



Funded by the European Commission

Seventh Framework Programme



# CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

## D 7.6 Report on FCCT 2015

Date of deliverable: 30/09/2015  
Actual submission date: 30/09/2015

Start date of the Project: 1st June 2014. Duration: 24 months  
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab  
Version: 0.5

| Project funded by the European Commission under the Seventh Framework Programme |   |   |
|---|---|---|
| Restriction Level   |   |   |
| PU  | Public  | X |
| 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)           |   |



D7.6 Report on FCCT

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 21

## Revision history

| Version | Object   | Date       | Author(s) |
|---------|----------|------------|-----------|
| 0.1     | Creation | 24/08/2015 | SBA       |
| 0.5     | Revision | 29/09/2015 | SBA       |
| 1.0     | Final    | 30/09/2015 | SBA       |



# D7.6

## Report on FCCT 2015

### Responsible

Peter Kieseberg (SBA)

### Contributor(s)

Peter Kieseberg (SBA)

**Summary:** The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism (FCCT 2015) was organized as a scientific workshop gathering and publishing new scientific endeavours in the area of detection, prevention and roadmapping in the area of cybercrime and cyberterrorism. Based on a rigorous scientific peer-review, the resulting disseminations were presented on the 24<sup>th</sup> of August at the ARES EU-Symposium in Toulouse, which was held in conjunction with the renowned ARES conference, and published by IEEE.

**Keywords:** ARES conference, scientific workshop, FCCT





## TABLE OF CONTENTS

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>INTRODUCTION.....</b>                  | <b>6</b>  |
| <b>2</b> | <b>SCIENTIFIC ORGANIZATION .....</b>      | <b>7</b>  |
| 2.1      | THE ARES CONFERENCE .....                 | 7         |
| 2.2      | IMPORTANT DATES .....                     | 7         |
| 2.3      | PEER-REVIEW AND QUALITY CONTROL.....      | 9         |
| 2.4      | CALL FOR PAPERS.....                      | 11        |
| 2.5      | THE CHAIRS AND THE PROGRAM COMMITTEE..... | 11        |
| <b>3</b> | <b>WORKSHOP ORGANIZATION .....</b>        | <b>13</b> |
| 3.1      | TRAVEL AND ACCOMODATION.....              | 13        |
| 3.2      | CATERING AND SOCIAL EVENTS.....           | 13        |
| 3.3      | ARES EU-SYMPOSIUM AND POSTER SESSION..... | 13        |
| <b>4</b> | <b>EXECUTION .....</b>                    | <b>14</b> |
| 4.1      | PRE-MEETING .....                         | 14        |
| 4.2      | WORKSHOP PROGRAM.....                     | 14        |
| 4.3      | ACCEPTANCE RATE AND VISITORS.....         | 15        |
| <b>5</b> | <b>ACCEPTED PUBLICATIONS.....</b>         | <b>17</b> |
| 5.1      | SCIENTIFIC POLICY .....                   | 17        |
| 5.2      | LIST OF ACCEPTED PAPERS.....              | 17        |
| 5.3      | PAPER ABSTRACTS.....                      | 18        |
| <b>6</b> | <b>FINANCING .....</b>                    | <b>20</b> |
| 6.1      | COSTS FOR TRAVEL .....                    | 20        |
| 6.2      | WORKSHOP ORGANIZATION .....               | 20        |
| 6.3      | COSTS FOR CATERING.....                   | 20        |
| <b>7</b> | <b>ATTACHMENTS.....</b>                   | <b>21</b> |



## 1 INTRODUCTION

The target of the “The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism” (FCCT) was to bring researchers in the area of Cybercrime and Cyberterrorism together in an academic event, where new scientific results could be published and disseminated in the course of peer-reviewed publishing. To this end, the FCCT was collocated with the tenth “International Conference on Availability, Reliability and Security” (ARES), together with the “ARES EU Symposium”, which further helped drawing attention to these pressing topics through gathering a much larger audience than would have been possible with a stand-alone event.

In addition to the academic part, where papers were presented in the form of academic presentations together with a keynote, the ARES EU Symposium hosted a poster session, where CyberRoad was able to participate. In order to better integrate the FCCT into the ARES conference, the FCCT sessions were located right before the ARES opening and the ARES best paper session, thus being capable of drawing even more attention. During the Symposium and the subsequent networking events, it was possible to interact with members from other projects, as well as scientists from all over the world, thus being able to spread the dissemination activities and getting even more people becoming aware of the CyberRoad results. Together with the second day of the ARES conference, where CyberRoad members attended in a large number, this activity enabled us to reach new and large parts of the research community. Due to the broad topics of the ARES, and the heavily international focus, this led to a lot of meaningful interaction with researchers from other areas.

Due to the strict peer-review that was performed on the FCCT submissions, it was possible to publish the accepted papers inside the ARES proceedings by IEEE. Thus, the accepted FCCT papers count as regular scientific dissemination that can be accessed through IEEE Xplore, as well as cited and referenced. The papers are indexed in all major scientific search engines and count as full research papers.

Due to the huge success of the FCCT, the ARES organization team already inquired, whether FCCT could become a regular ARES-Workshop. Thus, the team has already decided on a second installment collocated with ARES 2016 and continuation of this work beyond the CyberRoad project.



### 2.1 THE ARES CONFERENCE

The International Conference on Availability, Reliability and Security (“ARES”) brings together researchers and practitioners in the area of IT-Security and related research fields. ARES aims at highlighting the various aspects of security – with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of the research issues of security as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications. To this end, ARES emphasizes the interplay between foundations and practical issues of security in emerging areas and is devoted to the critical examination and research challenges of the various aspects of Secure and Dependable Computing and the definition of a future road map.

The acceptance rate of the ARES 2014 conference was 16% and ARES is ranked as B-conference in CORE (<http://103.1.187.206/core/?search=ARES&by=all&source=CORE2014&sort=atitle&page=1>).

The 2015 instalment of the ARES conference also yielded its tenth anniversary, together with a large amount of workshops and social events. It took place at Université Paul Sabatier in Toulouse (France), with support from the local scientific community and the city of Toulouse. In order to integrate the FCCT well into the overall conference, including the chance to generate good visibility and networking opportunities, FCCT was scheduled right at the start of the week with the first two sessions right before the ARES opening and the “best paper session” (one of the major highlights of ARES and the session with most attendants), and the poster presentation including Symposium right afterwards.

### 2.2 IMPORTANT DATES

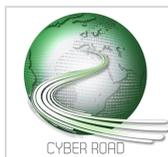
The following important dates were scheduled for the FCCT submissions and notifications, where an asterisk marks internal dates that were not communicated to the broader audience beyond the program committee:

**30.09.2014\***: *First draft of the Cfp* including decision by the ARES-organizers to host FCCT as an accompanying Workshop. Furthermore, this deadline included the first draft for the program committee, in order to be able to show a strong scientific committee.

**31.01.2015\***: *Final Cfp*: The Cfp was finalized and submission to various mailing lists, both, by the ARES conference organizers, as well as the members of the program committee and the

**10.04.2015**: *Original submission deadline*: The original submission deadline was selected to be very early in order to be able to get a first glance on the interest in the scientific community. It was planned right from the start to extend this deadline in order to match the larger share of the other ARES-Workshops, both inside and outside the ARES EU-Symposium.

**01.05.2015**: *Extended submission deadline*: The submission deadline was extended like planned one day before the end of the original deadline (09.04.2015) in order to take pressure from submitting authors and to circumvent bad submission quality due to pressure. Most submissions for FCCT were done before the end of this deadline, thus proving the good selection of the date. Since



requested by some (potential) author, we decided to extend the submission deadline for a second time, also given the large amount of resources for review we had through the well-selected and quite large program committee and the commitment of the members to review possible submissions at very short notice. Deadline extension was also published on the 01.05.2015.

**02.05.2015\*: Reviewer Allocation:** The required reviewers were allocated with submitted papers. In this process, the reviewers could announce interest for reviewing selected papers through the ARES conferencing tool. Even though the reviews were done in a double blinded process, no reviewer was allowed to review a paper having an author from the same affiliation. Also, except rare circumstances where the paper could be declined on the spot by the chairs due to formal reasons, at least two reviewers were selected for each paper. In case of rejection due to formal reasons, the chair informed the authors in order to facilitate them to correct their submission accordingly.

**25.05.2015: Review deadline:** The reviewers had to submit their recommendations including detailed analysis on the strengths and weaknesses of the papers until this date. In reality, the large majority of reviews was submitted far earlier, making it possible to have a first estimation on the ration of acceptable papers quiet early.

**26.05.2015: First decision:** In a first decision round, the chairs and members of the program committee took a first decision on the papers already submitted and reviewed. While no feedback was given to the authors at this point, a first preliminary decision was taken. Furthermore, in case of contradictory reviews, i.e. one reviewer accepting and one rejecting a paper, a third reviewer was assigned. Due to the commitment of the program committee, this could also be done with all of the papers that were in danger of rejection, except those being rejected for formal reasons.

**28.05.2015: Extended submission deadline:** The final submission deadline, which yielded only few additional submissions.

**01.06.2015\*: Final review deadline:** The final deadline for all reviews, especially those from submissions after the 01.02.105. This also included the additional reviews decided on at the conference call on 26.05.2015 during the first decision.

**02.06.2015\*: Final decision:** The final discussion on the acceptance of work during a conference call, including precedent communication with reviewers on unclear details. All reviews were suspect to a meta-review by the chairs, including the clarification of unclarities. The final decision yielded some discussion, especially regarding one submission, which was finally rejected.

**03.06.2015: Author notification:** The author were notified of the decision, including the detailed reviews: In case of an accepted submissions, the reviews often contained small mandatory, as well as optional requests for changes in the camera ready version. Together with the acceptance notification, all important information concerning the FCCT, the ARES EU-Symposium and the ARES-conference were sent to the authors. Subsequently, any organizational details were sent to the authors directly by the ARES organizers, who received the list of accepted papers, as well as the contact details of the respective corresponding authors.

**15.06.2015: Proceedings version:** The final deadline for all the authors to provide the camera ready version of their submissions with respect to the closing deadline for the whole ARES organization to provide IEEE with a printable version of the conference proceedings. Since this deadline was rather



hard, reminders of missing camera ready versions were sent out frequently starting on 10.06.2015. Still, response by the authors was very good and fast, which we see as an indication that the authors see FCCT as an important means for publishing their scientific work.

**24.08.2015: Workshop execution:** The FCCT took place on 24.08.2015 at Université Paul Sabatier in Toulouse, together with the ARES EU-Symposium ad embedded into the man conference.

### 2.3 PEER-REVIEW AND QUALITY CONTROL

The ARES conference is enforcing a double blindended review process, i.e. neither the reviewers know the authors, nor the other way round. This not only includes the actual names of the authors/reviewers in question, but also their affiliations. This procedure requires a pre-review screening of all submissions by the chair in order to ensure that authorship is not easily discernible, neither directly (by putting names or CVs somewhere in the text), nor indirectly (e.g. by referencing previous work as their own). This pre-screening was done by the chair right before distribution of the work to the respective reviewers. Authors of papers failing this screening were immediately contacted by the chair in order to allow them to send in a corrected version and held back for review until this anonymized version was made available.

On the other side, all reviews were checked by the chair with respect to anonymity of the reviewer. Furthermore, the chairs enforced quality control on the reviews, i.e. the reviews of each paper were meta-reviewed by the chairs in the context of the original paper, in order to be able to ensure as a high review quality as possible. Still, in the case of the FCCT, the original review quality was very high, thus no review had to be dropped or redone. This is an especially important testimonial for the dedication and also standing the quality of the FCCT had with the reviewers and the program committee.

The actual peer review followed the guidelines set by the ARES conference and consisted of several parts. The papers were accessed and the reviews were submitted using the “Confdriver”-tool set up by the ARES organizers, thus close to no work needed to be spent on setting up a review system. Furthermore, the ARES conference provided FCCT with minimum quality requirements for acceptable reviews and the communication and evaluation/ranking tools needed, as well as rating best-practices from the main conference. The reviews consisted of the following parts:

Comments to the authors: This section should be the most detailed one. Here the reviewer gives a short overview on the claims and actual achievements of the paper in question. Furthermore, a detailed analysis on the strengths and weaknesses of the paper need to be given, including an informal final verdict on the paper. In case of a positive or only slightly negative (weak reject) feedback on the paper, the reviewer can give advice on what to rectify for an eventual camera ready version in the case of acceptance. This section is the most detailed one and especially in the case of a reject, the chairs expect a very detailed analysis and a thorough argumentation on the reasons the paper needs to be removed from FCCT. This is also expected in case the reviewers give especially high recommendation for acceptance, i.e. in the case of reaching a verdict “strong accept”. Since this rating is usually reserved for extraordinary work, good argumentation needs to be done, why the authors achieved this level of quality. The “comments to the authors” section is not only important for the chair in order to be able to assess the paper, it is also used to assessing and controlling the quality of the review itself covering questions like: “Have the reviewers actually read the whole paper?”, “What were the premises for the verdict chosen”, and so on. This is especially important,



since the quality of a conference or a workshop is often building upon the quality of the reviews, especially considering a first instalment. Also, due to fairness reasons, authors need to be able to understand why their work was rejected using stringent arguments.

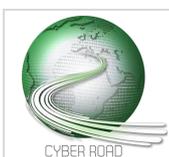
Comments to the chair: This section covers confidential information for the chair, usually used for summing up the comments to the authors. While this field can be left almost empty during normal reviews, it is important in case of suspected plagiarism.

Ratings: In addition to the more informal comments to the authors and to the chair, the following formal ratings need to be set by the reviewer. The verdicts for each rating lie between “strong accept” and “strong reject”. The final rank of the paper is then calculated using a weighted sum over all criteria together with the respective ratings. The following table gives an overview on the values and weights for each criterion and the ratings, the overall rating is then translated back according to the third and fourth column.

- **Originality:** The originality of the approach presented, especially considering related work in this field, or related approaches in other areas. This criterion gives a good overview on the novelty of a paper.
- **Quality:** The quality of the research carried out and the achieved results. This also includes comparison to related approaches in this field, as well as fundamental methodology. It does not cover issues of presentation though, but might be reduced in case important aspects are missing in the work.
- **Relevance:** Relevance of the work with respect to the topics of the conference or the overall workshop theme. Mainly used in order to mark work that seems legit, but may not be suitable due to thematic reasons. While this criterion per se does not have a high weight for the overall score, papers with a low score in “relevance” will be assess again by the chair solely regarding this topic.
- **Presentation:** The quality of the presentation of the work, including but not limited to topics like spelling, grammar, quality of pictures, as well as the overall structure of the work.
- **Recommendation:** This criterion gives feedback on the overall impression of the reviewer on the paper in question. It is the criterion most weight was allocated on,

| Criteria       | Weight | Rating        | Value |
|----------------|--------|---------------|-------|
| Originality    | 2      | Strong Accept | 7     |
| Quality        | 2      | Accept        | 6     |
| Relevance      | 1      | Weak Accept   | 5     |
| Presentation   | 1      | Neutral       | 4     |
| Recommendation | 6      | Weak Reject   | 3     |
|                |        | Reject        | 2     |
|                |        | Strong Reject | 1     |

Table 1: Criteria and Ratings



One especially problematic topic lies in having to deal with suspected plagiarism: In order to keep plagiarized papers away from the actual reviewers in order not to waste their time and energy, the organizers of the ARES conference review all submissions of all workshops for plagiarisms using specialized tools and following the same procedures as for the main conference. In case of detected plagiarism at this level, the organizers inform the Workshop chairs and discuss further actions which usually involve an instant reject of the work in question together with setting up contact with the authors. Further actions are depending on whether there is a case of self-plagiarism, or if only parts of the work were plagiarized, still, the ARES conference enforces a very strict course with respect to plagiarism, since the overall reputation of ARES is at stakes.

Since these tools do not work on a hundred percent bases, the reviewers are also checking for plagiarism during their reviews. In case of a suspected plagiarism, the reviewers notify the chair and write a note in the “comments to the chair” field. Nothing should be written in the “comments to the authors” field though. The chairs, who also have access to names and contact data of the authors, are then thoroughly checking the case on an individual basis and take further actions in coordination with the ARES organizers.

Fortunately, no case of plagiarism was encountered during the FCCT 2015.

#### 2.4 CALL FOR PAPERS

The Call for Papers (CfP) was designed by the consortium based on a draft provided by the workshop chairs during September 2014. It was finalized in January 2015 and subsequently distributed via various formal and informal channels, as well as by the official means of the ARES conference, i.e. the ARES Homepage (<http://www.ares-conference.eu/conference/ares-eu-symposium/fcct-2015/>) and the ARES mailing list. The original CfP is presented in its final version and can be found in the attachment section.

#### 2.5 THE CHAIRS AND THE PROGRAM COMMITTEE

The organization committee consisted of the following Workshop chairs:

- Angelo Consoli from partner “SUPSI”
- Giorgio Giacinto from partner “University of Cagliari”
- Peter Kieseberg from partner “SBA Research” (also acting as contact point)

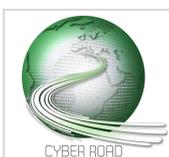
The program committee consisted of major staff from many partners from the CyberRoad consortium, as well as related professionals:

- Davide Ariu (Unica)
- Jart Armin (CyberDefcon)
- Elias Athanasopoulos (FORTH)
- Lorenzo Cavallaro (RHUL)
- Marina S. Egea (INDRA)
- Vivi Fragopoulou (FORTH)
- Enrico Frumento (CEFRIEL)
- Jorge L. Hernandez-Ardieta (INDRA)
- Evangelos P. Markatos (FORTH)
- Javier Martínez-Torres (INDRA)
- Manel Medina (UPC)
- Isidoros Monogioudis (HMOD)



- Fabio Roli (Unica)
- Olga Segou (NCSR Demokritos)
- Foy Shiver (APWG)
- Erik Tews (TU Darmstadt)
- Stelios Thomopoulos (NCSR Demokritos)
- Paolo Foti (CyberDefcon)

All reviews were done by members of the program committee, the final decisions were taken by the chairs together with interested members of the PC.



3.1 TRAVEL AND ACCOMMODATION

Traveling and accommodation were organized by the partners themselves at their own project expenses. Important information for travelling to Toulouse, as well as information on the venue, public transport and related issues were published by the organizers of the ARES conference to the respective speakers of FCCT, as well as to the consortium. Furthermore, the organizers had hotel recommendations, as well as a search engine for suitable accommodations on the official ARES homepage, thus FCCT did not take any further actions in this regard.

The same holds true for travels, this was in general organized by the partners themselves, with the exception of Mr Morana, who held the keynote. Since his travel expenses are covered by the Workshop budget allocated to SBA, the booking and coordination was also done by SBA for reasons of simplicity.

3.2 CATERING AND SOCIAL EVENTS

The catering was provided by the ARES conference, which also encompassed entrance to the social events. In case of attendants holding a reduced 2-days ARES EU Projects Symposium ticket, this includes attendance to all symposium sessions on Monday, August 24, and ARES Sessions on Tuesday, August 25, as well as the Welcome Reception on Monday. In case of FCCT attendants it was possible to facilitate additional free entrance to all main sessions of ARES during the week, thus allowing more efficient networking and dissemination, as well as setup of new partnerships for acquiring more visibility in the community.

The welcome reception on Monday took place in the City Hall of Toulouse, where the major of Toulouse held a speech accompanied by a networking event that allowed further dissemination activities and connecting to other related projects and especially interesting partners. The latter was especially useful considering the further propagation of results inside the scientific community, as well as finding important partners for qualitative and quantitative interviews and questionnaires.

3.3 ARES EU-SYMPOSIUM AND POSTER SESSION

The EU-Symposium not only featured the workshops and the integration into the ARES main conference, but also a symposium consisting of a get-together with participants from the other EU-related workshops “Workshop on Security and Privacy in Cloud-based Applications” (AU2EU) and “The First International Workshop on Security Testing And Monitoring – topic: Secure Interoperability” (STAM), as well as participants specific to the Symposium (holders of a special Symposium Ticket). The symposium was accompanied by a poster session featuring selected posters of over 20 different projects that had a focus or a strong dissemination record in the area of IT-Security.

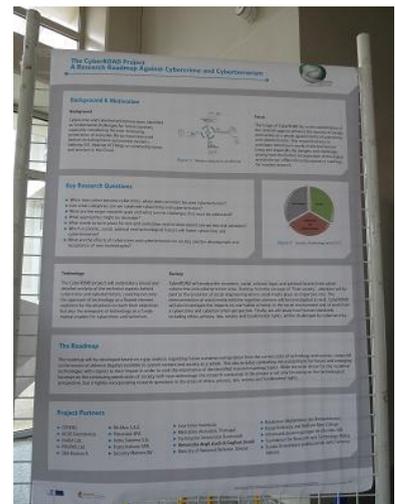


Fig. 1 – The CyberRoad Poster



#### 4.1 PRE-MEETING

Some participants already arrived on Sunday 23<sup>rd</sup> in Toulouse, thus allowing for a short and informal pre-meeting for discussing project related issues.

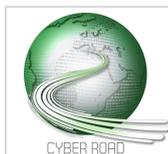
The link of the workshop chairs to the ARES organizers, Peter Kieseberg from SBA, already arrived on 17<sup>th</sup> in order to help setting up the needed rooms and to guarantee a seamless execution of the workshop.

#### 4.2 WORKSHOP PROGRAM

The workshop took place on the 24<sup>th</sup> of August at the Université Paul Sabatier, Toulouse, France and marked the start of this year's instalment of the ARES conference. Following the timeline for the first day of the event:

- 09:00 – 10:30: Session FCCT 1
  - Welcome & Presentation of the CyberRoad project (Davide Ariu)
  - Keynote by Marco Morana
  - Paper Presentation: “o-Day Vulnerabilities and Cybercrime” (Jart Armin, Paolo Foti)
  - Paper Presentation: “Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios” (Max Kilger)
- 10:30 – 11:00: Coffee Break
- 11:00 – 12:30: Session FCCT 2
  - Paper Presentation: “2020 Cybercrime Economic Costs: No measure No solution” (Giorgio Giacinto)
  - Paper Presentation: “Comprehensive Approach to Increase Cyber Security and Resilience” (Michal Choras)
  - Paper Presentation: “Yet Another Cybersecurity Roadmapping Methodology” (Davide Ariu)
  - Discussion with the audience.
- 12:30 – 14:00: Lunch
- 14:00 – 14:30: Opening of ARES
- 14:30 – 16:00: ARES – Best Paper Session
- 16:30 – 18:00: ARES EU Symposium
  - Poster session
  - Project presentation and networking
  - Around 20 projects involved, as well as the following Workshops: AU2EU-Workshop by the AU2EU-Project, FCCT by the CyberRoad-Project and STAM by the projects FP7-Inter-Trust, H2020-MUSA, H2020-CLARUS, Rapid-ISER/INTERSEC, and ANR-DOCTOR
- From 18:00: Welcome Reception by the mayor of Toulouse in the Capitol.

The second day stood in the focus of integration with the main conference, as well as on the keynotes, which were especially related to CyberRoad this year due to the participation of Mr. Afonso Ferreira from the Trust & Security Unit of the European Commission. He is currently in charge, amongst others, of the general secretariat of the Working Group on “Secure ICT Research



and Innovation” of the European Network and Information Security Platform, which provides the input for Horizon 2020 Work-Programmes in Digital Security, and is leading the planning and financing of cybersecurity activities through the Connecting Europe Facility programme. From this perspective, a large participation of CyberRoad members to this talk and the subsequent Q&A/networking was important. Following the program of the second day, which was shared with the main conference:

- 09:00 – 09:45: Invited Talk by Afonso Ferreira on “The European Strategic Agenda for Research and Innovation in Cybersecurity”
- 09:45 – 10:45: Keynote by Peter Eckersley on “Let’s Encrypt: Deploying free, secure, and automated HTTPS certificates for the entire Web”
- 10:45 – 11:15: Coffee Break
- 11:15 – 17:30: Regular ARES program including Workshops, accessible for FCCT participants:
  - ARES Full Papers sessions III – V
  - Workshops

The Workshop was fully embedded in the overall conference plan, as can be seen by the position of the ARES main events during and around the workshop execution. This helped in engaging with other researchers from related areas, in order to get a broader audience for the endeavours and results of the CyberRoad project.

| Preliminary Schedule ARES 2015<br>24 - 28 August 2015, Université Paul Sabatier, Toulouse, France |   |         |   |          |
|---|---|---------|---|----------|
| MONDAY, 24.08.  |   |         |   |          |
|   | LH A  | LH B    | LH C  | LH D     |
| 08:00 - 17:00   | Registration  |         |   |          |
| 09:15 - 10:45   | ARES EU Symposium   |         |   |          |
|   |   | FCCT I  | STAM I  | AU2EU I  |
| 10:45 - 11:15   | Break   |         |   |          |
| 11:15 - 12:45   | ARES EU Symposium   |         |   |          |
|   |   | FCCT II | STAM II   | AU2EU II |
| 12:45 - 14:00   | Lunch   |         |   |          |
| 14:00 - 14:20   | Opening   |         |   |          |
| 14:20 - 15:50   | ARES I - BEST PAPER SESSION<br>LH A   |         |   |          |
| 15:50 - 16:20   | Break   |         |   |          |
| 16:20 - 17:50   | ARES Full II  | IWCC I  | ARES EU Symposium -<br>Poster Session & Get2Gether<br>Coffee Break Area |          |
| 18:30 - 22:00   | Mayor's Reception<br>City Hall Toulouse<br><i>Meeting point: Place du Capitol</i> |         |   |          |

| TUESDAY, 25.08. |   |          |          |
|-----------------|---|----------|----------|
|                 | LH A  | LH B     | LH C     |
| 08:00 - 17:00   | Registration  |          |          |
| 09:00 - 09:45   | Invited Talk LH A<br>Afonso Ferreira, European Commission |          |          |
| 09:45 - 10:45   | Keynote LH A<br>Peter Eckersley, EFF                      |          |          |
| 10:45 - 11:15   | Break   |          |          |
| 11:15 - 12:45   | ARES Full III   | IWCC II  | MFSec I  |
| 12:45 - 14:00   | Lunch   |          |          |
| 14:00 - 15:30   | ARES Full IV  | IWCC III | MFSec II |
| 15:30 - 16:00   | Break   |          |          |
| 16:00 - 17:30   | ARES Full V   | IWCC IV  | WCSF     |

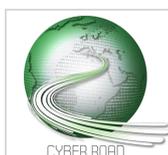
  

|                   |
|-------------------|
| Plenary Sessions  |
| ARES EU Symposium |
| ARES Sessions     |
| Workshop Sessions |
| Social Event      |

Fig. 2: The Symposium Agenda

#### 4.3 ACCEPTANCE RATE AND VISITORS

The FCCT had an acceptance rate of around 63%, which is rather low for a workshop. The main reason for this low rate was the quality criteria enforced by the FCCT program committee which focused on accepting papers of a good quality only. We are of the opinion that in order to make FCCT a lasting instalment with many more iterations to come, providing and guaranteeing quality is



one of the major concerns, furthermore, the quality of a new academic conference is, based on our observations, often based on the quality of the selection and review process. To this end, also the quality of the reviews was monitored by the workshop chairs.

In addition to member of the FCCT, the workshop was open to be visited by all attendants of ARES holding either a full ticket or the Symposium ticket. This is especially important, since research must not take place hidden, but needs to be disseminated to a broader audience in order to facilitate new research and new cooperation's, as well as to guarantee the quality of the research. This was one of the fundamental premises behind collocating the workshop with a major scientific conference in this field and we are proud to announce that over 40 attendants could be gathered during the presentations.



Fig. 3: The auditorium

#### 4.4 COMMENTS & TESTIMONIALS

FCCT was received very well in the ARES-community and we received testimonials by several persons. From the speaker **Max Kilger** we received feedback that the Workshop was well worth his journey from the University of San Antonio in Texas and that he would very much like to participate in any further events organized by the CyberRoad consortium. **Sebastian Schrittwieser**, head of the Josef Ressel-Zentrum for the consolidated analysis of targeted attacks, claims that the work done in CyberRoad and presented at FCCT is of vital importance for the future fight against targeted attacks.

### 5.1 SCIENTIFIC POLICY

All submitted publications were carefully reviewed by members of the program committee for their academic merits, especially taking into account the side parameters and quality requirements enforced by the main conference. This was especially important, since the publications accepted for FCCT are part of the ARES conference proceedings which are published with IEEE. Thus, the papers not only need to be suitable from a technical perspective, but also contain original, previously unpublished material as required for scientific papers in academia. Furthermore, all accepted papers are disseminated by IEEE through IEEE Xplore, therefore being indexed by all major scientific indexes, including Google Scholar, Scopus and Thomson Reuters. The work is therefore easily retrievable and citeable, which is one of the major benefits of publishing the CyberRoad-Workshop contributions with the ARES conference.

All submissions were subject to extensive peer-review, without a predefined drop-out quote or minimum amount of accepted papers, i.e. the reviewers, which were recruited from the program committee, were completely unbiased in their review with respect to organizational details like session sizes or a required dropout rate.

### 5.2 LIST OF ACCEPTED PAPERS

Following we give a list containing the papers accepted for publication in the FCCT. Due to reasons of privacy and probably future copyright, in case they are accepted in another venue, we cannot list the names, titles or even contents of the rejected disseminations here.

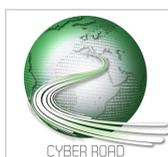
Michal Choras, Rafal Kozik, Maria Pilar Torres Bruna, Artsiom Yautsiukhin, Andrew Churchill, Iwona Maciejewska, Irene Eguinoa, Adel Jomni: ***Comprehensive Approach to Increase Cyber Security and Resilience***, The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism, 2015

Max Kilger: ***Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios***, The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism, 2015

Giorgio Giacinto, Davide Ariu, Fabio Roli, Piotr Kijewski, Bryn Thompson, Jart Armin: ***2020 Cybercrime Economic Costs: No measure No solution***, The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism, 2015

Jart Armin, Paolo Foti: ***0-Day Vulnerabilities and Cybercrime***, The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism, 2015

Davide Ariu, Luca Didaci, Giorgio Fumera, Enrico Frumento, Federica Freschi, Giorgio Giacinto, Fabio Roli: ***Yet Another Cybersecurity Roadmapping Methodology***, The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism, 2015



**o-Day Vulnerabilities and Cybercrime**

*Abstract:* The scope of this study is analyzing the different forms of cybercrime as well as investigating why it seems so difficult to estimate its turnover. In particular, o-day vulnerabilities and ‘o-day threats’ vs ‘o-day exploits’ are examined, also by means of real examples. A brief description of o-day exploit markets - from malware factories to their major customers - completes the overview.



Fig. 4: Paolo Foti and Jart Armin

**2020 Cybercrime Economic Costs: No measure No solution**

*Abstract:* Governments needs reliable data on crime in order to both devise adequate policies, and allocate the correct revenues so that the measures are cost-effective, i.e., the money spent in prevention, detection, and handling of security incidents is balanced with a decrease in losses from offences. The analysis of the actual scenario of government actions in cyber security shows that the availability of multiple contrasting figures on the impact of cyber-attacks is holding back the adoption of policies for cyber space as their cost-effectiveness cannot be clearly assessed. The most relevant literature on the topic is reviewed to highlight the research gaps and to determine the related future research issues that need addressing to provide a solid ground for future legislative and regulatory actions at national and international levels.



Fig. 5: Giorgio Giacinto

**Comprehensive Approach to Increase Cyber Security and Resilience**

*Abstract:* In this paper the initial results of the European project CAMINO in terms of the realistic roadmap to counter cyber crime and cyber terrorism are presented. The roadmap is built in accordance to so called CAMINO THOR approach, where cyber security is perceived comprehensively in 4 dimensions: Technical, Human, Organisational, and Regulatory.



Fig. 6: Michal Choras



## ***Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios***



*Abstract:* The development of future cyberterrorism scenarios is a key component in building a more comprehensive understanding of cyberthreats that are likely to emerge in the near- to mid-term future. While developing concepts of likely new, emerging digital technologies is an important part of this process, this article suggests that understanding the psychological and social forces involved in cyberterrorism is also a key component in the analysis and that the synergy of these two dimensions may produce more accurate and detailed future cyberthreat scenarios than either analytical element alone.

Fig. 7: Max Kilger

## ***Yet Another Cybersecurity Roadmapping Methodology***

*Abstract:* In this paper we describe the roadmapping methodology we developed in the context of the --- EU project, whose aim is to develop a research roadmap for cybercrime and cyber terrorism. To this aim we built on state-of-the-art methodologies and available guidelines, including related projects, and adapted them to the peculiarities of our roadmapping subject.

In particular, its distinctive feature is that cybercrime and cyber terrorism co-evolve with their contextual environment (i.e., technology, society, politics and economy), which poses specific challenges to a roadmapping effort.

Our approach can become a best practice in the field of cybersecurity, and can be also generalised to phenomena that exhibit a similar, strong co-evolution with their contextual environment.

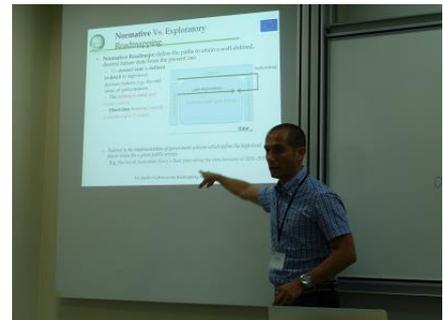


Fig. 8: Davide Ariu



### 6.1 COSTS FOR TRAVEL

All costs for travel such as hotel, train, airplane tickets will be reclaimed by the individual participants, thus SBA Research is not capable of defining the expenses with respect to this issue.

### 6.2 WORKSHOP ORGANIZATION

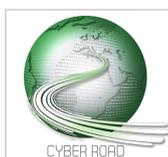
All rooms and services, including catering and social events were provided directly by the ARES conference, thus no direct costs with respect to actual organization can be attributed to the CyberRoad budget. Still, in order to cover the costs of the organization, participating at the ARES conference or the ARES EU-Symposium required the payment of a ticket:

- Authors that present a paper at an ARES-Workshop need to purchase a regular author ticket. This procedure is standard for all ARES-Workshops and not specific to the EU-Symposium or even FCCT. The price for one ticket is 500€.
- Authors that only wanted to participate at the ARES EU-Symposium could purchase either an ARES EU Projects Symposium 1-Day ticket (150€) or an ARES EU Projects Symposium 2-Day ticket (200€). The latter one also included admission to the keynotes and the talks on the second day.
- The normal registration fee without paper was 500€ for this year, which is also applied to workshop chairs.

Since no other financial obligations with respect to workshop organization were needed to be paid by the CyberRoad budget assigned to SBA for Workshop organization, the tickets for all members of the consortium were paid from this budget. This included three author registrations for papers, three full registrations for the chairs and several ARES EU Projects Symposium 2-Day tickets, the latter giving the additional benefit over the 1-Day tickets that the CyberRoad participants could participate at the keynotes, which were especially interesting in the scope of the project, as well as the networking sessions during the next day of the ARES conference.

### 6.3 COSTS FOR CATERING

Catering was provided by the ARES organization and all expenses have been covered by the admission fee. In case of a publication, admission to all social events during the week was included as well. No additional catering costs will be claimed for FCCT by SBA Research.



## 7 ATTACHMENTS

---

Attached to this document are the Call for papers and the poster. It must be noted that due to copyright issues it is not possible to put the full published papers into the public domain, since the copyright was given to IEEE for publications purposes. Thus, the attached papers are only available in the restricted version for the EC.





## 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 10<sup>th</sup> 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 24<sup>th</sup> - 28<sup>th</sup> 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 cyber-crime 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 CyberCrime and CyberTerrorism** 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 cyber-crime and cyber-terrorism 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 cyber-crime and cyber-terrorism. 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)



## **PROGRAM COMMITTEE**

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

## **CONTACTS**

Peter Kieseberg (SBA Research) [pkieseberg@sba-research.org](mailto:pkieseberg@sba-research.org)

# The CyberROAD Project A Research Roadmap Against Cybercrime and Cyberterrorism



## 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.

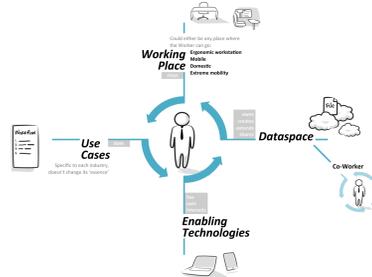


Figure 1: Modern ubiquitous workforces

### Focus

The target of CyberROAD lies in the identification of the research gaps to enhance the security of people and 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?
- ▶ Into 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 cyberterrorism?
- ▶ What are the effects of cybercrime and cyberterrorism on society and the development and acceptance of new technologies?

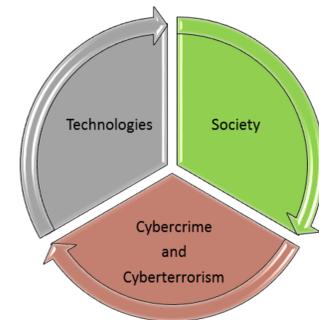


Figure 2: Society, Technology and CC/CT

### 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 "fluid 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 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         | ▶ McAfee S.A.S.       | ▶ Inov Inesc Inovacao                              | ▶ Naukowa i Akademicka siec Komputerowa                     |
| ▶ NCSR Demokritos | ▶ Vitrociset SPA      | ▶ Ministério da Justica, Portugal                  | ▶ Royal Holloway and Bedford New College                    |
| ▶ IVARX Ltd.      | ▶ Indra Sistema S.A.  | ▶ Technische Universität Darmstadt                 | ▶ Informatiksteuerungsorgan des Bundes ISB                  |
| ▶ PROPRS Ltd.     | ▶ Poste Italiane SPA  | ▶ <b>Università degli studi di Cagliari (lead)</b> | ▶ Foundation for Research and Technology Hellas             |
| ▶ SBA Research    | ▶ Security Matters BV | ▶ Ministry of National Defence, Greece             | ▶ Scuola Universitare professionale della Svizzera Italiana |