CYBER ROAD

CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D 7.1 Dissemination Plan and Calendar of Activities

Date of deliverable: 25/7/2014
Actual submission date: 31/7/2014

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	1/7/2014	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Erik Tews, Peter Kieseberg, Paraskevi Fragkopoulou
0.2	Revision	28/7/2014	Olga E. Segou, Stelios C.A. Thomopoulos, Fabio Roli, Davide Ariu, Giorgio Giacinto, Erik Tews, Peter Kieseberg, Paraskevi Fragkopoulou
0.3	Revision	29/7/2014	Olga E. Segou, Matteo Mauri, Fabio Roli
0.4	Revision	29/7/2014	Olga E. Segou
1.0	Final	31/7/2014	Olga E.Segou, Fabio Roli

D7.1
Dissemination Plan and Calendar of Activities

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 Fragkopoulou (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 (D7.1 "Dissemination Plan and Calendar of Activities") presents the preliminary planning of activities to be undertaken by the consortium towards the effective dissemination and exploitation of key CyberROAD results. This work includes the coordination of 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 a calendar listing of important dates for dissemination/exploitation activities and WP7 milestones.

Keywords: CyberROAD, Dissemination, Exploitation, Work Package 7, Calendar, Dissemination Plan, Exploitation Plan.

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

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.

During the official Kick-Off meeting, a presentation of the Dissemination and Exploitation Work Package (WP7) activities was delivered by NCSRD. The scope and goals of WP7 were identified and the main timeline of WP7 activities was discussed among the consortium members, thus providing an early overview of the adopted dissemination and exploitation strategy that is herein presented. During the Kick-Off meeting, the consortium members agreed on a reporting process for dissemination and exploitation activities. This process includes the preliminary reporting of activities in a standard input form available to partners both online and offline.

This document provides a preliminary planning of dissemination activities to be conducted during the typical duration of the project, thus setting up an appropriate dissemination and exploitation strategy. The activities completed by the consortium will be reported within the Preliminary and Final Dissemination Reports (D7.2 and D7.3 respectively), which which will be delivered in May 2015 (M12) and May 2016 (M24).

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 undertaken to ensure that CyberROAD has a continuing online presence, focusing on the construction of the project Website and Social Networking accounts, as well as the individual partner activities for awareness raising.
- **Chapter 3** provides the initial planning of the three CyberROAD workshops and Final Event.
- **Chapter 4** focuses on the scientific dissemination of CyberROAD results, via academic journals and any other means. It includes an overview of Access types and Intellectual Property management processes that typically govern the publication of research results and provides a preliminary list of journals that may be considered for the publication of CyberROAD research results.
- **Chapter 5** lists all other dissemination activities.
- **Chapter 6** focuses on providing examples of exploitation and networking activities.
- **Chapter 7** provides a calendar of WP7 activities.

This section details activities related to maintaining a continuous online presence for the project. These activities include the design, implementation and maintainance of the main project website, the set up and maintainance of the project's Social Media accounts, and the individual partner activities of dissemination to the general public. The project dedicates two tasks (T7.3 "Establishment of a digital presence" and T.7.5 "Generalized Awareness and Training Campaign") to maintaining the project's constant online presence and raising public awareness on project activities and issues of Cyber Crime and Cyber Terrorism research.

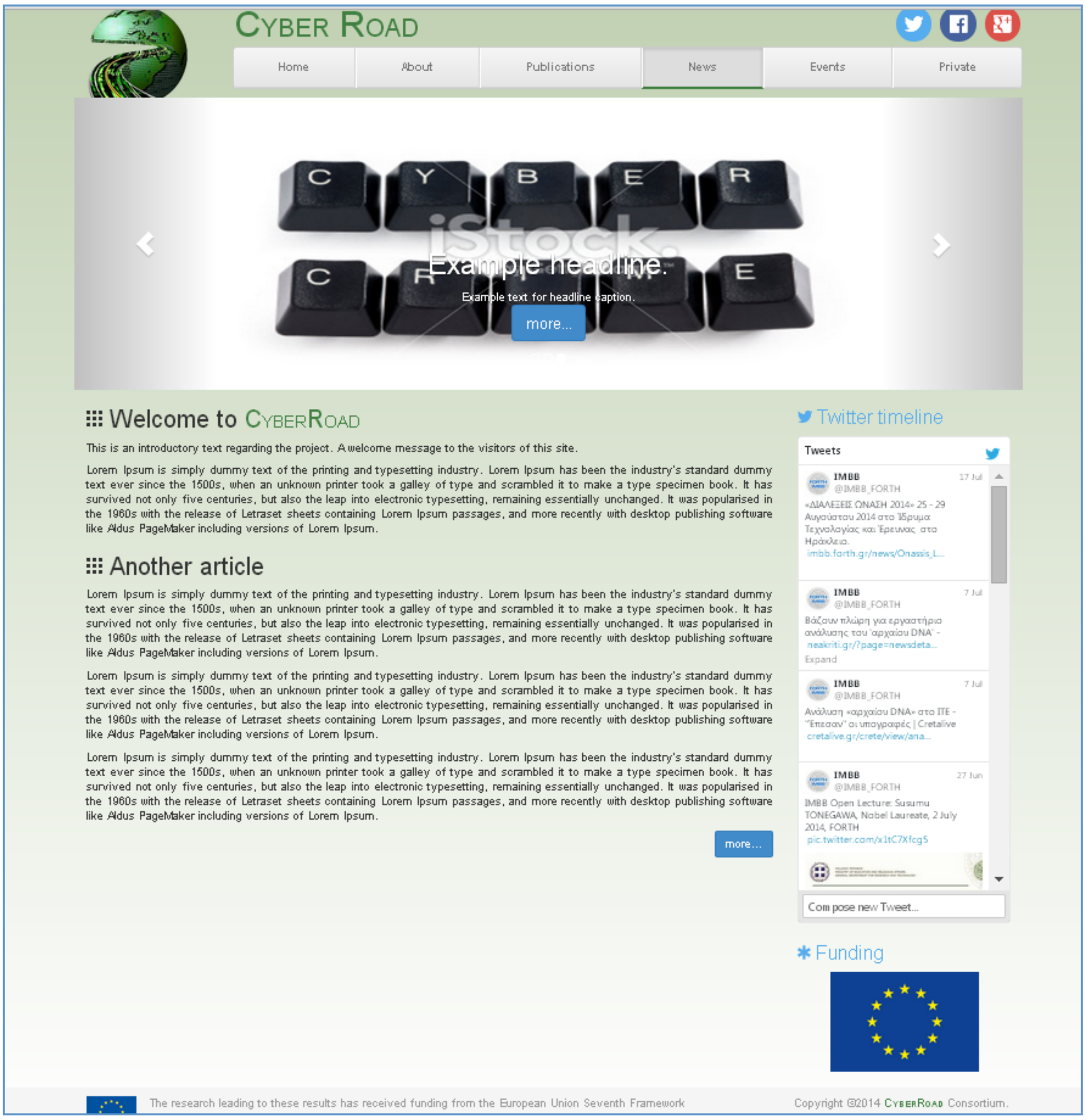
2.1 ONLINE PRESENCE

The CyberROAD main website is currently under development by FORTH. It will be delivered on August 2015 (M3) and will be maintained for at least two years after the project's end. This section describes the website design template, as well as the tools and methods used to design and implement the CyberROAD website. An overview of the hardware and network infrastructure used to run the site is also included herein. The dissemination reports (D7.2 and D7.3) will include the detailed implementation of the website and all related online communication tools, as well as their associated traffic analytics.

The domain http://cyberroad-project.eu has been reserved for the activities of the project. During the project Kick-Off meeting, on June 24-25, 2014, draft designs for the template of the website were presented by FORTH. The preliminary template that was chosen by the consortium is illustrated in Figure 2-1. The development of the template was commissioned by FORTH to an external company and was delivered on July 24, 2014. The website main contents are:

- Home: the main page of the website,
- About: relevant information on the project,
- Publications: featuring documents and publications,
- News: news of project activities etc.,
- Events: events planning, announcement and news,
- Private: this section provides restricted access to members of the consortium for various intents and purposes.

The following subsections detail the implementation of the project's website, focusing not only on the website's design but also on its flexibility and security. Other web services are currently being implemented by FORTH, such as the project's SubVersion (SVN) repository etc.



Welcome to CYBERROAD

This is an introductory text regarding the project. A welcome message to the visitors of this site.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Another article

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Twitter timeline

Tweets

IMBB @IMBB_FORTH 17 Jul
«ΔΙΑΛΕΞΕΙΣ ΩΝΑΣΗ 2014» 25 - 29 Αυγούστου 2014 στο Ίδρυμα Τεχνολογίας και Έρευνας στο Ηράκλειο.
imbb.forth.gr/news/Onassis_L...

IMBB @IMBB_FORTH 7 Jul
Βάζουν πλώρη για εργαστήρια ανάλυσης του 'αρχαίου DNA' -
neakriti.gr/?page=newsdeta...
Expand

IMBB @IMBB_FORTH 7 Jul
Ανάλυση «αρχαίου DNA» στο ΙΤΕ - "Έπεσαν" οι υπογραφές | Cretalive
cretalive.gr/crete/view/ana...

IMBB @IMBB_FORTH 27 Jun
IMBB Open Lecture: Susumu TONEGAWA, Nobel Laureate, 2 July 2014, FORTH
pic.twitter.com/x1tC7Xfcg5

Funding

The research leading to these results has received funding from the European Union Seventh Framework

Copyright ©2014 CYBERROAD Consortium.

FIGURE 2-1 The CyberROAD draft website template.

2.1.1 GRID BASED DESIGN

The CyberROAD website will feature a clean-cut visual while being easy to change in order to accommodate future needs. In order to satisfy this constraint, it will be designed and built using *Twitter Bootstrap*. Twitter Bootstrap[1] is a Cascading Style Sheets (CSS) framework that allows the rapid prototyping of *gridbased website designs* while working equally well when integrated into a production system. In grid based designs, the visual blocks that comprise the website (e.g., menus, text boxes, information boxes, ads etc) are not placed on arbitrary positions. Instead they are laid out on predefined rigid positions on a grid. This may sound restrictive but in practice the resulting design is much more efficient in communicating its contents to the visitor. This is because placing the visual blocks of the website on a grid results in *clear visual paths* and visual *structure and balance* on the design. Additionally, a grid based design also ensures consistency between the website pages and are much easier to update in order to accommodate any additional content. Currently, Bootstrap is the most popular project in GitHub. It contains a set of stylesheets that provide basic style definitions for all key HTML components, as well as plenty of well designed visual elements (buttons etc.) to use in the website. More importantly, it simplifies the positioning of new elements on the website grid.

2.1.2 BROWSER COMPATIBILITY AND WEB STANDARDS COMPLIANCE

The CyberROAD website pages have already been tested to comply with the *HTML5* standard, using the *W3C Markup Validator*. The situation is more complicated with regards to *CSS* compliance. FORTH has opted to use *CSS3* for the CyberROAD website as it greatly simplifies the implementation of aesthetic elements such as rounded element corners, element shadows etc. Without CSS3, these elements have to be rendered as bitmap images and then included in the page, which degrades the semantic integrity of the produced HTML output. The CSS3 standard, however, is currently a work in progress. So, while FORTH has taken every precaution for the CSS code, it has been proven difficult to have CSS3 code that both validates on the *W3C CSS Validator and* works on all popular browsers. Therefore, a more pragmatic approach was selected in order to have CyberROAD site pages render correctly with the latest versions of all popular web browsers.

2.1.3 WEBSITE HOSTING

The popular *LAMP software stack* will be used to serve the project's main site:

- **L**inux 2.6 as the operating system
- **A**pache 2.2 as the web server
- **M**ySQL 5.0 as the database backend
- **P**ython 2.5 for dynamically compiling the web pages

[1] Bootstrap web development tool: http://getbootstrap.com/2.3.2/ (Accessed on July 2104)

The later components of the stack have been distributed between two servers. The first server is dedicated to running the *MySQL server*, while the second runs the *Apache web server* and generates the dynamic pages using the python-based *Django* web framework. Django itself is a generic web framework that provides an *Object-Relational-Mapper* (ORM) that allows accessing objects stored in a relational database (in our case *MySQL*) as Python objects. For serving and managing our pages, the *Django-cms* Content Management System built on top of django will be used. The benefit of the Django/Django-cms combination is that they provide a clear, well-documented Application Programming Interface. They are much more compact than other solutions which makes tweaking and extending them much easier. This could prove useful in case there arises the need to extend the functionality of the CyberROAD website beyond the basics, adding flexibility to the design and implementation of the website. An additional benefit of this combination is the existing expertise of the consortium (specifically FORTH) on building and maintaining Django-cms sites. All the software components will be regularly updated in order to be immune to known (and patched) security vulnerabilities.

2.1.4 HARDWARE AND HOSTING

The CyberROAD website is hosted by FORTH on their premises in Heraklion, Crete (GR). The hosting server features two Intel Xeon dual-core CPUs running at 2.66GHz and a total memory of 4GB. It is connected to the Internet through FORTH's Gigabit connection to the GRNET backbone. The server has two high performance SAS disks (10k RPM) arranged as RAID-1 for fault-tolerance. Software and hardware firewalls protect the main server, so as to minimize the risk from cyber-threats. As an additional security measure, the database server used by the CyberROAD website will be located on a separate host with even more restricted access rules. Both hosts will be internally and externally monitored. Finally, remote backups through the *rsync* utility will be performed for both servers on a daily basis. It is also important that the hosts reside in a protected physical environment, in one of FORTH's data-centres. For ensuring optimal operating environment, the data centre is fitted with industrial-strength air conditioning with more than 240.000BTUs efficiency. In case of a power outage, a UPS power supply and an external power generator (which is engaged automatically) supports the data centre. Additionally, the date-centre features an automatic carbon dioxide fire-extinguishing system. The current planning will provide uninterrupted web hosting services and will ensure that the CyberROAD main website remains online at all times.

2.1.5 PROJECT SOCIAL NETWORKING ACCOUNTS

Social networking platforms have proven to be important tools allowing the immediate and fast access of the public to news and research results. NCSRD will create and maintain the project's social networking accounts in popular social networking platforms (such as Facebook, Twitter, Google Plus etc.), providing appropriate postings and updates according to consortium input. The Hootsuite platform will be utilized to manage the multiple accounts, while social analytics tools such as Klout, will be used to measure the impact of the project's social media presence. The results of this work will be reported within the D7.2 and D7.3 Dissemination and Exploitation reports. The social networking accounts will be delivered by the end of August 2014 (M3).

2.2 *INDIVIDUAL PARTNER ACTIVITIES*

CyberROAD partners are 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,
- Summer School and training/educational activities, etc.

Furthermore, UNICA prepared a Press Release, announcing the official start of the project. The press release is currently available in Italian and English. Both versions are included in Appendix A. Partners are encouraged to utilize the available press releases in order to announce the official start of the project. Partners are encouraged to also involve the Press and other Mass Media to publicly disseminate CyberROAD news and results. Such activities will also be fully reported within the D7.10 deliverable and summarized in the D7.2 and D7.3 reports. Currently, CyberROAD has already garnered significant attention from the Press and Mass Media. Specifically, the project's official Kick-Off has been extensively covered in Italian Press and Television (Table 2-2, Fig. 2-2).

A complete listing of partner online dissemination activities will be provided as part of a dedicated task and will be delivered within the D7.10 deliverable titled "Generalized Public Awareness and Training Campaign Report" when the project concludes. A brief summary of activities will also be presented within the D7.2 and D7.3 Dissemination and Exploitation deliverables. The appropriate forms for listing online dissemination capabilities and reporting individual partner activities for public awareness, training and education and online dissemination are included in Appendix B. The following table presents examples of such capabilities by the partners and will be maintained and updated throughout the duration of the project.

TABLE 2-1 Examples of Online Dissemination Capabilities and Activities.

Online Dissemination Channel	*Website*	**Description**	*Creation of a Project Information page*
Partner	*UNICA*	**Link**	[*http://pralab.diee.unica.it/en/CyberRoad*](http://pralab.diee.unica.it/en/CyberRoad)
Date	-		
Comments	-		
Online Dissemination Channel	*Newsletter*	**Description**	*Dissemination of the CyberROAD Press Release*
Partner	*NCSRD*	**Link**	*(Not available yet)*
Date	*July 2014*		
Comments	-		
Online Dissemination Channel	*Website*	**Description**	*Creation of a Project Information page*
Partner	*NCSRD*	**Link**	[*https://www.iit.demokritos.gr/project/cyberroad*](https://www.iit.demokritos.gr/project/cyberroad)
Date	-		
Comments			

TABLE 2-2 Press and Mass Media Activities for the Project.

Mass Media Activitiy	*Television coverage (RAI 3, Italy)*	**Description**	*Coverage of the project Kick-Off and project aims and goals, interview of project Coordinator, Prof. Fabio Roli.*
Partner	*UNICA*	**Link(s)**	[*https://www.youtube.com/watch?v=jGT2g_OFji4*](https://www.youtube.com/watch?v=jGT2g_OFji4)
Date	*24th June 2014*		
Comments	*Audio in Italian*		
Mass Media Activitiy	*Italian Press*	**Description**	*Coverage of the project Kick-Off meeting in multiple Italian newspapers*
Partner	*UNICA*	**Link(s)**	Unica News Online La Nuova Sardegna hinterlandcagliari.it

			sardegnaoggi.it laprovinciadelsulcisiglesiente.com sardanews.it castedduonline.it sardegnalive.net latestata.info
Date	*June 2014*		
Comments	-		

Mass Media Activitiy	*Newspaper*	**Description**	*Coverage of Intelligence Live event where CyberROAD Coordinator Prof. Fabio Roli delivered a speech related to CyberROAD activities*
Partner	*UNICA*	**Link(s)**	pralab.diee.unica.it unicaradio.it L'unione Sarda - Unica Press Review La Nuova Sardegna Unica News Online Unica News magazine, pdf, page 14 Unica News magazine, pdf, page 13
Date	*May 2014*		
Comments	-		

(a) (b)

FIGURE 2-2 The CyberROAD Kick-Off meeting received extensive television coverage. (a) screenshot from the TV presentation of CyberROAD, (b) Prof. Fabio Roli was interviewed on the significance of Cyber Crime and Cyber Terrorism research.

Throughout the duration of the project, three workshops are envisioned, as well as a larger scale Final Event for the project. The CyberROAD workshops aim to widely diffuse knowledge stemming from CyberROAD results, targeting the relevant stakeholders, the scientific community and the general public. The Final Event will showcase all aspects of CyberROAD research and related scientific accomplishments. This section details the planning activities that will be undertaken by the consortium members regarding the CyberROAD workshops and events organization.

3.1 FIRST CYBERROAD WORKSHOP

The first CyberROAD Workshop will take place near the end of the first year of CyberROAD activities. It will be organized and hosted by the Technical University of Darmstadt. Planning of the first Workshop has already started, with four suggested dates:

- May 5th - 8th 2015 (M12),
- June 9th - 12th 2015 (M13),
- June 15th - 19th 2015 (M13),
- June 22nd - 26th 2015 (M13).

This workshop will target a broad audience of attendees, including the scientific community, relevant stakeholders and policy makers, professionals in the areas of Cyber Security and Cyber Defense etc. It will focus on showcasing the current state of the CyberROAD project and results of the first year of activities. A dedicated workshop report will be delivered detailing the planning process and the results of this activitiy, expected one month after the Workshop takes place.

3.2 CYBERROAD WORKSHOPS WITH SCIENTIFIC FOCUS

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). The second scientific Workshop (third in total) will be held near the end of the project, preceeding the CyberROAD Final Event.

Among the possible titles are:

- the “First/Second International Workshop on Cyber Crime and Cyber Terrorism”,
- the “First/Second International Workshop on Advancements in Cyber Crime and Cyber Terrorism Research”,
- the “First/Second International Workshop on Advancements against Cyber Threats”,
- the “First/Second International Workshop on Protection against Cyber Crime and Cyber Terrorism” etc.

Planning for the first scientific CyberROAD workshop will begin on September 2014 (M4) and is scheduled as follows:

- **September 2014 (M4):**
  - 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,
- **October 2014 (M5):**
  - First Draft of the Call for Papers,
  - Identification of Areas of Interest,
  - The 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.),
  - The presentation of CyberROAD results in the Workshop,
- **December 2014 (M6):**
  - Identification of Programme Committee members,
  - Start of search for Reviewers,
  - Decision on venue/possible dates for the second scientific Workshop,
- **January 2015 (M7):**
  - Final Version of the Call for Papers,
  - Dissemination of the Call for Papers,
- **April 2015 (M11):**
  - Deadline for Submissions,
  - Reviewers fixed,
- **May 2015 (M12):**
  - Deadline for Reviews (double blinded),
  - Author Notification.

The ARES 2015 Conference is scheduled to take place in August/September 2015, along with the collocated CyberROAD workshop. Liaison activities with other consortia active in the Cyber Crime and Cyber Terrorism research area are also envisioned. Specifically, the CyberROAD consortium aims to invite delegates to submit their work and participate in relevant discussions within the first scientific Workshop. The planning for the second scientifically focused workshop is expected to begin approximately on December 2015 (M6) following the same planning activities, once the venue and conference details are finalized. Two workshop reports will be delivered, detailing the planning and results of each of these workshops.

3.3 *FINAL EVENT*

The CyberROAD final event will take place near the end of the second year of activities before the project officially concludes. It will provide a comprehensive overview of all CyberROAD research activities, results and conclusions. The final event is expected to be the focus of an extensive public relations campaign, in order to garner the attention of the public as well as the professional community, public authorities and policy makers etc.

The planning activities for the Final Event are expected to commence in November 2015 (M18) with the choice of an appropriate date and venue, the design and production of relevant dissemination material (in printed and multimedia form), the creation of personalized invitations etc. All available communication channels will be utilized to ensure the high impact of the final CyberROAD event, focusing on liaison and exploitation activities to complement the dissemination strategy and maximize the impact of the project. A dedicated report detailing the activities and results of the Final Event will be provided in the final month of the project (M24).

4 ACADEMIC DISSEMINATION OF RESULTS

Apart from the planning of the CyberROAD Workshops, the consortium members will be participating in scientific dissemination through the publication of research articles in highly regarded Journals, Conference Proceedings etc. This section will provide a list of outlets for scientific dissemination, covering:

- the listing of Conferences, Workshops etc. that members of the consortium can participate in and present results of CyberROAD research,
- the listing of academic Journals etc. for unsolicited submissions of research articles, and
- a brief introduction to types of scientific access and intellectual property rights management that govern the publication of scientific results in academic journals.

The list of scientific dissemination events, academic journal and related partner activities will be maintained and updated throughout the duration of the project. The preliminary and final dissemination reports (D7.2 and D7.3) will provide updated listings as well as a report of individual partner activities in the context of academic dissemination.

4.1 SCIENTIFIC DISSEMINATION EVENTS

This subsection lists relevant Conferences, Workshops etc. where consortium members may participate in so as to disseminate research results stemming from CyberROAD activities. This list will be maintained and updated throughout the course of the project (Table 4-1). Appropriate forms have been created for reporting events of interest and partner participation in such cases. The scientific dissemination forms are included in Appendix B.

TABLE 4-1 List of Scientific Dissemination Events.

Event	*Conference*	**Title (and acronym, if applicable)**	*ICISSP 2015 – International Conference on Information Security Systems and Privacy*
Description of Area of Focus	*Information Security and Privacy*		
Link	*http://www.icissp.org/*		
Date(s)	*9-11/2/2015*	**Location**	*Loire Valley, France*
Admission Fee (if applicable)	*N/A (registration not available yet)*	**Organized by**	*SBA, SUPELEC, University of Montreal*
Target Audience	*Scientific Community*	**Frequency**	*Annual*
Comments	***Regular Papers*** *Paper Submission: September 9, 2014* *Authors Notification: November 25, 2014* *Camera Ready and Registration: December 10, 2014* ***Position Papers*** *Paper Submission: October 28, 2014* *Authors Notification: November 28, 2014* *Camera Ready and Registration: December 10, 2014*		
Event	*Conference*	**Title (and acronym, if applicable)**	*InfoWar 2015*
Description of Area of Focus	*cyber warfare*		
Link	www.infowar.it		
Date(s)	*6/1/2015*	**Location**	*Rome, Italy*
Admission Fee (if applicable)	*5K-10K-15K for sponsorship*	**Organized by**	*MAGLAN*
Target Audience	*Scientific Community, Industry, Professionals etc.*	**Frequency**	*Annual*
Comments	-		
Event	*Conference*	**Title (and acronym, if applicable)**	XVIII Conference on Telecommunications and IT Security
Description of Area of Focus	Technical, organisational & legal aspects of implementation and integration of security solutions & new trends in attacks, threats and their mitigation		

Link	http://www.secure.edu.pl/en/		
Date(s)	22-23/10/2015	**Location**	Warsaw, Poland
Admission Fee (if applicable)	*Registration required-now open*	**Organized by**	NASK & CERT.PL
Target Audience	*Scientific Community, Industry*	**Frequency**	*Annual*
Comments	-		

Event	*Conference*	**Title (and acronym, if applicable)**	eCrime Sync-UP V
Description of Area of Focus	Mobile Security Symposium		
Link	http://ecrimeresearch.org/events/ecrsyncV/cfp		
Date(s)	6-7/11/2014	**Location**	Barcelona, Spain
Admission Fee (if applicable)	*Registration required*	**Organized by**	APWG EU - Anti Phishing Working Group: http://apwg.org/about-APWG/
Target Audience	*Scientific Community*	**Frequency**	*Annual*
Comments	Abstracts and short papers registration and submission due: July 15th, 2014. (strongly recommended, but not mandatory); Full Papers and Case Studies registration and submission due: August 31st , 2014 Giorgio Giacinto (UNICA) has already presented CyberROAD during his talk in the previous eCrime SyncUP IV (Tuesday, 1st April, 2014) which took place in Oberammergau, Germany.		

4.2 Publication of Results in Academic Journals

4.2.1 Access Type and Intellectual Property Rights

Typically, there are a number of fees and costs that are associated with the publication of a scientific article. The most usual paradigm allows for subscription-based access to scientific articles, with the cost burdening the reader or an institution that wishes to make the article available to their user base. A variety of scientific journals, however, have recently shifted to the paradigm of Open Access. Open Access can be described as the practice of providing unrestricted access to scientific publications free-of-charge for the interested reader. As such, "Open Access" is considered as a good way to maximize visibility of research results. The term "Open Access" can also be broadened to include free access to scientific data in raw or processed form. Specifically, the Budapest Declaration (2002) states the following definition of Open Access[2]:

> *"By open access to this literature, we mean its free availability on the public internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of these articles, crawl them for indexing, pass them as data to software, or use them for any other lawful purpose, without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. The only constraint on reproduction and distribution, and the only role for copyright in this domain, should be to give authors control over the integrity of their work and the right to be properly acknowledged and cited."*

Open Access (OA) is usually implemented in two ways:

- **"Green" OA:** "Green" access means that the publisher does not provide unrestricted access to a scientific publication, yet the author retains the right to self-archive the original manuscript after peer review, either in their respective institutional repository or any other online service (e.g. arXiv). In certain cases, there is a designated "embargo period" before which the author is not allowed to archive their work. In "green" access, the reader may chose the manuscript version free-of-charge or, alternatively, they will be burdened with a subscription fee for accessing the final version of the publication.
- **"Golden" OA:** "Golden" access means that the publisher will be providing full access rights to the reader without the need for a fee. The publication fee (also known as an "Article Processing Charge") is shifted to the author, or their respective institutions.

A large number of journals and publishing houses also require a transfer of Intellectual Property Rights prior to publishing a scientific article. This is considered the norm in cases of typical subscription-based journals or "green" access journals. The authors are usually required to sign an Intellectual Property Transfer Form, designating a journal or its associated publishing house as the sole holder of IPR for the publication. In "golden" OA it is not always necessary to transfer IPR to the publishing house or journal and the authors usually retain their IPR. Public Copyright licenses such as Creative Commons (CC) are often employed to protect authors' rights to their work in such cases.

Currently, most scientific journals offer some kind of Open Access option for the prospective authors. Hybrid access journals also exist, which offer the choice between either Open Access implementations or the typical subscription-based paradigm. Partners are encouraged to submit their research articles for publication, but authors should be cautioned to choose the appropriate access type, prior to submitting their work, taking into account the financial or IPR management implications. Furthermore, the CyberROAD Consortium Agreement that is in currently in effect delineates policies on IPR management of CyberROAD research results among the consortium members. Any CyberROAD consortium member should consider the Consortium Agreement stipulations prior to the submission of a scientific article for publication.

[2] Budapest Open Access Initiative: http://legacy.earlham.edu/~peters/fos/boaifaq.htm (Accessed July 2014, Last Revision: September 2012.)

4.2.2 Related Journals

This section provides a non-exhaustive list of journals, which are considered relevant to the themes of Cyber Crime and Cyber Terrorism that CyberROAD explores. This list will be maintained and updated throughout the project's lifecycle and may be considered and utilized by the partners for unsolicited article submissions. Specific submissions that are solicited by a Journal's Editorial team or Publishing House may also be considered for the publication of CyberROAD results. For each scientific journal, the following information is included:

- The title of the Journal and its associated publishing house,
- Indexing/Abstracting information, (including latest Impact Factor, if applicable),
- The frequency of publication,
- The Access Type, Cost and IPR management details,

Indexing and abstracting refer to the use of bibliographic databases, which collect article citations and provide relevant bibliographic metrics (also known as citation indices). Among the most well known citation indices, are the Science Citation Index Expanded (SCIE, maintained by Thomson-Reuters), Scopus (maintained by Elsevier), the Directory of Open Access Journals (DOAJ, maintained by the Infrastructure Services for Open Access, IS4OA), Google Scholar, CiteSeerX, etc. Bibliographic databases such as SCIE and Scopus offer impact metrics that can be used as proxy measures of a journal's "significance", although caution should be exercised, as the validity of the use of proxy measures is not always guaranteed.

The frequency of publication refers to the number of issues of a specific journal that are released within a year. This does not include Special Issues and other special publications. The following table (Table 4-2), includes examples of scholarly journals that may be considered for the publication of CyberROAD results. The appropriate forms for reporting scientific dissemination activities or for suggesting a relevant scientific dissemination outlet to the consortium members are included in Appendix B.

TABLE 4-2 List of relevant Journals and Publications for academic dissemination of CyberROAD results.

Publisher	Hindawi Publishing Corp.	**Title**	Intl. Journal of Distributed Sensor Networks (IJDSN)
Description	The International Journal of Distributed Sensor Networks focuses on applied research and applications of sensor networks.		
Link	http://www.hindawi.com/journals/ijdsn/		
Access Type	"Golden" Open Access	**IPR policy**	No IPR transfer, author retains rights, published under Creative Commons
Comments	**Article Processing Charge:** 1800$, burdens the author. Offers unrestricted access to the public. **Relation to CyberROAD:** research on emerging threats against sensor networks and Internet of Things will be part of WP4. **Indexed and Abstracted by (list is non-exhaustive):** Science Citation Index Expanded (SCIE – Thomson Reuters) with an Impact Factor of 0.727, Directory of Open Access Journals (DOAJ), Google Scholar, Scopus, Journal Citation Reports: Science Edition etc.		
Publisher	Springer	**Title**	Intl. Journal of Information Security
Description	Information and Systems Security		
Link	http://www.springer.com/computer/security+and+cryptology/journal/10207		
Access Type	Green or Golden OA	**IPR policy**	IP transfer necessary for Green Access. In Golden open access the author retains the rights and the work is licensed under Creative Commons.
Comments	**Article Processing Charge:** For golden access only, there is a processing charge of 300$ (2200€), which burdens the author and offers unrestricted access to the public. Otherwise, green access is allowed and a subscription fee is shifted to the reader. The author is allowed to provide an archived copy of the peer reviewed manuscript as long as a link to the final printed article is included. **Relation to CyberROAD:** The journal covers information security, system security and studies on the fundamentals (security, privacy etc.) in relation to WP4, WP5, WP6. **Indexed and Abstracted by (list is non-exhaustive):** Science Citation Index Expanded (SCIE – Thomson Reuters) with an Impact Factor of 0.480, Computer Science Index, Scopus, Google Scholar, Journal Citation Reports: Science Edition etc.		
Publisher	Elsevier	**Title**	Computers & Security
Description	This journal is aimed at the professional involved with **computer security**, **audit**, **control** and **data integrity** in all sectors - industry, commerce and academia.		

Link	http://www.journals.elsevier.com/computers-and-security/		
Access Type	Subscription-based	**IPR policy**	Requires IP transfer
Comments	Bimonthly publication **Relation to CyberROAD:** Relevant to the themes of WP4, WP5, WP6. **Indexed by:** Science Citation Index Expanded (SCIE – Thomson Reuters) with an Impact Factor of 1.158, Computer Science Index, Scopus, Google Scholar, Journal Citation Reports: Science Edition etc.		
Publisher	IEEE Computer Society	**Title**	Security and Privacy magazine
Description	The primary objective of *IEEE Security & Privacy* is to stimulate and track advances in security, privacy, and dependability and present these advances in a form that can be useful to a broad cross-section of the professional community--ranging from academic researchers to industry practitioners. It is intended to serve a broad readership.		
Link	http://www.computer.org/portal/web/computingnow/securityandprivacy		
Access Type	Subscription-based, Green Open access on conditions	**IPR policy**	Requires IP transfer
Comments	Self-archiving of the post-edited version is allowed only if the publisher is notified and the the source is linked; the author is not allowed to upload the final version (the publisher's version) of the work. **Relation to CyberROAD:** Relevant to the themes of WP3, WP4, WP5, WP6. **Indexed by:** Science Citation Index Expanded (SCIE – Thomson Reuters) with an Impact Factor of 0.96, Computer Science Index, Scopus, Google Scholar, Journal Citation Reports: Science Edition etc.		

5 OTHER RELEVANT DISSEMINATION ACTIVITIES

Apart from the participation of consortium members to scientific dissemination events (such as Conferences, Workshops, Symposia etc.), partners are also encouraged to participate to other events that target the industry, relevant stakeholders etc. and liaise with other entities and organizations relevant to the themes that CyberROAD explores.

5.1 LIAISON WITH OTHER CONSORTIA

Extensive Liaison activities will be undertaken by the consortium members to ensure the liaison with other EC-funded consortia, such as CAMINO, COURAGE, CIPHER etc. In particular, a restricted delegation of CyberROAD partners will be participating in the various events organized by other EC-funded consortia while liaison activities initiated by CyberROAD are also envisioned. For example, delegates from CAMINO and COURAGE will be invited to participate to the second CyberROAD workshop, which will be collocated with the ARES International Conference in 2015. A representative of the CyberRoad consortium will attend the first CAMINO workshop in Bern on September 18th, 2014. Planned activities are presented in more detail in the Calendar of WP7 activities that follows in Chapter 7.

5.2 OTHER RELATED EVENTS AND ACTIVITIES

This section lists other related events, targeting the Cyber Security industry, stakeholders, the general public etc. Partners are encouraged to participate in a variety of events where CyberROAD research results may be promoted in order to generate added impact. A non-exhaustive list of events is herein presented and will be updated and maintained throughout the project. Within the project's duration, partners are advised to:

- Report relevant events that come to their attention, so that the list can be populated with up-to-date information, and
- Report their participation to such events where dissemination of project results was conducted.

All other dissemination and exploitation activities that are not immediately related to those described in the previous sections, may be reported using the generic dissemination and exploitation form included in Appendix B. Activities include, for example, the design of dissemination material, redesign of the project logo etc.

TABLE 5-1 List of Other Dissemination Events.

Event	Info day	**Title (and acronym, if applicable)**	Intelligence Live - La ricerca sulla Cyber Intelligence al servizio della sicurezza dei cittadini
Description of Area of Focus	Cybersecurity trends		
Link	http://pralab.diee.unica.it/sites/default/files/Locandina-CAGLIARI_DEF_06052014%20%282%29.pdf		
Date(s)	15/05/2014	**Location**	Cagliari, Italy
Admission Fee (if applicable)	-	**Organized by**	Italian school "Scuola di formazione del Sistema di informazione per la sicurezza della Repubblica"
Target Audience	General Public and Government	**Frequency**	-
Comments	Fabio Roli(UNICA) presented CyberROAD during his talk		

Event	*Seminar*	**Title (and acronym, if applicable)**	Computer Security Seminar 2015
Description of Area of Focus	*Computer security and privacy*		
Link	http://pralab.diee.unica.it/it/SicurezzaInformatica		
Date(s)	*2/1/2015*	**Location**	*Cagliari, Italy*
Admission Fee (if applicable)	*Free*	**Organized by**	*PRA Lab (UNICA)*
Target Audience	*Scientific Community*	**Frequency**	*Annual*
Comments	*Requires B.Sc. and M.Sc. degree in Electronic and Telecommunications Engineering, Ph. D. in Information Engineering. A day of the seminar (organized by Giorgio Giacinto, Davide Ariu, Igino Corona - UNICA) will be dedicated to cyber security trends and CyberROAD project goals.*		

Event	*Summer School*	**Title (and acronym, if applicable)**	Building Trust in the Infomation Age 2014 (BTIA 2014)
Description of Area of Focus	*Computer security and privacy*		
Link	http://comsec.diee.unica.it/summer-school/		

Date(s)	*16-19/9/2014*	**Location**	*Cagliari, Italy*
Admission Fee (if applicable)	*TBD*	**Organized by**	*PRA Lab, UNICA*
Target Audience	*Scientific Community*	**Frequency**	*Annual*
Comments	*A day of the school (organized by Giorgio Giacinto, Davide Ariu, Igino Corona - UNICA) will be dedicated to cyber security trends and CyberROAD project goals. During a poster session, the results of the project will be shown.*		

Event	*Summer School*	**Title (and acronym, if applicable)**	*NCSRD Summer School 2015*
Description of Area of Focus	*Interdisciplinary Summer School with dedicated ICT workshops*		
Link	TBD		
Date(s)	*TBD, Summer 2015*	**Location**	*Athens, Greece*
Admission Fee (if applicable)	-	**Organized by**	*NCSRD*
Target Audience	*General Public (students)*	**Frequency**	*Annual*
Comments	*A session on Cyber Crime and Cyber Terrorism research may be planned and delivered by NCSRD in the 2015 Summer School.*		

Event	*Exhibition*	**Title (and acronym, if applicable)**	*InfoSec Europe*
Description of Area of Focus	*Information Security Exhibition*		
Link	*http://www.infosec.co.uk*		
Date(s)	*2-4/6/2015*	**Location**	*London, UK*
Admission Fee (if applicable)	*N/A (registration not available yet)*	**Organized by**	*InfoSecurity Group, Reed Organizers*
Target Audience	*Industry*	**Frequency**	*Annual*
Comments	-		

6 EXPLOITATION ACTIVITIES

This chapter provides examples of exploitation activities that are envisioned to be undertaken by the consortium members, aiming to properly utilize CyberROAD results to support their interests in their educational, commercial or research capacities.

6.1 LIAISON AND NETWORKING

CyberROAD dedicates a specific task (T7.2) 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 will be carried out throughout the duration of the project, and the partners are encouraged to leverage their existing affiliations for targeted dissemination activities. Such activities may include (but are not limited to):

- Personalized invitations to the CyberROAD workshops,
- Dissemination of project news,
- Dissemination of questionnaires or related material,
- Exploitation of CyberROAD knowledge within the different partner activities,
- Liaison with other consortia, which are active in Cyber Crime, Cyber Terrorism research, etc.

An appropriate reporting form for liaison activities is included in Appendix B.

6.2 EXPLOITATION OF CYBERROAD KNOWLEDGE

CyberROAD was based on a comprehensive workplan of activities, ensuring the delivery of high-impact research results. The partner activities that will be completed within the two-year duration of the project, aim to provide a concrete research roadmap for Cyber Crime and Cyber Terrorism. Partners are encouraged to exploit this significant know-how and expertise gained, to support their activities. Exploitation activities may include (but are not limited to):

- Utilization of CyberROAD results in an educational capacity: CyberROAD results may be utilized for training and awareness raising within the consortium member organizations. Other educational activities may include the organization of seminars, Summer Schools etc. targeting the general public.
- Utilization of CyberROAD results in a research capacity: CyberROAD results may be utilized to further the research agenda of consortium members in the areas of

The appropriate reporting forms for educational and various exploitation activities, is included in Appendix B.

7 CALENDAR OF WP7 ACTIVITIES

This section details the calendar of anticipated WP7 activities for the two-year duration of the project. Activities listed in Table 7-1 are colour-coded as follows:

- Green, marks Project Milestones,
- Blue, marks Delivery dates for WP7 documents etc.,
- Orange, marks partner activities,
- Purple, marks various other dates of interest.

The Calendar of WP7 activities will be maintained and updated throughout the project duration.

TABLE 7-1 Calendar of WP7 Activities.

Date	Activity	Partners involved
June 1, 2014 (M1)	Project Kick-Off	All
June 24-25, 2014 (M1)	Kick-Off meeting	All
July 4, 2014 (M2)	Online Dissemination/Exploitation Form	UNICA, NCSRD
July 11, 2014 (M2)	Deadline for Filling of form details	All
July 31st, 2014 (M2)	Expected delivery of D7.1 Dissemination plan and Calendar of Activities	NCSRD, UNICA
August 29th, 2014 (M3)	Expected delivery of project Social Networking accounts, Website and Web tools .	FORTH, NCSRD
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
September 18th, 2015 (M4)	Possible liaison with CAMINO workshop in Bern, Switzerland	Selected delegates.
October 13-17, 2014 (M5)	**Update for Workshop planning:** First Draft of the Call for Papers, identification of Areas of Interest, possible organization	UNICA, NCSRD, SBA, TUD

	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.	
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
January 5-9, 2015 (M8)	**Update for Workshop planning:** Call for papers released and disseminated	UNICA, NCSRD, SBA, TUD
1st March 2015 (M10)	Update on liaison activities with CAMINO workshop in Montpellier, France	Selected delegates
1st March 2015 (M10)	Update on liaison activities with COURAGE workshop.	Selected delegates
April 1st, 2015 (M11)	**Update for Workshop planning:** Status of Reviewer team	UNICA, NCSRD, SBA, TUD
May 31st,, 2015 (M12)	Expected delivery of D7.2 (Preliminary Dissemination and Exploitation Report)	NCSRD, UNICA, SBA, TUD.
May 31st , 2105 (M12)	Conclusion of first year of CyberROAD activities	All
June 15th -16th, 2015 (M13)	Possible liaison activitiy with CAMINO, at the third CAMINO workshop, in London, UK	Selected Delegates
May 31st, 2016 (M24)	Conclusion of project activities	All
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)	WP7 partners
TBD	Delivery dates for D7.6, D7.7, D7.8 to be redefined according to Workshop planning	SBA, TUD, UNICA, NCSRD
TBD	Scheduled dates for CyberROAD workshops to be defined	SBA, TUD, UNICA, NCSRD

LIST OF FIGURES

LIST OF TABLES

CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

CyberROAD è un progetto di ricerca finanziato dalla **Commissione Europea** con 1.300.000 euro nell'ambito del Settimo Programma quadro. Ha il compito di redigere il ***piano di ricerca europeo sui crimini e gli atti terrorismo informatici***. A fronte di un'analisi innovativa dello scenario tecnologico, politico, sociale ed economico nel quale il ***cyber crime*** e il ***cyber terrorism*** affondano le proprie radici, il progetto CyberROAD stilerà il piano strategico europeo che identificherà le priorità per le future attività di ricerca.

Recenti studi sull'evoluzione dei comportamenti su internet hanno evidenziato scenari caratterizzati da una costante crescita delle attività criminali perpetuate attraverso strumenti informatici. Sebbene sia aumentato il livello di allerta sui rischi che si celano dietro l'utilizzo di smartphone, computer e tablet, i danni derivanti da attività illegali compiute attraverso il web hanno raggiunto costi insostenibili.

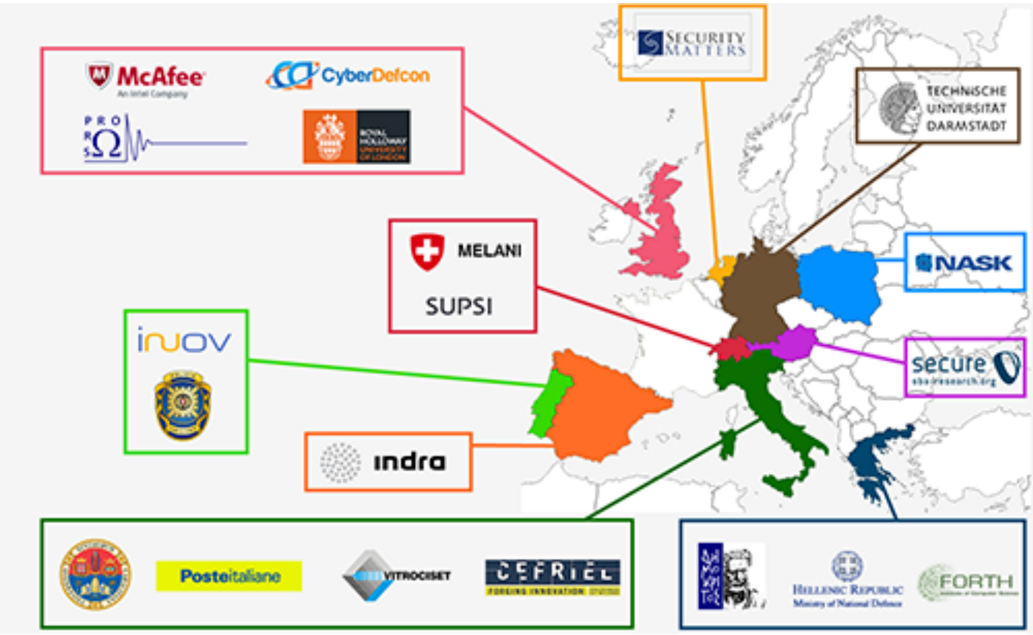
Le stime più recenti documentano un costo di circa **500 miliardi** di dollari l'anno, con 500 milioni di vittime, **18 vittime al secondo**. Più di 600.000 profili Facebook vengono compromessi ogni giorno.

Oltre alle motivazioni prettamente economiche, dietro agli attacchi informatici non di rado si nascondono **motivazioni politiche e sociali** che costituiscono un serio pericolo per la sicurezza nazionale (attivismo, terrorismo, spionaggio industriale).

CyberROAD è un progetto guidato dal PRA Lab - Pattern Recognition and Applications Laboratory, dell'Università di Cagliari (http://pralab.diee.unica.it). Il laboratorio diretto dal Professor Fabio Roli coordinerà un team di 20 partner europei, coinvolti da sempre nella lotta al cyber crime.

- PRA Lab, University of Cagliari, Italia;
- CEFRIEL - Forcing Innovation, Italia;
- CyberDefcon, Regno Unito;

- Demokritos National Centre for Scientific Research, Grecia;
- FORTH - Institute of Computer Science, Grecia;
- Governo de Portugal - Ministério da Justiça, Portogallo;
- Hellenic Republic - Ministry of National Defence, Grecia;
- Indra, Spagna;
- INOV - Inesc Inovação, Portogallo;
- McAfee, Regno Unito;
- MELANI - Reporting and Analysis Centre for Information Assurance, Svizzera;
- Nask, Polonia;
- Poste Italiane, Italia;
- PROPRS - Professional Probabilistic Risk Solutions, Regno Unito;
- Royal Holloway - Università di Londra, Regno Unito;
- SBA Research, Austria;
- Security Matters, Olanda;
- SUPSI - Scuola Universitaria Professionale della Svizzera Italiana, Svizzera;
- Technische Universitaet Darmstadt, Germania;
- Vitrociset, Italia.



Riferimenti web per Cyber ROAD:

http://pralab.diee.unica.it/it/CyberRoad

Progetto finanziato dalla Commissione Europea, Settimo Programma Quadro.

CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

CyberROAD is a research project funded by the **European Commission** under the Seventh Framework Programme (total budget: 1.300.000 €). 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.

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 **500 billion dollars** (more than 500 million victims per year, **18 victims per second**). More than 600000 Facebook accounts are compromised every day.

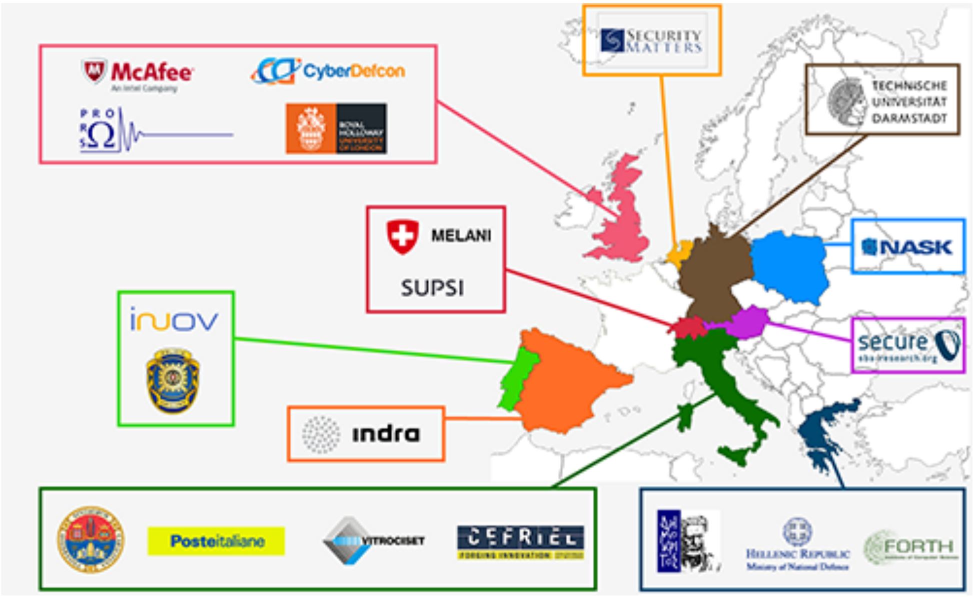
In addition to the economic reasons, cyber attacks often hidden political and social motivations which constitute a serious threat to national security (hacktivism, cyber espionage, cyber warfare).

The CyberROAD project is led by the **PRA Lab** (University of Cagliari - http://pralab.diee.unica.it) and has a duration of 24 months (starting from June 2014).

The consortium running the CyberROAD project is made up of **20 international partners**, involved in the fight against cybercrime and cyberterrorism, and includes universities, public and private companies, and national ministries of the European Union:

- PRA Lab, University of Cagliari, Italy (Project coordinator);
- CEFRIEL - Forcing Innovation, Italy;
- CyberDefcon, UK;
- Demokritos National Centre for Scientific Research, 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, California, 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.



Web links for Cyber ROAD:

http://pralab.diee.unica.it/en/CyberRoad

With the financial support of the European Commission, Seventh Framework Programme.

Appendix B: Dissemination Reporting Forms

A. Reporting Forms for Scientific Dissemination Activities

Publisher	*<Insert Publ.House>*	**Title of Journal**	*<Insert Journal Title>*
Authors/Partners	*<List of authors and their affilications>*	**Link**	*<Link to Journal and publication if applicable>*
Title of Article	*<Title of Article>*		
Date of Submission	*<Date of Submission>*	**Date of Acceptance**	*<Please indicate the Date of Acceptance/Publication, or if the publication is still under review>*
Access Type	*<Subscription-based, green OA, or golden OA etc.>*	**IPR policy**	*<Was IP transferred or is it held by the author?>*
Comments	*<Additional comments if necessary>*		

Event	*<Name of Event>*	**Event Type**	*<Conference, Workshop, Symposium etc.>*
Presenter/Partner	*<Name of presenter and/or authors and their affiliation>*	**Activity**	*<presentation, poster session, exhibition etc, or indicate your simple attendance and dissemination of information through liaison activities and use of dissemination material etc.>*
Date of Presentation	*<Date>*	**Locale**	*<Location of Event>*
Comments	*<Any additional information, if necessary>*		

B. Reporting Forms for Partner Online/Educational/Press Activities

Online Dissemination Channel	*<Website, Newsletter, Blog, Social Media account etc>*	**Description**	*<Brief Description of Dissemination Activity>*
Partner	*<Partner who participated in the activities>*	**Link**	*<link to website, blog etc.>*
Date	*<Date of activity>*		
Comments	*<Any additional information, if necessary>*		

Educational/Training Activity	*<Activity Name>*	**Description**	*<Brief Description of Educational or Training Activity which utilized CyberROAD results>*

Partner	*<Partner who participated in the activities>*	**Link**	*<link to website if applicable>*
Date	*<Date of activity>*	**Locale**	*<Location of Event>*
Comments	*<Any additional information, if necessary>*		

Mass Media Activity	*<Newspaper, Magazine, Television coverage etc.>*	**Description**	*<Brief Description of Mass Media Activity>*
Partner	*<Partner who participated in the activities>*	**Link**	*<link to website, blog etc.>*
Media	*<television channel, name of newspaper etc.>*	**Language**	*<available languages>*
Date	*<Date of activity>*		
Comments	*<Any additional information, if necessary>*		

C. Generic Reporting Forms for all other activities

Activity	*<Any other activity may be reported with this form>*	**Description**	*<Brief Description of Activity>*
Partner	*<Partner who participated in the activities>*	**Link**	*<link if applicable>*
Date	*<Date of activity>*		
Comments	*<Any additional information, if necessary>*		

Exploitation or Liaison	*<Actitivities which involve liaison with other consortia, researchers, stakeholders, special interest groups etc or activities which .>*	**Description**	*<Brief Description of Activity>*
Partner	*<Partner who participated in the activities>*	**Link**	*<link if applicable>*
Date	*<Date of activity>*		
Comments	*<Any additional information, if necessary>*		

D. Forms for reporting relevant dissemination outlets to the consortium

Publisher	*<Publishing House>*	**Title**	*<Title of Journal and acronym, if applicable>*
Description	*<main area of focus>*	**Link**	*<URL of journal>*
Access Type	*<hybrid, green, golden OA etc.>*	**IPR policy**	*<Is IPR transfer necessary for submission?>*
Comments	*<Any additional Information if necessary>*		

Event	*<Exhibition, Information day, Conference, Workshop, Forum, Seminar, Summer School, other>*	**Title (and acronym, if applicable)**	*<Title of Event>*
Description of Area of Focus	*<Area of Focus of Event>*	**Link**	*<URL of event>*
Date(s)	*<Dates of event>*	**Location**	*<Location of event>*
Admission Fee (if applicable)	*<Please specify admission fee and currency>*	**Organized by**	*<Organizing Committee>*
Target Audience	*<Scientific Community, Industry, Professionals, Policy Makers etc.>*	**Frequency**	*<annual, semiannual, monthly etc.>*
Comments	*<for any other important information such as registration and submission deadlines etc.>*		

Call for Papers

The First International Workshop on <TBD>

To be held in conjunction with the 9th International Conference on Availability, Reliability and Security (ARES 2015 – http://www.ares-conference.eu).

<Date>

<Venue unknown>

<unknown>

<Short Description of Workshop scope and aims>

Topics of interest include, but are not limited to:

- Topic 1
- Topic 2
- …

Important Dates

Submission Deadline	**TBD, 2015**
Author Notification	TBD, 2015
Author Registration	TBD, 2015
Proceedings Version	TBD, 2015
Conference	**TBD, 2015**

Submission Guidelines

The submission guidelines valid for the workshop are the same as for the ARES conference. They can be found at http://www.ares-conference.eu.

Program Chair

<**Name**> (Chair)

<Affiliation>, <Country>

<Email>

Program Committee

- **<Name and Title>, <Affiliations>, <Country>**
- **<Name and Title>, <Affiliations>, <Country>**
- **<Name and Title>, <Affiliations>, <Country>**
- **…**