A CIP-PSP funded pilot action
Grant agreement n°325188

Deliverable	**D6.1.1 – User profiles and categorization**
Work package	WP6
Due date	30/05/2013
Submission date	17/07/2013 (1st version – 1st review) 31/08/2014 (2nd version – interim review)
Revision	1.03
Status of revision	Final
Responsible partner	Engineering Ingegneria Informatica
Contributors	Paolo Rocetti (EII), Barbara Pirillo (EII), Véronique Pevtschin (EII), Wout de Natris (eco), Paolo De Lutiis (TI), Aleš Černivec (XLab), Ulrich Seldeslachts (LSEC), Christian Keil (DFN-CERT Services), Anamarija Soric Custic (CARNet)
Project Number	CIP-ICT PSP-2012-6 / 325188
Project Acronym	ACDC
Project Title	Advanced Cyber Defence Centre
Start Date of Project	01/02/2013

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Version history

Rev.	Date	Author	Notes
0.1	17/05/2013	EII	ToC and first draft
0.2	22/05/2013	ECO	Initial comments to sections 3, 5
0.3	23/05/2013	EII	Contribution to sections 3, 4, 5
0.4	27/05/2013	ECO	Comments
0.5	29/05/2013	EII	Refined section 5.3
0.6 -> 0.9	25/06/2013	CARNet, Eco, TI, XLab, EII	Revision of comments, added contributions to sectors and positioning tables
1.0	26/06/2013	EII	Final revision for circulation
1.1	16/07/2013	DFN-CERT, LSEC	Integration of comments on final revision
1.2	17/07/2013	EII	Submission
1.3	28/08/2013	EII	Submission

Glossary

ACDC	Advanced Cyber Defence Centre
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DoW	Description of Work
EC3	European Cybercrime Centre
ECI	European Critical Infrastructure
EEC	European Economic Community
ENISA	European Network and Information Security Agency
EU	European Union
FS-ISAC	Financial Services - Information Sharing and Analysis Centre
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
INTUG	International Telecommunications Users Group
ISAC	Information Sharing and Analysis Centre
ISACA	Information Systems Audit and Control Association
ISIC	International Standard Industrial Classification of All Economic Activities
ISP	Internet Service Provider
LAP	London Action Plan
LEA	Law Enforcement Authority
MAAWG	Messaging Anti-Abuse Working Group
NACE	Statistical Classification of Economic Activities in the European Community
RIPE (NCC)	RIPE Network Coordination Centre
SCADA	Supervisory Control and Data Acquisition
US	United States

Table of contents

Table of figures

Table of tables

1. Executive summary

The creation of a stakeholders' community is a major contribution to the out-reaching approach proposed by the ACDC project in fighting the botnet issue across Europe. This document is the first one dedicated to the creation and animation of the stakeholders' community, focusing on the overall process leading to the creation of the community and linking back to project deliverables in the context of WP6.

As detailed in section 3, the creation of the ACDC community follows two connected lines of action. The first line focuses on the identification of potential stakeholders, the definition of their relevance with respect to cyber-security in general, and to the botnet topic in particular, and the initial contact to invite them to join the community. A critical aspect for this action line concerns the support ACDC will get from governments of involved EU countries that may strongly influence stakeholders' involvement in the ACDC community. The second line of action focuses on the definition of the community governance, and on the creation of the community platform, used as the main channel for community members to interoperate. In particular, the community governance includes the stakeholders involvement model, that will be provided as input to the stakeholders contact, carried out in the first line of action.

The importance of the governance is to clearly identify and separate different roles that stakeholders can take, including in their relationship and usage of the ACDC clearing house. To specify this relationship, the governance will detail the rights and obligations linked to providing data related to botnets, using / retrieving aggregated data, providing new solutions, using solutions etc. The initial contacts made by ACDC prior to elaborating this deliverable show that the governance issue is complex in relation to both the data and the solutions aspects of ACDC. Therefore, the community building process detailed in D6.1.1 is also important as a preparation step that foresees the future management of this complexity.

Stakeholders categorization is also introduced in this document (section 4). The categorization is based on four criteria varying from general ones, i.e. the country(ies) and Sector(s) where the stakeholder operates, down to Positioning(s) in the cybersecurity field, and to the Interest(s) stakeholders have with respect to the botnet topic in particular.

Finally, the parameters modelling stakeholders' information are described (section 5), as well as the initial set of values for each parameter. The modelling will be used across all phases of the WP6 activities, from the stakeholders' identification process to the customization of the community platform.

Following the first release of this deliverable in July 2013, a second release is made in August 2014. The evolution between the two versions focuses on section 5.5, namely moving from the initial selection of additional criteria to the final selection, based on the experience gained during contacts with organisations with signed letters of intent, the challenges of creating a data sharing environment from a legal point of view and the preparation for the community launch, for which incentive pages addressing separately the profiles in this document have been prepared (see updated release of D6.3.2). In this revision, section 5.5 has evolved from "ACDC potential involvement" to "ACDC interaction channels".

2. Introduction

The ACDC project is a 30 months pilot whose technical goal is to create a set of solutions provided to network operators and to end-users to support the detection, mitigation and prevention of botnets.

However, this technical goal will only be successful if ACDC also acts pro-actively to ensure adoption of the ACDC approach, and the different activities supporting adoption include:

- the creation of a central clearing house, providing Europe with the access to data focused on botnets in Europe
- the spreading of botnet detection and mitigation solutions through 8 national centres spread across Member States
- the deployment of an online platform oriented towards supporting stakeholders in interacting with ACDC

All these steps are therefore oriented towards creating, supporting and animating an active community, and ACDC devotes a specific work package, WP6, to this activity.

As described in the next section, this deliverable constitutes the first deliverable in a set of coherent activities designed to bring the community to life, including:

- the approach adopted by ACDC to create the community: what are the different steps implemented by ACDC partners? How will each partner contribute to this approach?
- the criteria used to classify target stakeholders, ensuring that the community approach is tailored to specific needs and therefore encourages adoption by addressing each sub-group. For instance, tools oriented to the network operators will not be the same as those oriented to end-users; the community platform should reflect this type of difference through user profiles.
- detailed information about the different parameters for the criteria to be implemented in the social community platform

3. Approach to ACDC community building

The aim of this section is to introduce the overall process leading to the ACDC community building. The overall process is shown in Figure 1. Each block in the diagram represents a step in the process, while the links between the steps represent the information that is provided by each step to the following one. The black rectangle in the lower part of the diagram represents a synchronization point for activities 3.4 and 3.5, meaning that activity 3.6 can be started from a stakeholder once the community platform is available (from step 3.5) and the stakeholder has been contacted (in step 3.4).
Also, step 3.6 – Stakeholders starting the joining process is not introduced here as it is part of the community activities that will be described as part of D6.3.1 – Involvement model for users in ACDC.

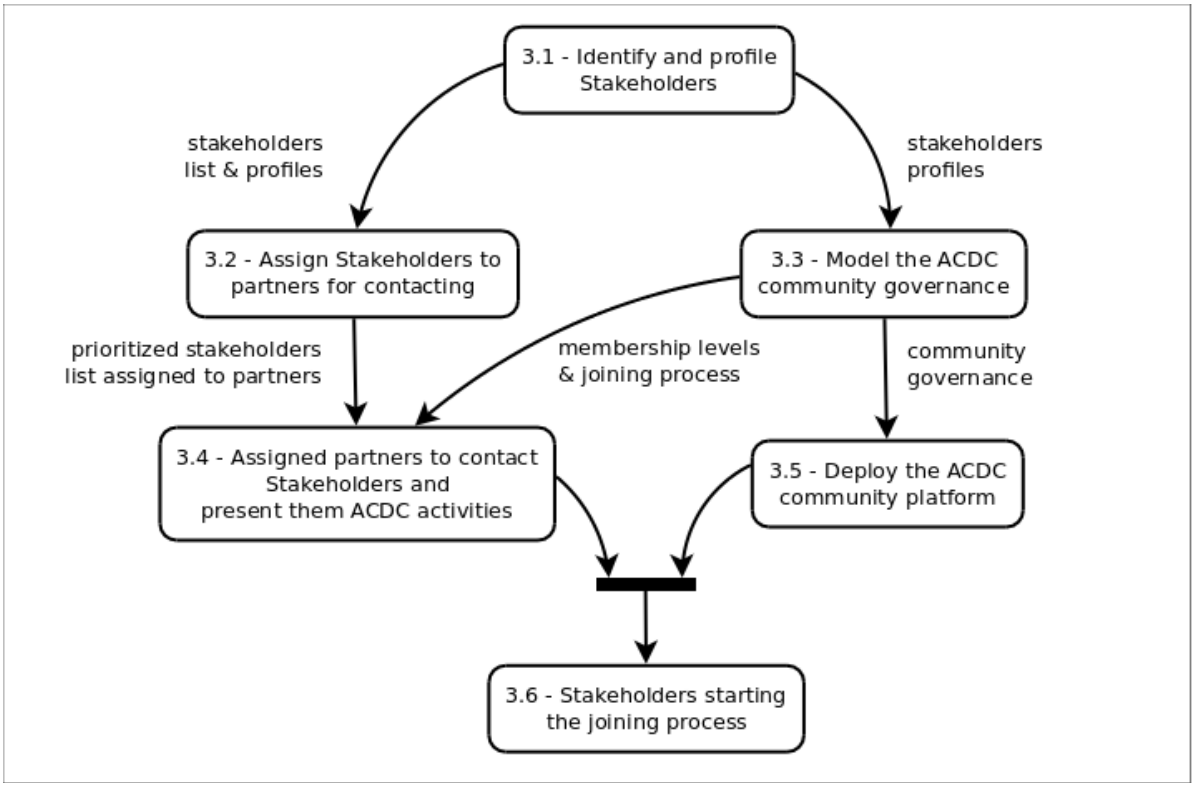

Figure 1 – ACDC Community building process

Another important aspect to highlight concerns the relation of steps in the above diagram with deliverables expected from WP6. Starting from the ACDC DoW, the following diagram shows the relationships among steps and deliverables.

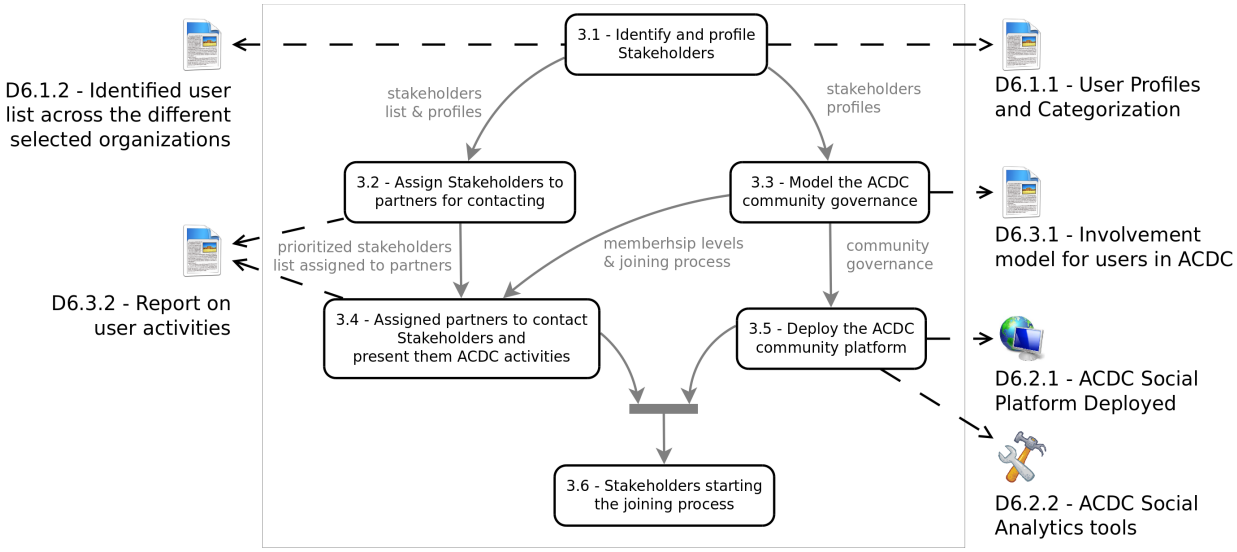

Figure 2 – ACDC Community building steps and project deliverables

Each step of the process is briefly described in a dedicated subsection below. The purpose is to give an overall view of each step, while details about each step will be provided in the related deliverables.

3.1. Identify and Profile Stakeholders

This step aims at defining the parameters to identify and profile stakeholders for the ACDC community. The criteria identified for the profiling will constitute the main content of the present document, where the rationale for the stakeholders profiling, and the profile parameters, together with some sample values, are explained.

This step also includes the creation of an initial stakeholders list prepared by partners involved in the WP6 - User Community Management work package, as described in task T6.1 - User Community profiles and identification[1]. The list of the identified stakeholders, profiled according to the set of parameters defined in this document, will constitute the main content of deliverable D6.1.2 - Identified user list across the different selected organizations.

In order for the community to be useful for ACDC aims, the identification of stakeholders should start from considerations such as to whom does ACDC bring benefits as well as which stakeholders can usefully contribute to increase ACDC's knowledge base, and the involvement criteria that need to be met. While these considerations will be detailed in D6.1.2 - Identified user list across the different selected organizations, they are initially introduced in this document (see section 4), as they have an impact on the stakeholders' categorization criteria.

Since the outreach to potential external partners, as intended by WP6, has already started, expertise and insights are available with regard to initial responses to the outreach activity. This is reflected in the ACDC outreach reports provided by eco [1]. The message that several relevant national stakeholders give to ACDC points to the fact that they see national governments and the EU as the most important partners for ACDC. An active support is needed for the central clearing house, and to a somewhat lesser extend the national support centres, to become a success. A national government should decide to make ACDC a national priority, e.g. by adding to the national cyber security strategy, by bringing relevant and necessary stakeholders together, by granting resources for and giving priority to this work, by providing relevant training, etc.

[1] See ACDC reports on EC3 at Europol 27-5-13, Interpol, 22-5-13, MinEZ, 24-5-13 and LAP, 16/17-4-13

The support that ACDC will get from national governments is therefore of primary importance for the ACDC outreach. This has been reflected in the first of the stakeholders' categorization criteria and parameters in sections 4 and 5 of this document.
Concerning international initiatives, EC3 at Europol has decided to make ACDC a top priority, with all the assistance needed towards national police agencies. The support from EC3 is subject to the delivering ability of ACDC (i.e. deliver data that makes it possible to catch criminals and/or shut down their operations within the EU). This offer makes EC3 automatically a top priority for ACDC.
What the outreach reports also show is that it is currently difficult to actively involve governmental agencies for several reasons, even if their participation would be very valuable for ACDC purposes. The latter point is the reason they have to be taken into account in defining stakeholders categorization; the first point means that this category would score low(er) in the stakeholders assignment to partners made in the next step (3.2).

Another element that emerges from the initial set of contacts is that the roles related to data (providing data related to botnets detected by one or more stakeholders) to a central clearing house can be complex and will, in many cases, require a one-to-one partnership. This element will be addressed in the governance document, but also influences this deliverable in characterising stakeholders in terms of whether they have access to data, they are interested in providing this data and what would be the constraints on this sharing.

3.2. Assign Stakeholders to partners for contacting

As the resulting list of identified stakeholders will likely be large, stakeholders will be prioritized based on a set of criteria defined as part of the D6.1.2 deliverable. The aim of the prioritization is to define an ordering in which the stakeholders will be contacted to introduce them to ACDC topics and activities (see next step). Also in this step each stakeholder will be assigned to one of the identified partner, which will be in charge to contact the stakeholder as described in the next step. The assignment avoids duplication of the work and confusion for stakeholders that could arise as a consequence of multiple concurrent interactions. The criteria for assignment will also be defined in deliverable D6.1.2.
In assigning stakeholders in outreach activities to potential partners or participants it is important that each, where possible, is active in its own environment, but that all present the same basic story line added with unique arguments towards the specific targets.
At the international level ACDC will most likely be looking for existing stakeholder infrastructures and ask to be invited to these stakeholder group meetings. Only where these do not exist ACDC needs to take the initiative itself, provided that this stakeholder (group) scores high enough to take this action or ask assistance, e.g. from DG Connect, ENISA, Europol, etc.
At the national level this could be harder to achieve. It is also likely hard for an ACDC partner working only at the European level to identify stakeholder groups in one country both for reasons of language, and for not knowing the country well enough. The lead role in these cases is probably better held by national ACDC partners.
As there are many different stakeholders within a country, it is advised for the ACDC partner to contact the relevant partner(s) in the national government. Active support of the government may be a guarantee towards success. This could lead to the organisation of one national meeting bringing all different stakeholders together, in which ACDC contributes with experts presenting. After that, when interest is made known within a country, one on one talks of the national support centres with potential national partners are made possible and ACDC withdraws, at least as leading, from a reach out point of view.
Where international outreach generates national interest, it is necessary that national support centres know of this interest so they can follow up and become leading in second level reach out.

3.3. Model the ACDC community governance

This step aims at modelling the ACDC community governance starting from the stakeholders' profiles already identified.
Governance is a major component of the ACDC community; starting from the benefits and goals of ACDC, the governance is designed to clarify how the community members interact, how information can be accessed and delivered, etc.
Community governance includes, for instance, the processes for stakeholders to join/leave the ACDC community, the membership levels that will be available, the community structure, as well as the organization of community bodies and activities. This information will be used both to implement the ACDC community platform, and as additional input during the contact between partners and stakeholders (see next step). An important aspect to be taken into account in modelling the community governance is related to the sustainability of the community after the end of the ACDC project. Clearly, the sustainability of the community is closely linked to the sustainability of the overall ACDC outcomes (solutions, centres, ...), that will be part of the D5.3-Sustainability Plan, expected by the final stage of the ACDC project. Therefore, the community governance will be designed to be open with respect to the sustainability mechanisms defined at a later stage. This will be done in particular by allowing different levels of involvement in the community that could be later linked to the sustainability mechanisms from D5.3. The outcome of this work will be part of deliverable D6.3.1 – Involvement model for users in ACDC.

Beyond these community oriented features and as mentioned earlier in this document, the governance will also tackle the aspects related to the provision, usage and aggregation of data as well as the use of the clearing house as a channel for new solutions. Elements in the "solutions" dimension include for instance the fact that a provider could make a solution available freely as a fully-featured but time limited trial through ACDC or as a more limited version with a mechanism for the user to move to acquiring a full version on a commercial basis from the original provider.
It is important that these mechanisms be well established to guarantee a win-win situation for all stakeholders, as without these the sustainability of ACDC will be at risk for lack of valuable and up-to-date content.

3.4. Assigned partners to contact Stakeholders

In this step we select and assign which partner(s) is/are in charge to contact specific (groups of) stakeholders and present to them the ACDC topics and activities. At that time, stakeholders will also be informed about the level of membership and involvement (as defined in the previous step) they can choose when joining the ACDC community. The result of this work will be reported in deliverable D6.3.2 – Report on user activities.
At an international level, actions are different from those at national level, as explained in section 3.2. In particular, considering the very large number of potential stakeholders for the ACDC community, at least in the starting phase of the project, priority should be given to stakeholder groups that gather multiple stakeholders, e.g. EU financial ISAC, MAAWG, RIPE, LAP, etc. It is important to understand that these groups are mostly informal gatherings of individual stakeholders. Some have a budget to organise meetings, some don't, but a common characteristic is the lack of a formal command chain, the absence of decision powers and participation is mostly voluntary. For this reason the involvement of stakeholders groups should go through an initial phase that is more oriented to introducing the ACDC topics and listening for current activities and questions, instead of asking for immediate decisions or actions from the groups themselves. In this initial phase it is important to be there, to present and listen very carefully to comments made and questions asked. Also you have to be prepared to ask questions. This phase also allows

ACDC to understand the interests of individual stakeholders within those groups, and to better plan ACDC activities in order to come back with results during subsequent interactions with those groups.
When reporting on the presentation it is very important to be as precise as possible in arguments used, reservations that were formulated and mention activities or present initiatives that could be of interest for ACDC to associate with in the future. Also, we need to clarify what are the challenges we can address and present a solution for, and what are true obstacles. Also when the obstacles are impossible to cure for ACDC, we need to formulate them precisely as they have to be passed on to relevant stakeholders outside of this project, e.g. the European Commission for potential further actions.
At the national level it is important to be one on one with most stakeholders. There are a limited number. They need to be identified and targeted, either individually or as group. E.g. are the banks and critical infrastructure organised, the ISPs, the hosters, etc.? Police, regulatory, relevant government bodies are individual targets.
In the end partners and participators become involved on an individual basis; attracting their attention are mostly collective actions.

3.5. Deploy the ACDC community platform

In this step the community platform will be deployed and configured to support the community governance defined in step 3.3. The platform will be initially tested internally by the consortium and later on opened to external stakeholders for joining.
The platform will be designed to support community activities by easing the retrieval of information about community members, their topics of interests, role, and current activities in the cyber security domain. Moreover, the platform will enable fast and effective information sharing among members, by providing functionalities that allows for a fine-grained selection of communication targets for messages. This will result in increasing the effect of each message, while reducing at the same time the waste of time due to the reception of irrelevant messages. It will also support specific activities (e.g. surveys, feedback from adoption of ACDC solutions, etc.) that will be defined as part of the task T6.3- User Community governance and animation[1].

In addition to the role of the community platform as described in the ACDC Description of Work, the consortium is currently analysing extending this role to position the community platform as the single front-end to also control the access to the clearing house. The idea is to reinforce the interest of the community platform as an access point, but this increases the complexity of the approach as a fully-fledged authorisation mechanism has to be integrated in the platform. This element is currently under analysis and will be reported in D6.2.1.

4. Stakeholders Categorization Criteria

This section introduces the Stakeholders categorization criteria. The aim of the categorization is threefold. Firstly, it creates, among the consortium, a shared vocabulary and a common understanding of the terms and concepts related to the stakeholder's identification processes. Secondly, it allows the analysis of the ACDC community composition and behaviour from different points of view. Thirdly, it impacts the modelling of the ACDC community governance and, later on, the development of the related community platform. Therefore, the stakeholders' categorization criteria are of primary importance for the activities and for the success of WP6 work package. In particular, four categorization criteria are introduced in this section.

> Note on the direct involvement of citizens in the ACDC community:
> Given the potentially very large number of end users for some of the ACDC solutions (i.e. "multipurpose tools for end users" and "support centre") their direct involvement in the community could be problematic. Instead, we propose to limit community membership to organizations only, and involve citizens through citizens associations. These associations will be in charge of representing citizens within the ACDC community and participate to the activities. Moreover, the project could use the citizens' associations capacity to reach a large number of citizens to increase the spread of ACDC solutions among the population.

The criteria introduced below vary both in purpose and in scope, ranging from the most general ones (*Country* and *Sector*), to the cybersecurity field (*Positioning*), down to the botnet topics that are covered by the ACDC activities (*Interest*). For each criterion the related parameters and corresponding values are introduced in section 5.

4.1. The *Country* criteria

The definition of the categorization criteria starts from considerations about the types of stakeholders that are particularly relevant for ACDC project activities. Firstly, considering the European dimension of the ACDC initiative, it is important to understand how the different countries are involved in the fight against botnets.

In this context, it is important to diversify between national-level stakeholders and international, European-level, ones. The way ACDC is positioned at present, by distinguishing between National Support Centres and the European Data Clearing House, calls for this difference. Therefore, a *Country* categorization criterion is important to highlight differences on the way how stakeholders may interact in the community. For instance, stakeholders at national level could mainly interact with national support centres of the country they belong to, while European-level stakeholders could be more interested to interact with European-wide entities, like the ACDC Clearing House or Signal Spam.

The *Country* criterion has an impact on the stakeholders' identification process as well, in particular at national level, where national support centres could be foreseen as one of the main contributors for stakeholders identification and involvement.

Whilst for the first year of the project ACDC only focuses on involving EU/EEC partners and participants, this does not preclude the voluntary participation of partners outside the EU/EEC. Based on the results of the first year of activity, in the second year the project will evaluate the extension to non-EU/non-European partners presently working on botnet mitigation and/or online threats.

4.2. The *Sector* criteria

The proposed European cybersecurity directive[3] aims at addressing security of critical infrastructures in the societal dimension. To this aim the directive pushes for rules and obligations that will reduce the risk of cyber attacks and improve reporting of cyber incidents. Whether or not the proposed directive will be approved, the concept of having common understanding of the cybersecurity context, as well as adopting the same rules and obligations for all critical infrastructure players, regardless of the sectors where they operates (finance, energy, etc.), is a valuable approach.

Of course, once we move from the higher regulations level down to the processes and their implementation, differences will likely be found from sector to sector in the way how rules are applied and obligations must be fulfilled. This mainly because business models, common ways of operations and interaction and systems are different from sector to sector, thus leading to a different definition of solutions for the constraints imposed by regulations (either be the proposed directive or the existing ones, where/whether they exists)

The difference highlighted above also introduces a difference in the kind of vulnerabilities that may affect players from different sectors, that also may reflect in different ways of exploiting these vulnerabilities, or instance by a botnet. For this reason the introduction of a Sector criteria that categorizes stakeholders basing on their sector(s) of operation is valuable for the ACDC community.

Such a sectorial categorization will has many advantages, mainly, partitioning stakeholders basing on sectors allows the project to understand the main cybersecurity concerns for each sector, thus enabling the identification of which set of solutions better fits the needs of each sector. Moreover, the targeting of communications and interactions to the set of stakeholders operating in a given sector

The initial list of Sectors identified for stakeholders of the ACDC community is introduced in section 5.2. The current list is derived from the sectors initially identified by the ECI Directive proposal [7], which have been reduced to two sectors (Energy and Transport) in Appendix I of the final version [3]. This list will likely be subject to changes and additions once the set of potential stakeholders will be identified as part of step 3.1 (see Figure 1 and section 3.1)

4.3. The Cybersecurity Positioning criteria

The *Positioning* criteria refers to the positioning of the stakeholder with respect to the cybersecurity field. The present picture in the cybersecurity landscape is complex and subject to changes. Moreover, most of the actors in cybersecurity usually play more than one role (e.g. an ICT company acting both as ISP and mobile operator, and also running its own CSIRT).

For this reason the Positioning criteria has been structured in an initial list of positioning areas (Operational, CI Operators, Research, Policy Makers, Providers, etc.), that groups the possible positioning(s) each stakeholder can have in the field (ISP, CSIRT, LEA, Initiative, national government, etc.). The areas and the positioning values inside each one, are not seen as static, but are likely to evolve during the stakeholders' identification step, or even later on, following evolutions of the cybersecurity domain.

The initial set of areas and values can be found in section 5.2 below. These also take into account the target categorization already introduced in D5.1.1 – Dissemination Plan, even if those targets are defined for the broader audience reached by the dissemination activity.

4.4. The Botnet Interests criteria

The *Interest* criterion refers in particular to the interest of the stakeholder with respect to the ACDC activities and solutions. This is important to analyse how the interest of the community is linked to botnets and related issues. In particular, this criteria could evaluate the level of interest (and the possible involvement) of the stakeholder with respect to (i) the ACDC solutions, (ii) the ACDC experiments and (iii) other ACDC activities (conferences, workshop, ...).
This diversification will differentiate between potential funding as opposed to just participation. Most likely this calls for very different approaches. E.g. police agencies are important to have on board, but will in all likelihood never fund ACDC. So the criteria for gathering secondary interest in full partnership are different from participation. They go passed interest in free data (analyses), so have to concentrate on problem solving and offered solutions. Hence, we need to concentrate on/know what it is these potential full future partners are looking for. We need to have a set of questions ready to put to potential full partners (and participants), in addition to the criteria we can come up with ourselves when reaching out to them.
Concerning in particular the involvement in experiments, we need to focus on a very limited number of partners for the experiments. Reach out activities so far show that response on participation requests formulated at a general level is low. Most agencies have no idea, limited knowledge and/or resources or are just overwhelmed. By selecting and directly inviting pre-selected partners and providing more detailed information in terms of specific benefits, it is possible to work one on one with them, actively get input and assistance in setting up the experiments and receive feedback during the experiment.
Another valuable aspect for the community would be to distinguish among potential adopters vs. providers of a solution. The same applies to data that relates to a solution or experiment. For instance, knowing that a *Critical Infrastructure* is *Interested* into a solution available in ACDC, or into results of an experiment can also create an interest of both the research communities and the IT providers to base their research and evolutions on data sources collected in European contexts.
Finally, stakeholders might be involved or Interested into a specific activity or even a specific single task of the ACDC project (e.g contributing a document, organising a conference, organising a workshop, etc.).

4.5. The ACDC potential involvement criteria

This criteria prepares for the future work on the governance. It will be further analysed as to whether it remains a single criteria or evolves into multiple one in D6.1.2.
Its goal is to identify at this stage stakeholders who have access to botnet related data (for instance ISPs detecting on their networks etc), willing to provide data, interested in accessing data, requiring one-to-one partnerships for data sharing, providing new solutions at trial level etc.
The granularity of this criteria will be further refined during the out reach activities, as the initial contacts have shown an increasing but sometimes diverging availability of information.

5. Stakeholders profiling

Based on the Stakeholders categories identified above, this section focuses on identifying the parameters that will be used for stakeholders profiling. The purpose of the profiling is functional to the ACDC community building needs. These needs mainly relate to the activities described in section 3, and should lead to a profiling that is useful in assigning identified stakeholders to partner, and in the modelling / deployment of the ACDC community platform. Starting from these considerations, the following parameters are identified for the stakeholders profiling.
It is worth noticing that parameter values introduced here are not exclusive. Most of the stakeholders will likely be assigned to more than one value for each parameter. For instance, considering again the example from section 4.3, an international Telecom operator could act both as Internet Service Provider and as mobile operator, running its own CSIRT and also selling security solutions. Such a stakeholder will be associated to multiple countries of the *Country* criteria, as well as to multiple values of the *Positioning* with respect to the cybersecurity domain (as it belongs both to the Operational and to the Provider areas).

5.1. Organization information

The Organization information distinguishes among stakeholders that are relevant for the ACDC community. This information is used in multiple steps during the ACDC project, starting from the collection of information about potential stakeholders, see section 3.1 of the ACDC community building, to the stakeholders contacting phase, see section 3.4, down to the modelling of stakeholders in the portal, and, finally, during the interaction of members in the community. For this reason it is important to have a common modelling and understanding of stakeholders' information. This section introduces the parameters that are used to model stakeholders (either potential ones or actual ones) of the ACDC community.
With this respect, the possibility for sharing stakeholders' contacts information (such as name, surname, email, etc.) across the consortium is of particular importance. The sharing of such information across consortium partners poses two main problems. The first one relates to the privacy of the person whose contact details are shared with third parties (i.e. other consortium partners). From the current data protection directive[4] and its adoption by EU countries, the sharing of personal information requires the informed consent of the subject that is difficult to obtain and manage in the initial phase of the project. The second problem is related to the protection of business contacts, that usually represents a valuable asset for each partner. This is even more important when considering that some of the partners (e.g. telco operators), can be competitors with respect to the stakeholders they identify as relevant for the ACDC community.
For the reasons above the sharing of information will be limited to organizations details (listed below) and to the position (i.e. the role in the external organization) of the person who constitutes the physical contact a partner has in the external organization. Furthermore, the presence of a physical contact in the external organization is not a prerequisite for a stakeholder to be identified. This because a partner may identify one or more stakeholders whom he is not in direct contact with (or not yet), but may be of evident relevance for the ACDC community.
The table below shows the set of parameters that will be used to identify stakeholders for the ACDC community.

Parameter Name	Parameter Description	Notes

Organization name	Organization Legal Name	This field is mandatory.
Organization address	Organization Legal Address.	This field is mandatory.
Organization scope	The scope of the organization, either national or European. This parameter derives from the Country categorization from section 4.1.	This field is mandatory. It indicates that an organization operates at the European scale and has no particular linking to one or more countries of the EU.
Country(ies) of operation	The set of countries where a national organization is operating. This parameter also derives from the Country categorization from section 4.1. The initial set of options for this information will include EU countries only.	If the Organization Scope is national, one or more countries must be specified for the organization. This parameter is empty for European organizations.
Website	The website of the organization	This field is optional. This allows to identify "just-born" organizations that do not have their website online yet
Contact work positioning	This is the working positioning of the contact in the organizational chart. To avoid dealing with details of each organization's chart, the choice is limited to the following positions: • *Top Level* – e.g. owner, CEO, etc. • *High Level* – e.g. director, general manager, etc. • *Middle Level* – e.g. young manager, project coordinator, etc. • *Entry level* – e.g. junior worker, specialist, etc.	This field is optional. In case more than one contact is known in the organization the most relevant one (usually the higher in the organization's hierarchy) should be indicated.

It is worth noticing that from the set of parameters introduced in the previous table the Scope and Country ones are those derived from the categorization criteria from section 4. Other parameters introduced in the table above are used only to distinguish stakeholders among each other, but does not takes part to the categorization.

5.2. Sector Information

As described in section 4.2, the Sector criteria aims at identifying the domain in which the stakeholder is operating.

A number of taxonomies have already been introduced, and are currently used to classify companies. Some examples are the NACE (Statistical Classification of Economic Activities in the European Community) from Europe and the ISIC (International Standard Industrial Classification of All Economic Activities) from U.S. These classifications may be based on different criteria ranging from production, to market, to legal nature of the company, etc. A list of classifications can be found at[5].

The main consequence in adopting one of these fine-grained taxonomies is the very detailed classification that we obtain for the ACDC stakeholders. Having such a detailed partitioning is not

so important for the ACDC community, as the intention here is not to classify the whole market, but instead to provide a coarse-grained indication of the critical sector where stakeholders carries out its activities, and therefore promote its interaction in the community to other stakeholders from the same sector. For this reason the classification that has been created for the sector criteria mainly derives from the one initially introduced in the ECI Directive proposal. The main reason to not limiting to the sectors in the final ECI Directive[3] (energy and transport) is the need to involve in the community also stakeholders from other sectors (health, finance, etc.).The current set of sectors for the ACDC community is listed below, with a short description for each one:

Sector	**Description**
Energy & Nuclear Industry	Oil and gas production, refining, treatment, storage and distribution by pipelines; electricity generation and transmission; production and storage/processing of nuclear substances
Information, Communication Technologies, ICT	Information system and network protection; instrumentation automation and control systems (SCADA, etc.); internet; provision of fixed telecommunications; provision of mobile telecommunications; radio communication and navigation; satellite communication; broadcasting
Water	Provision of drinking water; control of water quality; stemming and control of water quantity
Food	Provision of food and safeguarding food safety and security
Health	Medical and hospital care; medicines, serums, vaccines and pharmaceuticals; bio-laboratories and bio-agents
Financial	Payment and securities clearing and settlement infrastructures and systems; regulated markets
Transport	Road transport; rail transport; air transport; inland waterways transport; ocean and short-sea shipping
Chemical industry	Production and storage/processing of chemical substances; pipelines of dangerous goods (chemical substances)
Research facilities	Research facilities
Security services	Police structures and equipments; military structures and equipments

Tabella 1 – Critical Infrastructure sectors

It is worth noticing that the cardinality of the association between a given stakeholder and sectors may vary from *0* to *n*, meaning that there could either be stakeholders not associated to any particular sector (e.g. university doing primary research in security), or stakeholders that are associated to more than one sector (e.g. an electricity and gas distributor, like ENI, www.eni.com). Also, the previous list of sectors may be subject to changes depending on the list of ACDC stakeholders that will be identified as part of deliverable D6.1.2.

5.3. Cybersecurity Positioning information

Section 4.3 introduced the need and the rationale for the categorization of stakeholders with respect to the cybersecurity field. The purpose of this section is to present the parameter that is used to model the Positioning of stakeholders. To this aim, the cybersecurity field has been partitioned based on the different kind of information and activities with respect to a cyberattack. The partitioning identified five different areas that have been further divided to distinguish the kind of organizations that can be associated to each area. The following diagram shows a view of the current partitioning.

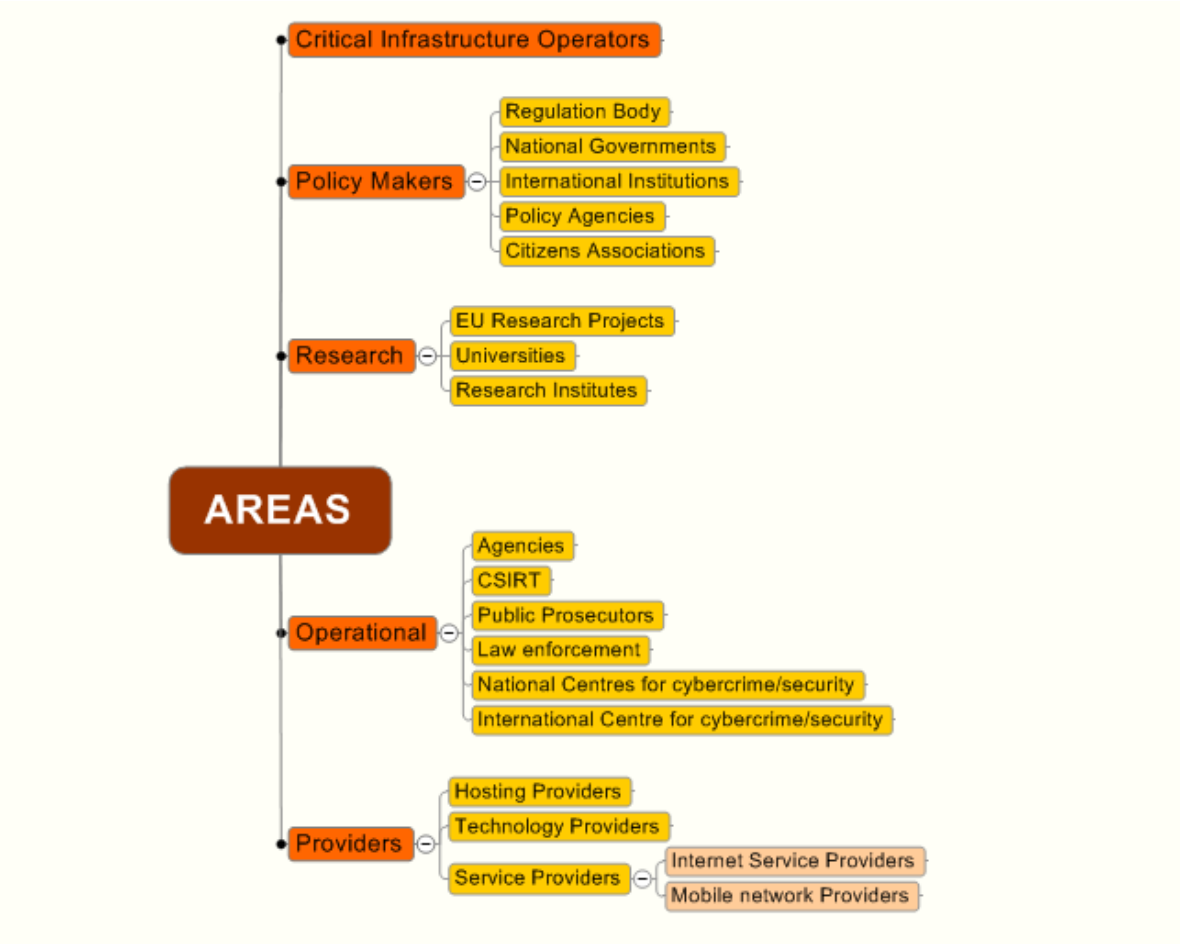

Figure 3 - Identified Areas for the Stakeholders Positioning

Each of the positioning from the previous diagram is briefly introduced in the following table.

Value	Description
Critical Infrastructure Operator	Operator of a Critical Infrastructure, where "'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"[3]. Note that the sector in which the Critical Infrastructure Operator actually operates is defined by the value(s) of the Sector parameter.
Research	A single (e.g University, Research Institute) or a temporary grouping of organizations (e.g. EU research projects) conducting research related to the cybersecurity field. This category groups stakeholders whose main interest is to find new solutions, instead of creating and maintain applications & services for the existing ones (see Providers below).
Policy Makers	Policy makers are those dealing with regulations related to cybersecurity. Stakeholders associated to this area aims at defining (or contributes to) rules promoting and supporting other stakeholders in fighting cyberattacks. Regulation Body and International Institutions

	Relevant European, National or local authority, agency or body, that is involved in, or closely related to, the definition of regulations impacting the cybersecurity field (i.e.: ENISA and ICANN, RIPE (NCC), IETF, MAAWG, IGF, ...) Citizens' Associations Represents citizens directly interacting with the solutions ACDC proposes to end-users. (see note in section 4 about citizens' involvement in the ACDC community). National governments Relevant ministries dealing with cybersecurity regulation.
Operational	This area groups stakeholders that fight against cyberattacks on a daily basis. They can belong to public, national, international, or private organizations. National centres relating to cyber crime and security Present national initiatives concerning the mitigation of online threats in the broadest sense of the word, that collect, analyse and/or act on data at national level. International centres relating to cyber crime and security International initiatives concerning the mitigation of online threats in the broadest sense of the word, that collect, analyse and/or act on data at international level. CSIRT/CERT Computer Security Incident Response Team – "A CSIRT is a team that responds to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution of them."[2] Public prosecutors The prosecutor is the chief legal representative of the prosecution in countries with either the common law adversarial system, or the civil law inquisitorial system. The prosecution is the legal party responsible for presenting the case in a criminal trial against an individual accused of breaking the law1. Law enforcement Government institutions that enforce laws related to cyber offences or offenses made through cyber space.
Providers	This area groups providers of applications and services. Differently from the Research area (above), where the focus is more on finding new solutions, stakeholders in this area mainly aims at transfer solutions to production by creating and maintaining derived applications and services.

[1] http://en.wikipedia.org/wiki/Public_prosecutors

	Hosting Providers Web Hosts, Data Centres who can contribute valuable data on botnets and infections and provide supporting infrastructure Technology Providers Providers of solutions aiming to fight botnets willing to implement their solutions as part of ACDC or to contribute their solutions into ACDC. 1. Security Technologies Providers of dedicated security technologies such as malware analysis, botnet monitoring, network technology solutions. Provider of applications and services related to the cybersecurity field. Contrary to the "Critical Infrastructure Operator" category, this category focuses on applications and services and may include non-commercial organizations providing specific solutions relevant to the cybersecurity domain. It also includes system integrators and resellers, as well as providers of existing solutions & services that may be impacted by cybersecurity issues. These can be hardware solutions, applications or solutions provided as a services on premise or from within the cloud. 2. System Integration Providers of integration services, integrating security technologies in networks, systems and applications ISPs Internet Service Providers. Mobile network providers Mobile phone network operators that are interested in deploying solutions provided by the ACDC and contribute the results back to ACDC in order to refine and improve the tools.
Intermediaries	End User Organizations and industry collaborations Organizations bringing together interests of end users on topics related to cyber security, such as telecom and internet user associations (INTUG), ISAC's (FS ISACS), security professionals (ISSA, ISACA), ... Industry Associations & Sector Federations Organizations bringing together interests of organizations such as company associations, trade unions, vertical interest groups, ... with an interest and dedication to cyber security. (Examples : EOS, ADS, VBO, Agoria ICT, TeleTrust, LSEC, ...)

Table 1 – Description of Stakeholders Positioning Areas

As for the sector parameter, the relationship between a given stakeholder and the positioning values can also be multiple. This is the case for instance for a company carrying out research related to the cybersecurity field and also selling security products, or for a government agency acting both as policy maker and, at the same time, running the national CERT for its country.

5.4. Botnet Interests information

While the Cybersecurity Positioning information identifies the role of the stakeholder with respect to the cybersecurity field as a whole, the Botnet Interest information details the particular interest a stakeholder may have with respect to the botnet topic, as introduced in section 4.4.
This section aims at describing the parameters that model the level of interest in the specific topic of botnets, and the values they can take for a given stakeholder. The starting point for this modelling is the ACDC description of work, because this provides the consortium and the community a clear picture of the kind of information that can be of interest for each stakeholder. Linking stakeholders to project activities also promotes their involvement in the community and in the experiments.
With respect to ACDC solutions, the stakeholder may express interest in acting as a provider (or contributor) of the solution itself, as well as a provider or contributor of data related to botnets and easing the detection, mitigation of botnets as well as creating a knowledge base for further developments, vs. being a potential adopter (thus providing feedback on the solution usage, or even data that originates from the usage, if possible). The set of solutions taken into consideration is derived from the ACDC DoW[1], and briefly introduced below:

- Sensors & Detection Tools – Advanced integration of different sensors to detect malicious traffic.
- Infected website Analysis – Detect and analyse the malicious behaviour of infected Web sites.
- Multipurpose tools for end users – Detection of malicious activities in personal infrastructures and end points, including mobile phones.
- Centralized data clearing house – Collect and analyse data from different data feeds Generate single EU common reporting picture
- Support Centre – Provide help and support to infected users, based on the results of the detection through the central clearing house

Concerning experiments, stakeholders can express their interest in participating to one or more (thus generating results) vs. just accessing the experiment's results. The set of experiments taken into consideration is derived from the ACDC DoW[1], and briefly introduced below:

- Spam-Botnet – aiming at detecting and taking down botnet used to send large amount of spam messages.
- Fast-Flux – used to address fast flux techniques that are used by cyber criminals to hide phishing and malware delivering sites.
- Website – aiming at carry out large scale scans of websites in order to detect malicious code of various kinds and drive-by downloads in specific.
- Distributed Denial of Service – targeting Distribute Denial of Services attacks in general and with a specific focus on the case of Cloud-based DDoS attacks
- Mobile Bot – aiming at validating our strength in terms of identification of botnets operating out of mobile networks.

Apart from the interest in experiments and solutions, stakeholders may express their interest toward specific ACDC activities, like participation to an event (workshop, conference, etc.) as well as contribution to requirements and documents (reports, deliverables, statistics, etc.). The introduction of parameters specific to these participations heavily depends on the stakeholder's

initial involvement in the ACDC community and will be evaluated later on in the project, once the community will be in place and activities will have started.

5.5. ACDC interaction channels

As described earlier, this criteria represents the future involvement / interaction of the stakeholder with ACDC. Each stakeholder may select one or more channels of interaction, but the important lessons learnt from the 1st year of ACDC is that each model has to be clearly identified, and therefore supported by the appropriate access control measures between the ACDC entry point for all interactions, i.e. the ACDC Community portal and the actual central data clearing house (CCH). This also builds on the work carried out in WP1 to move from a higher level of "sharing data" to more precise levels in which "data retrieval and contribution work flows".
The second modification is the introduction of the "level", ranging from 1 to 3, with

- Level 1: the criteria information can be acquired for engagement level 8 ("Information gathering initiated, refer to D6.1.2)
- Level 2: the criteria information can be acquired after engagement level 12 ("Signed level of interest")
- Level 3: the criteria information will be refined when the stakeholder has tested the interaction.

The introduction of these different levels builds on the fact that when a stakeholder signs a letter of interest, he has not yet experienced ACDC and therefore we need to support progressive levels of engagement.

The importance of these values is to enable ACDC to build a best practice approach to data sharing that can benefit beyond the ACDC CCH, as data sharing is and remains one of the most critical issues in fighting botnets.

Value	Level	Description
Information related to the provision of data by a stakeholder		
Data creation	1	Access to data specific to the operations / activity of the stakeholder. This parameter reflects the fact that data relevant to botnets is detected and stored by this stakeholder.
Data provision	1	This stakeholder is available to provide data to the ACDC clearing house. The conditions under which the data could be provided are further described in other parameters.
Data external channel required	1	This parameter identifies whether the stakeholder can only provide this data through a third party (for instance, through a national police force or other bodies, as detected in the initial contacts).
Data modified by owner	2	This parameter identifies whether the stakeholder will handle anonymisation / aggregation or other modification of data prior to providing it to the ACDC clearing house. This will be used also to refine the work to be done by the clearing house itself
Data sharing limitations selected by owner	2	This parameter identifies whether the data provided by the owner will only be made available to certain categories or even individual stakeholders. This paves the way for sharing limitation between for instance two member states that have signed an agreement or two institutions and are interested in using the "clearing house" service of ACDC. Providing this feature is of importance in supporting the adoption of ACDC as a service to all.
One to one	3	This parameter identifies that the owner will only provide data based on a

data sharing		bilateral relationship (identified organisation requesting access to data).
One to many data sharing	3	This parameter identifies that the owner is available to provide the data to one or more clearly identified groups (all CERTs, all police forces etc)
Geographical limitation	3	This is an additional parameter that can *restrict* the data sharing, allowing the data owner to specify that he will share only with stakeholders from specific countries.
Full data sharing	3	This parameter identifies that the owner who releases this data does not put limitation on the retrieval accessibility (meaning who accesses data). The usage is managed separately.
Full data availability delay introduced by owner	2	This parameter indicates that the data can become fully available after a certain period of time. This helps handle data that is sensitive when generated, but becomes less sensitive as time moves on and can be used to forensic and statistical analysis.
Data usage limitations selected by owner	2	Separately from the "sharing limitation" introduced on the previous line, an owner may also restrict in all cases the actual usage that could be done of the data, ranging from, for instance, whether data can be only used for statistical purpose, whether data can be used for research purpose etc.
Information related to the retrieval of data from the ACDC clearing house by a stakeholder		
Data retrieval	1	This parameter identifies if the stakeholder is interested in retrieving data.
Data foreseen usage	1	This parameter identifies what type of usage the stakeholder foresees with the data retrieved; for instance, development of new solutions, testing of algorithms, statistical analysis, impact evaluation etc.
Information related to the provision of solutions to the ACDC clearing house by a stakeholder		
Solutions provision	1	This stakeholder develops new solutions and is interested in providing them through the ACDC clearing house
Beta-testing interest	1	The stakeholder is interested in using the ACDC community as beta-testers. This could apply both to research level solutions or to commercial solutions under development.
Trials availability	1	Solutions can be provided as trials on a free basis, either fully fledged for a limited duration or limited features.
Components level	1	This stakeholder is interested in using ACDC to make a specific component available (for future integration in another solution)

Table 2 –list of parameters for ACDC interaction channels

6. References

[1] ACDC Description of Work, 2012

[2] What is a CSIRT? Enisa website, http://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

[3] COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 8/12/2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[4] COUNCIL DIRECTIVE 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24/10/1995, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[5] List of Industry Classifications, https://en.wikipedia.org/wiki/Industry_classification

[6] Critical Infrastructures, http://en.wikipedia.org/wiki/Critical_infrastructure

[7] Proposal for a DIRECTIVE OF THE COUNCIL on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:EN:HTML