



## SecurePART Project

Objective FP7- SEC-2013.7.3.1

Support Action

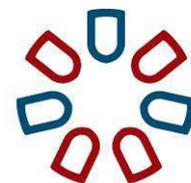
Increasing the engagement of civil society in security research

Project Number: 608039

## D1.8 SWOT Analysis

Version 1.0

13<sup>th</sup> May 2015



**SecurePART**

Increasing the Engagement of  
Civil Society in Security Research



## 1. Change Control

### 1.1. Document Properties

Deliverable No.		D1.8	
Work Package No	WP1	Work Package Title	Analyse current CSO involvement in FP7
Author/s		Elizabeth Isaacs (Bantec)	
Reviewer		Luis Botifoll (Bantec)	
Name		SWOT Analysis Report	
Date		21 April 2015	
Dissemination Level		PU	

### 1.2. Revision History

Version	Date	Comments
0.1	31 March 2015	Initial draft
0.2	15 April 2015	First version circulated
0.3	21 April	Discussed in the Steering Committee ConfCall,
0.4	05 May	Final version delivered
1.0	13 May	Approved in the Steering Committee ConfCall, pending formal arrangements

*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.*

*All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view.*



## 2. Contents

1.	Change Control.....	2
1.1.	Document Properties.....	2
1.2.	Revision History .....	2
2.	Contents.....	3
3.	Abstract.....	4
4.	Specific SWOT analysis of the interviews .....	4
4.1.	Thematic areas.....	4
4.2.	Intra-CSO capability .....	6
4.3.	Inter-CSO networking .....	7
4.4.	Trans-CSO networking .....	8
4.5.	Priorities of security research:.....	9
4.6.	Project participation assessment .....	10
4.7.	Involvement in project execution: description of the activities carried out.....	11
4.8.	Friendly policy/programme framework .....	12
5.	Comprehensive SWOT analysis.....	13
6.	Conclusions .....	23



### 3. Abstract

The document contains a qualitative analysis of the interviews done through a SWOT analysis with the purpose of identifying the crucial points for evaluating the strengths and weaknesses for CSO involvement.

The activity reflected in this report corresponds to the Task 1.9 (SWOT analysis). It takes into account the interviews activity carried out in Task 1.6 (Interviews with CSOs, other stakeholders and experts) and the quantitative analysis done in Task 1.8 (Concatenation and statistical analysis).

This SWOT analysis will be used in the Conclusions Report and the activities related to WP3: intra-CSO analysis (task 3.1), inter-CSO analysis (task 3.2), trans-CSO analysis (task 3.3), identification of CSO priorities related to other key stakeholders (task 5.4) and tap the potential of CSOs to steer future security research planning (task 5.7).

### 4. Specific SWOT analysis of the interviews

Seven thematic areas of interest have been identified in order to qualitatively analyse the 62 interviews held. After the reporting of each of the interviews, relevance of these seven areas were assigned. In this way, all interviews, irrespective of the interviewer can be assessed according to the same criteria. The identification of the thematic areas has been established through keywords added at the end of the interview, by both the interviewer and the task leader.

At this qualitative level, and differently of what has been done in the quantitative analysis, distinction between the answers coming from CSO representatives and independent experts has not been established.

In order to realize this analysis, all interviews dealing with a specific thematic area have been analysed through strengths, weaknesses, opportunities and threats method. Firstly, by the task leader and after in exchange with the different interviewers.

#### 4.1. Thematic areas

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.



## D1.8 – SWOT Analysis Report

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.

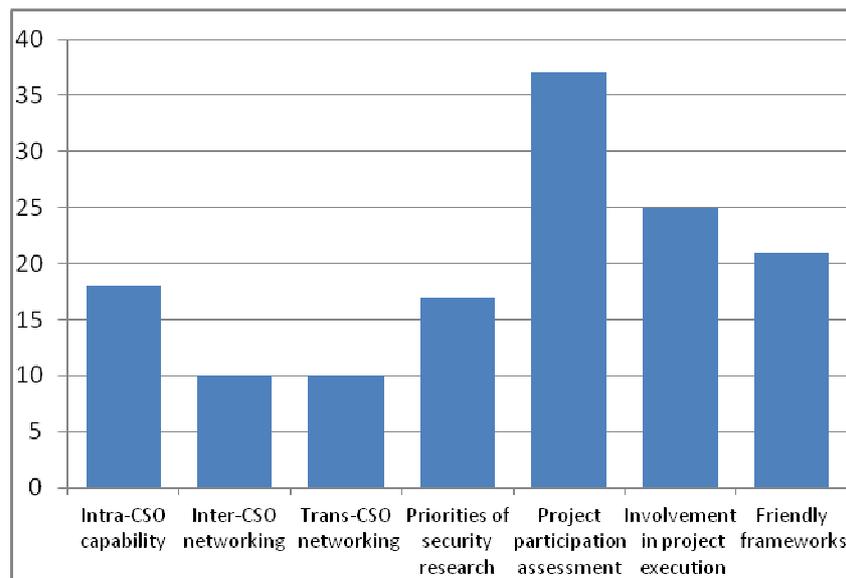


Figure 1: Relevance of the different themes in the interviews

This SWOT analysis will be used in the Conclusions Report and the activities related to WP3: intra-CSO analysis (task 3.1), inter-CSO analysis (task 3.2), trans-CSO analysis (task 3.3), identification of CSO priorities related to other key stakeholders (task 5.4) and tap the potential of CSOs to steer future security research planning (task 5.7).



## 4.2. Intra-CSO capability

A first aspect to which attention is paid concerns the need for CSOs of internally reinforcing their capacity. 16 of the respondents (26%) have considered the issue relevant. Interviews #46 and #57 are specific to the details of internal capacity of CSOs and summarise most of the problems related.

### Strengths

- Only those medium and large CSOs have the focus in the permanent reinforcing of capabilities.
- CSOs have a technical knowledge and an expertise that is often appreciated by the rest of stakeholders.

### Weaknesses

- CSOs are usually small, they work on project-based activities and, because of this, they are not too sustainable and in fact cannot always work on their long-term objectives.
- CSOs are not all the time well-structured and they cannot reach all the information. For example, some processes are too complicated and time consuming, that is why CSOs prefer not to get involved.
- They are reluctant to be involved in unknown or 'uncontrolled' issues. The lack of the necessary human resources is a very repeated comment.
- Only a minority of these CSOs have the knowledge and the administrative expertise related to H2020 to handle this participation.
- Usually, access to his information comes from personal or professional knowledge of the representatives or managers (#25), not directly through a plan prepared by the CSO or as a natural evolution of a previous work carried out by the CSO.

### Opportunities

- For an average CSO, H2020 is more seen as a problematic area, rather than as an opportunity.
- Often, it is seen that an external organization can leverage this role. In this sense, the existence of an umbrella organisation at European level that supports the activity of small CSOs, provides information, give training and advice them (#51) is welcome.

### Threats

- CSOs that improve their capacities become service or consultancy oriented and are losing their identity as grassroots motivated. Professionalization does not go necessarily in the same direction of the preferences of the CSO members.

Interviews analysed	#3, #16, #21, #22, #25, #29, #39, #43, #44, #46, #48, #50, #51, #52, #56 and #57.
---------------------	---



### 4.3. Inter-CSO networking

A second point to which attention is paid concerns the relationships among civil society organizations; this is what has been called as “inter-CSO networking”. Considering the reduced number of respondents (8 of them, a 13%), this is the aspect in which lower interest is appreciated.

#### Strengths

- Inter-CSO networking is perceived as a method for becoming more influential and able to obtain first hand information (i.e. #37).

#### Weaknesses

- Some CSOs need to feel connected among them but this is probably a second step to be taken; firstly, they have to identify by themselves the big concept of security research and what is the particular role they can play there (#47).
- In one case, even a CSO representative said that “they do not have time to network with other CSOs” (#58).

#### Opportunities

- A service point for civil society organizations that ensures this horizontal collaboration among CSOs is in some interviews mentioned as a feasible solution (#52).
- Networking among CSOs that can represent the members interest is seen as a way to obtain more active coordination; to know where, how and what is being researched (#29).

#### Threats

- However, some skeptical also view arise: those umbrella organizations, as 2<sup>nd</sup> level CSOs, will develop its own agendas and interests beyond the individual grassroots CSOs. (#55).

Interviews analysed	#29, #37, #39, #47, #52, #54, #55 and #58
---------------------	---



#### 4.4. Trans-CSO networking

Stable cooperation with other stakeholders (industry, researchers, academia, administration, etc.) not specifically CSOs, raise slight more interest (12 of them, a 16%) than the reduced collaboration only with CSOs; however not with a significant difference.

##### Strengths

- A structured environment (platform, forum) in which CSO participate is usually seen as a very positive scenario.
- The need of reinforcing the links with other stakeholders is a dominant idea as a way of minimizing a prejudice that undermine their potential role as an actor in research.
- In other fields of research there are multi-stakeholder platforms at national and European levels, but none in security (#25). There is a negative specificity in this field.

##### Weaknesses

- There is a very extended comment: “CSOs usually are not invited, no matter how much a CSO would like to be invited”.

##### Opportunities

- Concerning the objectives of a multi-stakeholder platform, it is appreciated by several interviewees but the interest in conducting research activities in conjunction with other stakeholders (from funders to international organizations on the ground, technology developers, etc.).
- Specially in interview #9 it is said that would be possible to develop a multi-dimensional understanding of the challenges that society face, explore potential responses, evaluate their effectiveness and devise means to implement them appropriately.

##### Threats

- However, respondents do not consider all stakeholders at the same level: local authorities (#61) and universities (#38) are preferred as a sort of privileged stakeholders.

Interviews analysed	#9, #21, #25, #38, #41, #44, #46, #54, #55, #56, #58 and #61
---------------------	--



#### 4.5. Priorities of security research:

Discussion about vertical or thematic priorities that may be included in new security research calls or work programmes has been treated in 17 of the interviews (a 27%).

##### Strengths

- Some of the most active CSO have multi-topic interests in research and particularly in security; this aspect can be learned from the experience of Magen David Adom (#7).
- Thematic areas mentioned by the interviewers that can raise the interest of CSOs are varied: health risks, environmental risks, peace, privacy, cybersecurity, individual civil rights, minority's rights, etc.

##### Weaknesses

- Most of the interviewees find difficult to identify topics directly connected with the experience or knowledge acquired by a CSO.
- Give added value in current calls is difficult.

##### Opportunities

- Sometimes, respondents prefer to mention the social problem behind, and not directly its translation in terms of security research; in this sense, the problem of illegal immigration and refugees and the rising of extremism have been mentioned.
- Other non thematic topics concern ethical issues or end user needs. It is even considered from an independent expert that societal impact topics have more presence (what is in the benefit of the participation of CSOs) than those more technologically related (#12).

##### Threats

- It is appreciated that sometimes the responses given are more directly related to the personal interest of the interviewee than of the CSO (#2).

Interviews analysed	#2, #7, #12, #13, #19, #22, #28, #29, #33, #34, #37, #38, #45, #49, #52, #53 and #61.
---------------------	---



#### 4.6. Project participation assessment

Most of the participants (37% of them, a 60%) give an assessment about the participation of CSOs in already executed projects. It is to be noted that sometimes the experience presented is assessed externally (the case of the experts); in some other cases, the respondent gives his/her own experience that is not linked to the current CSO where works; in other cases, the interviewee summarize the overall experience acquired in different projects, etc. The fulfillment of expectations and those met/unmet have been the most popular topic of conversation held with the interviewees. Participation is judged very differently and there is no clear trend among respondents.

##### Strengths

- Among the factors that interviewees consider positive are the usefulness of the involvement of different type of partners, stakeholders from different countries, as they can contribute with different points of view; proactivity within the consortium members.
- Also, some participants point out that the final project results include the technical specifications proposed by the CSO (#54).

##### Weaknesses

- Usually, a bad assessment for project participation is linked to the internal problems of the CSO: problems of funding, lack of experienced resources; and those of the limitations of the CSO: the activity carried out was not central to the aims of the CSO and distracted precious resources.

##### Opportunities

- Not appreciated

##### Threats

- Not appreciated

Interviews analysed	#1, #2, #3, #5, #6, #9, #10, #11, #12, #13, #14, #15, #16, #18, #19, #20, #23, #24, #25, #26, #27, #28, #30, #31, #32, #33, #35, #36, #40, #41, #42, #44, #54, #56, #57, #59 and #62.
---------------------	---



#### 4.7. Involvement in project execution: description of the activities carried out.

The second more popular theme (26 of them, a 42%) in the interviews is concern aspects related to the activities carried out in FP and the roles played in previous projects, irrespective if they took place in the field of security or in other research fields. Even in some cases the interviewee refers about his/her experience acquired in other European programmes out of FP (#60)

##### Strengths

- Reasons for involvement are described in detail for instance in interview #2. They are related to cooperate with other stakeholders (academia, industry, policy advisors, etc.); move from a regional or national level to a global one; and, be associated to new technological developments. The quantitative analysis gives more details to this aspect.

##### Weaknesses

- Interviewees generally see the CSO as a partner, not as a coordinator, in projects. It is noted by some interviewees (for instance #54) that CSOs are just taking an external position to the Consortium in an advisory board, with no funding and no involvement in the workplan.

##### Opportunities

- Roles already played in a Consortium are those expected to be played in the future: mostly related to the accompaniment of project research: conducting desk studies, organizing workshops, participating in inter-stakeholder dialogues; and conferences and other activities of dissemination. Coordination and Support Actions seem to be the appropriate funding scheme.
- Legitimacy of CSOs is specially seen in these complementary activities. Only a minority of CSO representatives mention a more direct involvement in research, i.e. as end-users or commissioners of research (#54) and in other aspects that are not directly related to the project execution (linked to the influencing of the security agenda or the projects evaluation).

##### Threats

- CSOs that are better adapted to participate in European programmes of R&D become service or consultancy oriented and are losing their identity as grassroots motivated. Fitness of CSOs to H2020 does not go necessarily in the same direction of the preferences of the CSO members.

Interviews analysed	#1,#2, #4, #5, #6, #8, #9, #11, #14, #15, #17, #18, #20, #23, #24, #26, #27, #28, #30, #32, #33, #41, #44, #51, #54, #60 and #62.
---------------------	---



#### 4.8. Friendly policy/programme framework

A significant part of the respondents (24 of them, a 39%) are concerned about a more friendly policy/programme framework. There are transversal aspects related to the rules of participation, submission procedure, evaluation, etc. that can facilitate the involvement of CSOs.

##### Strengths

Not appreciated.

##### Weaknesses

- In part, responses were predictable by the interviewers: less and easier procedures in H2020; required administrative work to be involved in FP is too high (#6, #7, #41). Reporting, preparing project proposals, briefings, etc. all these administrative aspects take a lot of time and require human resources focused only on these issues; as for example a CSO needs to do a report of hours employed per person at the level of work package and this is a type of activity that a small organisation cannot support.
- Interviewees compared H2020 with other European frameworks they are familiar in disadvantaged terms (#38, #48) Even, an interviewee (#38) associated a request for smaller projects within the frame of an easier administrative procedure.

##### Opportunities

- A suggestion to split in independent calls those more societal and ethical oriented topics from the rest of the thematic programme of security (#2). The emphasis in the transparency of the topic definition at early stages (#41): “there should be made a better public definition of the processes which lead to the final call, in order to improve participation opportunities of CSOs”.
- Solution: a public debate before the call is made, with potential participants, so that they know ahead and get prepared or improve the call’s requirements”.
- Also, it has been requested by an interviewee an acceptable success rate for the submissions: CSOs are not lazy to apply, but now they perceive they have small chances to be successful. So much energy is wasted in not retained proposals (#48).

##### Threats

- Even with more friendly procedures, CSO involvement is not guaranteed. In grassroots CSOs there is a sort of hostility to have CSO activity framed: “CSO actively seeks an alternative type of relationship (...) CSO was founded by a group of "frustrated individuals". They produced a list of things they liked and things they don't like. They don't want to tender for work, be employed in a traditional client-consultant relationship or undertake research projects that are of little value or interest.” (#61)

Interviews analysed	#2, #3, #6, #7, #10, #11, #14, #17, #26, #29, #31, #32, #35, #38, #41, #42, #43, #46, #48, #51, #53, #54, #57 and #61.
---------------------	--



## 5. Comprehensive SWOT analysis

According to the list of criteria and indicators developed in D1.1 (Criteria & indicators list), a comprehensive SWOT analysis has been developed including results from both the qualitative and the quantitative analysis on CSOs and FP7 participation. This SWOT analysis compiles the information collected from CSOs and other parties and does not express the position of the SecurePART Consortium that will be presented in further deliverables.



## Capacity

CSOs capacity to undertake security research (SR) related activities

	Strengths	Weaknesses	Opportunities	Threats
<b>CSOs' legal structure</b>	Most CSOs have legal personality (as association or foundation)		Permanent basis facilitates continuity of action and long term planning.	
<b>CSOs' durability</b>	Duration is not usually predefined. Open continuity of action is the rule.	Lack of funding for general operational expenses		
<b>CSO functional structure</b>		Small size. Lack of federated services	Creation of common services by a network or federation of CSOs can be considered	Creation of their own agendas separated (specialized, professionalized) from the grassroots CSO in contact with the society
<b>CSOs geographical range</b>	Most of CSOs are local and grassroot oriented, following a bottom-up approach			
<b>Interrelation with CSOs from other territorial levels</b>	Good internalized integration of CSOs	Lack of connection with other non-integrated CSOs.	Interrelation between territorial levels may lead to an easier inter-CSO activity	
<b>Networking with other CSOs and other stakeholders</b>		Lack of connection with other stakeholders.  Limited number of initiatives of stakeholder associations bringing together CSOs with other actors of research		
<b>CSO's material resources</b>	-Important activity in fund raising. Used to look for funding in a plurality of public-private sources	Short-term funding, permanent financial problem.		



D1.8 – SWOT Analysis Report

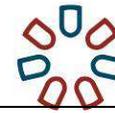
		<p>Mostly, CSOs have limited resources: more than 60% are really small</p> <p>Need to constantly find funding, Problem in the permanence of resources.</p>		
<b>CSOs' personnel resources</b>	Involvement of volunteers, donors or supporters.	<p>Persistent limitation of financial resources in small and very small CSOs.</p> <p>Personnel are working indistinctly in different unspecialised activities: technical, administrative, relations with the members.</p>	Social networks and crowdfunding can support CSO strategies	
<b>CSO's scope of activities</b>	Scope of the CSOs activity is large and is defined. Most of the CSOs have a defined mission and a activities defined.	Sometimes due to budget constraints they have to be involved in activities that are not central to their aims.		

Table 1: CSO capacity



Relevance of CSOs in security research (SR) issues

	Strengths	Weaknesses	Opportunities	Threats
<b>CSOs with concerns that include security and / or research.</b>	<p>The number of CSOs with a theoretical interest in SR is significant (irrespective of their particular involvement under FP7).</p> <p>The specificity of their concern is also varied (from crisis management, infrastructure protection or physical protection)</p>		<p>CSOs can ‘translate into practice’ the mission or objectives they have.</p>	<p>Creation of their own agendas separated (specialized, professionalized) from the grassroots CSO in contact with the society</p>
<b>Concerns in security research are leading CSOs to specific action</b>		<p>Number of CSOs that have current experience in SR is very reduced (93 CSOs under FP7)</p>		
<b>Type of concerns</b>	<p>Orientation of their public/general interest is varied: health risks, environmental risks, peace, privacy, individual civil rights, minorities rights, religious and ethical issues, etc. (irrespective of their particular involvement under FP7);</p>	<p>Number of CSOs that eventually may be involved in SR actions is limited according to their size and budget.</p> <p>Difficulty in overcoming factors that make an</p>		
<b>Type of technologies</b>	<p>Technology fields in which CSOs are interested is also varied.</p>	<p>increased involvement, both internal (improved staff capacity, advisors support, more funding available, better networking or</p>		



**D1.8 – SWOT Analysis Report**

		<p>collaboration with other CSOs and rest of stakeholders) or external (simplified EC procedures, more public budget lines available specifically addressed to CSOs, etc).</p> <p>Concerns are often linked to the personal interest of the managers or staff, not directly connected to the aims of the CSO (internal demand, large societal impact, etc.)</p>		
<b>CSOs collaboration with other stakeholders in SR issues</b>		<p>Networks of stakeholders initiatives in security research involving a plurality of actors (at national, European or international level) is reduced</p> <p>Number of activities (projects, fora, evaluations, etc.) carried out under FP7 in collaboration with other stakeholders is very low.</p> <p>Collaboration established with other stakeholders, if any, is developed in informal frameworks</p>	<p>Creation of common services by an association or platform of stakeholders can be considered, as it is the case for other areas of research (European platforms or social for a can be models).</p>	
<b>CSOs scope of activities</b>	<p>CSO can play a very wide range of activities in SR: influencing, monitoring,</p>	<p>Activities that CSO usually play are tangential to the project, basically as advisors,</p>	<p>CSOs are interested specially in developing a more proactive activity in the</p>	



**D1.8 – SWOT Analysis Report**

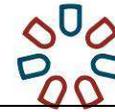
	evaluation, testing, etc. that can be carried out by CSOs in SR (irrespective of their particular involvement in FP7)	in raising awareness or dissemination campaigns, dialogue actions, etc.	monitoring and in influencing the SR agenda as well as actors of research.	
<b>CSOs expectations in becoming involved in SR issues</b>	Type of motivation at the origin of the CSOs involvement is varied: ethical obligation, mandate from the statutes, bottom-up demand from the CSO members, interpretation of civil society demands, request from other CSOs, request from public institutions, request from SR actors, etc.			
<b>Type of engagement</b>	Easy reaction capacity to be engaged in new initiatives.  Commitments can be splitted and managed as independent activities .	CSOs cannot provide long-term commitments if funding sources are not clarified.	Proactively engagement can be provided (by organising projects, by involving top CSO representatives are concerned, having a dedicated budget)	
<b>CSOs have target audiences for their SR activity</b>	CSOs have easier access to large audiences compared with other stakeholders	Difficulty in targeting specialised audience composed by stakeholders (EU/national policy-makers, FP7 programme officers, industrial stakeholders, research stakeholders, civil society, etc.)		

Table 2: Relevance of CSOs activity



## Effectiveness of CSO in implementing SR activities

	Strengths	Weaknesses	Opportunities	Threats
<b>Level of implementation of CSO strategies and plans</b>		Number of activities planned that have been executed is unappreciated. There is a lack of strategic planning Assessment about the completion / success / satisfaction does not take place.	Plan strategic involvement in SR under a long term strategy	Lack of financial resources is underpinning long-term strategy positioning.
<b>CSOs have requested / found the support needed (transparency, invitation to be associated) from governmental agencies and/or technology platforms managing SR issues.</b>		Type of support offered is low: reactive (after initial demand and commitment) and not specialised in SR.	Specific mechanisms can be put in place in order to endure a more proactive support to CSOs from governmental agencies	Evolution towards a model of specialized, top-down, service-oriented and professionalized CSO.
<b>Expected targets have properly been reached according to the different roles</b>	Globally, only in participation in consultation groups (advisory committees) CSO activity can be considered that has fulfilled expected targets.	In most of the roles to be played, CSO involvement is low or very low.	There are successful individual cases of CSOs planning and implementing their intervention in SR: good practices and examples can be useful tools to be	
<b>Adequate activity have been implemented with respect to the concerns and</b>		Only a minority of CSOs have implemented a successful strategy		



**D1.8 – SWOT Analysis Report**

<p><b>expectations of the CSOs</b></p>			<p>employed.</p>	
<p><b>The diversity of viewpoints and perspective of CSOs have been properly addressed</b></p>		<p>CSOs have problems to meet the conditions to express their diversity of viewpoints</p>		

*Table 3: Effectiveness of CSOs in implementing their actions*

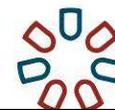


## D1.8 – SWOT Analysis Report

**Impact**

CSO's influence in new ideas, initiatives or programmes on SR. Impact of CSOs to establish a shared vision of potential risks and ethical issues associated with SR

	Strengths	Weaknesses	Opportunities	Threats
<b>As observers, CSOs have been informed and consulted about SR initiatives and these initiatives have evolved;</b>	Special interest exist in CSOs to become more active	Number of regulations in which CSO have taken an active discussion role in direct relation to the implementation of FP7 is unappreciated.		
<b>As influencers, CSOs have been associated in the definition of the SR agenda and their priorities have been taken into account</b>	Special interest exist in CSOs to become more active	Number of priorities (challenges, topics) with a contribution of CSOs under FP7 is unappreciated		
<b>As programme evaluators, CSO representatives have been involved in SR programme evaluation and they have introduced new viewpoints and sensitiveness</b>		Number of programmes /challenges /topics evaluated under FP7 in relation to SR is unappreciated		
<b>As project evaluators, CSO representatives have been involved in SR proposals evaluation and they have introduced new viewpoints</b>		Number of proposals evaluated under FP7 in relation to SR is unappreciated.	Creation of common services by a network or federation of CSOs can be considered	Evolution towards a dominant second level of CSO with no direct contact with society, specialized,



**D1.8 – SWOT Analysis Report**

<b>and sensitiveness;</b>				top-down, service-oriented and professionalized.
<b>As actors of research, CSOs have undertaken SR projects that reflect to some extent the CSO concerns and civil society expectations;</b>	Special interest exist in CSOs to become more active in core SR activities	Number of projects in which CSOs have played a role as actors of research is appreciable (as end user, mainly) but low. Mostly, involvement takes place according to accompanying activities (disseminator, advisor, etc.)		
<b>As commissioners of research, CSOs have requested the collaboration of third parties in SR (research centres, other CSOs, etc.)</b>		Number of projects that are commissioned by CSOs under FP7 is unappreciated.		
<b>As disseminators, CSOs have raised awareness to key targets or lay public on SR hot issues</b>	Number of raising awareness sessions, campaigns or projects in which CSOs have been involved under FP7 is appreciable.	Lack of topics of the raising awareness activities		
<b>CSO assess/register the impact of their activities</b>		Evaluation carried out by CSOs (both formal or informal) is unappreciated.		

*Table 4: Impact of CSOs activity*



## 6. Conclusions

Based on this SWOT analysis, it is seen that civil society organisations poses significant strengths and weaknesses which need to be taken into account for either ameliorating the weak points or for further enhancing the good ones. Significant questions that need to be taken into account as a result of this SWOT are:

- **How can CSOs can maximize the use of the strengths?**
  - Specifically the specific competences they have, the acceptability they can provide to new SR developments, societal acceptance they can contribute to produce with the variety of viewpoints and priorities they express.
- **How can CSOs overcome the threats identified?**
  - CSOs have limitations specially in terms of material resources, limited margin of maneuver due to their financial resources and the unstructured environment with other stakeholders and other CSOs they face in security research;
- **What do CSOs need to do to overcome the identified weaknesses?**
  - Evaluate the creation of new support structures, to be carried out at CSO inter-networking level and at stakeholder level with other actors of research.
- **How can CSOs take advantage of the opportunities?**
  - Exchange of views and analysis can lead to a shared understanding could help to propose some recommendations addressed to CSO themselves and the rest of stakeholders involved in security research.

A very important conclusion of this exercise that needs to be taken into great account when forming relevant recommendations- the main outcome of the SecurePART project in WP5- is the fact that by turning threats into strengths, and matching strengths with opportunities, we could maximize our chances of success.