



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



Deliverable	D6.1.2 – Identified user lists across different organisations
Work package	WP6
Due date	30/06/2013
Submission date	15/01/2014
Revision	3.04
Status of revision	Final
Responsible partner	Engineering Ingegneria Informatica
Contributors	Paolo Rocetti (EII), Barbara Pirillo (EII), Véronique Pevtschin (EII), Ioana Cotoi (EII), Wout de Natris (eco), Raul Jurdado Tejedor (Inteco), Paolo De Lutiis (TI), Aleš Černivec (XLab), Klaus-Peter Kossakowski (DFN-CERT Services), Darko Perhoc (CARNet), Dan Tofa (CERT-RO)
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	
Document 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	15/06/2013	EII	Creation of first format for gathering of contributions
0.2	21/06/2013	EII	Modification of format – alignment to community portal structure
0.3	22/07/2013	EII	Circulation to partners for contributions (all partners, not restricted to WP6)
1.01	26/7/2013	TI	Integration of contribution
1.02	29/07/2013	XLab	Integration of contribution
1.03	30/07/2013	Inteco	Integration of contribution
1.04	30/07/2013	CERT-RO	Integration of contribution
1.05	01/08/2013	DFN-CERT	Integration of contribution
1.06	05/08/2013	CARNet	Integration of contribution and updates
1.07	13/08/2013	EII	Analysis and preparation of revision
1.08	9/9/2013	EII	Revision for circulation
2.00	15/9/2013	Eco / EII	Integration of outreach information following the list of outreach activities
2.00	15/9/2013	Eco / EII	Integration of outreach information following the list of outreach activities
2.01	30/09/2013	EII	Integration of contacts with Lol
2.02	15/10/2013	EII / xLAB/ Carnet / eco	Evolution of format of source information I preparation of ICT 2013
2.03	19/12/2013	EII	Review circulation
2.04	19/12/2013	Eco	Update of conclusions and analysis
2.05	14/1/2014	EII	Update analysis, next steps, conclusions Detailed review
2.06	15/1/2014	EII	Review
3.01	18/1/2014	EII / eco	Review and update
3.02	21/1/2014	EII	Review
3.03	23/1/2014	EII	Submission
3.04	7/2/2014	EII	Submission updated – addition of edited annex

Table of contents

1. Executive summary	5
2. Overview of the link between WP5 and WP6 deliverables (M12 deadline)	6
3. Introduction	7
4. Methodology	8
5. Analysis of the results	12
5.1. ACDC country partner presence	12
5.2. Scope of Organisation	14
5.3. Sector	14
5.4. Cyber-security positioning	14
5.5. Possible interaction	15
5.6. ACDC stakeholder owner	16
5.7. Process status	16
5.8. First Contact	17
5.9. Priority to engage	17
5.10. Proposed by ACDC Partner	18
5.11. Stakeholders participation in the ACDC National Support Centres countries	18
6. Analysis	19
7. Next steps in building the community	20
8. ACDC elements contributing to outreach	22
8.1. <i>National support centres (NSCs)</i>	22
8.2. <i>Data Clearing House (DCH)</i>	22
9. Conclusion	23
10. Annex I – overview of stakeholders list	24

Table of tables

Table 1 – overview of the WP5 – WP6 deliverables over the first 12 months of operation	6
Table 2–Countries	13
Table 3–Top Countries in Europe	13
Table 4– Scope of Organisation	14
Table 5–Sector	14
Table 6–Cyber-security positioning	14
Table 7– Policy makers/contributors	15
Table 8– Operational teams	15
Table 9– Providers	15
Table 10– Intermediaries	15
Table 11–Stakeholder Owner	16
Table 12– Process status (LoI : letter of interest)	17
Table 13– First Contact	17
Table 14– Priority to Engage	18
Table 15– Stakeholder proposed by ACDC Partner	18
Table 16- National participation in the ACDC NSC's countries	18
Table 17 – overview of ACDC potential stakeholders and follow-up	71

Table of figures

Figure 1– Possible interaction	16
Figure 2– LoI received divided per sector	17

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
LoI	Letter of interest
MAAWG	Messaging Anti-Abuse Working Group
NACE	Statistical Classification of Economic Activities in the European Community
NSC	National Support Centres (ACDC relay nodes)
RIPE (NCC)	RIPE Network Coordination Centre
SCADA	Supervisory Control and Data Acquisition
US	Unites States

User Profiles and Categorization

1. Executive summary

The creation of a stakeholders' community is a major contribution to the outreach approach proposed by the ACDC project in fighting the botnet issue across Europe.

This document is the second 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. This deliverable assumes that the reader has read deliverable D6.1.1. which presents the philosophy used in creating the ACDC community.

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 a key support 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.

Deliverable D6.1.2 builds on D6.1.1 and is focused on managing the outreach activities conducted under WP6 and supported by WP5 (dissemination). It was used throughout the first year as a living document; it builds on source information contained in an Excel file used to structuring the stakeholders' involvement. While D6.1.2 as a formal deliverable is complete, the Excel file on which the content is based will continue to evolve as a key tool to manage the community contacts. In this sense, deliverable D6.1.2 is delivered as a static document, but it also lives on beyond its delivery date as a dynamic table that is used to continuously update the status of a relationship with the different stakeholders.

Due to the information identified in the source file for managing the contacts, and the fact that D6.1.2 is public, the actual source Excel file is not delivered with the deliverable. However, the source file is available on request on a restricted basis for the project reviewers and the European Commission project officer. In addition, an annex with part of the information is integrated in this document.

The key findings in D6.1.2 are the following

- over 400 stakeholders were identified, with close to 90% contacted and made aware of ACDC
- 5% have signed letters of interest
- 80% have national coverage in terms of their activities, making the ACDC relay centres a key element of success
- sector stakeholders from finance, utilities and transport represent a little under 30% - a number that needs to increase to include all critical infrastructure operators
- the percentage of stakeholders signing letters of interest is higher in the countries where ACDC partners already operate, under some form, support services close to those that will be proposed by the ACDC centres

2. Overview of the link between WP5 and WP6 deliverables (M12 deadline)

As WP6 has a last number of deliverables within the first 12 months, this section provides an overview of which deliverable provides what information. In addition, due to the close link to the dissemination activities of WP5 two deliverables from WP5 are also included in the description below.

This section is repeated in all WP6 deliverables.

Deliverables	What is in the deliverable?
D6.1.1 – user profiles and categorization	The different attributes used to categorize stakeholders, easing the prioritisation of the outreach activity of WP6 and the analysis of the different groups contributing to creating the ACDC community
D6.1.2 – identified users list	The analysis of the stakeholders identified through different activities. This analysis is based on contacts established with 90% of the 426 identified stakeholders.
D6.2.1 – ACDC social platform	The description of the ACDC platform and the extension of its functionalities with respect to the original role foreseen in the DoW
D6.2.2 – Adding social analytics to ACDC social platform	The addition of tools in the ACDC platform to monitor the activities and create a statistical overview of user activities
D6.3.1 – Involvement model for users in ACDC	A detailed description of the different activities that users can choose to be involved in ACDC, presented a UML graphs.
D6.3.2 – Report on user activities	A list of the activities carried out by ACDC partners over the first 12 months of existence to lead to user involvement. First results are the letters of intent signed by 5% of the stakeholders identified in D6.1.2. Next steps identify the different activities proposed to users to become involve in ACDC; these activities are supported by the detailed approach in D6.3.1.
D5.1.1 – dissemination plan	The full list of activities defined to create awareness about ACDC and support the outreach activities of WP6
D5.1.2 – intermediate dissemination report	The report of the dissemination activities of the first 12 months; this report is complemented by D6.3.2 for the section on individual meetings with organisations to reach the first level of involvement, i.e. letters of interest.

Table 1 – overview of the WP5 – WP6 deliverables over the first 12 months of operation

3. 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.

This deliverable is a follow-on of D6.1.1 and focuses on applying the categorization of stakeholders to different organisations to attract them to the ACDC community.

The document is organised in the following sections: after the presentation of the methodology used to classify and qualify the stakeholders included in chapter 3, the tables and figures containing the numerical information are presented in chapter 4. The actual analysis of these tables and figures is done in chapter 5.

4. Methodology

The identification of stakeholders has been done using an Excel file circulated among all partners, containing the following information:

Stakeholder contact information

- Organisation Name
- Website
- Contact Job position: this indicates the level of the proposed contact point in the organisation. To avoid any privacy related issue and allow for circulation and sharing of information, the actual name of the individual contact is not stored in this sheet, but is managed by the ACDC partner directly. The different values for this field are:

<i>Top Level</i>	e.g. owner, CEO, etc.
<i>High Level</i>	e.g. director, general manager, etc.
<i>Middle Level</i>	e.g. young manager, project coordinator, etc.
<i>Entry Level</i>	e.g. junior worker, specialist, etc.

Categorization information (Refer to D6.1.1)

- Scope: this provides an indication of the size of the area of influence. The different values for this field are:

International-level
EU-level
National-level
Regional-level
City-level

- Country: specifies the country in which the organisation is based. All Member States are included as well as an “International” choice. The primary focus of ACDC is however to create a European community of stakeholders.

- Sector: this indicates the economic domain of activity, with the following values.

Chemical industry
Chemical industry - Pipelines of dangerous chemical substances
Chemical industry - Production and storage/processing of chemical substances
Energy & Nuclear industry
Energy & Nuclear Industry - electricity generation
Energy & Nuclear Industry - electricity transmission
Energy & Nuclear Industry - oil and gas distribution
Energy & Nuclear Industry - oil and gas production
Energy & Nuclear Industry - production and storage/processing of nuclear substances
Financial
Financial - Payment and securities clearing and settlement infrastructures and systems including banking
Financial - regulated markets

Food
Food - provision of food
Food - safeguarding food safety and security
Health
Health - biolaboratories and bio-agents
Health - medical and hospital care
Health - medicines, serums, vaccines and pharmaceuticals
Information & Communication Technologies
Information & Communication Technologies - broadcasting services
Information & Communication Technologies - information systems & network protection
Information & Communication Technologies - instrumentation automation and control systems
Information & Communication Technologies - Internet including e-commerce
Information & Communication Technologies - provision of fixed telecommunications
Information & Communication Technologies - provision of mobile telecommunications
Information & Communication Technologies - provision of radio and satellite communications
Research facilities
Security services
Security services - military structures and equipments
Security services - police structures and equipments
Transport
Transport – air
Transport - inland waterways
Transport - ocean and short-sea shipping
Transport – rail
Transport – road
Water
Water - control of water quality
Water - control of water quantity
Water - provision of drinking water
Sector not found in list!

- Cyber positioning: this field indicates the activity of the organisation in terms that are relevant to the cyber-security domain. Values for this field include:

Critical Infrastructure Operators
Research
Policy maker / contributor: international bodies and institutions
Policy maker / contributor: public authority, national government
Operational team: CERT, CSIRT
Operational team: national centres on cyber-security / defence
Operational team: international centres on cyber-security / defence
Operational team: public prosecutor
Operational team: law enforcement
Providers: storage (data centres, cloud operators)
Providers: security solutions

Providers: system integrators
Providers: Internet Service Providers (ISPs)
Providers: mobile network providers
Intermediaries: end users & citizens organizations
Intermediaries: industry associations & sector federations
Intermediaries: focus groups including trade associations

Potential interaction with ACDC's clearing house

This field is an initial indication of how the organisation could use information from / provide information to the ACDC clearing house. When a contact is identified or proposed, it is either filled in by the ACDC partner who initially provided the contact or left open, to be managed during the actual contacts with the stakeholders.

Management of relationship to stakeholder fields

The next five fields all relate to manage the relationship to the stakeholders.

- ACDC Stakeholder Owner: this identifies which ACDC partner is the primary contact to the stakeholder. In case multiple ACDC partners propose the same organisation, it also helps to avoid double channels and confusion in the initial contacts to a stakeholder. In case the contact is not yet clear, the field is set to "Contact to be found" (refer to field "Proposed by ACDC partner" below).
- Process Status: the process status is used to follow-up the level of contact and all the way up to the start of engaging the stakeholder. Once a stakeholder is engaged, the process moves from this management to becoming part of the ACDC community through the community portal.

Important to note is that the process status is incremental information – meaning that if a stakeholder has a process status of, for instance, 6 (introduction meeting taken place), this means that he has been contacted before (status 3), then responded with interest (status 5) etc.

1: Identified
2: Prioritised
3: Contacted – awaiting response
4: Contacted – no interest
5: Contacted – interested
6: Introduction meeting taken place
7: Follow up contact sent
8: Information gathering initiated
9: All information received
10: Lolrequested ^(*)
11: Lolsent ^(*)
12: Lolreceived ^(*)

^(*) Lol - Letter of Interest

- **Priority to Engage:** this field identifies a priority level, defined by the ACDC partner who proposed the contact initially. The different values for this field are high, medium and low, enabling a prioritising.
- **Proposed by ACDC partner:** in most cases, ACDC partners propose stakeholders for whom they have a direct contact. However, the possibility is also open for partners to propose stakeholders with a perceived interest but without a direct contact. The requests will then be made to all partners to analyse whether this stakeholder can be contacted and through which channel.
- **First contact:** this field indicates the first moment when a stakeholder was identified, being classified per month and year. This classification enables the identification of the monthly activities carried out by the Consortium and to categorize and prioritize the stakeholders based on moment the contact was reached for the first time.

5. Analysis of the results

D6.1.2 contains a list of a 426 identified stakeholders, categorised using the definitions elaborated in D6.1.1. It is interesting to analyse the results at this stage, meaning prior to the actual creation of the community.

All ACDC partners have contributed to the identification of stakeholders, bringing in their own expertise and domain.

As indicated in the introduction, the list of stakeholders presented here is not meant to be final: the list will grow and be refined during the life of the project.

5.1. ACDC country partner presence

426 stakeholders (*as of 17.12.2013*) have been initially identified by the ACDC partners, of which:

COUNTRY	Number of Contacts	Percentage	European States	Percentage	Member States	Percentage
Australia	2	0,47%				
Austria	1	0,23%	1	0,26%	1	0,27%
Belgium	9	2,11%	9	2,31%	9	2,45%
Brasil	2	0,47%				
Bulgaria	1	0,23%	1	0,26%	1	0,27%
Canada	1	0,23%				
Croatia	141	33,02%	141	36,25%	141	38,32%
Cyprus	1	0,23%	1	0,26%	1	0,27%
Estonia	3	0,70%	3	0,77%	3	0,82%
Finland	6	1,41%	6	1,54%	6	1,63%
France	14	3,28%	14	3,60%	14	3,80%
Germany	17	3,98%	17	4,37%	17	4,62%
Greece	4	0,94%	4	1,03%	4	1,09%
Hungary	4	0,94%	4	1,03%	4	1,09%
India	1	0,23%				
Ireland	5	1,17%	5	1,29%	5	1,36%
Israel	2	0,47%				
Italy	11	2,58%	11	2,83%	11	2,99%
Japan	4	0,94%				
Korea	3	0,70%				
Lithuania	3	0,70%	3	0,77%	3	0,82%
Luxembourg	2	0,47%	2	0,51%	2	0,54%
Malaysia	1	0,23%				
Moldavia	1	0,23%	1	0,26%		
Montenegro	1	0,23%	1	0,26%		
Nigeria	1	0,23%				
Panama	1	0,23%				

Poland	5	1,17%	5	1,29%	5	1,36%
Portugal	2	0,47%	2	0,51%	2	0,54%
Republic of Maldives	1	0,23%				
Romania	8	1,87%	8	2,06%	8	2,17%
Russia	4	0,94%	4	1,03%		
Slovakia	1	0,23%	1	0,26%	1	0,27%
Slovenia	30	7,03%	30	7,71%	30	8,15%
South Africa	1	0,23%				
Spain	30	7,03%	30	7,71%	30	8,15%
Sweden	3	0,70%	3	0,77%	3	0,82%
Switzerland	6	1,41%	6	1,54%		
The Netherlands	50	11,71%	50	12,85%	50	13,59%
Turkey	1	0,23%	1	0,26%		
Ukraine	2	0,47%	2	0,51%		
UK	17	3,98%	17	4,37%	17	4,62%
USA	16	3,75%				
European level	6	1,41%	6	1,54%		

Table 2–Countries

As can be seen in **Erreur ! Source du renvoi introuvable.**, based on the total number of stakeholders identified by the ACDC Partners, 91% are European organisations, of which 86% from the European Union, covering 24 European Union Member States (except Czech Republic, Denmark, Latvia, Malta).

This is similar to ACDC's geographical coverage based on its partnership, with a 90% presence in European Union states.

The Table below highlights the European states where the organisations responded in a more positive way. The Table reflects the consistency between the results and the outreach activities established for the first reporting year of the project.

COUNTRY	European States	Percentage
Croatia	141	36,25%
The Netherlands	50	12,85%
Slovenia	30	7,71%
Spain	30	7,71%
Germany	17	4,37%
United Kingdom	17	4,37%
France	14	3,60%
Italy	11	2,83%
Belgium	9	2,31%
Romania	8	2,06%

Table 3–Top Countries in Europe

5.2. Scope of Organisation

From the **426** stakeholders identified:

Criteria	Organisation Scope	Percentage
National-Level*	345	79,86%
European-Level	46	10,77%
International-Level	35	8,20%
*National, regional and city level		

Table 4– Scope of Organisation

This table highlights the importance of the activities done at national level – i.e. the creation of local relays such as the ACDC national support centres.

5.3. Sector

From the **426** stakeholders identified:

Criteria	Organisation Sector	Percentage
Information & Communication Technologies	184	43,09%
Research facilities	63	14,99%
Financial	57	13,35%
Other (Mostly Policy Makers)	44	10,30%
Security services - police structures and equipments	22	5,15%
Energy & Nuclear Industry	21	4,92%
Water	15	3,51%
Transport	14	3,28%
Unknown	5	1,17%
Food	1	0,23%

Table 5–Sector

5.4. Cyber-security positioning

From the **426** stakeholders identified:

Criteria	Organisation Sector	Percentage
Critical Infrastructure Operators	118	28,23%
Providers	111	26,56%
Research	66	16,03%
Operational Team	48	11,00%
Policy maker/contributor	46	11,24%
Intermediaries	29	6,94%
Unknown	8	1,88%

Table 6–Cyber-security positioning

- 46 policy makers/contributors were identified, from which:

Criteria	Organisation Sector	Percentage
International bodies and institutions	11	23%
Public authority, national government	35	77%

Table 7– Policy makers/contributors

-48 operational teams were identified, from which:

Criteria	Organisation Sector	Percentage
CERT, CSIRT	23	47%
Operational team: law enforcement	18	38%
National centres on cyber-security / defence	3	7%
International centres on cyber-security / defence	2	4%
Operational team: public prosecutor	2	4%

Table 8– Operational teams

- 111 providers, from which:

Criteria	Organisation Sector	Percentage
Internet Service Providers (ISPs)	52	47%
System integrators	32	29%
Security solution providers	19	17%
Storage (data centres, cloud operators)	5	4%
Mobile network providers	3	3%

Table 9– Providers

- 29 intermediaries, from which:

Criteria	Organisation Sector	Percentage
End users & citizens organizations	11	48%
Industry associations & sectoral federations	15	52%
Focus groups including trade associations	3	10%

Table 10– Intermediaries

Due to some incomplete information, the cyber-security positioning of 8 stakeholders has to be verified further.

5.5. Possible interaction

This criteria was introduced early on in the community outreach activity to enable ACDC to build on the possible interactions of community members with ACDC. This is a criteria which will be further refined in terms of relationship in the coming months – and also used to influence the different types of activities proposed to the community members.

From **426** stakeholders identified:

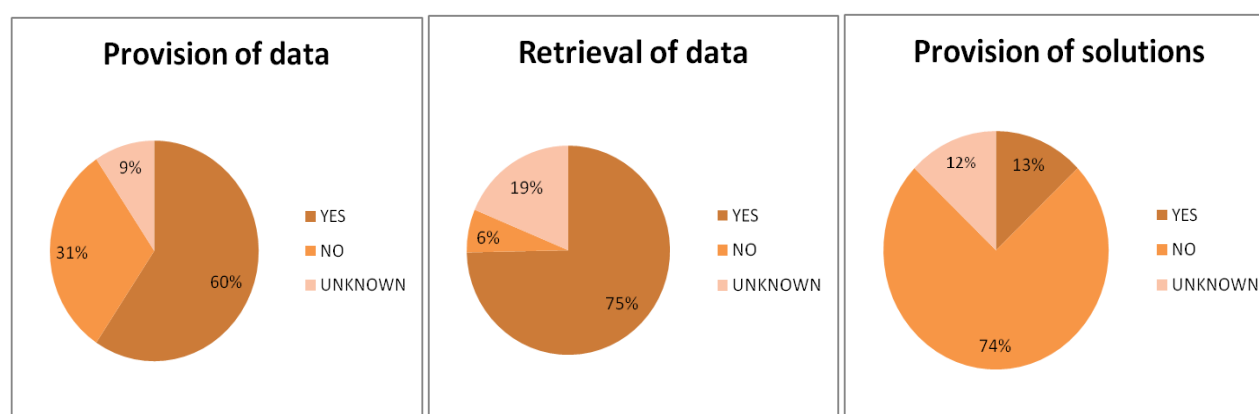


Figure 1– Possible interaction

5.6. ACDC stakeholder owner

From **426** stakeholders identified, 65% of them are owned by an ACDC Partner. According to the strategy for the second reporting year of the project, the stakeholders not yet assigned to a partner will be managed as follows: the stakeholders identified at the ICT 2013 Conference (13%) and those proposed by the consortium (22%) are going to be assigned, to the ACDC Partners, based on different criteria.

ACDC Partner	Stakeholder Owner	Percentage
CARNet	144	64,86%
XLAB	28	12,61%
INTECO	26	11,71%
CERT-RO	8	3,60%
DFN-CERT	8	3,60%
TI	5	2,25%
ECO	2	0,90%
EII	1	0,45%

Table 11–Stakeholder Owner

5.7. Process status

As introduced in the first section, the process status is an incremental information – meaning that out of 426 stakeholders, we have been in contact with 379 of them through our various outreach activities.

Criteria	Process Status	Percentage
1: Identified	40	9,37%
2: Prioritised	6	1,41%
3: Contacted - awaiting response	1	0,23%
4: Contacted - no interest	0	0,00%
5: Contacted – interested	9	2,11%
6: Introduction meeting taken place	198	46,37%

7: Follow up contact sent	0	0,00%
8: Information gathering initiated	147	34,66%
9: All information received	0	0,00%
10: Lol requested	4	0,94%
11: Lol sent	1	0,23%
12: Lol received	20	4,68%

Table 12– Process status (Lol : letter of interest)

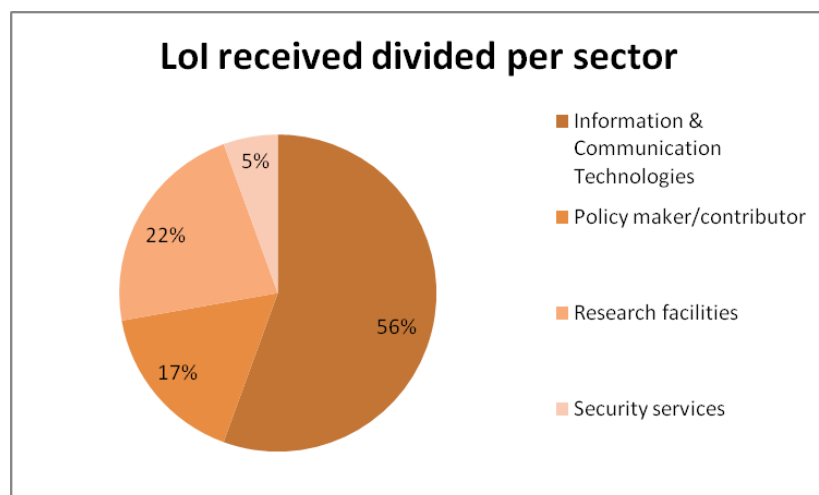


Figure 2– Lol received divided per sector

5.8. First Contact

From **426** stakeholders identified, during the first reporting year, a first contact has been established with 379 of them. The following table provides an overview of the evolution of the contacts over time.

Criteria	First contact	Percentage
May 2013	7	1,8%
June 2013	15	4,0%
July 2013	1	0,3%
August 2013	125	33,0%
September 2013	10	2,6%
October 2013	27	7,1%
November 2013	113	29,8%
December 2013	81	21,4%

Table 13– First Contact

5.9. Priority to engage

From **426** stakeholders identified:

Criteria	Priority to engage	Percentage	Total
High	44	10,33%	426
Medium	168	39,44%	
Low	12	2,82%	
Unknown	202	47,42%	

Table 14– Priority to Engage

This “priority to engage” parameter has not been used in the first year as a strong indicator, but will be further updated in the second year of activity, based on the engagement in collaborating more concretely with ACDC etc. The reason is that in the first year the focus was on not only creating awareness but also being in contact with as many stakeholders as possible to understand the best approach to overcome some of the barriers and scepticism around the sharing of data.

5.10. Proposed by ACDC Partner

From **426** stakeholders identified:

Criteria	Proposed by ACDC Partner	Percentage	Total
CARNet	142	39,44%	360
ECO	109	30,28%	
XLAB	36	10,00%	
INTECO	26	7,22%	
LSEC	25	6,94%	
CERT-RO	8	2,22%	
DFN-CERT	8	2,22%	
TI - EII	6	1,67%	

Table 15– Stakeholder proposed by ACDC Partner

The other stakeholders were not proposed by a specific ACDC partner, but were identified at ICT 2013 Conference.

5.11. Stakeholders participation in the ACDC National Support Centres countries

From **426** stakeholders identified, the following table provides information about which ones are established in countries where ACDC plans to deploy national support centres during the lifetime of the project.

Country	Contacts	LoI received
Croatia	141	3
Spain	30	2
France	17	3
Germany	14	0
Italy	11	0
Belgium	9	0
Romania	8	0
Portugal	2	0

Table 16- National participation in the ACDC NSC's countries

6. Analysis

The deliverable D6.1.2 has presented a detailed list of stakeholders across the major categories identified by ACDC. The stakeholder identification is therefore an essential stage of the information gathering process, providing the basis for a structured community of stakeholders upon which different activities, as already mentioned, are to be made.

ACDC has used the source information on which this deliverable is built in a structured approach to contact the stakeholders and has used different events to directly contact stakeholders, like the ICT event in Vilnius, November 2013, where a presentation session and a set of demonstrations were prepared, which gave ACDC the opportunity to move from bilateral contacts into a large dissemination event. Other events like e.g. Botconf 2013, Internet Security Days, MAAWG, NL Road show, Octopus Conference 2013, EC3-ENISA meeting etc. were carefully chosen to present and promote ACDC to a wide number of potential stakeholders, as is reflected in the raised interest as shown above.

In addition, bilateral meetings were organised with a selected subset of stakeholders. The overall set of activities is reported in D5.1.2 through the dissemination monitoring report.

Analysing the tables and figures presented, we can summarise the key points as follows:

- 1) The proactive approach to outreach has been successful, ACDC has contacted 90% of identified stakeholders and has got an overall positive response in terms of « interest »
- 2) The 5% of stakeholders who have signed letters of interest is higher in countries where ACDC partners already have a support activity, i.e. Germany, Spain, Croatia. The other 5 countries where ACDC plans to set up a centre have to reach the same level of success. For instance, in Italy, ICSTI, Telecom Italia and Engineering are currently defining the practical steps to set up a centre and the expectations are that together this will then increase the visibility at national level. One initial contact has been made, for instance, with Poste Italiane and negotiations are on going to create an operational collaboration in managing the Italian ACDC node. This in turn will ease the signing up of stakeholders.
- 3) The current profiles of stakeholders with signed LoI includes ICT and research – but lacks operators of critical infrastructures, a gap that has to be addressed in 2014
- 4) The opportunity of larger events (such as ICT 2013) is useful to speed up the outreach
- 5) The sectoral coverage of identified stakeholders has to increase : the current spread of 43% for ICT, 15% for researchers, 10% of policymakers, 13% in the financial world, 10% of utilities, 3% of transport operators shows that we are still lacking visibility in terms of the operators themselves.
- 6) The national relays are a key point for ACDC to move to success – with 80% of the stakeholders identified operating at national level

7. Next steps in building the community

The ACDC stakeholder identification report gives an overview of an initial pool of 426 stakeholders identified. In the first year a number of 426 stakeholders from 30 European countries were reached and also international stakeholders were identified which match with ACDC's strategy and intentions.

The analysis of the data presented above, reflects the results of all reach out activities made in 2013, i.e. the achievements of the consortium to date. This also allows for a number of decisions and strategies that need to be made for the second year in order to achieve the ACDC's goals.

The next steps include the following list of actions:

- *Assign to each stakeholder* identified an ACDC Partner (ACDC Stakeholder Owner) based on different criteria, like country, language, similar sector etc. An ACDC owner handles all communication and engagement with the stakeholder throughout the ACDC project, to create an efficient collaboration between the external partners and the consortium. These external stakeholders must be introduced to the optimal consortium partners so one-on-one relationships are established. They are to be made responsible for the integration and participation of those stakeholders within the project.
- *Priority to engage:* There is a very large number of potential stakeholders, a number that will continue to grow in 2014. It is impossible for ACDC to actively involve all of them at the same level of interaction. A priority mechanism will be introduced, with priorities defined, among other criteria, in terms of the sectorial domains that are selected by the members and the actual level of commitment already expressed by the stakeholders. Stakeholder engagement is a critical factor for the success of the ACDC, due to the fact that without an effective strategy of stakeholder engagement, the project will not receive the necessary (financial) support to have a meaningful impact after July 2015. One key element in the priority to engage is based on the information analysed in terms of which stakeholders can contribute data / solutions to ACDC, which ones are interested in adding the national relay centres etc. Given the large number of national stakeholders identified (80%) this is a key issue.
- *Following up on the signed Letters of interest*
For those stakeholders who have signed a Letter of Interest, it is important to move forward and propose concrete activities, including provision of data, active collaboration, participation to experiments etc.
- *Increasing signature and sectoral coverage of interested stakeholders:*
As of December 2013, 5% of the stakeholders identified have signed the Letter of interest expressing their interest in joining the External Consultative Board and this number is growing, with 35% of the stakeholders having indicated that they contemplate a possible collaboration with ACDC.
Based on Figure 2, a large number of Letters of Interest were signed in the technical community and academia, a lower number in the policy maker and security services, and none in the critical infrastructure operators.
These results must be followed up in 2014 by an active approach on behalf of the ACDC Partners going all the way up to the start of engaging actively the stakeholders.

- *Pursuing outreach activities to identify stakeholders and contact new ones:*

ACDC will continue with the identification of new stakeholders based on the different criteria that came out from this report while at the same time ensuring that the interested stakeholders can become actively involved in one or more activities, ranging from experiments to using / providing data.

As ACDC strives to identify a complete number of stakeholders that cover all the countries in Europe, the next steps will also build on two major components of ACDC, i.e. the national support centres and the central clearing house database. One key conclusion from the analysis is that the current geographical coverage of identified stakeholders is unequal across countries – and this point will be addressed strongly in the second year of ACDC.

8. ACDC elements contributing to outreach

In addition to the outreach activities listed above, it is important to understand how two key components of ACDC, namely the national support centres and the ACDC clearing house contribute to the community building process.

8.1. *National support centres (NSCs)*

ACDC partners responsible for setting up a national support centre are key contributors to the identification of stakeholders. The outreach activity proposes to further involve them by asking them to increase the list of potential stakeholders.

A form of government support is important for NSCs to succeed. This support at this stage seems fundamentally lacking in most countries. Talks with the European Commission on how to ensure awareness on ACDC at government level and thus invite them to engage with ACDC have started in late 2013 and need to be taken one step further in winter 2014.

First ACDC Partners responsible for NSCs need to identify which potential future stakeholders are essential to have on board. Next steps need to be taken on reach out and from there convince them that their participation is in their interest. The NL road show approach is one example on how to reach as many potential stakeholders as possible within a country.

8.2. *Data Clearing House (DCH)*

Many identified stakeholders are interested in data within or coming from the CCHD. At this stage it is important to identify the most interesting external stakeholders¹. This can be done on two criteria:

1. Through their own offer on active collaboration;
2. Through identification from inside ACDC: consortium partners have to identify their must have's.

The stakeholders that at present are interested in ACDC will be divided into priorities and non-priorities. The first category will receive extra attention in 2014. How they can contribute to ACDC will be further analysed and on this basis they will be directly invited to participate in or even co-generate the experiments and thus ensure their future participation. These external stakeholders, as said before, must be introduced to the optimal consortium partners so one-on-one relationships are established. The assigned partners are to be made responsible for the integration and participation of those stakeholders within the project.

¹The mentioned criteria here may well be of use at national level.

9. Conclusion

The main conclusion is that the interest for ACDC is high. The active reach out program that is a part of ACDC has put the project on the map.

For sure, scepticism is still there from different angles, the main one being whether ACDC will be able to build the necessary trust for active sharing and provision of data on the one hand, and on whether its approach will be agile enough to cater to real-time needs.

However, several important stakeholders have not only given ACDC the benefit of the doubt, they also have declared they will actively participate in trying to make ACDC succeed. This is a main change since spring 2013 and a direct benefit from the active outreach approach.

The key challenge for the second year of the project is to move to a list of concrete activities for involvement by the interested stakeholders.

At national level the main focus must be put on participation and acceptance of the national support centres in the countries that are to have one in 2015.

Internationally the main focus must lie on intensifying reach out and securing participation. On the one hand crucial stakeholders that have not yet committed have to be convinced to do so in 2014 through an intensified reach out program, showing first results that are to their benefit. On the other hand those that have committed must be internalised within the project through active reach out and cooperation from within the ACDC consortium.

One year into the ACDC project it is safe to conclude that most important players were exposed to ACDC. The next step is to make sure they actively participate in developing ACDC further.

10. Annex I – overview of stakeholders list

The following table is an extract of the detailed Excel file used for follow-up and management of relationships to organisations contacted to join ACDC.

The list does not show the detailed contact person information to avoid publication of detailed emails and names.

External stakeholder – contact information				Cyber information	ACDC Partner contact and follow-up of relationship			
Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Australia	ACMA (Australian Communications & Media Authority)	National-level	Information & Communication Technologies	Policy maker / contributor: public authority, national government	10: Lol requested	ECO	Internet Security Days	24/09/13
Australia	The University of Melbourne	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Austria	TTTech	National-level	Transport	Critical Infrastructure Operator	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Belgium	Actif-europe SARL	EU-level		Intermediaries: industry associations & sectoral federations	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Belgium	CERT EU	EU-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13
Belgium	Consilium (Europe)	EU-level		Policy maker / contributor: international bodies and institutions	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Belgium	European Alliance for Innovation	EU-level	Information & Communication Technologies	Intermediaries: end users & citizens organisations	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Belgium	IBM Belgium	EU-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	ICT 2013 Conference	06/11/13
Belgium	IMind	National-level	Research	Research	6: Introduction	LSEC	ICT 2013 Conference	06/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Belgium	LSEC Leaders In Security	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
Belgium	Council of European National Top Level Domain Registries (CENTR)	EU-level	Research facilities	Critical Infrastructure Operator	8: Information gathering initiated	XLAB		27/08/13
Belgium	DG CNECT - Unit Trust & Security	EU-level	Information & Communication Technologies	Research	8: Information gathering initiated	LSEC		20/12/13
Brasil	Centro de Informatica UFPE	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Brasil	Organisation Name missing	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	CITEL, ISOC, ITU anti-spam meeting	08/10/13
Bulgaria	Mozaika	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Canada	CCIRC - Canadian Cyber Incident Response Centre	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Croatia	Croatian Telekom	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	12: Lol received	CARNet		01/10/13
Croatia	Fakultet organizacije i informatike (Faculty of informatics and organization)	National-level	Research facilities	Research	12: Lol received	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	Tehničko veleučilište u Zagrebu	National-level	Research facilities	Research	12: Lol received	CARNet		27/08/13
Croatia	Diverto d.o.o	National-level	Information & Communication Technologies	Providers: system integrators	5: Contacted - interested	CARNet		17/12/13
Croatia	HT d.d.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	5: Contacted - interested	CARNet		27/08/13
Croatia	Ministarstvo unutarnjih poslova (Ministry of interior)	National-level	Security services - police structures and equipments	Operational team: law enforcement	5: Contacted - interested	CARNet		27/08/13
Croatia	Posluh	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	5: Contacted - interested	CARNet		27/08/13
Croatia	ZSIS CERT (Information systems security bureau CERT)	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	5: Contacted - interested	CARNet		27/08/13
Croatia	Banco Popolare Croatia d.d.	International-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Banco Popolare Croatia d.d.	International-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Banka Kovanica d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	Banka splitsko-dalmatinska d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	BKS bank d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	BKS bank d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Croatia banka d.d	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Croatia banka d.d	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Erste&Steiermaerkische Bank	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Erste&Steiermaerkische Bank	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Erste&Steiermaerkische Bank	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	HPB-Stambena stedionica d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Hrvatska postanska banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	Hypo Alpe-Adria-Bank	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Imex banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Istarska kreditna banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Jadranska banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Karlovacka banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	KentBank d.d.	International-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	KentBank d.d.	International-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Kreditna banka Zagreb d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Ministarstvo uprave RH (Ministry of public administration)	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	CARNet		27/08/13
Croatia	Nava banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	OTP banka d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Partner banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Partner banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	PBZ stambena stedionica d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	PBZ stambena stedionica d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Podravska banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Primorska banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Privredna banka Zagreb d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Privredna banka Zagreb d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Prva stambena stedionica d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	Raiffeisen stambena stedionica d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	RaiffeisenBank Austria d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Samoborska banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Sberbank d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Slatinska banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Splitska banka d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Splitska banka d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Stedbanka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Tesla stedna banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Tesla stedna banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	TRILIX (on behalf of Wuestenrot)	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	VABA dd. Banka Varazdin	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Veneto banka d.d.	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Zagrebacka banka d.d.	Regional-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	CARNet		17/12/13
Croatia	Agrokor d.d.	National-level	Food	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	American College of Management and Technology	National-level	Research facilities	Research	8: Information gathering initiated	CARNet		27/08/13
Croatia	AMIS TELEKOM d.o.o.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	APIS (data center-government agency)	National-level	Information & Communication Technologies	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	ATLANTSKA PLOVIDBA d.d. (shipping company)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Avalon	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	B.NET HRVATSKA d.o.o.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Brod-plin d.o.o. (gas distribution)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	BSP Hosting	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Combis (IT integrator)	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	CARNet		27/08/13
Croatia	Croatia Airlines d.d.	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	CRODUX DERIVATI DVA d.o.o. (oil industry and petrol distribution)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	DARKOM društvo s ograničenom odgovornošću za komunalnu djelatnost (water supply Daruvar)	City-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Elektra Zagreb (electricity distribution operator)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Elektrotehnički fakultet Osijek	National-level	Research facilities	Research	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	Erste Bank	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	EVN Croatia Plin d.o.o.	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Fakultet elektrotehnike i računarstva	National-level	Research facilities	Research	8: Information gathering initiated	CARNet		27/08/13
Croatia	Fakultet elektrotehnike, strojarstva i brodogradnje	National-level	Research facilities	Research	8: Information gathering initiated	CARNet		27/08/13
Croatia	Financijska agencija - FINA (Financial agency)	National-level	Information & Communication Technologies	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Globaldizajn	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	GRADSKA PLINARA ZAGREB - OPSKRBA d.o.o. (Zagreb gas distribution)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	H1 TELEKOM d.d.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	HAC (Croatian highways)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	HEP d.d.	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP plin (gas distribution)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP-Obnovljivi izvori energije d.o.o (electricity generation)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP-Operator distribucijskog sustava d.o.o. (electricity distribution operator)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP-Operator prijenosnog sustava d.o.o. (electricity distribution)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP-Opskrba d.o.o. (electricity distribution)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP-Proizvodnja d.o.o. (electricity generation)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HEP-TOPLINARSTVO d.o.o. (heating energy distribution)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HNB (Croatian national bank)	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		17/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	HP-HRVATSKA POŠTA d.d. (Croatian post)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Hrvatska agencija za poštu i elektroničke komunikacije HAKOM	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	CARNet		27/08/13
Croatia	Hrvatska kontrola zračne plovidbe (Croatian flight control)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Hrvatska poštanska banka (Croatian post bank)	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	HŽ (Croatian railways)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	INA-INDUSTRIJA NAFTE d.d. (oil industry, petrol and gas distribution)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Infonet	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Inside	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	ISKON INTERNET d.d.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	ISTARSKI VODOVOD d. o. o., za proizvodnju i distribuciju vode (water supply Istra)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	JADROLINIJA (national shipping company)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	JANAF d.d. (national oil pipeline)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	KOMUNALAC d.o.o. (gas distribution)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Komunalno društvo VODOVOD I KANALIZACIJA društvo s ograničenom odgovornošću za vodoopskrbu i odvodnju (water supply Rijeka)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Končar-elektroindustrija d.d (scada)	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	CARNet		27/08/13
Croatia	Luka Rijeka d.d. (Rijeka port)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	MEĐIMURJE-PLIN d.o.o. (gas distribution)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	MEĐIMURSKE VODE, d.o.o. za vodnogospodarsku djelatnost, vodoopskrbu i odvodnju (water supply medjimurje region)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	METRONET TELEKOMUNIKACIJE d.d.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Mntelektro d.o.o (scada)	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	CARNet		27/08/13
Croatia	Optimus Hosting	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Orbis	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	OT - OPTIMA TELEKOM d.d.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	PBZ d.d. (Privredna bank)	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Peek d.o.o (scada)	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	PIS d.o.o. (gas distribution)	Regional-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	PLINACRO d.o.o. (National gas pipeline)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Plus hosting	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Podzemno skladište plina (the national gas storage operator)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Raiffeissen bank	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	S&T (IT integrator)	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	CARNet		27/08/13
Croatia	SISAČKI VODOVOD društvo s ograničenom odgovornošću za opskrbu pitkom vodom, odvodnju i pročišćavanje otpadnih voda (water supply Sisak)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	TANKERSKA PLOVIDBA d.d. (shipping company)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	TE PLOMIN d. o. o.	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Tehnički fakultet - Rijeka	National-level	Research facilities	Research	8: Information gathering initiated	CARNet		27/08/13
Croatia	TEKIJA, društvo s ograničenom odgovornošću za obavljanje komunalnih djelatnosti	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Termoplin d. d. (gas distribution)	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Valkira	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	VARKOM dioničko društvo za opskrbu vodom i odvodnju otpadnih voda (water supply Varazdin)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Vinkovački vodovod i kanalizacija društvo s ograničenom odgovornošću (water supply Vinkovci)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	VIPnet d.o.o.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	Visoka škola za informacijske tehnologije	National-level	Research facilities	Research	8: Information gathering initiated	CARNet		27/08/13
Croatia	VODOVOD DUBROVNIK d.o.o. za vodoopskrbu i komunalnu hidrotehniku (water supply Dubrovnik)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	VODOVOD I KANALIZACIJA društvo s ograničenom odgovornošću za opskrbu pitkom vodom, odvodnju i pročišćavanje otpadnih voda (water supply Karlovac)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	VODOVOD I KANALIZACIJA, društvo s ograničenom odgovornošću za vodoopskrbu, odvodnju i pročišćavanje otpadnih voda (water supply Split)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	VODOVOD I ODVODNJA društvo s ograničenom odgovornošću za vodoopskrbu, te odvodnju i pročišćavanje otpadnih voda (water supply Sibenik)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Croatia	VODOVOD PULA d. o. o. za skupljanje, pročišćavanje i distribuciju vode (water supply Pula)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	VODOVOD, d.o.o. za usluge opskrbom pitkom vodom (water supply Zadar)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Voljatel	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	CARNet		27/08/13
Croatia	Volksbank d.d. (Sberbank d.d.)	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Zagrebačka banka d.d. (Zagrebacka bank)	National-level	Financial	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	ZAGREBAČKI HOLDING d.o.o. - Podružnica Vodoopskrba i odvodnja (water supply Zagreb)	Regional-level	Water	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Croatia	Zračna luka Zagreb (Zagreb airport)	National-level	Transport	Critical Infrastructure Operator	8: Information gathering initiated	CARNet		27/08/13
Cyprus	SignalGenerix - advance signal solutions	EU-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Estonia	Cybernetica AS	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Estonia	FocusIT	National-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Estonia	RKK ICDS	EU-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Europe	European Government CERTs	EU-level	Information & Communication Technologies	Operational team: CERT, CSIRT	1: Identified	DFN-CERT		10/09/13
Europe	ENISA	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	6: Introduction meeting taken place	ECO	EU CERTS annual meeting (Europol)	02/10/13
Europe	ENISA	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	6: Introduction meeting taken place	EII	EOS	05/07/13
Europe	SURBL	National-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
Europe	CERT.EU	EU-level	Information & Communication Technologies	Operational team: CERT, CSIRT	8: Information gathering initiated	LSEC		20/12/13
Europe	eduroam	EU-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	XLAB		27/08/13
Europe	European Internet Exchange Association (Euro-IX)	EU-level	Research facilities	Critical Infrastructure Operator	8: Information gathering initiated	XLAB		27/08/13
Finland	F-Secure	International-level	Information & Communication Technologies	Providers: security solutions	12: Lol received	ECO	Outreach individual meeting	21/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Finland	F-Secure	International-level	Information & Communication Technologies	Providers: security solutions	12: Lol received		ICT 2013 Conference	06/11/13
Finland	FICORA	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Internet Security Days	24/09/13
Finland	Jamk University of applied sciences	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Finland	VTT	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Finland	VTT	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	ETSI	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	1: Identified	TI		26/07/13
France	Atos	Eu-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
France	Bull	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	CEA-LIST	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	CERT France	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
France	France Police	National-level	Security services - police structures and equipments	Operational team: law enforcement	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13
France	French cyber crime Unit of the Gendarmerie	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Presentation to the Interpol European Expert Group on IT crime	22/05/13
France	Symantec	International-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	Telecom SudParis	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	LSEC	ICT 2013 Conference	06/11/13
France	Telecom SudParis	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	Thales Communication & Security S.A.S	International-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	Thales Communication & Security S.A.S	National-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
France	Together against Cybercrime	International-level	Information & Communication Technologies	Operational team: international centres on cyber-security / defence	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
France	The European Union Institute for Security Studies (EUISS)	EU-level	Research facilities	Policy maker / contributor: international bodies and institutions	8: Information gathering initiated	XLAB		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Germany	BITKOM	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	1: Identified	DFN-CERT		10/09/13
Germany	Several German State Governments	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	1: Identified	DFN-CERT		10/09/13
Germany	Avira	International-level	Information & Communication Technologies	Providers: security solutions	12: Lol received	ECO		09/10/13
Germany	Cyscon	National-level	Information & Communication Technologies	Providers: security solutions	12: Lol received	ECO		09/10/13
Germany	Hasso Plattner Institute	National-level	Research facilities	Research	12: Lol received	ECO		15/12/13
Germany	Trusted Introducer / 200 CERTs in Europe	EU-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	5: Contacted - interested	DFN-CERT		10/09/13
Germany	1&1	EU-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
Germany	Cassidian	EU-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Germany	CTO BRI-Business Risk Intelligence	Eu-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
Germany	Fraunhofer AISEC	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Germany	Fraunhofer IGD	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Germany	LINK11	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	De-Cix	17/10/13
Germany	TU Darmstadt	National-level	Research facilities	Research	6: Introduction meeting taken place	LSEC	ICT 2013 Conference	06/11/13
Germany	University of Potsdam	National-level	Research facilities	Research	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
Germany	Vodafone Group Services GmbH	International-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Germany	Vodafone Group Services GmbH	International-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Germany	Bankenverband	National-level	Financial	Intermediaries: industry associations & sectoral federations	8: Information gathering initiated	LSEC		20/12/13
Greece	ENISA – CERT Team	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	5: Contacted - interested	DFN-CERT		10/09/13
Greece	NCSR "Demokritos"	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Greece	Optionsnet	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Greece	Paragon S.A.	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Hungary	CERT Hungary	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13
Hungary	National Innovation Office	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Hungary	Search-Lab	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Hungary	Search-Lab	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
India	Ansal University	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Ireland	CSIRT-IE	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	10: LoI requested	ECO	ENISA EC3 event (Europol)	07/10/13
Ireland	CERT IE	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13
Ireland	Espion Group	International-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Ireland	Police Ireland	National-level	Security services - police structures and	Operational team: law enforcement	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
			equipments					
Ireland	HEAnet Ireland	National-level	Research facilities	Research	8: Information gathering initiated	ECO		18/10/13
Israel	Comsec Group	International-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	LSEC	ICT 2013 Conference	06/11/13
Israel	IBM Research Lab in Haifa	National-level	Research facilities	Research	6: Introduction meeting taken place	LSEC	ICT 2013 Conference	06/11/13
Italy	cnaipic	National-level	Security services - police structures and equipments	Operational team: law enforcement	1: Identified	TI		26/07/13
Italy	EIT ICT LABS "Privacy, Security & Trust in Information Society"	EU-level	Information & Communication Technologies	Research	2: Prioritised	TI		26/07/13
Italy	POLITO	EU-level	Information & Communication Technologies	Research	2: Prioritised	TI		26/07/13
Italy	UNITO	EU-level	Information & Communication Technologies	Research	2: Prioritised	TI		26/07/13
Italy	Contactlab	EU-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Italy	Enco Engineering & Consulting	EU-level		Critical Infrastructure Operator	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Italy	Istituto Superiore Mario Boella	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Italy	Level7	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Italy	Poste Italiane	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated		Bilateral meeting	13/12/2013
Italy	Sapienza Università di Roma	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Italy	University of Calabria - Mechanical Department	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Italy	University of Trento	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Japan	GREE Inc.	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO		18/10/13
Japan	Internet initiative Japan Inc.	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	ECO		18/10/13
Japan	NICT	National-level	Research facilities	Research	8: Information gathering initiated	ECO	Outreach individual meeting	21/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Japan	Nomura Research Institute	International-level	Research facilities	Research	8: Information gathering initiated	LSEC		20/12/13
Korea	KISA - Korea Internet & Security Agency	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Brühl meeting	21/11/13
Korea	Samsung Electronics	International-level	Information & Communication Technologies		6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Korea	KISA - Korea Internet & Security Agency	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	ECO	Outreach individual meeting	21/11/13
Lithuania	Baip - Critical IT Infrastructure	National-level	Information & Communication Technologies	Critical Infrastructure Operator	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Lithuania	Embassy of the Russian Federation	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Lithuania	Uzupis Creative Cluster	National-level		Intermediaries: focus groups including trade associations	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Luxembourg	itrust consulting s.a.r.l.	National-level	Information & Communication Technologies	Providers: storage (data centres, cloud operators)	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Luxembourg	Luxinnovation	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Malaysia	TM Applied Business	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	LSEC		20/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Moldavia	Prosecutor Office	National-level	Security services - police structures and equipments	Operational team: Public prosecutor	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Montenegro	Montenegro CIRT	International-level	Information & Communication Technologies	Operational team: CERT, CSIRT	5: Contacted - interested	CARNet		27/08/13
Nigeria	Economic & Financial Crimes Commission	National-level	Security services - police structures and equipments	Operational team: law enforcement	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Panama	CSIRT-Panama	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Poland	AGH University of Science and Technology	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Poland	ITTI e-technologies & business	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Poland	NASK/CERT Polska	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	Internet Security Days	24/09/13
Poland	Police Academy	National-level	Research facilities	Research	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Poland	Central and Eastern European Networking Association (CEENet)	EU-level	Research facilities	Research	8: Information gathering initiated	XLAB		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Portugal	Caixa Magica	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Portugal	Anubis Networks	International-level	Information & Communication Technologies	Providers: security solutions	8: Information gathering initiated	LSEC		20/12/13
Republic of Maldives	National Centre for Information Technology	National-level	Information & Communication Technologies	Operational team: national centres on cyber-security / defence	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Romania	RCS-RDS	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	CERT-RO		27/08/13
Romania	ROEDUNET-ROCSIRT	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	1: Identified	CERT-RO		27/08/13
Romania	ROMTELECOM	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	CERT-RO		27/08/13
Romania	TELETRANS	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	CERT-RO		27/08/13
Romania	TRANSELECTRICA	National-level	Energy & Nuclear Industry	Critical Infrastructure Operator	1: Identified	CERT-RO		27/08/13
Romania	STS	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	3: Contacted - awaiting response	CERT-RO		27/08/13
Romania	CLAX.RO	Regional-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	CERT-RO		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Romania	INTERLAN	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	CERT-RO		27/08/13
Russia	Dr. Web	National-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Russia	Group-IB Cyber Crime Investigation	National-level	Security services - police structures and equipments	Operational team: national centres on cyber-security / defence	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Russia	State Research Institute of Aviation Systems (GosNIIAS)	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Russia	Highload Lab	National-level	Information & Communication Technologies	Providers: security solutions	8: Information gathering initiated	ECO		18/10/13
Slovakia	Csirt-sk	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	12: LoI received	ECO	EC3-ENISA meeting	03/10/13
Slovenia	Arnes	National-level	Information & Communication Technologies	Critical Infrastructure Operator	1: Identified	XLAB		27/08/13
Slovenia	Slovenian Internet Exchange (SIX)	National-level	Information & Communication Technologies	Critical Infrastructure Operator	1: Identified	XLAB		27/08/13
Slovenia	Institute for corporative security studies (ICS)	National-level	Research facilities	Research	2: Prioritised	XLAB		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Slovenia	SI-Cert	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	2: Prioritised	XLAB		27/08/13
Slovenia	Simobil	National-level	Information & Communication Technologies	Providers: mobile network providers	2: Prioritised	XLAB		27/08/13
Slovenia	ISKRATEL	EU-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Slovenia	LTFE - Laboratory for Telecommunications	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Slovenia	Amis	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Criminal investigation police office	National-level	Security services - police structures and equipments	Operational team: law enforcement	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Informatics and telecommunications association	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Information commissioner	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Institute for open code promotion (IPROK)	National-level	Information & Communication Technologies	Research	8: Information gathering initiated	XLAB		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Slovenia	Institute Jožefa Stefana	National-level	Research facilities	Research	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Ministry of justice	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Ministry of the interior	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13
Slovenia	National investigation office	National-level	Security services - police structures and equipments	Operational team: law enforcement	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Police	National-level	Security services - police structures and equipments	Operational team: law enforcement	8: Information gathering initiated	XLAB		27/08/13
Slovenia	SAFE-SI	National-level	Information & Communication Technologies	Intermediaries: end users & citizens organisations	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian association for corporate security	National-level	Information & Communication Technologies	Intermediaries: end users & citizens organisations	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian communications networks and services agency	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian council for electronic communications	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Slovenia	Slovenian federation of educational networks Eduroam	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian governments office for the protection of clasified information	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian inspectorate for electronic communications and electronic signatures	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian NSA (SOVA)	National-level	Security services - police structures and equipments	Operational team: law enforcement	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Slovenian open code center (COKS)	National-level	Information & Communication Technologies	Research	8: Information gathering initiated	XLAB		27/08/13
Slovenia	T2	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Telekom	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	XLAB		27/08/13
Slovenia	Tušmobil	National-level	Information & Communication Technologies	Providers: mobile network providers	8: Information gathering initiated	XLAB		27/08/13
Slovenia	UPC Telemach	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	XLAB		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
South Africa	Cyber Police Force	National-level	Security services - police structures and equipments	Operational team: law enforcement	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
Spain	Agencia Española de Protección de Datos	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales (AMETIC)	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	1: Identified	INTECO		27/08/13
Spain	Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI)	National-level	Information & Communication Technologies	Intermediaries: end users & citizens organisations	1: Identified	INTECO		27/08/13
Spain	Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía	National-level	Security services - police structures and equipments	Operational team: law enforcement	1: Identified	INTECO		27/08/13
Spain	CCN-CERT	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	1: Identified	INTECO		27/08/13
Spain	Centro Español de Rederencia de Aplicación de las TIC Basadas en Fuentes Abiertas (CENATIC)	National-level	Research facilities	Research	1: Identified	INTECO		27/08/13
Spain	Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Spain	Comisión del Mercado de las Telecomunicaciones (CMT)	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	Confianza Online	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	1: Identified	INTECO		27/08/13
Spain	Cuerpo Nacional de Policia	National-level	Security services - police structures and equipments	Operational team: law enforcement	1: Identified	INTECO		27/08/13
Spain	Entidad Pública Empresarial Red.es	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	Fiscalía General del Estado, Fiscal de Sala Coordinador en materia de Criminalidad Informática	National-level	Security services - police structures and equipments	Operational team: Public prosecutor	1: Identified	INTECO		27/08/13
Spain	Grupo de Delitos Telemáticos de la Guardia Civil	National-level	Security services - police structures and equipments	Operational team: law enforcement	1: Identified	INTECO		27/08/13
Spain	Guardia Civil	National-level	Security services - police structures and equipments	Operational team: law enforcement	1: Identified	INTECO		27/08/13
Spain	INTECO-CERT	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	1: Identified	INTECO		27/08/13
Spain	IRIS-CERT	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	1: Identified	INTECO		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Spain	Ministerio de Industria Turismo y Comercio	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	Ministerio de Justicia	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	Ministerio del Interior	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	ONO	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	INTECO		27/08/13
Spain	Orange	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	INTECO		27/08/13
Spain	Punto Neutro Español de Internet (ESpanix)	National-level	Information & Communication Technologies	Critical Infrastructure Operator	1: Identified	INTECO		27/08/13
Spain	RedIRIS	National-level	Research facilities	Research	1: Identified	INTECO		27/08/13
Spain	Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información	National-level		Policy maker / contributor: public authority, national government	1: Identified	INTECO		27/08/13
Spain	Telefónica	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	INTECO		27/08/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Spain	Vodafone	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	1: Identified	INTECO		27/08/13
Spain	Industrial Cybersecurity Center	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	12: LoI received		ICT 2013 Conference	06/11/13
Spain	University of Granada	National-level	Research facilities	Research	12: LoI received	ECO	ICT 2013 Conference	06/11/13
Spain	Centro Universitario de Tecnogía y arte digital	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Spain	Prodigy Consultores	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Sweden	CERT SE	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13
Sweden	Chalmers University of Technology	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Sweden	Polisen	National-level	Security services - police structures and equipments	Operational team: law enforcement	8: Information gathering initiated	ECO		15/11/13
Switzerland	Swiss MELANI	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	12: LoI received	ECO	Internet Security Days	24/09/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Switzerland	CYCO - Cyber crime Unit	National-level	Security services - police structures and equipments	Operational team: law enforcement	6: Introduction meeting taken place	ECO	Presentation to the Interpol European Expert Group on IT crime	22/05/13
Switzerland	Google	International-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Switzerland	Malwageddon	National-level	Information & Communication Technologies		6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13
Switzerland	Switch - national CERT	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	6: Introduction meeting taken place	ECO	Presentation to the Interpol European Expert Group on IT crime	22/05/13
Switzerland	Swisscom	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	ECO		18/10/13
The Netherlands	National Coordinator Security and Counterterrorism (NCTV)	National-level		Policy maker / contributor: public authority, national government	10: LoI requested	ECO		07/10/13
The Netherlands	Quanza Engineering	National-level	Information & Communication Technologies	Providers: storage (data centres, cloud operators)	11: LoI sent	ECO		10/12/13
The Netherlands	ACM	National-level		Intermediaries: end users & citizens organisations	12: LoI received	ECO	NL Roadshow	22/11/13
The Netherlands	ACM	National-level		Intermediaries: end users & citizens organisations	12: LoI received	ECO	Internet Security Days	24/09/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
The Netherlands	Dutch Hosting Providers Association (DHPA)	National-level	Information & Communication Technologies	Intermediaries: focus groups including trade associations	12: LoI received	ECO	Outreach individual meeting	12/06/13
The Netherlands	EC3	EU-level	Security services - police structures and equipments	Operational team: international centres on cyber-security / defence	12: LoI received	ECO	Outreach common meeting	28/05/13
The Netherlands	Europol	EU-level		Policy maker / contributor: international bodies and institutions	12: LoI received	ECO	Outreach common meeting	28/05/13
The Netherlands	Europol	EU-level		Policy maker / contributor: international bodies and institutions	12: LoI received	ECO	Outreach common meeting	28/05/13
The Netherlands	NCSC	National-level		Policy maker / contributor: public authority, national government	12: LoI received	ECO	Internet Security Days	24/09/13
The Netherlands	ABN AMRO	National-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Abuse Hub	National-level	Information & Communication Technologies	Operational team: national centres on cyber-security / defence	6: Introduction meeting taken place	ECO	Internet Security Days	24/09/13
The Netherlands	AuditZie	National-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		NL Roadshow	22/11/13
The Netherlands	DearBytes	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
The Netherlands	Esperantoxl	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
The Netherlands	FI-ISAC	International-level	Financial	Intermediaries: end users & citizens organisations	6: Introduction meeting taken place	ECO	ECP Conference	16/11/13
The Netherlands	Gpersoon	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	High Tech Crime	National-level	Security services - police structures and equipments	Operational team: law enforcement	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	ING Bank	EU-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
The Netherlands	ING Bank CCERT	EU-level	Financial	Critical Infrastructure Operator	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Intermax	EU-level	Information & Communication Technologies	Critical Infrastructure Operator	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Leaseweb	EU-level	Information & Communication Technologies	Providers: storage (data centres, cloud operators)	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	MINDEF	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
The Netherlands	Ministry of Economic Affairs	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Ministry of Economic Affairs	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Outreach common meeting	11/06/13
The Netherlands	National Coordinator Security and Counterterrorism (NCTV)	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Outreach common meeting	11/06/13
The Netherlands	National Prosecutor Cyber Crime (NP)	National-level	Security services - police structures and equipments	Operational team: law enforcement	6: Introduction meeting taken place	ECO	Outreach common meeting	11/06/13
The Netherlands	NCSC	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Omerta Information Security	National-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Organisation Name missing	National-level	Unknown	Unknown	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Organisation Name missing	National-level	Unknown	Unknown	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	SemLab	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
The Netherlands	Solcon	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Surfnet	National-level	Information & Communication Technologies	Intermediaries: focus groups including trade associations	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	TNO - Innovation for life	National-level	Research facilities	Research	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Unit 4 IT Solutions	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	UPC Nederland	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	Vodafone Netherlands	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	XS4ALL Internet bv	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place	ECO	NL Roadshow	22/11/13
The Netherlands	AMSIX	EU-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	ECO		20/11/13
The Netherlands	Consumentenbond	National-level		Intermediaries: end users & citizens organisations	8: Information gathering initiated	ECO		22/11/13
The Netherlands	ENCS	EU-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	8: Information gathering initiated	LSEC		20/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
The Netherlands	Ministry of Economic Affairs	National-level		Policy maker / contributor: public authority, national government	8: Information gathering initiated	ECO	Outreach individual meeting	24/05/13
The Netherlands	Open University	National-level	Research facilities	Research	8: Information gathering initiated	ECO		22/11/13
The Netherlands	RIPE NCC	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	8: Information gathering initiated	ECO	NL Roadshow	22/11/13
The Netherlands	RIPE NCC	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	8: Information gathering initiated	ECO		18/10/13
The Netherlands	SIDN	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	ECO		22/11/13
The Netherlands	Terena	EU-level	Research facilities	Research	8: Information gathering initiated	XLAB		27/08/13
The Netherlands	Tilburg University	National-level	Research facilities	Research	8: Information gathering initiated	ECO		22/11/13
The Netherlands	TU Eindhoven	National-level	Research facilities	Research	8: Information gathering initiated	ECO		08/11/13
The Netherlands	Vigilo Consult	National-level	Information & Communication Technologies		8: Information gathering initiated	ECO	NL Roadshow	22/11/13
Turkey	USAK - International Strategic Research	National-level	Research facilities	Research	6: Introduction meeting taken place	LSEC	Botconf2013	06/12/13



Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
Ukraine	Intron Innovations	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
Ukraine	Ministry of internal affairs, cybercrime Division	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
United Kingdom	Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)	International-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	12: LoI received	ECO		03/12/13
United Kingdom	Borwell - Custom software solutions	National-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
United Kingdom	BT	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
United Kingdom	Dante	EU-level	Information & Communication Technologies	Critical Infrastructure Operator	6: Introduction meeting taken place	XLAB		27/08/13
United Kingdom	Deep-Secure	Eu-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
United Kingdom	EXUS	EU-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
United Kingdom	Mira	International-level	Transport	Critical Infrastructure Operator	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
United Kingdom	National Security Secretariat	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	EC3-ENISA meeting	03/10/13
United Kingdom	University of Southampton	National-level	Research facilities	Research	6: Introduction meeting taken place		ICT 2013 Conference	06/11/13
United Kingdom	Akamai	International-level	Information & Communication Technologies	Providers: storage (data centres, cloud operators)	8: Information gathering initiated	LSEC		20/12/13
United Kingdom	Birmingham City University	National-level	Research facilities	Research	8: Information gathering initiated	LSEC		20/12/13
United Kingdom	Geant	EU-level	Information & Communication Technologies	Critical Infrastructure Operator	8: Information gathering initiated	XLAB		27/08/13
United Kingdom	Huawei	International-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	LSEC		20/12/13
United Kingdom	Liverpool JMU	National-level	Research facilities	Research	8: Information gathering initiated		ICT 2013 Conference	06/11/13
United Kingdom	Liverpool JMU	National-level	Research facilities	Research	8: Information gathering initiated		ICT 2013 Conference	06/11/13
United Kingdom	Nominet	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	8: Information gathering initiated	ECO		18/10/13
United Kingdom	Surevine	National-level	Information & Communication Technologies	Providers: system integrators	8: Information gathering initiated	LSEC		20/12/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
USA	FIRST	International-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	1: Identified	DFN-CERT		10/09/13
USA	TM-Forum	International-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	1: Identified	DFN-CERT		10/09/13
USA	Team Cymru	International-level	Information & Communication Technologies	Providers: security solutions	5: Contacted - interested	DFN-CERT		10/09/13
USA	Damballa	International-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
USA	Department of Justice, computer crime division	National-level		Policy maker / contributor: public authority, national government	6: Introduction meeting taken place	ECO	Octopus Conference 2013	09/12/13
USA	Facebook	International-level	Information & Communication Technologies		6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
USA	GSMA	International-level	Information & Communication Technologies	Providers: mobile network providers	6: Introduction meeting taken place	ECO	Webinar of CITEL	17/11/13
USA	Internet Identity	International-level	Information & Communication Technologies	Providers: security solutions	6: Introduction meeting taken place	ECO	RIPE 67	16/10/13
USA	ISOC	International-level	Information & Communication Technologies	Intermediaries: end users & citizens organisations	6: Introduction meeting taken place	ECO	CITEL, ISOC, ITU anti-spam meeting	08/10/13
USA	MAAWG	EU-level	Information & Communication Technologies	Policy maker / contributor: international bodies and institutions	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13

Country	Organisation Name	Scope	Sector	Cyber security positioning	Process status	Proposed by ACDC partner	Context	First contact on
USA	Shadowserver foundation	National-level	Research facilities	Research	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
USA	University of Oregon	National-level	Research facilities	Research	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
USA	University of Washington	National-level	Research facilities	Research	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
USA	Visa	International-level	Information & Communication Technologies	Providers: system integrators	6: Introduction meeting taken place	ECO	MAAWG meeting	09/06/13
USA	ISOC	International-level	Information & Communication Technologies	Intermediaries: end users & citizens organisations	8: Information gathering initiated	ECO	Outreach individual meeting	15/10/13
USA	SourceFire	International-level	Information & Communication Technologies	Providers: security solutions	8: Information gathering initiated	LSEC		20/12/13

Table 17 – overview of ACDC potential stakeholders and follow-up