SecurePART Project

Objective FP7- SEC-2013.7.3.1
Support Action
Increasing the engagement of civil society in security research
Project Number: 608039

D1.10. Conclusions Report

Version 1.0

13 May 2015

1. Change Control

1.1. Document Properties

Deliverable No.		**D1.10**	
Work Package No	**WP1**	**Work Package Title**	**Analyse current CSO involvement in FP7**
Author/s		**Luis Botifoll**	
Reviewer		**Elizabeth Isaacs**	
Name		**Conclusions Report**	
Date		**15 May 2015**	
Dissemination Level		**PU**	

1.2. Revision History

Version	Date	Comments
0.1	**5 May 2015**	**Initial draft**
0.2	**13 May 2015**	**Approved in the Steering Committee ConfCall, pending formal arrangements**
1.0	**15 May**	**Final version delivered**

This document has been produced in the context of the SecurePART Project. The research leading to these results has received funding from the European Community's Seventh Framework Programme under Grant Agreement SEC-2013-608039.

2. Contents

3. Abstract

This Conclusions report present a synthesis of all obtained data and results of the different tasks carried out under work package 1 devoted to the analysis of the CSO involvement in FP7. This report contains:

- A brief presentation of the context and objectives of the study;
- An overview of the methodology;
- A summary of the data;
- The findings, conclusions and recommendations.

4. Brief presentation of the work package 1

In more detail, the results to be extracted from WP1 should provide knowledge for action, by helping CSO representatives, project and programme managers in the EC and in Member States:

- to identify and disseminate towards CSO representatives, decision-makers and opinion formers relevant and evidence-based information on programme achievements and on the value of CSO involvement carried out in security research;
- to improve project and programme design, monitoring, exploitation and dissemination of results through accurate understanding of success and failure factors.

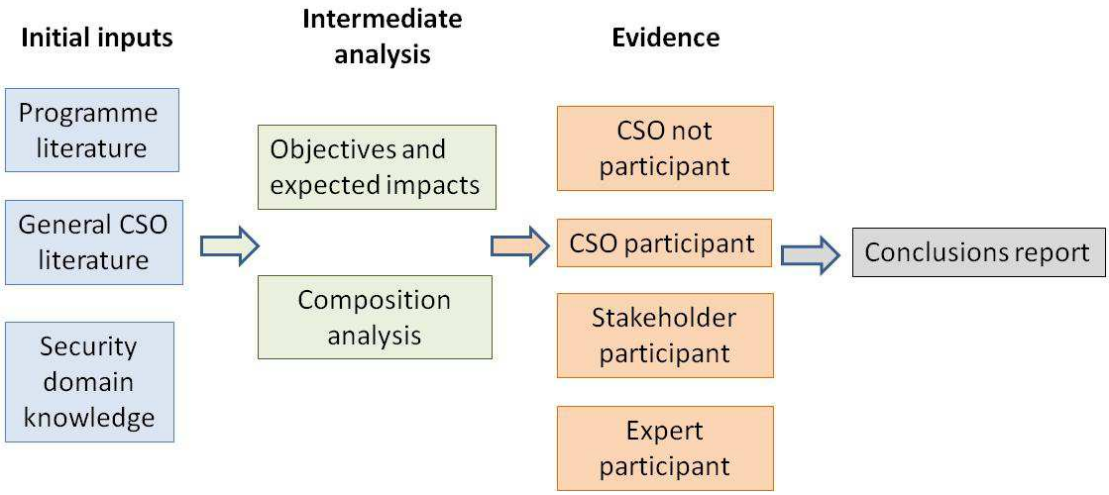


Figure 1: Main steps

The structure of WP1 is based on 3 core elements of analysis to be performed for the formulation of an assessment about CSO participation at programme level: the Objectives Hierarchy analysis, defining Objectives and Expected Impacts and the Composition Analysis. When combined with the Proofs of Evidence, the findings of these analyses are intended to lead to the Conclusions on CSO involvement on overall security research programme level.

Whereas the Objectives Hierarchy is based on literature and the experts' knowledge and expertise

in evaluation, impact assessment as well as on nanotechnologies related issues, the Composition Analysis can also build on the information obtained from the Commission's databases (interim reports, final reports, etc.) as well as on information and insight obtained from the projects' interviews.

The SecurePART project evaluated in its WP1 the efforts done by civil society organisations during the period 2007-2013 in security research. WP1 has assessed how they answered to the FP7 framework, what were their expectations and concerns and which has been their results and impact in society.

The following evaluation tools were used:

- Desk study: policy documents, project deliverables, reports and studies, project websites, etc;
- Internet-based survey conducted among FP7 project participants and members of different stakeholders. The survey was addressed to more 15..000 potential respondents, of those 275 filled in completely the questionnaire;
- 62 Interviews with the different experts and CSO representatives, in order to investigate achieved and expected outputs, results and impacts of their intervention, as well as identify their barriers and problems;
- Expert group support: An advisory Board composed of 8 experts in civil society organisations has provided feed-back and reviewed the WP1 results;
- Six case-studies on the role of communication actions;
- One workshops to discuss with experts, project participants and stakeholders the results obtained.

5. Overview of the methodology

The evaluation methodology used in this project aims at answering evaluation questions focusing the evaluation work on a limited number of key points, thus allowing better reflection on judgement criteria (also called reasoned assessment), more targeted data collection, more in-depth analysis and a more useful report.

This evaluation is pursuing the following objectives:

1. Gathering data and evidence that guided the involvement of CSOs in FP7;
2. Measuring CSO's action implementation and how planned activities have been carried out;
3. Measuring shorter term changes in beliefs, attitudes and behaviour because of the involvement of CSOs in security research under FP7.

The approach followed by the Consortium is based on 4 steps being:

1. Collection: getting the appropriate data to the evaluation;

2. Observation: categorising the data;
3. Appraisal: by applying criteria over the obtained data that will allow our team to identify the important and/or most interesting results obtained through all analyses;
4. Extraction of conclusions.

The main evaluation question has been formulated as follow:

"To what extent have CSOs been involved in FP7 security research?"

This general question has been declined in three sub-questions highlighting the judgment criteria that were used as the main unit of analysis:

Three questions highlighting the judgment criteria used were formulated:

- **Q1. Relevance:** To what extent CSO's activity have been relevant in security research (SR) issues?
- **Q2. Effectiveness:** To what extent CSO's have implemented effective SR activities?
- **Q3. Impacts:** To what extent CSO's activity allowed to change ideas, initiatives or programmes on security research and to establish a shared vision of potential impacts, risks and/or ethical issues associated with SR?

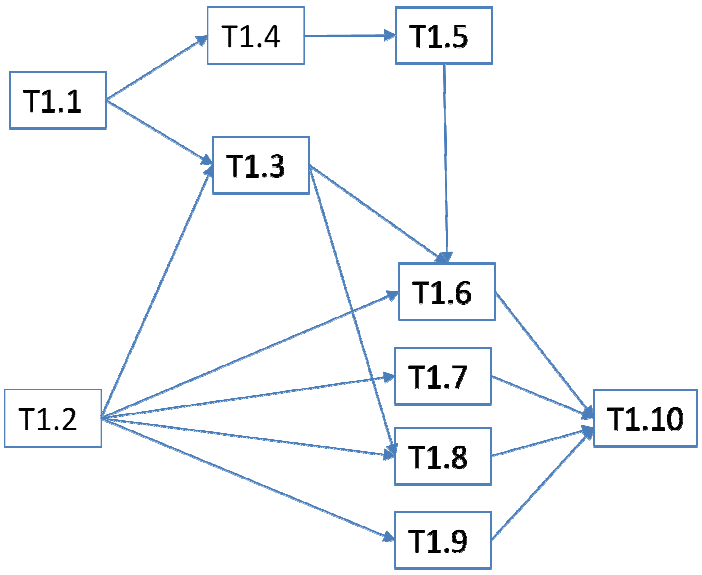
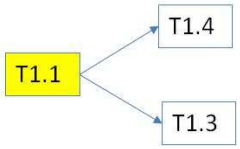


Figure 1: WP1 Dependencies

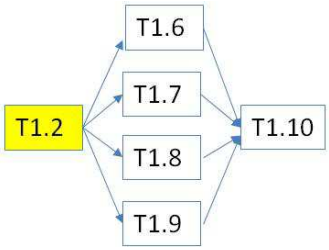
1.1. Criteria/indicators list with definition



This task provided a table of dimensions, criteria, and indicators to be considered when studying the engagement of CSOs in security research. This table will be calibrated, and weighted until the end of the project, complemented by the findings of WP3 (Intra- Inter- and Trans-CSO

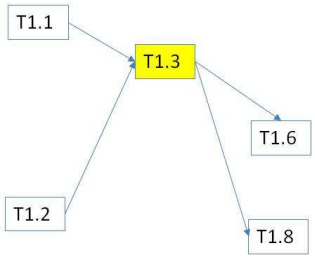
Involvement), and serve the policy objectives of WP5 with regard to increasing CSO engagement in the ESRP.

1.2. Desk-based research



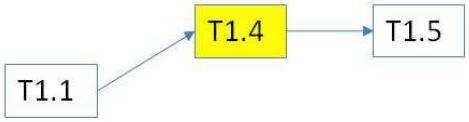
A desk based research took place in order to identify main aspects on CSOs and security research, treated mainly in European projects and other European sources. A review of literature was carried out. The purpose of this review was to gather information about the status-quo and currently followed approaches, major problems and barriers.

1.3. Database building

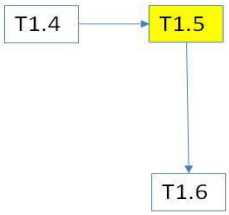


It was decided to carry out a web survey aimed at gathering the opinions of a large sample of people involved in civil society organisations and, in this way, create sufficient content for a database needing specific IT development. This survey was especially addressed to one main target, people associated to CSOs in Europe that may or may not be involved in the last six years in activities related to security, research or both. The survey was addressed to 18.000 people, covering the ENNA network of CSOs at pan-European level. The return obtained was about 1,5%. The web survey was available at www.securepart.eu.

1.4. Sampling



Groups to be interviewed were defined in seven: Researchers, industry, CSOs, academia, public administration, consultancy and facilitators. All stakeholders groups were in this way represented. A decision to focus the attention in CSO representatives was taken: 75% of the total, in its turn divided according to different geographic outreach of the organization and pan-European coverage. The definition adopted of 'CSO representative' included different positions: staff (on payroll or freelancers), elected posts (direction, advisory boards) or active internal collaborators (volunteers). Additionally, a 15% should be researchers and the rest homogenously distributed in the different remaining six segments.

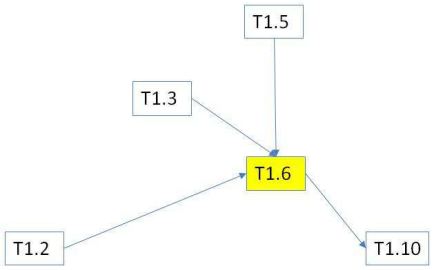


1.5. Interviewees selection

The identity of the interviewees was selected by different means:

- Each of the partners' contacts, according to their previous knowledge;
- CSOs representatives and other stakeholders that participated in FP7 security research (data taken from Cordis and/or previous contact);
- Suggestions from the Stakeholders Board members;
- Respondents of the web survey;
- Suggestions from other previous interviewees;
- Interest expressed to ENNA to be involved in the interviews (based on a previous mailing addressed to all the pan-European network).

1.6. Interviews with CSOs, other stakeholders and experts



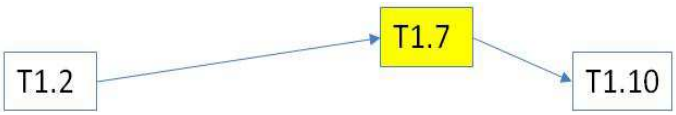
Between October 2014 and March 2015 62 interviews were carried out. Data of the interviews were divided into 5 sections for each interview: implication and knowledge, CSO identity, opinion about CSO involvement and other additional aspects. Seven thematic areas of interest were also identified in order to qualitatively analyse them. Areas subjectively affecting the CSO as an actor:

1. Intra-CSO capability: CSO capacity building aspects;
2. Inter-CSO networking: relationship with other CSOs;
3. Trans-CSO networking: relationship with other stakeholders, not specifically CSOs.

Areas objectively affecting the CSOs as a player in a multi-stakeholder environment:

4. Priorities of security research: topics and themes to be included in new security research programmes;
5. Project participation assessment: evaluation of the experience acquired in projects.
6. Involvement in project execution: description of the activities carried out;
7. Friendly policy/programme framework: transversal aspects (not thematic ones) to be included in new security research programmes.

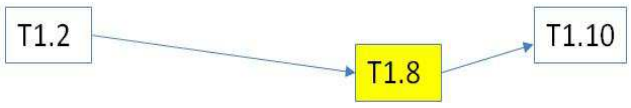
1.7. Case studies:



The case studies were chosen based on the problems identified in the desk research, the results of the web survey, the quantitative study as well as on a consultation that the respective project team had with the Stakeholder Board meeting held in Strasburg which was appointed for assisting and guiding the results and outcomes of this study:

- Selection of CSOs matching security research.- The involvement of CSOs in technology driven security research projects is a new and unfamiliar situation for a research team. Stakeholders usually do not realize the long-term benefits of CSOs involvement in security research projects.
- Analysis of Red Cross participation as CSO in security research projects.- Magen David Adom has participated in various security research projects (FP7-funded research projects: ESS, CATO, CRISMA, ETTIS, OPSIC, EDEN, S-Help and DRIVER) following a long-term strategy. Example of a good practice case.
- Role of CSOs in FP7 Security Research Projects.- Qualitative answer about the general characteristics of EC FP7 Security Research projects compared to other projects as well as about the involvement and role of CSOs in such projects.
- National variations in CSOs' participation in FP7 Security Research Projects.- Evidence about the number and type of CSOs involved in security projects in the EU member states, the national variations and possible influencing factors.
- CSO split personality.- Identification of the the features of hybrid CSOs. Eight elements are proposed in order to determine hybridity of the organizations: non profit making legal form, public interest mission / objectives, common purpose, independence, grass-root origin, open participation, involvement of non-professionalized staff, diversity of members, fundraising activity.
- Acceptance" and "Acceptability" of security-related technologies.- Distinction between "acceptance" that is associated with the factual or expected degree of adoption of a security-related technology *in practice and* "acceptability" that contains a *principle-led* view, as a pedigree of a technology to be responsible in its application, and responsive to the needs and concerns of citizens.

1.8. Concatenation and statistical analysis



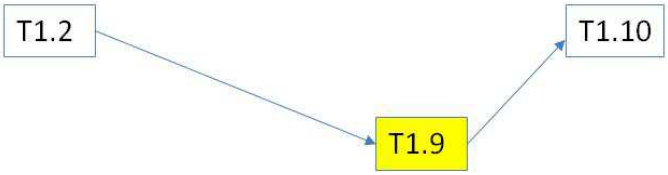
The quantitative analysis of the 275 respondents of the web survey and the 62 interviews carried out only enables to extract some conclusions regarding relevance of the CSO activity. It has not been possible to extract some findings regarding effectiveness or impact of CSO activity.

Some of the conclusions of the quantitative analysis are the following:

- Resources available such as number of employees and budget presents that 91% of the respondents indicate that their CSO is very small or small. CSOs with more than 100 employees and 5M€ are a minority in Europe. Critical mass is a very significant limitation.
- CSOs do not have sufficient resources to be committed in activities that are out of the main aim of the organization. Only large CSOs, with an international or European focus, have enough resources or a specific units devoted to research activities. But this is not a rule as there are very small and small CSOs with European activity focused in research.
- A part of the respondents show they have an interest in security research (52%). A 20% is not sure about their interest, perhaps because they need more information about what it means or how they can be involved in it. 28% of them think that security research is not an interesting aim of the CSO.
- A wide spectrum of fields and technologies where they would like to be involved regarding security research is appreciated. The first concern will be 'individual civil rights' followed by 'minority's rights', 'privacy', 'environmental risks', 'cybersecurity' or 'health risks'.
- When asking about their past involvement in security research during the last 6 years, only a 51% of the respondents remember at least one experience. From them, a 69% had a direct involvement in this activity and only a 31% of them had an indirect relationship.
- Analyzing the periodicity or frequency when this involvement took place, a 25% of them were involved in it in a daily basis. A 31% were usually working with it, 32% in occasional moments and for a 12% was a rare or specific occasion.
- 54% of the activities in security research where CSOs were involved had a European background, 22% of them in a national level, 20% in an international level, and 4% in a regional or local level.
- Most of the CSOs that are involved in security research are medium or large organizations with branches at international, European, national and also at regional or local level. This is why; depending on the focus of activity or project where they are working, they can involve any of the specific levels.
- Regarding the technologies that CSOs are more interested in we can highlight the fact that 100 of interviewees did not know how to answer. In line with the security research fields most interesting for CSOs, crisis management is by large, the most important, followed by infrastructure protection, counter-terror, physical protection or borders.
- The roles that are more usual to be played by CSOs in security research by order or frequency are: observer, actor of research, disseminator of research results, influencer. Also a small percentage of them has worked as users of the research, project evaluators, programme evaluator or commissioner of research.
- Respondents were also asked about the specific disadvantages, internal and external barriers that have to face CSOs. 70% of the interviewees think that CSOs face specific disadvantages in security research compared with other stakeholders, a 60% when dealing with security issues and an 81% opinion is that CSOs should be more involved in security research than they are now.

- If the internal barriers are analyzed, CSOs find more difficult for them to be involved in security research, by order, we find that are staff structure or size of the CSO, CSOs mandates or priorities, inappropriate staff skills, poor involvement of the members and other collaborators and inappropriate plan of the activities to generate interest.
- Regarding external barriers that CSOs face, relationship with other stakeholders is the key factor, followed by a perception of a complex environment and the lack of interest of the civil society in general. This shows that the respondents think the interest in security research should be increased. Relationship among CSOs does not seem to be a significant barrier compared with the rest.

1.9. SWOT analysis



The following table summarizes Strengths, Weaknesses, Opportunities and Threat aspects for CSO engagement:

Strengths	Weaknesses
• Number of projects that have a CSO is relatively high: 35% of the Security projects had CSOs involved; • Involved in almost every issue concerning society; • Have a multi-topic interest, varied societal concerns and technology preferences; • Information gathering → increases legitimacy and effectiveness; • Outreach; number of members/ Networks; • Interest in networking, specially with other stakeholders • Mobilization of people (active members, volunteers, participants); • Society is trusting them/They promote trust.	• Small involvement of CSOs under the period (4,8%, 93 organisations, 129 projects); • Need of critical mass, size and budget, to undertake activity. Only medium and large CSOs have the capacity; • Growing numbers of CSOs, → impossible to keep track/ include all; • Interest going beyond the expectations of the elected managers or staff; • Small transnational activity out of the framework of FP7; • Internal issues effecting transparency, accountability and legitimacy; • Role of CSOs in most of the projects is limited to a role of end user with no real influence on the project execution; • Accompanying conventional roles played: advisor, disseminator • Question how to present evidence; • Effectiveness and impact of CSO

	involvement cannot be measured because of the lack of critical mass; • Communication issues, cannot fully get into the process; • Funding problems/Stability and durability.
Opportunities	**Threats**
• Democratize the system; • Watchdog; • Need of examples, good practices. Experience in other areas; • Involving new methods of participation and the specific schemes; • Need of clarifying definition effort : hybridity and definition problems; • Agenda Setting and setting standards; • Effective Implementation/Valorization; • Evaluate the processes/research/ technology; • Moderator between the government and society.	• Creation of professionalised, service oriented CSO 'superstructures' • Focused on their own particular interest and agenda; • Located mostly in Western/Northern Europe; • Difficult to connect to research topics; • Funding could make them dependent on their donor; • Not democratically accountable for their actions

Table 1: SWOT Analysis for CSO engagement in security research

Contract No. FP7- 607858 FORCE is a project co-funded by the European Commission under the Seventh Framework Programme

www.securepart.eu

www.bantec.es

www.vdlconsult.de

www.enna-europe.org

www.nexusinstitut.de

www.uni-frankfurt.de

www.salford.ac.uk

www.loba.pt