAfee
CyberDefcon
SECURITY MATTERS
TECHNISCHE UNIVERSITÄT DARMSTADT
MELANI
SUPSI
NASK
inov
secure
indra
Posteitaliane
VITROCISET
CEFRIEL FORGING INNOVATION
HELLENIC REPUBLIC Ministry of National Defence
FORTH

VISIT OUR WEBSITE

http://www.cyberroad-project.eu/en/

JOIN US IN SOCIAL MEDIA

https://twitter.com/cyberroad_eu

https://www.facebook.com/cyberroadproject

https://www.linkedin.com/groups/CyberROAD-8184478

CONTACT THE COORDINATOR

Prof. Fabio Roli
Department of Electrical and Electronic Engineering
University of Cagliari - Piazza d'Armi 09123, Cagliari, Italia.
E-mail: roli@diee.unica.it, **Phone:** +39 070 675 5779, **Fax:** +39 070 675 5782

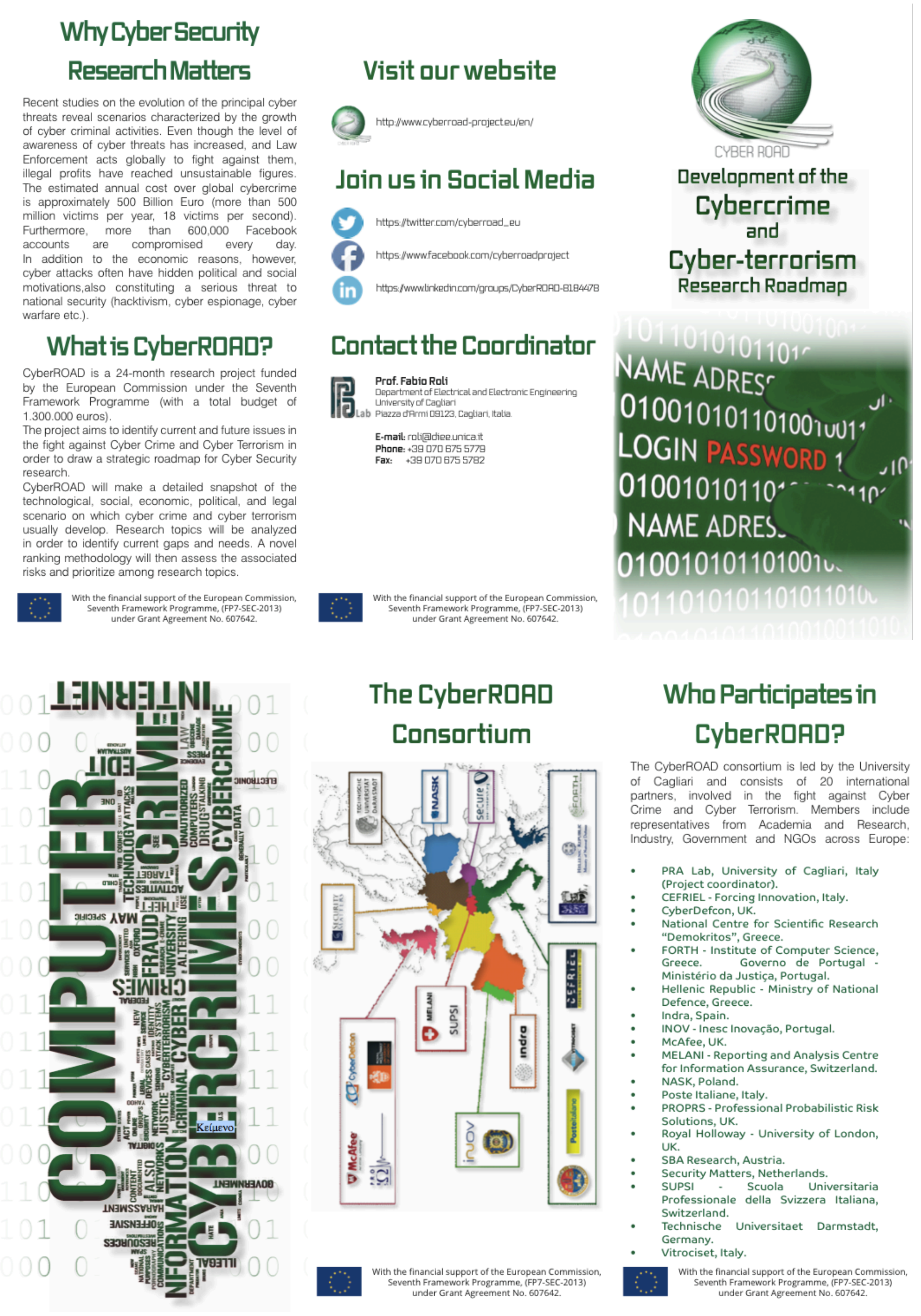
With the financial support of the European Commission, Seventh Framework Programme, (FP7-SEC-2013) under Grant Agreement No. 607642.

Front Page **Back Page**

Brochure is available in the project website in grey, green, white editions and in multiple languages.

FIRST A4 FLYER DESIGN

Additional flyers presenting specific results will be designed throughout the project’s second year.



Why Cyber Security Research Matters

Recent studies on the evolution of the principal cyber threats reveal scenarios characterized by the growth of cyber criminal activities. Even though the level of awareness of cyber threats has increased, and Law Enforcement acts globally to fight against them, illegal profits have reached unsustainable figures. The estimated annual cost over global cybercrime is approximately 500 Billion Euro (more than 500 million victims per year, 18 victims per second). Furthermore, more than 600,000 Facebook accounts are compromised every day. In addition to the economic reasons, however, cyber attacks often have hidden political and social motivations,also constituting a serious threat to national security (hacktivism, cyber espionage, cyber warfare etc.).

What is CyberROAD?

CyberROAD is a 24-month research project funded by the European Commission under the Seventh Framework Programme (with a total budget of 1.300.000 euros).

The project aims to identify current and future issues in the fight against Cyber Crime and Cyber Terrorism in order to draw a strategic roadmap for Cyber Security research.

CyberROAD will make a detailed snapshot of the technological, social, economic, political, and legal scenario on which cyber crime and cyber terrorism usually develop. Research topics will be analyzed in order to identify current gaps and needs. A novel ranking methodology will then assess the associated risks and prioritize among research topics.

With the financial support of the European Commission,
Seventh Framework Programme, (FP7-SEC-2013)
under Grant Agreement No. 607642.

Visit our website

http://www.cyberroad-project.eu/en/

Join us in Social Media

https://twitter.com/cyberroad_eu

https://www.facebook.com/cyberroadproject

https://www.linkedin.com/groups/CyberROAD-8184478

Contact the Coordinator

Prof. Fabio Roli
Department of Electrical and Electronic Engineering
University of Cagliari
Piazza d'Armi 09123, Cagliari, Italia.

E-mail: roli@diee.unica.it
Phone: +39 070 675 5779
Fax: +39 070 675 5782

With the financial support of the European Commission,
Seventh Framework Programme, (FP7-SEC-2013)
under Grant Agreement No. 607642.

CYBER ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

The CyberROAD Consortium

Who Participates in CyberROAD?

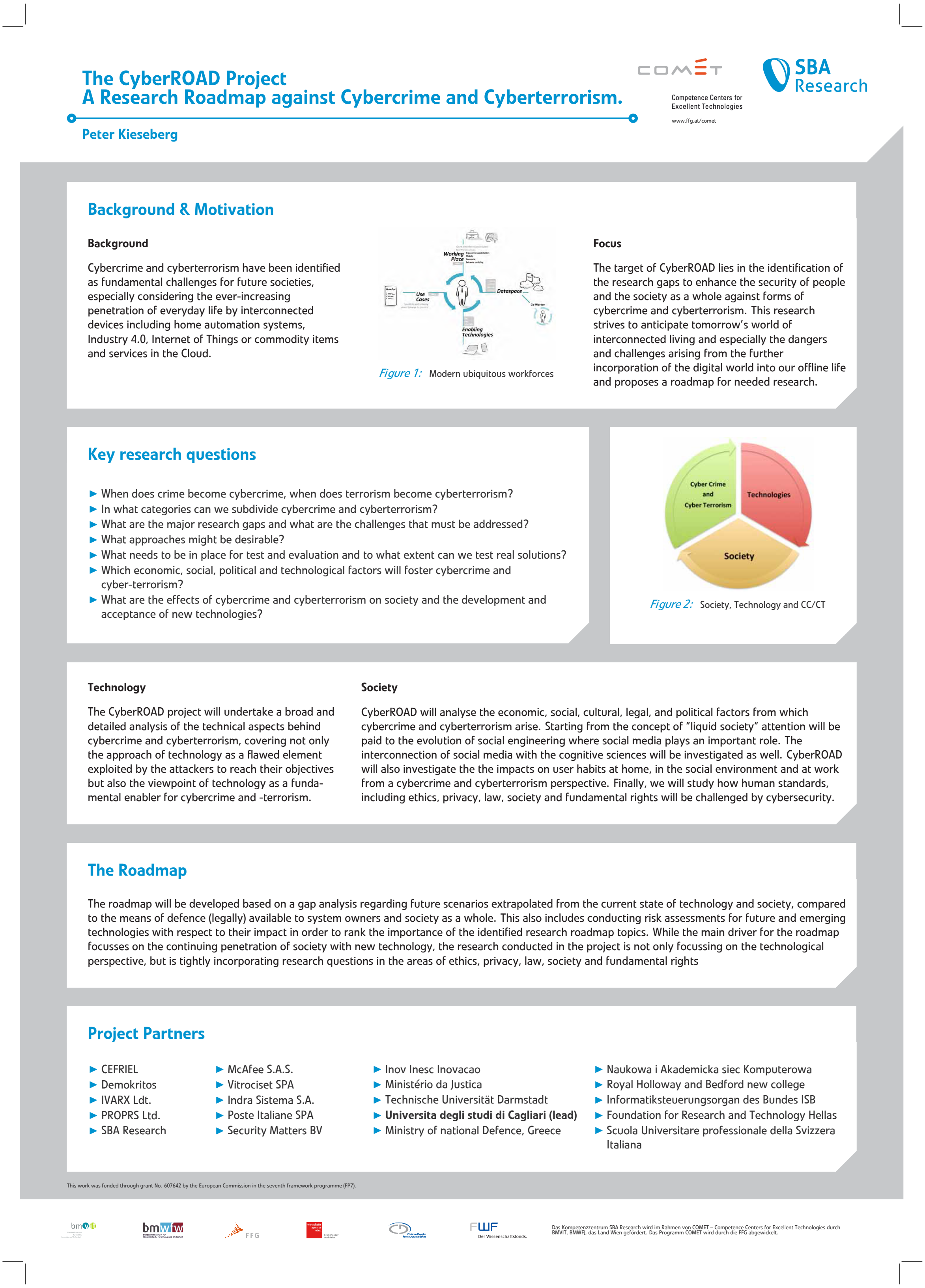
The CyberROAD consortium is led by the University of Cagliari and consists of 20 international partners, involved in the fight against Cyber Crime and Cyber Terrorism. Members include representatives from Academia and Research, Industry, Government and NGOs across Europe:

- PRA Lab, University of Cagliari, Italy (Project coordinator).
- CEFRIEL - Forcing Innovation, Italy.
- CyberDefcon, UK.
- National Centre for Scientific Research “Demokritos”, Greece.
- FORTH - Institute of Computer Science, Greece. Governo de Portugal - Ministério da Justiça, Portugal.
- Hellenic Republic - Ministry of National Defence, Greece.
- Indra, Spain.
- INOV - Inesc Inovação, Portugal.
- McAfee, UK.
- MELANI - Reporting and Analysis Centre for Information Assurance, Switzerland.
- NASK, Poland.
- Poste Italiane, Italy.
- PROPRS - Professional Probabilistic Risk Solutions, UK.
- Royal Holloway - University of London, UK.
- SBA Research, Austria.
- Security Matters, Netherlands.
- SUPSI - Scuola Universitaria Professionale della Svizzera Italiana, Switzerland.
- Technische Universitaet Darmstadt, Germany.
- Vitrociset, Italy.

With the financial support of the European Commission,
Seventh Framework Programme, (FP7-SEC-2013)
under Grant Agreement No. 607642.

With the financial support of the European Commission,
Seventh Framework Programme, (FP7-SEC-2013)
under Grant Agreement No. 607642.

DRAFT PROJECT POSTER



The CyberROAD Project
A Research Roadmap against Cybercrime and Cyberterrorism.

Peter Kieseberg

Competence Centers for Excellent Technologies

www.ffg.at/comet

SBA Research

Background & Motivation

Background

Cybercrime and cyberterrorism have been identified as fundamental challenges for future societies, especially considering the ever-increasing penetration of everyday life by interconnected devices including home automation systems, Industry 4.0, Internet of Things or commodity items and services in the Cloud.

Figure 1: Modern ubiquitous workforces

Focus

The target of CyberROAD lies in the identification of the research gaps to enhance the security of people and the society as a whole against forms of cybercrime and cyberterrorism. This research strives to anticipate tomorrow's world of interconnected living and especially the dangers and challenges arising from the further incorporation of the digital world into our offline life and proposes a roadmap for needed research.

Key research questions

- When does crime become cybercrime, when does terrorism become cyberterrorism?
- In what categories can we subdivide cybercrime and cyberterrorism?
- What are the major research gaps and what are the challenges that must be addressed?
- What approaches might be desirable?
- What needs to be in place for test and evaluation and to what extent can we test real solutions?
- Which economic, social, political and technological factors will foster cybercrime and cyber-terrorism?
- What are the effects of cybercrime and cyberterrorism on society and the development and acceptance of new technologies?

Figure 2: Society, Technology and CC/CT

Technology

The CyberROAD project will undertake a broad and detailed analysis of the technical aspects behind cybercrime and cyberterrorism, covering not only the approach of technology as a flawed element exploited by the attackers to reach their objectives but also the viewpoint of technology as a fundamental enabler for cybercrime and -terrorism.

Society

CyberROAD will analyse the economic, social, cultural, legal, and political factors from which cybercrime and cyberterrorism arise. Starting from the concept of "liquid society" attention will be paid to the evolution of social engineering where social media plays an important role. The interconnection of social media with the cognitive sciences will be investigated as well. CyberROAD will also investigate the the impacts on user habits at home, in the social environment and at work from a cybercrime and cyberterrorism perspective. Finally, we will study how human standards, including ethics, privacy, law, society and fundamental rights will be challenged by cybersecurity.

The Roadmap

The roadmap will be developed based on a gap analysis regarding future scenarios extrapolated from the current state of technology and society, compared to the means of defence (legally) available to system owners and society as a whole. This also includes conducting risk assessments for future and emerging technologies with respect to their impact in order to rank the importance of the identified research roadmap topics. While the main driver for the roadmap focusses on the continuing penetration of society with new technology, the research conducted in the project is not only focussing on the technological perspective, but is tightly incorporating research questions in the areas of ethics, privacy, law, society and fundamental rights

Project Partners

- CEFRIEL
- Demokritos
- IVARX Ldt.
- PROPRS Ltd.
- SBA Research
- McAfee S.A.S.
- Vitrociset SPA
- Indra Sistema S.A.
- Poste Italiane SPA
- Security Matters BV
- Inov Inesc Inovacao
- Ministério da Justica
- Technische Universität Darmstadt
- **Universita degli studi di Cagliari (lead)**
- Ministry of national Defence, Greece
- Naukowa i Akademicka siec Komputerowa
- Royal Holloway and Bedford new college
- Informatiksteuerungsorgan des Bundes ISB
- Foundation for Research and Technology Hellas
- Scuola Universitare professionale della Svizzera Italiana

This work was funded through grant No. 607642 by the European Commission in the seventh framework programme (FP7).

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.