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

Deliverable	**D5.1.1 – Dissemination plan**
Work package	WP5
Due date	30/04/2013
Submission date	03/05/2013
Revision	1.05
Status of revision	Final
Responsible partner	Engineering Ingegneria Informatica
Contributors	Véronique Pevtschin (EII), Barbara Pirillo (EII), Toni Felguera (BDIGITAL), Dan Tofan (CERT-RO), Jochen Schoenfelder (DFN-CERT), Christian Nordlohne (Institute for Internet Security), Ignacio Caño Luna (INTECO), Edgardo Montes de Oca (Montimage), Michael Weirich (eco), Goran Skvarc (CARNet), Aleš Černivec (XLAB), Will Rogofsky (CyDef), Jeronimo Nuñez Mendoza (TID), Rumen Dontchev (BGPOST), Ann Mennens (KUL), Tiziano Inzerilli (ISCTI), Fernando Kraus Sanchez (ATOS), Paolo De Lutiis (Telecom Italia), Monika Josi (MICROSOFT EMEA).
Project Number	CIP-ICT PSP-2012-6 / 325188
Project Acronym	ACDC
Project Title	Advanced Cyber Defence Centre
Start Date of Project	01/02/2013

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

Version history

Rev.	Date	Author	Notes
1.03	18/03/2013	Véronique Pevtschin	First table of content for contribution
1.04	22/04/2013	Barbara Pirillo All partners	Integration of all contributions

Glossary

ACDC	Advanced Cyber Defence Centre

Table of contents

Table of tables

D5.1.1 – Dissemination plan

1. Executive summary

ACDC is a large pilot project, run as a European co-funded initiative until July 2013, with the aim to continue beyond this deadline as a community run centre, providing not only botnet fighting services but also additional cyber-protection services to a wide community.

The seed activities are all included in the ACDC project, and the dissemination plan is an important component supporting these activities.

The dissemination plan detailed below involves all partners, identifies key stakeholders and how these will be adressed along awareness, participation and adoption directions.

2. Introduction

Deliverable D5.1.1 is the first version of the ACDC pilot project dissemination plan.
The ACDC dissemination plan is part of a wider community oriented approach in which ACDC aims to deploy a comprehensive interconnected set of support centres to help European citizens and organisations to fight the negative impacts of botnets.

This pilot project is set in a wider context of the European Cyber-Security Strategy and the ACDC dissemination plan therefore defines the overall umbrella under which the ACDC pilot project

- Sets up specific visibility actions to create *awareness*
- links to the project exercises to foster *adoption* through best practices as well as *contributions* of new solutions to the ACDC European centre
- identifies and animates a community of stakeholders beyond the ACDC partners (WP6)

To fully understand the choices of the dissemination plan, D5.1.1 is structured in the following sections:

- section 1 introduces the European context in which ACDC operates
- section 2 identifies the dissemination goals
- section 3 structures the target audience into categories and specifies the dissemination messages for awareness, adoption and contribution
- section 4 lists the concrete set of activities envisaged by ACDC
- section 5 introduces the metrics to monitor the dissemination activity and which will be detailed in D5.1.2, D5.1.3 and D5.1.4 to evaluate the impact of dissemination and, if needed, realign the initial plan

3. The European and national contexts for cyber-defence

This section provides an overview of the key initiatives on-going within and across Member States and at European level to build up a cyber-defence capability.

Initiative	*National / regional / European*	*Relevance to ACDC*
European Cyber Security Month 2013	European	European program, managed by ENISA, In accordance with the EU CyberSecurity Strategy, with the scope of promoting cyber-security across Europe. Romania will be part of this initiative in 2013 and will help in promoting the message and results of the ACDC project.
National Cyber Security Strategy	National (Romania)	Romania`s National Cyber-Security Strategy has been released recently. It is in accordance with the EU Cyber-Security Strategy and its main purpose is to strenghten the security of the national cyber-space. The results of the ACDC project could be used in achieving our objectives.
National CyberCrime Defence Center – SMIS code 37595	National (Romania)	EU funded project that aims to prepare a 40 persons trained cyber-security team within Romanian public institutions that deal with cyber-crime.
Romanian Digital Agenda	National (Romania)	As part of Europe Digital Agenda 2020

EU Cyber Security Strategy	European Joint presentation by DG-Home, DG-CNECT, EEAS	The EU Cyber Security Strategy recommends the enhancement of European and international cooperation, including the launch of an initiative to fight botnets. It also lists a key number of stakeholders that are direct targets for the ACDC dissemination and community activities
Cyber-Europe exercises	European / ENISA	The Cyber-Europe exercises are managed by ENISA to create collaboration for managing cyber-threats across Europe. This initiative is relevant to ACDC as a target for collaboration with the ACDC clearing house.
Telefónica Security Services	National/ Telefónica Group: Spain, UK, German, Ireland and Czech Republic	Telefonica provides security services to its users. This services are aligned with the fight against spam, malware and others security problems. (http://www.telefonica.com/es/digital/html/digital_services/security.shtml)
Spanish Digital Agenda	National (Spain)	One of the main objectives of the Spanish Digital Agenda is to strengthen the citizens' confidence in new technologies. One of the courses of actions for this objective points at INTECO as centre of excellence in digital trust. This initiative is relevant to ACDC for the Spanish support centre.
Spanish Cibersecurity Strategy	National (Spain)	Standards and best practices develop in cibersecurity and promotion of its adoption. The Strategy also develops cibersecurity exercises program.
Institutional cooperation with other MS using local agreement (Spain) between Ministry of Home Affairs and Ministry of Industry • Agreement with Critical Infrastructure Protection • Cooperation with Law Enforcement Agencies (cibercrime, and ciberterrorism) • Awareness, training and ciber-exercises	National (Spain)	The direct contact with key govermental organizations and authorities may allow an open communication channel and discussion about new possible lines of agreement specifically related to botnets incidents
Working Group	National (Spain)	Possibility to use a similar strategy and to localize the acquired

with national ISPs to develop a collaborative protocol in order to prevent cybercrime. This working group has recently started and the protocol is not yet available		knowledge.
CCN-CERT	National (Spain)	Provide security alert services for public administration, alert bulletins, incident management, security training, …
Mando de Defensa del Ciberespacio (Defense Control of Ciberspace)	National (Spain)	National initiative that contributes to the appropriate response in the cyberspace to threats or attacks that may affect national defense.
FCCN	National (Portugal)	Formal network of CSIRTs, which includes members from ISPs, Banks, Critical Infrastructure operators, etc... FCCN is also a partner of the Portuguese Safer Internet Program and operates de Academic Network.
CSA-SI (CSA Slovenian Chapter)	National (Slovenia)	CSA-SI promotes security mechanisms available for the use within cloud computing. It also promotes localisation of research on the Slovenian level. ACDC could benefit by dissemination through CSA-SI where potential end-users could be obtained.
RESOLUTION on the National Security Strategy of the Republic of Slovenia	National (Slovenia)	Act states that Slovenia will create a national strategy for responding to cyber threats and the misuse of information technologies, and adopt necessary measures to ensure effective cyber defence.
ICS – Institute for Corporate Security Studies (http://www.ics-institut.com/en)	National (Slovenia)	The mission of the ICS Ljubljana is to incorporate and develop new knowledge, experiences, findings and needs as well as to promote interests in the field of corporative security in, both, national and international environments. ACDC could find additional stakeholders and interested parties with collaboration with ICS.
European Cyber Crime Centre (EC3)	European	The Centre will become the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of cyber attacks. It will support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners. *EC3 actively fights botnets in Europe and contributes to the ACDC*
FCCU – Federal Computer Crime Unit	National (Belgium)	The Federal Computer Crime Unit FCCU of the Belgian Federal Judicial Police is the central service coordinating, organising the working environment for Belgian police services in the field of : - Combating cybercrime (hacking, espionage, sabotage, fraud, …) - Digital forensics (computers, networks, internet) The FCCU is active on policy level as well as on operational level. It is trying to create partnerships and circumstances for a safer cyberspace. It works therefore on national

		and international level on different platforms : the Belgian Network for information security – BELNIS (advisory body to the Federal government), the European Cybercrime Task Force (EUCTF – association of EU heads of national cybercrime units), Europol with the European Cybercrime Centre, Interpol and many others *FCCU is actively involved in identification, analysis and takedown of botnet command and control servers* *http://www.polfed-fedpol.be/org/org_dgj_FCCU_RCCU_nl.php*
CERT.be	National (Belgium)	CERT.be is the federal cyber emergency team and its constituency is providers of key resources and critical infrastructures: Banks; ISPs; Energy providers; Transport providers; Any institution or company identified as CIP; Federal, Regional and Community Public bodies as well as the individual internet users. *CERT.be is an essential part of the cyber resilience preparedness and tracks cyber-threats such as botnets in the Belgian territory.* *www.cert.be*
Cyber Security Strategy for Belgium	National (Belgium)	The Belgian federal Cyber Security Strategy identifies 3 strategic objectives which are to be realised through different initiatives in eight identified action domains: 1) a safe and reliable cyberspace, 2) an optimal security and protection for critical infrastructures and governmental information systems, 3) the development of national cyber security capabilities *The Strategy will help Belgium to identify and fight cybersecurity menaces (including botnets) more efficiently.* *See www.b-ccentre.be*
B-CCENTRE – Belgian Cybercrime Centre of Excellence for Training, Research and Education	National (Belgium) – European as part of the 2CENTRE network	B-CCENTRE provides a platform for exchange of knowledge and information for actors involved in fighting cybercrime in Belgium. It conducts research, provides training and contributes to awareness raising regarding cybercrime, including botnet related issues. It collaborates with similar centres throughout the EU Member States.
Law of July 1st 2011, transposing the EC Directive 2008/114/EC on the identification and designation of critical infrastructures	National/European	The law calls for an enhanced level of protection of electronic communications and aims to reducing vulnerability of this critical infrastructure. For the ACDC, it means Belgium is focused in preventing large scale attacks (e.g. botnets) that may compromise electronic communications operations in the country.
Government CERT BG	National	BG national CERT - a potential client of ACDC data and tools.
Joint Cyber Unit – MOD BG	National (Bulgaria)	Newly established initiative from NATO(NATO Computer Incident Response Capability(NCIRC)) collaborating with Bulgarian MOD to counter national cyber threats. A potential client of ACDC data and tools.
Security Service	National	An initiative with Chief Directorate "Combating Organized Crime" (CDCOC) focusing on investigating cyber threats from foreign agencies.

GovCertUK	National (UK)	UK's national CERT, run by GCHQ. A potential client of ACDC data/tools.
Joint Cyber Unit	National (UK)	Newly-established initiative from GCHQ/MOD to counter national cyber threats. A potential client of ACDC data/tools.
Security Service	National (UK)	An initiative from GCHQ/MOD focusing on investigating cyber threats from foreign agencies.
Centre for the Protection of National Infrastructure	National (UK)	An extension of the Security Service that uses its intelligence to inform work on standards and vulnerabilities.
European Public-Private Partnership for Resilience (EP3R)	European	EP3R is investigating strategies enhance the security and resilience in Europe. Specific work packages have been established about botnet: Tracking Down Botnets Offenders, Cyber Attacks Mitigation and Response, Wide-Scale and Systematic Malware Disinfection. It is important to maintain a strict relationship with that WPs in order to avoid duplication of work and at the same to cover all the aspects needed by an effective anti-botnet strategy
ETSI	European	ETSI is one of the main European SDO and is active in many security aspects of the telecom industry (e.g. NGN, Smart Card, etc.). The security and resilience of the Telco architecture is one of the main concern of ETSI and ACDC can collaborate with many ETSI Technical Committee.
ITU-T	Worldwide	ITU-T has many ongoing security standardization activities (e.g. Cybersecurity Information Exchange or CYBEX, offers the tools to ensure rapid, internationally-coordinated responses to cyber threats). ACDC can collaborate in particular with the SG17, which is dedicated to the security.
Nemesys	European	EU funded project dedicated to the mobile botnet. etc.
TERENA TF-CSIRT	European	TF-CSIRT is a task force that promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions, whilst liaising with relevant organisations at the global level and in other regions. TF-CSIRT provides trusted exchange between CSIRT teams on a European basis. It also provides team accreditation and certification services. Both activities provide opportunities for ACDC dissemination especially inside the CERT community, with the accreditation process also being relevant to user management.
National Information Security Act	National (Croatia)	Act that says that CARNet operates National CERT as a separate department. National CERT is in charge for the security of all Internet users in Croatia except government users, and is at the same time National Point of contact (PoC) for incident reporting when the source of the incident is foreign.
Regulation of the national telco agency (HAKOM) about "The means and deadlines for the implementation of measures for		This Regulation instructs all ISPs to cooperate in solving severe incidents on their infrastructure with CERTs in charge for this.

protection and security of integrity of information networks”		
Initiative-S	National (Germany)	A website monitoring service for the security of the Internet presences of national customers
Botfrei.de	National (Germany)	A Web Project dedictated to give information about PC security and provides Tools and Tests related to security software and PC security in general. It includes the following dissemination platforms, which are already well-known and highly frequented: • website (www.botfrei.de), • weblog http://blog.botfrei.de, • several threat optimized landing pages (e.g. www.bka-trojaner.de or www.dnschanger.eu) for dedicated types of incidents and • support-forum (http://forum.botfrei.de).
Anti-Botnet-Center	National (Germany)	In order to help affected customers, eco provides with the Anti-Botnet-Beratungs-Zentrum (ABBZ) a national Support Centre solution for Germany, elaborating incident based step-by-step advisories and assisting end customers getting rid of reported security incidents.
CESICAT	Regional	CESICAT (*Centre de Seguretat de la Informavió de Catalunya*) is the Catalan Goverment security agency. As such its mission is to provide awareness about on-line security amongst the Catalan public administration and particularly its associated critical infrastructures. CESICAT can be a strong ACDC recommender at its local and regional influence domain.

Table 1 – list of key initiatives relevant to ACDC

4. Dissemination goals

The previous section highlights that ACDC operates in an extensive environment at EU and Member States level. While on the one hand the dynamics of this environment provide ACDC with a real opportunity for visibility and impact, its complexity requires that the dissemination plan identify clear goals, supported by a detailed implementation approach.

The dissemination activity aims to achieve the following goals:

- Create awareness
- Raise interest
- Foster adoption as user of one or more of the ACDC services
- Foster adoption as contributing one or more solutions to the ACDC services

4.1. Awareness

The awareness activity is organised to provide a first level of information about ACDC, to create visibility about its existence, main goals and milestones. The awareness will be enhanced by paying specific attention to demonstrate the “tangible” outcome of the project, in clear and comprehensible language.

4.2. Interest

Raising interest is a second goal of dissemination, in which the main focus is to position ACDC as providing an interconnected set of support centres that can be useful to

- Users / victims of cyber-attacks to restore their devices to normal operation
- Organisations to understand the potential negative impact of botnets to their processes and how to avoid them
- Operators of critical infrastructures in the benefits of increasing their level of protection and the need for collaboration
- etc

4.3. Adoption by users

The "*adoption by users"* goal is designed to ensure that the services designed by ACDC are actually used by end-users, citizens, public administrations, industrial and research organisations to mitigate the results of a cyber-attack.

4.4. Adoption by providers

The "*adoption by providers*" goal is designed to ensure that ACDC's continuous service oriented approach remains dynamic, in enticing providers of innovative solutions to make them available to users through the ACDC central clearing house or national support centres.

5. Dissemination audiences: target categories and messages

Category	Awareness	Interest	Adoption as user	Adoption as contributor
Category name: EP / PM *Description*: EU Parliament Policy makers (at EU level and at Member States level)	ACDC exists and is the first step of a networked cyber-security approach	ACDC is working to create a set of interconnected support centres to fight botnets. This is in direct support of the European cyber-security strategy.	Not applicable	Not applicable
Category name: MS Users *Description*: Member States (as users, national governments)	ACDC exists and is open to expansion Cooperation and collaboration with other MS National CERTs Institutional cooperation with other MS using local agreement (Spain) between Ministry of Home Affairs and Ministry of Industry ...	ACDC is available to link to new Member States support centres INTECO can make available its network of CERT contacts... CERT interested in international view of fighting botnets MS governments interested in selling their activities related to fight against botnets and promoting a trustworthy internet	Join the ACDC network and benefit from the availability of different services; Higher impact when mitigating international networks of botnets and C&C servers Promoting e-commerce, improving protection and avoiding disruptions in critical infrastructures	Join ACDC and contribute by linking one or more support centres to the ACDC infrastructure Implementing ACDC project recommendations in their countries Using ACDC platform solution and services
Category name: EC *Description*: EU Commission	ACDC exists and is a key step in the fight of botnets	ACDC directly addresses the European cyber-security strategy (mentioned in the strategy in the fighting botnets initiative)	Connect to ACDC to protect the European infrastructures	Link the EU-CERT facility as a support centre in the ACDC set of interconnected centres

Category	Awareness	Interest	Adoption as user	Adoption as contributor
Category name: Agencies *Description*: EDA, ENISA, CEPOL, Europol (EC3), JRC	ACDC exists and is a key step in the fight of botnets	ACDC's community is open for agencies to join	Use the services provided by ACDC Integrate one or more services in Cyber-Europe exercises Use ACDC as a training support for specialised officers (CEPOL, Europol)	Contribute information to the data collection phase service of ACDC
Category name: law enforcement *Description*: EDA, ENISA, JRC Description: Europol, Interpol, Cepol, national institutions	ACDC exists and is a key step in the fight of botnets	ACDC's community is open for agencies to join	Use the services provided by ACDC Integrate one or more services in Cyber-Europe exercises Use ACDC as a training support for specialised officers (CEPOL, Europol) Use the data gathered by ACDC for further analysis	Contribute information to the data collection phase service of ACDC
Category name: R&D projects	ACDC exists and is open to expansion	Using the tools and technologies developed in ACDC for new R&D projects with the objective of fighting botnets.	-	Technologies and products developed in ACDC could be used in R&D projects for further developing new products for botnet fighting.
	ACDC exists and is a new way in the fight of botnets	New algorithms for detection the network topology	Use ACDC to detect the botnets master	Provide ACDC users the knowledge about who is managing the botnets.
	European projects: ASASEC, Cloud CERT, SCADA LAB National projects: Cybersecurity tools and services	Spread ACDC knowledge to other international projects	Reuse solutions in the area of cyber-security.	Lessons learned from similar projects.

Category	Awareness	Interest	Adoption as user	Adoption as contributor
Category name: universities	ACDC exists and is a key step in the fight of botnets	Universities could be attracted to use the tools and technologies developed in ACDC for keeping their networks clean.	The tools can be used by individuals (e.g. students) to protect themselves against botnets.	Connect to ACDC to protect and offer expertise in protecting European infrastructures and also spread the ACDC message. The ACDC project could also be extended to universities that can contribute in the detection.
		Expand the Cluster on Security Technologies that Telefonica Maintains in cooperation with various universities.	Research projects.	Seeking opportunities for information sharing and collaboration in research projects of common interest.
		ACDC is open for new ideas and technology provided by researchers	Not applicable	Contribute information to the different phases of ACDC

Category	Awareness	Interest	Adoption as user	Adoption as contributor
Category name: General Public	ACDC exists and is a key step in the fight of botnets	ACDC is working to create a set of interconnected support centres to fight botnets. Around the field of botnets has developed a real underground cybercrime economy. The normal user can fall as a victim every moment. Eurostat 2010[1]: 22% of internet users in E.U encountered infections in the last 12 months.	General public can join the ACDC network and benefit from the availability of different services, including protection, tutorials and support, by using the tools provided in the project.	Contribute information to the data collection phase service of ACDC, if possible.
	-	ACDC is going to allow fighting against bots at the network connection point of the infected user.	Connect to a network that allows to stop and to correct their infections.	Feeding bots database of ACDC.
	ACDC exists and is a key step in the fight of botnets.	-	Use ACDC to get help in case of a Virus infection.	Not applicable
	Citizens: getting closer to a trustworthy internet society Companies: measures to avoid business interruption	Citizens: how to disinfect and mitigate botnet damage Companies: how to disinfect and mitigate botnet damage	Citizens: enhance knowledge society Companies: enhance e-commerce	Citizens: rating of tools and services for continuous improvement. Companies: idem

[1] Giles HOBBEN (ed.), *Botnets: Detection, Measurement, Disinfection & Defence*, ENISA, p.28

Category	Awareness	Interest	Adoption as user	Adoption as contributor
Category name: Internet Service Providers	ACDC exists and is a key step in the fight of botnets.	ACDC is working to create a set of interconnected support centres to fight botnets. The ISP has to provide the user with the security it needs. Botnets are a constant danger in the cyber security environment. Maintaining a clean network is one of the objectives of an ISP.	Join the ACDC network and benefit from having real time information regarding botnet activity.	An ISP can be of great importance to the project, because they can provide valuable information regarding botnet activities within their network. They can contribute with information to the data collection phase service of ACDC, if possible.
	ACDC exists and is a key step in the flight of botnets.	ACDC's community is open for agencies to join.	Use ACDC to get reports, protect own infrastructure and benefit from the availability of different services	Contribute information to the data collection service (Data Clearing Centre) of ACDC.
	Working procedures and SOPs in the ACDC project, benchmarks, standards	-	-	-
Category name: Health facilities operators	ACDC impacts Critical Infrastructure Protection	How ACDC protects CIP infrastructures	My facilities are not disrupted by botnets	Being associate party as part of ACDC community
Category name: Utilities facilities operators	ACDC impacts Critical Infrastructure Protection	How ACDC protects CIP infrastructures	My facilities are not disrupted by botnets	Being associate party as part of ACDC community
Category name: Companies (SMEs, Large companies) in other sectors	ACDC exists and is a key step in the fight of botnets. Understand the threats and help find solutions	Help and support to fight botnets	Join the ACDC network and benefit from the availability of different services	Contribute information to the data collection. Evaluate ACDC solutions to improve usability.
Category name: National Level Agencies and Administrations	ACDC exists and is a key step in the fight of botnets. Understand the threats and help find solutions	Help and support to fight botnets	Join the ACDC network and benefit from available services, including data on infections and tools. Use data and tools to keep servers clean.	Contribute information to the data collection. Evaluate ACDC solutions to improve usability. Possibly provide supporting infrastructure.

Category	Awareness	Interest	Adoption as user	Adoption as contributor
Category name: technology providers	ACDC exists and is a key step in the fight of botnets. CheckPoint, MS Spain, Google Spain, Panda Security, etc.	ACDC can be incorporated as new features in existing IT security solutions. Interoperable standards	Connect to existing security solutions. How to implement their solutions as part of ACDC	Provide information to ACDC provider to apply for innovative security solutions against botnets. Commercial solutions to plug into ACDC
Category name: Hosting Providers *Description:* Web Hosts, Data Centres	ACDC exists and is a key step in the fight of botnets	ACDC is working to create a set of interconnected support centres to fight botnets. Reducing the prevalence of botnets on customers' servers has a positive impact on hosting providers' reputations. Integrating botnet-related tools can drive further revenue.	Join the ACDC network and benefit from available services, including data on infections and tools. Use data and tools to keep servers clean. Use tools as an additional sales channel.	Contribute valuable data on botnets and infections (as with Internet Service Providers). Possibly provide supporting infrastructure.
Category name: Standard Development Organization	ACDC exists and is a key step in the fight of botnets	ACDC directly addresses the European cyber-security strategy (mentioned in the strategy in the fighting botnets initiative)	Not applicable	Many ETSI TCs could contribute to the technological/scientific aspects of the Pilot
Category name: industry	ACDC exists and is point of contact for information and help	ACDC provides information on cyber security	Use ACDC to protect own infrastructure	
Category name: Financial institutions	ACDC exists and is a key step in the fight of botnets	ACDC exists and is a powerful European initiative committed to prevent and eradicate financial fraud caused by botnets	Use of the services to be offered by ACDC, specially for detection and mitigation	Contribute to the collection of information on real attacks in a federated and aggregated manner

Table 2 – target audiences and messages

6. Dissemination actions

6.1. ACDC partners

The following table lists for each partner involved in task T5.1 the concrete contributions made to the dissemination activity.

Partner	Contribution to dissemination
ATOS	• Inform the different areas in Atos involved in IT security solutions of the ACDC initiative and address ACDC in our yearly international Atos Defence and Security workshop • Include ACDC in our Atos Marketing e-boletin, in Axia magazine, in the Lookout Report, in ARI 2013 Handbook and in next issues of AscentJourney • Raise awareness of ACDC in presentation to customers, roundtables, seminars, workshops, etc.
BDIGITAL	BDIGITAL develops several technological dissemination activities through the year, being on-line security a topic which, due to its societal relevance, it is always under the scope. The proposed contribution to ACDC dissemination will be by hosting a session on ACDC in the BDigital Global Congress 2014 edition. In addition the BDIGITAL's ACDC team will also attempt to disseminate the project along the following lines: - Participating in the Antiphising Working Group (APWG) - Dissemination within the Dorothy Project organization - Dissemination within the Cloud Security Alliance (Spanish chapter and internationally) - Dissemination within the ISMS Forum –Spain and participating in the Spanish Cyber Security Institute (SCSI) events BDIGITAL will also disseminate the project through the companies and organizations that belong to the ICT Cluster as well as through the project Be.Wiser, a Coordinated and Support Action within the Regions of Knowledge (ROK) program, on wireless and Internet Security in European regions.
BGPOST	• In the very beginning ACDC will be deployed and tested in BGPOST network • ACDC dissemination inside network infrastructure the Ministry of Transport, IT and Communications and to some government agencies and organizations • The next step is to involve some bank institutions and private companies. • Building awareness in Universal Postal Union (UPU) and in other bodies in which Bulgarian posts participate. • Meetings with the Cyber defense and antivirus laboratory of Bulgarian Academy of Sciences (BAS) • Participation in International Telecommunication Union' (ITU) Cyber defense conferences, International Data Corporation's (IDC) IT Security Roadshow 2014/5 in Bulgaria • Meetings with the Chief Directorate "Combating Organized Crime" (CDCOC) focused on investigating cyber threats and anti-botnet

	• Advertising relevant ACDC services in BGPOST' website. • Explain and examine the ACDC' role at a minimum of 2 national Cyber security conferences
CARNet	Croatian Academic and Research Network – CARNet (national NREN) together with its Department for National CERT will conduct a nationwide dissemination campaign about the ACDC project and anti-botnet platform to all Internet users and service providers in Croatia. This will include CARNet contribution to preparation of the dissemination plan and its implementation on a national level with all PR means at our disposal.
CERT-RO	• At least 1 international conference in 2013 on cyber security threats, (''New Global Challenge in Cyber Security 2013''); the ACDC project will also be addressed. • 3 or more technological seminars (with closed audience) on the subject of efficiently handling cyber security threats; the ACDC solutions will also be addressed. • Providing a strong connection to the Romanian community of users through our site, www.cert-ro.eu and our social media channels (Facebook, Twitter, LinkedIn etc.). • Press releases for the national press regarding the message and solutions of the project. • TV spots on the Romanian national public television network (TVR) meant to promote the ACDC project & message and the struggle against botnet activity (if the video-clips are provided within the project). • Providing a strong link to the Romanian internet service providers, and a lobby for the adoption of the solutions provided in the project. • National support center, which we are about to implement in the next steps of the project, designed to offer tools, tutorials and all the necessary information for both normal and experimented user to utilize in the fight against cyber security threats such as botnet.
CyDef	• Advertise relevant ACDC services in public reports (World Hosts Report and White Papers). • Explain and examine the role of ACDC at a minimum of 3 conferences (these are dependent on invitations, but as examples, conferences recently spoken at include APWG, Clusit, MAAWG, NATO and OSCE). • Refer clients to ACDC services where relevant and appropriate. • Provide a detailed dossier on UK stakeholders (as listed in *The European and national contexts*) where required.
DFN CERT	Link to the European CERT community through the means of TF-CSIRT cooperation. Presentations and tutorials for DFN-CERT's constituency which forms of universities and research institutions throughout Germany and Europe.
ECO	• Link to the German community of users and providers • eco will provide a (locally) centralized reporting infrastructure, distributing all relevant data to the necessary stakeholders. (all relevant industry partners, like ISPs or anti-virus vendors, national authorities, like law enforcement agencies or national CERTs) • Publications • Infrastructure for public and project website • Active promotion in social network platforms (like Google+ and Facebook)
EII	Link to Italian community of users and providers

	Coordination of dissemination implementation Dissemination monitoring Public Web site: structure, content update and content definition (in collaboration with eco) Presentations preparation ACDC Graphical chart definition Publications and events coordination
FCCN	Dissemination inside the “National Network of CSIRTs”, reaching ISPs, banks, CI, etc… Interation with the Portuguese Safer Internet project to find common ground and dissemination opportunities. Enrollement of the Portuguese Telecom Regulator in the project, to establish a partnership for, among other tasks, disseminate the ACDC project on national level.
IF(IS)	Select security conferences and scientific journals to present the ACDC results to an academic audience
INTECO	• OSI Website: the website may be a support tool for dissemination in Spain. • Point of contact with Spanish LEAs, ISPs and other interested areas • Scientific papers and publications • Promotion through industry events such as ENISE • Media coverage to the general public • Online channels to spread project results • Social media posts: twitter, tuenti, facebook, google+ • INTECO blogs • Newsletter channel • Printed material providing high-level information • Contact with policy makers • Seminars • Workshops • Online training • Press releases • Reports • Guides and support materials • Events & conferences • Working groups • Press conferences • Media Interviews (press, radio, and TV)
ISCTI	ISCTI will contribute to the consolidation of relevant project results within the following bodies where it participates as active member: • ENISA (European Network and Information Security Agency) • ITU (International Telecommunication Union) Italian national support center web site might be used as a means for implementing awareness campaign by ISCTI in collaboration with the other Italian partners. ISCTI plans to organize a workshop at the Ministry site at the end of the project to disseminate project results. Relevant events in the field of cyber security with national and international scope will be considered for participation of ISCTI in order to disseminate the project results
KUL	KUL will actively contribute to the implementation of the dissemination

	strategy as the coordinator of the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE), a platform for cooperation between academic, governmental and private partners in the fight against cybercrime in Belgium and beyond. The B-CCENTRE has a large multi-disciplinary network of experts dealing with cybercrime, including different target categories for dissemination. KU Leuven will provide content for the central ACDC website and will disseminate the results of its tasks through participation in conferences and workshops and publication of results in Journals and conference proceedings with a high impact, e.g., USENIX. The B-CCENTRE will use its network of expertise and contacts in Belgium, as well as in the rest of Europe to spread the word on the project and its activities and results to a targeted audience, including by means of the B-CCENTRE website and awareness raising initiatives. The B-CCENTRE website (www.b-ccentre.be) will be hosting the Belgian localised section of the ACDC portal.
LSEC	To be included in the next release of D5.1.1
MontImage	• Create general awareness about project objectives and expected results • Establish links with related initiatives and projects. • Increasing the market potential involving the presentation of the tangible/exploitable results • Publications presentation in relevant exhibitions and events • Organisation of an international workshop • Define a open source strategy for our tool Examples of activities done or about to be done: • Contribution to the System@tic's (regional competitivity pole's) R&D Book • Presentation of project to the French DGA (meeting in Rennes) and in Thales' PME Security Day • Presentation of project in the APWG (CeCOS VII)
Microsoft EMEA	• Dissemination to contacts to potential stakeholders such as National CERT's, ISP's as well as other industry players • Dissemination of the results of ACDC through Microsoft Events such as Digital Crimes Consortium • Policy recommendations from our EU Policy group
Telecom Italia	• Link to Italian community of users and providers • participation to the dissemination actions (event presentation, paper, articles publications, etc.) • Public Web site (Italian "localization"): structure, content update and content definition (in collaboration with other Italian ACDC partners) • Advertise the ACDC Pilot resources (Public Web site, Pilot events, etc.) through Public Telecom Italia Web Sites and corporate magazines. • Advertise the ACDC Pilot resources through TI corporate strategic accounts on Social Networks (e.g. Linkedin)
Telefónica I+D	• ACDC dissemination inside different areas and companies of Telefónica Group. • Participation in standard bodies such as IETF, 3GPP, ITU-T and ETSI. • Building awareness in ISOC and in other bodies in which Telefónica participates. • Attempted participation in relevant events like Campus Party.

	• Meetings with the university cluster on Security Technologies hosted by Telefonica. • Participation in conferences of the Spanish Network Operators Group (ESNOG/GORE). http://www.esnog.net/
XLAB	dissemination on local conferences in Slovenia and Croatia, dissemination activities of the Consortium as a whole: • co-authoring papers, • providing materials for the ACDC web page, webinars, demonstrators

Table 3 – list of partners role in dissemination

Partner	Contact	Email
ATOS	Pedro Soria	Pedro.soria@atos.net
ATOS	Fernando Kraus	Fernando.kraus@atos.net
BDIGITAL	Antoni Felguera	afelguera@bdigital.org
BGPOST	Rumen Donchev	rdontchev@bgpost.bg
BGPOST	Katia Velikova	k.velikova@bgpost.bg
CARNet	Goran Skvarc	Goran.Skvarc@CARNet.hr
CERT-RO	Daniel Ionita	daniel.ionita@cert-ro.eu
CERT-RO	Mihai Rotariu	mihai.rotariu@cert-ro.eu
CERT-RO	Dan Tofan	dan.tofan@cert-ro.eu
CERT-RO	Gabi Ene	gabriel.ene@cert-ro.eu
CyDef	Jart Armin	jart@cyberdefcon.com
CyDef	Will Rogofsky	will@cyberdefcon.com
DFN CERT	Klaus-Peter Kossakowski	acdc@dfn-cert.de
ECO	Thorsten Kraft	Thorsten.kraft@eco.de
ECO	Yvonne Vering	Yvonne.vering@eco.de
ECO	Michael Weirich	Michael.weirich@eco.de
EII	Véronique Pevtschin	Veronique.pevtschin@eng.it
EII	Barbara Pirillo	Barbara.pirillo@eng.it
FCCN	Luis Morais	Luis.morais@fccn.pt
FCCN	Tomás Lima	Tomas.lima@fccn.pt
IF(IS)	Christian Nordlohne	nordlohne@if-is.net
INTECO	Ignacio Caño Luna	ignacio.luna@inteco.es
ISCTI	Tiziano Inzerilli, Sandro Mari	tiziano.inzerilli@mise.gov.it, sandro.mari@mise.gov.it
KUL	Ann Mennens	ann.mennens@b-ccentre.be
LSEC	Ulrich Seldelslachts	ulrich@leadersinsecurity.org
MontImage	Edgardo Montes de Oca	edgardo.montesdeoca@montimage.com
Microsoft EMEA	Monika Josi	Monikaj@microsoft.com
Telecom Italia	Paolo De Lutiis Sebastiano Di Paola	paolo.delutiis@it.telecomitalia.it Sebastiano.DiPaola@it.telecomitalia.it
Telefónica I+D	Jerónimo Núñez Mendoza	jnm@tid.es
Telefónica I+D	Pedro García Parra	pedrogp@tid.es
Telefónica I+D	Diego R. López	diego@tid.es

XLAB	Daniel Vladušič Aleš Černivec	daniel.vladusic@xlab.si ales.cernivec@xlab.si

Table 4 – list of contacts per partner involved in the dissemination task T5.1

6.2. Links to the community approach (WP6)

The community approach deployed in WP6 forms an integral part of the dissemination plan and is considered as one of the implementation tools of dissemination.
The strategy for the community approach is to enable stakeholders beyond the ACDC partners to become involved in ACDC with different levels of involvement; the link is implemented by directly mapping the different levels of involvement to the different dissemination goals, i.e. from staying aware to becoming active participants.

The mapping to the different levels of involvement will be further detailed in D6.1.1 where the users will be identified.

6.3. Channels of dissemination

ACDC uses multiple channels for dissemination, including

- ACDC graphical chart
- Web site
- Participations to events
- etc

The following table provides a link between the dissemination goals and the contribution of each of the dissemination channels.

Channel	Contributes to dissemination goal	Detailed information
Graphical chart	All	The graphical chart of ACDC directly links to the goal of “fighting botnets”. Annex 1 details the elaboration of the logo concept
Public Web site www.acdc-project.eu	Awareness Interest Adoption	This is the central entry point to ACDC at European level in terms of information, community and participation. It is therefore also the key online visibility presence for ACDC. It is NOT used to access the actual botnet fighting solutions, for which dedicated Web site www.botfree.eu is used.
Public Web site Www.botfree.eu	Adoption (as users of services)	This is the services access point for ACDC. This online portal is set up to access the solutions by ACDC, and links to the acdc-project.eu for more information. The point is to simplify access for solutions through this very simple design.

Channel	Contributes to dissemination goal	Detailed information
Community social platform	Interest Adoption	The public Web site will link to the community social platform (WP6) designed to allow both public and user-identified access to ACDC. The specific contribution of this section is to allow users and providers to share information and create discussion threads. This approach will be further developed in WP6. The goal is to also use the community social platform to present more detailed information and statistics such as those providing from WP4. Integration of graphical interactive visualisation tools such as Gephi will be investigated for integration in this platform.
Newsletters / news feeds	Awareness Interest	ACDC will investigate whether to publish printed newsletters or use a more dynamic news feed approach.
Press visibility	Awareness Interest	ACDC intents to create press visibility with press releases at specific milestones, including kickoff and availability of ACDC clearing house and tool groups. Target publications include: - European Parliament Magazine http://www.theparliament.com/magazines/parliament-magazine/ - SecEUR (www.seceur.eu) - CORDIS research*eu publications (http://cordis.europa.eu/research-eu/research-focus_en.html)
ACDC information kit	Awareness Interest Adoption	ACDC information kit is designed to provide a first level introduction to ACDC. Two versions will be prepared: an online presentation and a printable flyer
Organisation of events	Awareness Interest Adoption	ACDC will analyse the opportunity to create events either as isolated occurrence or through participation to wider conferences to promote its activities
Participation to events	Awareness Interest	ACDC will maintain a list of events of relevance to its activity and monitor participation by one or more consortium members
Social Media	Awareness Interest Adoption	ACDC will integrate to its public website the most common social media channels (Facebook, Twitter, LinkedIn, Google Plus). The action will help users find information about ACDC faster and this way ACDC information becomes more viral in the online environment. It can also be an effective method to offer real time support.
TV spots	Awareness Interest Adoption	Some partners may be able to promote the project through TV spots. Some clips should be developed and translated into languages of the project.
Universities	Awareness	Meetings among clusters on Security Technologies of

Channel	Contributes to dissemination goal	Detailed information
	Interest	universities.
Presentation at conferences and events	Awareness Interest Adoption	ACDC partners can present findings of the project at high level conferences, including possible recommendations for policymakers. This will contribute to awareness on proposed solutions and raise interest for adoption.
Publication of scientific articles	Awareness Interest adoption	ACDC partners can produce scientific articles outlining research done and main findings to date, including possible recommendations for policymakers. Publication in well-known journals will contribute to acceptance of the proposed solutions
White papers	Awareness Adoption	By releasing White Papers, from ACDC as a whole or from individual partners, feasibility of the technical measures can be explored in depth. Focusing on case studies can demonstrate the real-world effects, which will drive adoption as well as promote awareness of the centre.
Tutorials	Awareness Interest adoption	ACDC will provide tutorials aimed towards Botnet and DDoS handling, thus raising awareness for end users and research organisations as well as enabling them to handle botnet incidents using the ACDC processes.

Table 5 – the ACDC Dissemination channels

6.4. Attendance to events

The following table provides a list of events; this list will be manage dynamically by the ACDC partners, therefore the table below is simply a static view for the deliverable purpose.

Event	Start date	End date	Web site	Relevance to ACDC
Technical seminar 1	April-May 2013	April-May 2013	www.cert-ro.eu	Technical seminar, with closed audience, on cyber-security related subjects. CERT-RO organises at least 3 cyber-security seminars per year, with audience from the public sector.
APWG	April 23, 2013	April 25, 2013	http://www.apwg.org/apwg-events/cecos2013	Attendees are largely professionals of the counter-cybercrime industry. Thus, they are an important type of client to ACDC. In addition, the sponsors of the event are large bodies to which ACDC is relevant. Being one of the most-attended events of this kind, it is an important showcase for ACDC This event is annual and will be important in 2013, 2014 and 2015.

Event	Start date	End date	Web site	Relevance to ACDC
Clusit	April 16, 2013	April 16, 2013	http://www.clusit.it/	Security summit with a strong focus on Italian public administration and Italian corporations. Relevant to the outcomes of the Italian sub-pilot as well as other pilot tools.
Trust in the Digital World Conference	April 18, 2013	April 19, 2013		
eco Kongress	April 17, 2013	April 17, 2013	Eco.de	Presentation of ACDC project to the eco members
London Action Plan	April 16, 2013	April 17, 2014	http://londonactionplan.org	Presentation of ACDC (two presentations)
The Antivirus Laboratory of BAS	May 2013	May 2014	www.bgpost.bg www.bas.bg	Meeting with the Cyber Defense and antivirus Laboratory of Bulgarian Academy of Sciences (BAS)
TERENA TF-CSIRT	May 23, 1013	May 25, 2013	https://www.terena.org/events/details.php?event_id=2448	TF-CSIRT is a task force that promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions, whilst liaising with relevant organisations at the global level and in other regions.
MAAWG	June 4, 2013	June 6, 2013	http://www.maawg.org	Presentation
TERENA Networking Conference	June 3, 2013	June 6, 2013	https://tnc2013.terena.org/	The TERENA Networking Conference (TNC) is the largest and most prestigious European research networking conference - over 500 participants including decision makers, networking specialists and managers from all major European networking and research organisations, universities, worldwide sister institutions and industry representatives attend.
Chief Directorate "Combating Organized Crime" (CDCOC)	June 2013	July 2015	www.mvr.bg	Meetings with the Chief Directorate "Combating Organized Crime" (CDCOC) focused on investigating cyber threats and anti-botnet
OTS (annual event)	June 18, 2013	June 18, 2013	http://www.ots.si	The event focuses among other topics also on security and trust, and development on mobile platforms.
Security Summit	June 5, 2013	June 6, 2013	https://www.securitysummit.it/	It is organized by CLUSIT and it is addressed to representative of economic, research, public administration interested to the ICT security issues

Event	Start date	End date	Web site	Relevance to ACDC
Campus Party Spain 16 in Madrid	July 09, 2013	July 14, 2013	http://www.campus-party.org/	Workshops, conferences and competitions make Campus Party in a training event among youth. In order to collect concerns and behaviors among youth may be an important point to guide and analyze the ACDC project approach.
Technical seminar 2	September 2013	September 2013	www.cert-ro.eu	Technical seminar, with closed audience, on cyber-security related subjects. CERT-RO organises at least 3 cyber-security seminars per year, with audience from the public sector.
eCrime research Summit	Sep. 17, 2013	Sep. 18, 2013	http://www.antiphishing.org/apwg-events/upcoming/ecrime2013	This conference is organised by the Antiphishing Working Group, an American-based organization international impact on on-line security, addressed to eCrime and malware researchers and counter-eCrime developers. This conference will examine crimeware's evolution, behavioral vulnerabilities and human factors that contribute to eCrime's success, the roles of Registrars, Registries and DNS in managing phishing attacks, public health approaches to managing the eCrime scourge, as well as breaking news on counter-eCrime efforts and resources.
Anti Spam Meeting	September 13, 2013	September 15, 2013	Eco.de	ISP and Abuse Team meeting with the Antivirus / security industry. Spread the word about ACDC
Campus Party Europe 3 in London	September 03, 2013	September 08, 2013	http://www.campus-party.org/	Workshops, conferences and competitions make Campus Party in a training event among youth. In order to collect concerns and behaviors among youth may be an important point to guide and analyze the ACDC project approach.

Event	Start date	End date	Web site	Relevance to ACDC
‘’New Global Challenge in Cyber Security’’ 2013	October 2013	October 2013	www.cert-ro.eu	CERT-RO organizes on annual basis a conference whose main objective is promoting both national and international cooperation regarding cyber-security threats. Botnets are often at the top of the priorities discussed. It is a moment to continue and initiate new and essential ways of cooperation to solve such common cyber security problems, like joint response to incident handling. It is also a proper way to disseminate information regarding ACDC project.
ENISE	October	October	http://www.enise.inteco.es	The Spanish “Information Security International Meeting” (ENISE) may be used to support ACDC awareness
ENISA Cyber Security Month 2013	October 2013	October 2013	http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-2013-get-involved	The European Cyber Security Month (ECSM) 2013 team is addressed to public and private sector organisations concerned with Network and Information Security the event is on the EU Cybersecurity Strategy.
Internet Governance Forum 2013	October 21, 2013	October 25, 2013	http://www.intgovforum.org/cms/	Creating awareness and uptake from ISPs
ISSE conference 2013 (same in 2014)	October 22, 2013	October 23, 2013	http://www.isse.eu.com/	Forum where key security topics will be discussed. Special emphasis placed on case studies and innovative and robust security solutions implemented by European organisations. Facilitates remaining up to date with relevant security solutions, cybercrime and countermeasures as well as the relevant legal framework
Forum Expo ICT Security 2013	October 29, 2013	October 30, 2013	http://www.tecnaeditrice.com/forumict13_presentazione.php	It is addressed to security specialists from the public administration and private sector and is about cybercrime, cyber warfare and intelligence
Technical seminar 1	November-December 2013	November-December 2013	www.cert-ro.eu	Technical seminar, with closed audience, on cyber-security related subjects. CERT-RO organises at least 3 cyber-security seminars per year, with audience from the public sector.

Event	Start date	End date	Web site	Relevance to ACDC
ICT 2013	November 6, 2013	November 8, 2013	https://ec.europa.eu/digital-agenda/en/ict-2013-conference	Opportunity to demonstrate and share ACDC results and enlarge the ACDC community
"3rd National CSIRT Seminar"	November 2013		www.cert.pt	Annual seminar, organized by FCCN, which brings to Portugal interesting Information Security topics.
"2º Congresso das Comunicações"	November 13, 2013	November 14, 2013	http://www.apdc.pt/Default.aspx?change_lang=1	Congress organized by and for the Telecom sector in Portugal. The major one in this sector, and the most relevant. Good opportunity to promote ACDC among Portuguese ISPs.
Vitel – telecommunication workshop (annual event)	November 2013	November 2013	http://ww.ezs-zveza.si/vitel/28delavnica/	Workshop from the field od telecommunications (Internet of Things), includes topics from internet security
Living bits and things (annual event)	November 12, 2013	November 13, 2013	http://www.livingbitsandthings.com	Conference focuses on the communication infrastructure (IoT/M2M services)
INFOSEK 2013 (annual event)	November 21, 2013	November 23, 2013	http://www.infosek.net/	One of the most notable information-security event in Slovenia – attendance would contribute to the recognition of the ACDC project
15th CARNet Users Conference	November 20, 2013	November 22, 2013	cuc.carnet.hr	CARNet national conference that unites all academic IT staff in one place, usually includes industry partners as well.
XIII Jornada internacional de Seguridad de la información de ISMS en Madrid (The XIII International Conference on Information Security of ISMS)	November 28 , 2013	November 28, 2013	http://www.ismsforum.es	The International Conferences congregate international speakers from top level to address the most topical issues of special relevance and Information Security. This in an environment that facilitates professional relationships and knowledge sharing. Being a great value for the objectives of ACDC.
Scientific botnet conference	December 5, 2013	December 6, 2013	https://www.botconf.eu/	Enlargement of the research community; publicise the access to data gathered by ACDC
ETSI Security Workshop	Mid of January 2014	Mid of January 2014	http://www.etsi.org/news-events/events/411-8th-etsi-security-workshop	ETSI Security event is an opportunity to spread ACDC information to the big audience of the people committed in the field of the security standardization
International Data Corporation	February - March 2014	February - March 2015	www.idc.com	Participation in International Data Corporation's (IDC) IT Security Roadshow 2014/5 in Bulgaria

Event	Start date	End date	Web site	Relevance to ACDC
Rooted CON 2014 in Madrid	March 2014	March 2014	http://www.rootedcon.es/	Rooted CON congragates speakers from top level in order to promote safety expertise.
Securmática	April 2014	April 2014	http://www.securmatica.com/	Securmática combines knowledge, experience and point of view of security directors and managers of ICT companies and public and private organizations, consultants, auditors, researchers, teachers, product developers and service providers. Provides important global source of knowledge from different points of view in order to cover the objectives of the ACDC.
Belgian Internet Security Conference	October 24, 2014	October 24, 2014	http://bisc.belnet.be/ (not up to date yet)	Belgian Internet Security Conference provides the opportunity to contribute to a coordinated approach across sectors to fight cybercrime, including botnets. Newest trends will be presented and the possibility will be provided to exchange experience and ideas on cybersecurity with key players and policy makers.

Table 6 – list of events

7. Dissemination metrics

Measuring and evaluating results is recognised as an activity which can provide the vital information needed to determine how successful we were (or were not) at our dissemination / communication activities. A well designed measurement and evaluation program is in fact key in leading us to continued improvement, effectiveness and success.

Starting from the targets and from the dissemination activities already identified in the previous sections of this deliverable, the initial metrics for the next period have been fixed.

Per each "Category", specific communication objectives and the most appropriate dissemination tools have been identified. In the "Metrics" column quantitative monitoring indicators to measure the effectiveness (or ineffectiveness) of the dissemination activities are established.

Comparing the actual results achieved with the specific, time bound and measurable goals set up will also help to re-adapt the dissemination strategy in case it will be needed.

The indicators will be constantly monitored and updated basing on the experience gained during the next years of the project life.

Target		Objective	How	
Category	Who		Dissemination Tool	Metrics
EP / PM, Agencies, Policy Makers, EC	EDA, ENISA, JRC, Europol (EC3), CEPOL, Interpol, National Institutions, etc.	Raise awareness Foster Interest	Newsletters	3 per year
			Sessions & panels organised by ACDC, panel participation, presentations, attendance to events, etc.	List of events identified (35 events already listed in previous section of the deliverable)

			Poster to be shown at relevant events	1 generic Poster (to be periodically updated) + specific posters whenever requested
			Flyer	1 per year (to be periodically updated) + specific information material to be produced whenever requested
			Press Releases	Target publications include: European Parliament Magazine http://www.theparliament.com/magazines/parliament-magazine SecEUR (www.seceur.eu) CORDIS research*eu publications (http://cordis.europa.eu/research-eu/research-focus_en.html)
Member States	CERTs	Foster collaboration	Direct Contact	+8 CERTs to be involved by the end of the project
			Information Kit	1 (specific versions to be produced as needed)
			Social Community Platform	Monitoring the aggregated information on how many input (technologies, solutions) are proposed/provided
R&D projects	ASASEC, Cloud CERT, SCADA Lab, etc.	Foster collaboration Raise Awareness	Cluster meetings	[to be decided]
			Cross linking promotion through the ACDC and projects' websites	Linking to ACDC from cyber security relevant project's websites
Universities	Existing (in the consortium) and new ones	Foster collaboration; Raise Awareness	Participation to Cluster meetings on Security Technologies	List of events identified
			Social Community Platform	Monitoring the aggregated information on how many input (technologies, solutions) are proposed/provided
General Public	Companies	Getting them closer to trustworthy internet society ; Help them to avoid business / private operations interruptions	Tutorial for disinfection	1 (to be updated and / or customised whenever needed)
	Citizens		Social Media groups	1 LinkedIn Group 1 Facebook Group 1 Twitter Group
			Social Community Platform	Monitoring the aggregated information on how many downloads of tools for disinfections are done
Critical Infrastructure (users)	Health, Utilities, Internet operators, etc.	Raise awareness	Website	Measurement: Google Analytics
			Social Media groups	1 LinkedIn Group 1 Twitter Group
		Keep them informed on how ACDC impacts the critical infrastructure	Social Community Platform	Monitoring aggregated information on the number of accesses / contributions per category

8. Conclusion

The ACDC dissemination plan is a key pillar of ACDC to create uptake and to initiate an operational community. The dissemination plan is implemented through the activities in WP5 in terms of events, conferences, publications and workshops, and through the activities in WP6 in terms of community creation.

The ACDC dissemination activities started as soon as the project itself started as is made evident by the list of events; the dynamic information in terms of events and impact will be reported on in the future deliverables linked to dissemination.

9. Annexe 1: ACDC logo

The ACDC logo was designed to fully reflect the three key aspects of ACDC, namely

- The "end to end approach”
- The "fighting against botnets”
- The "infrastructure” concept of a centre surrounded by national / regional / specialised centres

This is reflected through three components, assembled into a single logo.

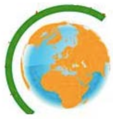
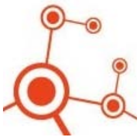
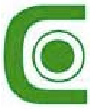
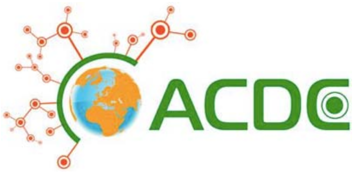
	end to end approach	the green line represents the end to end approach, combined with a "defensive” image (against the botnets which in the logo are positionned on the left)
	Fighting botnets	A set of networked devices linked into a bot
	Cyber defence centre surrounded by a set of national centres actions as local relays	A central centre visualised by the inside green point linking to the centres represented by the « C » shape form
	ACDC logo	Bringing the concepts together in a single project ACDC Botnets are figured on the left, with the green line representing « protection » and « end-to-end », while on the right the concept of « centre » appears in the Centre word of the logo

Table 7 – the ACDC logo