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

Deliverable	**D5.2.1 - Conception Exploitation plan**
Work package Due date Submission date Revision Status of revision	WP5, Full name Dissemination, Exploitation and Long Term Viability 31/01/2014 04/03/2014 Final 6.2
Responsible partner Contributors	Atos Spain Peter Meyer, Michael Weinrich, Wout de Natris (ECO); Alena Hochenberger (TEC); Elsa Prieto, Kazim Hussain, Beatriz Gallego-Nicasio (Atos); Katia Velikova (BGPOST); Darko Perhoc, Anamarija Soric Custic (CARNET); Dan Tofan (CERT-RO); David Bizeul (CSD); Wolfgang Tremmel (DE-CIX); Christian Keil (DFN-CERT); Véronique Pevtschin, Ioana Cotoi (EII); Jonathan P. Chapman (Fraunhofer); Andreas Fobian (GData); Christian Nordlohne (IF(IS)); Ángela García (INTECO); Karine e Silva (KUL); Thomas Fontvielle (Signal Spam); Paolo De Lutiis (TI); Antonio Pastor (TID); Ales Cernivec (XLAB); Marc Rivero (Bdigital); Tiziano Inzerilli, Sandro Mari (ISCTI); Edgardo (MI).
Project Number Project Acronym Project Title Start Date of Project	CIP-ICT PSP-2012-6 / 325188 ACDC Advanced Cyber Defence Centre 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
1.0	20/12/2013	Elsa Prieto (Atos)	Initial draft
2.0	09/01/2014	Elsa Prieto (Atos)	Inputs to glossary, Introduction, PEST, Market description, ACDC offering, MI + Atos initial inputs, and Annex I.
3.0	16/01/2014	Elsa Prieto (Atos)	Inputs to sections: PEST, ACDC offering (based on comments by CARNET), exploitation strategy, Integration of inputs from INTECO and XLAB Annex II.
4.0	23/01/2014	Elsa Prieto (Atos) Véronique Pevtschin (EII)	Updated glossary section. Updated Introduction and PEST section. Inputs to value proposition. New structure and contents for exploitation strategy. Inputs from ECO, EII, TI, CARNET, TI.
5.0	31/01/2014	Elsa Prieto (Atos) Ionana Cotoi (EII) Peter Meyer (ECO)	Executive summary and conclusions Updated Problem Statement, PEST, Methodology and standardization sections. Value chain subsection added. Inputs from TID, IF(IS), ISCTI, Fraunhofer, GData, TEC, DFN-CERT All sections updated according to the internal review
6.0	06/02/2014	Elsa Prieto (Atos)	Update market overview, revenue models (with cost structure) Inputs from DE-CIX, CERT-RO, BDigital
6.1	20/02/2014	Elsa Prieto (Atos) Wout de Natris (ECO)	Trademark considerations. Inputs from BDigital, Signal Spam, KUL Second internal review and contents update.
6.2	04/03/2014	Elsa Prieto (Atos)	Final version

Glossary

ACDC	Advanced Cyber Defence Centre
ADSL	Asymmetric Digital Subscriber Line
APAC	Asia-Pacific
AV	Anti-Virus
ARIMA	AutoRegressive Integrated Moving Average
B2B	Business to Business
B2C	Business to customer
BIOS	Basic Input-Output System
BYOD	Bring Your Own Device
CAGR	Compounded Annual Growth Rate
CCH	Central Data Clearing House
CERT	Community Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CP	Community Portal
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
C&C	Command & Control
DAE	Digital Agenda for Europe
DDoS	Distributed Denial of Service
DLP	Data Loss Protection
DMR	Direct Market Resellers
DNS	Domain Name System
DoW	Description of Work
DPI	Deep packet Inspection
EBITDA	Earnings Before Interest, Taxes, Depreciation, and Amortization
EC	European Commission
EC3	EU Cybercrime Centre
ECSM	European Cyber Security Month
ENISA	European Network and Information Security Agency
EP3R	European Public-Private Partnership for Resilience
EU	European Union
FFTH	Fiber From The Home
FP7	Seventh Framework Programme
FPGA	Field Programmable Gate Array
GCM	Google Cloud Messaging
GDP	Gross Domestic Product
JV	Joint Venture
H2020	Horizon 2020
HSDPA	High Speed Downlink Packet Access
HW	Hardware
IaaS	Internet as a Service
ICT	Information and communications technology
IDS	Intrusion Detection System
iOS	Iphone Operating System
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Right
ISP	Internet Service Provider
IT	Information Technology
LEA	Law Enforcement Agency

LTE	Long Term Evolution
M2M	Machine to Machine
MDM	Mobile Device Management
MS	Member State
NIS	Network and Information Security
OEM	Original Equipment Manufacturer
OS	Operating System
OVA	Open Virtualization Appliance
PaaS	Platform as a Service
PEST	Political Economical Societal Technological
PP	Restricted to other programme participants (including the EC Services)
PU	Public
PUF	Physical Unclonable Function
R&D	Research & Development
ROI	Return on Investment
SaaS	Software-as-a-Service
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined networking
SME	Small Medium Enterprise
SMS	Short Message Service
STIX	Structured Threat Information Expression
SW	Software
SWOT	Strengths Weaknesses Opportunities Threats
TV	Television
URL	Uniform Resource Locator
VAR	Value-added reseller
VoIP	Voice over Internet Protocol
WP	Work Package

Table of contents

1. Executive summary 7
2. Introduction 8
2.1. Purpose and scope 8
2.2. Intended Audience 8
2.3. Definitions 8
2.4. Structure of the document 9
2.5. Relation to the work plan 9
2.6. Problem statement 10
2.7. Mission statement 11
3. Market Analysis 12
3.1. PEST Analysis 12
3.2. Market description 19
3.2.1. End-point Security Protection 19
3.2.2. Enterprise Network Firewall 23
3.2.3. Information Sharing 24
3.3. ACDC Positioning 24
3.3.1. ACDC offering 24
3.3.2. Target users 28
3.3.3. Competitive advantage and initial SWOT Analysis 28
3.3.4. Value Proposition and expected impact 29
3.4. Offering strategy 31
3.4.1. Sustainability 31
3.4.2. Other exploitation lines 37
3.5. Business impact drivers 40
3.5.1. In the short term 40
3.5.2. In the long term 41
3.6. Preliminary individual exploitation plans 42
3.6.1. Industrial partners 42
3.6.2. Academic and research partners 59
3.6.3. Public Community Emergency Response Team and Institutional Organisations 63
4. Conclusions and future work 73
5. References 74
6. Annex I.ACDC Services 79
7. Annex II. ACDC Public Deliverables List 82

Table of figures

Figure 1: Local infections in January 2014 10
Figure 2: Global Activity Map. All Botnets. 11
Figure 3: Euro area GDP growth and ARIMA 15
Figure 4: Gartner Hyper Cycle for Cloud Computing 2012 17
Figure 5: Endpoint security vendor landscape 21
Figure 6: Enterprise network firewall landscape 23
Figure 7: ACDC solution – conceptual view 25
Figure 8: ACDC logo 27
Figure 9: ACDC value chain 31
Figure 10: ACDC 5-year plan 31
Figure 11: ADCD operation model 33

Figure 12: Atos business model 45
Figure 13: Engineering’s revenues split across markets 49
Figure 14: The structure of cyber security of Telecom Italia 52
Figure 15: Telefónica Cyber security Service 55
Figure 16: MI business model 58

Table of tables

Table 1: PEST Analysis 12
Table 2: Comparison of Endpoint security vendors’ solutions 22
Table 3: Ownership of ACDC tangible assets 26
Table 4: ACDC initial SWOT analysis 28
Table 5: Pricing mechanisms 36
Table 6: Standardization bodies relevant for ACDC 39
Table 7: CARNET map of interests 63
Table 8: ACDC tool classification per solution 79
Table 9: ACDC services 79
Table 10: Technical Services 81
Table 11: ACDC tools per consortium partner 81

1. Executive summary

This document is deliverable D5.2.1 Conception Exploitation plan of the project Advanced Cyber Defence Centre (ACDC) ICT-PSP-325188. The document describes the initial exploitation approach showing the relationship between exploitation and sustainability activities within the project.

The exploitation plan starts with a P.E.S.T analysis aiming at understand the political, economic, social and technological forces that can have an impact on the business environment of ACDC. Different aspects are introduced, such as The EU cyber security strategy, the digital currencies (bitcoin), the increasing mobile malware, the Bring Your Own Device paradigm or the digitally connected society, to mention but a few.

A market analysis was performed in order to position ACDC. The market analysis provides an insight of three domains: endpoint security, considering as main players those security suites that integrate a set of functionality for simplified management and integrated visibility (such as Symantec, Microsoft, McAfee or Sophos), enterprise network firewall, and information-sharing, with special emphasis on the Information Sharing and Analysis Centres and the European Information Sharing and Alert System for citizens and SMEs.

Following, the ACDC offering is introduced. This offering is a mixture of tangible and intangible results and relies on three pillars: botnet detection and mitigation, information sharing, and a stakeholders' community. The core of the ACDC solution consists of a Central Data Clearing House, a network of national support centres, a community portal and a portfolio of services ranging from detection to support. For each of these elements, the ownership and licensing options are identified.

A later section of this document describes the general exploitation strategy, consisting on two main branches: sustainability (considered as joint-exploitation) and other exploitation lines or possibilities, involving commercial (profit oriented) and non-commercial exploitation (knowledge dissemination and transfer, standardization, development of stakeholders' competences and mainstreaming of legal aspects).

With regard to sustainability, several considerations are made in order to guide the final implementation of the solution at the end of the project. For that purpose, a 5-year plan is envisaged, covering the project execution and beyond. This includes a rough description of a general operation model, along with considerations about possible legal structures and the analysis of two business models: commercial and non-commercial.

Finally, the document presents the consortium partners' individual exploitation plans, where each beneficiary describes the usage of ACDC results in alignment with the general exploitation plan. This exploitation plan covers different exploitation lines consistent with the nature of the organisation (industrial, academic or CERT) and the exploitable items identified at the current stage of the project.

2. Introduction

2.1. Purpose and scope

This document is deliverable D5.2.1 - Conception Exploitation plan of the Advanced Cyber Defence Centre (ACDC) project ICT-PSP-325188. Its purpose is to describe the initial exploitation approach of the project, establishing suitable actions to make ACDC a successful and sustainable project beyond its lifetime.

More specifically, the objectives of this document are:

- To identify and analyse the ACDC target market.
- To identify an effective approach to counter botnet threats for the common benefit of citizens and enterprises at European level.
- To identify the project’s exploitable results suitable for the generation of business opportunities and favour spreading of secure ICT services and development of market opportunities.
- To show how the results of ACDC create a competitive advantage for the participating partners and European businesses.
- To discover and outline possible mechanisms for effective exploitation.
- To show the relationship between exploitation and sustainability within the project and discuss different alternatives.
- To align the activities carried out within the project towards the exploitation.

Exploitation is understood as the use or utilisation of project results for additional socio-economic value outside of the project. Even though exploitation is most commonly associated with profit, other aspects, such as know-how management and collaborative activities and gratuitous public services, constitute an important part of the ACDC project as a European anti-botnet facility and bring an overall benefit at European level for all the entities operating in the ICT market. All such goals are possible only through a tight collaboration between private and public entities.

In this sense, this document does not make any decision about the final implementation of the ACDC solution, but offers different alternatives for consideration.

2.2. Intended Audience

The dissemination level of this document is "PU" and it will be publicly delivered on the project web site: http://www.acdc-project.eu.

As this deliverable contributes to defining the perspective and needs of the ACDC project, the target audience includes the ACDC consortium, the ACDC community, and the European Commission.

2.3. Definitions

“ARIMA”. In statistics and econometrics, and in particular in time series analysis, an autoregressive integrated moving average (ARIMA) model is fitted either to better understand the data or to predict future points in the series (forecasting).

“Business Model”. The concept of the business model in the literature on information systems and business refers to ways of creating value for customers, and to the way in which a business turns market opportunities into profit through sets of actors, activities and collaboration

“Endpoint”. An endpoint device is an Internet-capable computer hardware device on a TCP/IP network. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware such pints of sales terminals and smart meters.

“Mainstreaming” is the planned process of transferring the successful results of programmes and initiatives to appropriate decision-makers (convincing them to take into account the project results) in regulated local, regional, national or European systems.

“Multiplication” is the planned process of convincing individual end-users to adopt and/or apply the results of programmes and initiatives.

“Original Equipment Manufacturer” (OEM). OEM is used to refer to the company that acquires a product or component and reuses or incorporates it into a new product with its own brand name.

“Software as a Service (SaaS)” is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

“Value-added reseller” (VAR) is a company that takes an existing product, adds its own "value" usually in the form of a specific application for the product and resells it as a new product or "package."

2.4. Structure of the document

D5.2.1 is a general exploitation plan and, as such, gives an overall framework for the initial exploitation strategy of ACDC.

After this introductory chapter, chapter 3 provides a market analysis. It is broken down in several sections. The first section of the market analysis gives an overview of the environmental background (political, economic, societal and technological aspects) that can influence or hamper the development and success of the project. In the second section, three possible are analysed, describing the main players on the field. A last section provides a description of the ACDC offerings from the exploitation angle, including the benefits to the target users.

Chapter 4 presents the preliminary exploitation plan of the project during the project lifetime and beyond, including the partners’ individual exploitation plan.

Finally, Chapter 5 includes the conclusions and future work on the exploitation side.

2.5. Relation to the work plan

The ACDC exploitation plan is part of the sustainability and exploitation strategy defined by Work Package 5 (WP5). We should note that sustainability of ACDC beyond the lifetime of the project is a subset of the exploitation actions taken by consortium partners. Many actions taken to exploit specific results are done independently of the joint sustainability actions aimed to maintain the ACDC capability. For example national CERTs and other public bodies committed in the protection of ICT infrastructures can take advantage of the results of the project to deliver enhanced capabilities and a harmonized global approach to combat security incidents at European level. In addition, academic partners will publish scientific results and increase awareness on botnet threats and remedies in the stakeholders operating in the ICT market. They will also maintain and increase their academic credibility and the positioning of European technical and scientific expertise in the world. These actions can be considered exploitation or can be considered contribution to sustainability objectives but are not necessarily directly linked. Having said that, sustainability of the ACDC facility is the primarily exploitation objective for ACDC and a major part of the exploitation plan.

In the description of work (DoW) the exploitation activity is carried out within the WP5-Dissemination, Exploitation and Long Term Viability. There are two deliverables related to the

exploitation activity: D5.2.1 - Conception Exploitation plan (this deliverable), due at the end of the first project period (M12), and D5.2.2 - Final Exploitation plan, due at the end of the project (M30).
In addition, this activity is very closely related to dissemination (WP5), community (WP6) and sustainability aspects, which will contribute to- and make use of- these exploitation deliverables.

For that reason, D5.2.1 is highly tied to the following list of project deliverables, which contain information about the exploitable results of the project, and help to explain their value.

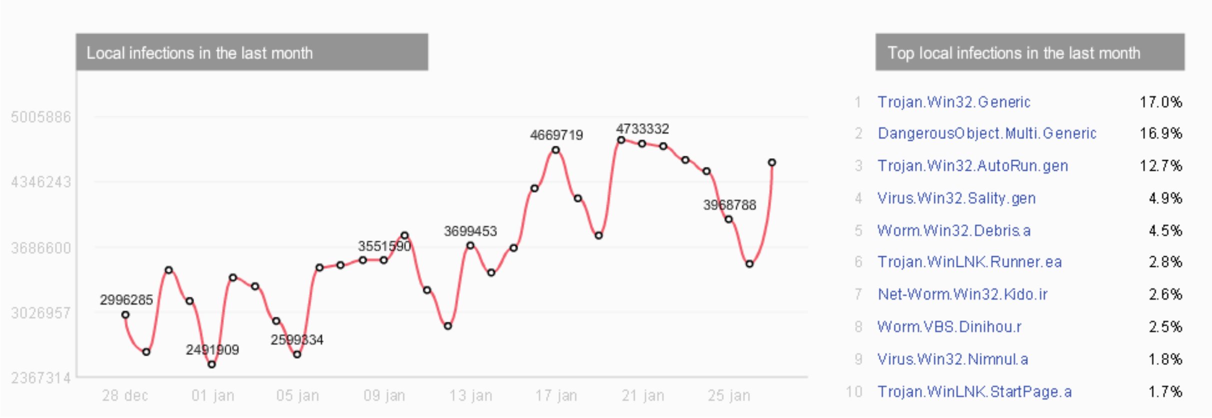
- D1.3.1 Specification of Tool Group "Support Centre"
- D1.2.1 Specification of Tool Group "Centralised Data Clearing House"
- D2.3 – Technology Development Framework outlining basic models for integration and delivery principles.
- D5.1.1 – Dissemination plan.
- D6.1.1 - User profiles and categorization
- D6.1.2 - Identified user list across the different selected organisations
- D6.3.1 – Involvement model for users in ACDC

Furthermore, this document will, over the lifetime of the project, be enriched with the forthcoming project's achievements and contributions from all partners, input that will be consolidated in its updated version at M30.

2.6. Problem statement

Botnets are cyber infrastructures consisting of thousands of compromised hosts (called "bots", "drones" or "zombies") that are all under the control of criminals. Botnets organized themselves in a hierarchical manner, with a central command and control (C&C) server for the attacker (called "bot master" or "bot herder" to send commands to the single computers. By relaying commands through the C&C, the attacker is able to control remotely the network and use the computers for a variety of undesired purposes.

Botnets would not be as dangerous of a force online today if it were not for the dramatic numbers of compromised systems. For a botnet to form and grow, it must accumulate drones, and each drone must be individually infected, exploited, and assimilated into the botnet. The more drones a bot master has at his disposal, the more impact the botnet can have on the internet at large. As an example, the ZeroAccess botnet[1] is one of the largest known botnets in existence today with a population upwards of 1.9 million computers. The magnitude of the problem is shown in **Figure 1**, showing the monthly number of local infections, as reported by Securelist[2] , as well as the top botnets detected.



Top local infections in the last month

1	Trojan.Win32.Generic	17.0%
2	DangerousObject.Multi.Generic	16.9%
3	Trojan.Win32.AutoRun.gen	12.7%
4	Virus.Win32.Sality.gen	4.9%
5	Worm.Win32.Debris.a	4.5%
6	Trojan.WinLNK.Runner.ea	2.8%
7	Net-Worm.Win32.Kido.ir	2.6%
8	Worm.VBS.Dinihou.r	2.5%
9	Virus.Win32.Nimnul.a	1.8%
10	Trojan.WinLNK.StartPage.a	1.7%

Figure 1: Local infections in January 2014

Source: Securelist. January 2014. http://www.securelist.com/en/statistics#/en/map/oas/month

The proliferation of botnets in cyberspace threatens to undermine the efficiencies, innovation, and economic growth of the Internet and diminishes the trust and confidence of online users. The very nature of botnets gives criminals plenty of power on the internet at large. With control over a large number of compromised systems, bot masters can engage in quite more damaging activities. Botnets are indeed responsible for most of the illegal activities on the Internet today: spam, denial of service attacks, theft of sensitive information (passwords, banking details and intellectual property), and spread of further malware. For example, the mentioned ZeroAccess botnet targeted search requests and advertising links in browsers and routed them towards malicious sites. This provided the bot masters with a revenue stream of $2 million every month [3] , according to Microsoft's estimations.

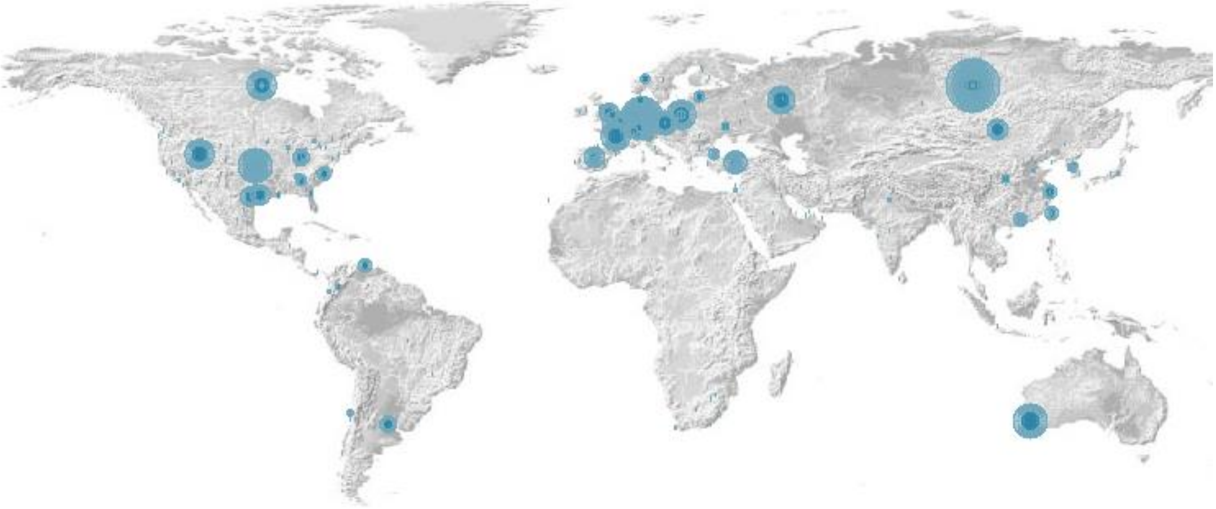


Figure 2: Global Activity Map. All Botnets.

Source: Arbor's Threat Level Analysis System (ATLAS), January 2014. http://atlas.arbor.net/worldmap/index

2.7. Mission statement

The purpose of the Advanced Cyber Defence Centre (ACDC) is to set up a pan-European infrastructure of national relay centres to support, locally, users who are victims of a botnet in providing mitigation approaches and solutions. In parallel, the goal of this infrastructure is to improve the level of awareness of users and thereby decrease the impact of botnets.

In order to deliver this goal, ACDC builds up the necessary sharing of knowledge and solutions through a centralised clearing house – offering

- providers the possibility to build up new botnet fighting approaches by linking pre-existing solutions
- ISPs the possibility to provide data to the clearing house, thereby speeding up the detection of botnets through a larger data base with faster trends detection and supporting research and innovation through a European centric knowledge base of attacks

In the longer run, the ACDC infrastructure of national relays and centralised clearing house paves the way to detect and mitigate other types of attacks and address detection and mitigation needs for a wider range of cyber-needs. However, in the short run, 2014 opened with the first so-called "Thingbots" attack - the first botnet focused attack on televisions and fridges[4] , botnets already cater to an important and increasing form of cyber-risk and will therefore remain at the centre of ACDC's mission.

3. Market Analysis

3.1. PEST Analysis

This section describes the framework of macro-environmental key factors (Political, Economic, Social & Technological f= P.E.S.T) which can drive and have an impact on the exploitation of the solutions from the ACDC project. **Table 1** represents a summary of each aspect. The following sections provide further information about each.

Table 1: PEST Analysis

PEST Analysis	
Political • The end of the Stockholm Programme • Launch of the EU cyber security strategy • Set-up of CERT-EU, EC3 and NIS platform • Extension of ENISA mandate • Beginning of Horizon 2020	**Economical** • Slow economy growth as of mid-2014 • Ubiquitous access to information • The rise of the digital currencies (esp. bitcoin).
Societal • Digitally connected society • Cyber awareness • Impact on work, learning, leisure • Impact on relations to society	**Technical** • Malware sophistication • Increasing mobile malware • The BYOD paradigm • Software as a Service • Internet of Things

3.1.1.1. Political and legal

The global network security problems cannot rely on one country, one enterprise or one technology to solve. Cyber security involves government, industry, individuals and international cooperation and requires the joint efforts of all sides. The national government takes full responsibility for protecting and managing networks but it needs the decisive support by private stakeholders operating in the ICT security field as well as by the users of the network themselves. Notably, the network service providers bear responsibility for ensuring the network security of the infrastructures they operate, and the individual users should consciously accept the network norms and be aware of the threats which they can encounter in the Internet. They should be in particular conscious of the fact that they can become an unwilling vehicle of massive attacks against public and private organisations acting in the Internet and damage strategical services and critical infrastructures if their equipment is not suitably protected and monitored. In addition, users can be also the target of attacks by botnets and suffer from personal/reserved data exfiltration.

In turn, governments should give adequate attention to botnets, and train related managers (for example by means of government awareness programs such as the Netherlands Taskforce Bestuur Informatieveiligheid en Dienstverlening - Taskforce BID- [5] on Administration Information Security and Services) , formulate corresponding acts and regulations to crack down malicious behaviour launched by botnet. At the same time the government should disseminate the danger of botnets among the public, call on the whole society to fight against.

The end of the Stockholm Programme

The European Union (EU) has been working on a number of fronts to ensure cyber security in Europe. The Stockholm Programme [6] was adopted in 2009. It is a five-year plan with guidelines for justice and home affairs of the member states of the EU. In the programme there are also plans for a new European security framework through the extension of cooperation in the areas of police, military and secret services and measures in the area of border-crossing data exchange between state authorities and surveillance of the Internet. The programme contains a number of actions with respect to cyber-security, mostly revolving around legal instruments regarding cybercrime and critical infrastructures protection. As the programme expires in 2014, in 2013 the European Council obliged all EU Member States (MS), to start discussions on the basis of which the EC will develop further priorities of freedom, security and justice area for the post-2014 period.

National CERTs and CERT-EU

Another European initiative is the Digital Agenda for Europe (DAE)[7] , adopted in 2010. The DAE sets out 14 actions to improve cyber security readiness. Particularly the action 38 called on Member States (MS) to establish well-functioning Computer Emergency Response Teams (CERTs) by 2012. The EC also committed itself to establishing a CERT for the EU institutions, agencies and bodies (CERT-EU), as part of the EU's commitment to a reinforced and high level EU Networking and Information Security Policy in Europe. The CERT-EU was set up in 2012. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, and Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the MS and beyond as well as with specialised IT security companies.

The EC also created in 2012 the EU Cybercrime Centre (EC3)[8] in The Hague (The Netherlands). The EC3 aims to become the focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and cooperation with international partners in the pursuit of an EU free from cybercrime. It serves as the European information hub on cybercrime, developing cutting edge digital forensic capabilities to support investigations in the EU and building capacity to combat cybercrime through training, awareness raising and delivering best practice on cybercrime.

The EU cyber security strategy

In February 2013, the EC, together with the High Representative of the Union for Foreign Affairs and Security Policy, published the communication "A Cyber security Strategy of the European Union - An Open, Safe and Secure Cyberspace"[9] , intended to enhance European cyber-security through European and international cooperation and information sharing. The Strategy sets out five priorities for the EU's cyber-security vision: achieving cyber resilience; drastically reducing cybercrime; developing cyber policy defence policy and capabilities related to the Common Security and Defence Policy (CSDP); developing the industrial and technological resources for cyber-security; and establishing a coherent international cyberspace policy for the European Union and promoting core EU values. Following the Strategy, EU Member States have two years following the adoption to transpose the Directive into national laws (except for Denmark, which decided to opt out of it). Each MS is responsible for the writing of its own policy paper on national cyber-security, the document highlight the necessity of a mutual support including solidarity clause.

The Strategy was accompanied of a proposal for a Directive on Network and Information Security (NIS)[10] . The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). Among other measures, the NIS directive requires that Operators of critical infrastructures in specific sectors (financial services, transport, energy, and health), enablers of information society services and public administrations adopt risk management practices and report major security incidents which occurred by attacks to their core services.

In accordance with the proposed NIS directive, the EC set up in 2013 a NIS platform[11] , bringing together relevant public and private stakeholders, to identify good cyber security practices across the value chain and create favourable market conditions for the development and adoption of secure ICT solutions. The NIS Platform aims to contribute to the implementation of the measures set out in the

NIS Directive and to ensure its convergent and harmonised application across the EU. The findings of the Platform will feed into Commission recommendations on cyber security proposed for adoption in 2014.

The ENISA mandate

The EU Cyber security Strategy also foresees a key role for the European Union Agency Network and Information Security Agency (ENISA)[12] in protecting Europe's cyberspace. ENISA received in 2013 a new Regulation[13] , granting it a seven year mandate with an expanded set of duties. The new Regulation enshrines ENISA's achievements in areas such as CERTS in Member States, and cyber security exercises, such as Cyber Europe 2012.

ENISA also seeks to increase the involvement of the private sector. In 2009 the European Public-Private Partnership for Resilience (EP3R) [14] was established in the context of the policy initiative on Critical Information Infrastructure Protection (CIIP). The objectives of EP3R are to support Information sharing and stock taking of good policy and industrial practices, and foster common understanding, discuss public policy priorities, objectives and measures, improve the coherence and coordination of policies for security and resilience in Europe and identify and promote the adoption of good baseline practices for security and resilience. The EP3R consists of eight tasks forces related to Trusted Information Sharing Mechanisms, Tracking Down Botnets Offenders, Cyber Attacks Mitigation and Response, or Wide-Scale and Systematic Malware Disinfection to mention but a few.

ENISA is also responsible for the European Cyber Security Month (ECSM)[15] , an advocacy campaign that aims to promote cyber security among citizens, to change their perception of cyber-threats and provide up to date security information, through education and sharing good practices.

Horizon 2020

On the research arena, the EC contributes to the field of Cyber security by means of the Horizon 2020[16] . From 2014 onwards, this will be the framework for Research, Development and Innovation in the field of Cyber security and Online Privacy. With this research, the EC wants to develop trustworthy ICT solutions ensuring a secure and reliable digital environment in Europe. In the "*Proposal for a Council decision establishing the Specific Programme implementing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020)*", it is stated that "Cyber security is a prerequisite for people, business and public services in order to benefit from the opportunities offered by the Internet or any other additional data networks and communication infrastructures."

3.1.1.2. Economic

The economic context

The near-term economic outlook is for a continued moderate recovery in activity in the major economies according to the OECD Economic Outlook from November 2013 [18] . In the euro area, growth has restarted and confidence is improving in almost all member states, with some of the vulnerable economies exiting from recession or close to doing so. However, the recovery remains hesitant, reflecting remaining fiscal pressures, high unemployment and the lingering effects of the euro area crisis on balance sheets and credit conditions. Growth is projected to move above trend rates from mid-2014 onwards.

Figure 3 shows the Gross domestic product (GDP) rate (in percentage change) in the euro area from 2012 to 2014. In the third quarter of 2013, the GDP advanced 0.1% over the previous quarter, down from 0.3% in the previous three-month period. The ARIMA curve shows the projected growth for 2014.

The European Commission autumn forecast [17] also indicates a moderate acceleration in 2014 to 1% in the euro area, before growing more robustly in 2015 to 1¾%. The recovery is expected to occur at multiple speeds with diverging growth patterns outside the EU and growth differentials across EU Member States.

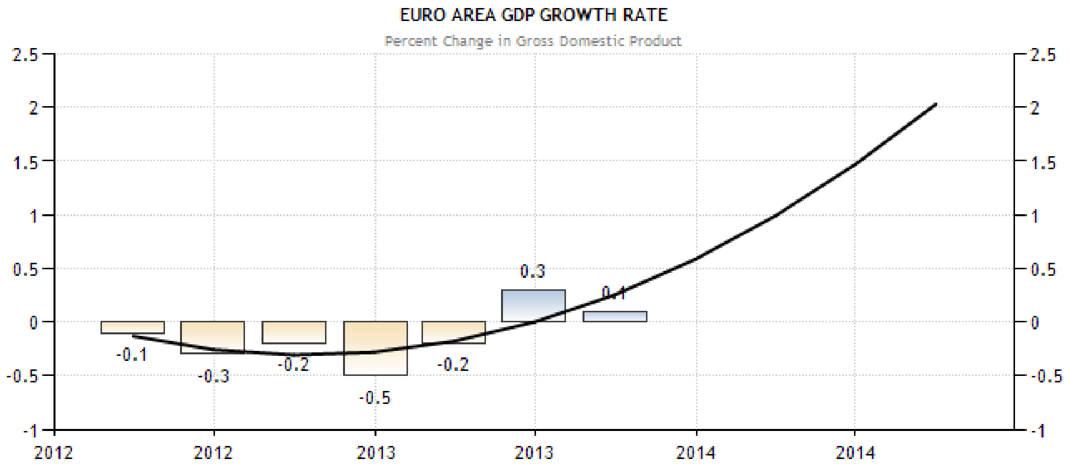


Figure 3: Euro area GDP growth and ARIMA
Source: Eurostat and Tradingeconomics [20] [21]

Because of this slow recovery, businesses are required to spend less money and so many security investments have been put on hold. The challenge for security teams is how to respond to new challenges with limited IT budgets. This seems to change in the short term. According to a Forrester paper [19] the global technology market will grow by 5% to 6% in 2014. 2015 will be a stronger year but IT purchases will lag behind economic growth rates. Business and government purchases of software will post the fastest 2014 growth (7.8% in US dollars, 7.1% in local currency terms) of any tech category, followed by IT consulting and systems integration services (7.3% in US dollars, 6.6% in local currencies).Analytics and applications in general and software-as-a-service (SaaS) applications in particular will attract the fastest growth of any IT spending category.

Ubiquitous access to information

Information is rapidly becoming a commodity. Knowledge is becoming the new competitive advantage. Consumers, wherever they live, will increasingly have information about and access to the same products and brands. If information, for instance in the form of content, is ubiquitous, it will be largely valueless. Information is no longer scarce and therefore it is not data, but knowledge drawn from the clutter of information that will become valuable.

The rise of bitcoin

The term “bitcoin” defines nonmaterial virtual currency (also called “crypto-currency”) introduced as open source software in 2009. What makes Bitcoin unique is that it has no central bank, no government that issues or regulates the currency, but is instead held in place by the vast user base whose machines validate the creation and peer-to-peer transactions that take place. Users send payments by broadcasting digitally signed messages to the network. Participants (known as miners) verify and timestamp transactions into a shared public database called the block chain[22] , so that the record of its entire transaction history clearly identifies its owner at any single moment, thereby preventing potential ownership conflicts. Bitcoins can be obtained by mining or in exchange for products, services, or other currencies.

In its initial four years Bitcoin has overcome the first challenge of a monetary system. Though it is supposed to be an alternative currency designed to operate outside of the banking system, in practice bitcoin holders are constantly swapping back and forth into real currency. As bitcoin has no issuing authority it has no country of residence or origin: it is truly global money. It can be used for payment anywhere worldwide without going through banking systems or foreign-exchange markets. By November 2013 the total market capitalisation of all bitcoins in existence exceeded US$10 billion for the first time [23] .

This increasing public attention did not go unnoticed by cybercriminals who have begun unleashing Bitcoin-mining malware. This malware install Bitcoin miners in users' systems to control their computer resources.

3.1.1.3. Technical

Malware sophistication

The rise in the number of malware variants continues at a steady pace. Indicatively, McAfee reported a growth in the number of new malware samples of about 8–12 million per quarter for 2012, while as of April 2013 they have more than 128 million malware samples in their database [25] .

The need for sophistication in botnet technology is driven by the many security solutions in the market that combat these challenges. Malware developers are expected to have an advanced level of network, system, and cryptography knowledge. Advanced evasion techniques like code obfuscation, packing, and polymorphism are now the standard in most instances of malicious code [26] . The endpoint attack surface is no longer just the Operating System (OS) and its vulnerabilities, but includes the complete software computing stack: the BIOS, OS, applications, data, and cloud.

The sophistication of the bot and botnets themselves also drives security technologies forward, creating a very complex measure-versus-countermeasure relationship between malware writers and security vendors.

As stated in a research study on advanced malware protection and detection by the Enterprise Strategy Group[27] , the majority of respondents have seen an uptick in more sophisticated and targeted malware attacks over the last two years. 62% of organisations surveyed said endpoint security software is not effective for detecting zero-day and/or polymorphic malware, which leaves them vulnerable to these attacks. To combat this malware, 51% of enterprise organisations replied that it would be needed a new layer of endpoint software to protect against zero day and other types of advanced malware. 49% would collect and analyse more security data; 44% would automate more security operations tasks; and 41% would design and build a more integrated information security architecture.

Increasing mobile malware and the Bring Your Own Device paradigm.

Mobile devices and apps are becoming ubiquitous to both personal and professional lives, allowing for near anytime access to critical information. As reported by IDC, tablet shipments alone to outpace the entire PC market by 2015 [28] .

Mobile devices have caught the attention of attackers who are now commonly targeting their applications and their access to even more valuable backend data, such as bank accounts, corporate (organisational) intellectual property and personal health information. For this reason, there has been a marked increase in mobile malware. According to a Juniper Networks report [33] , the total amount of mobile malware across all mobile platforms grew 155% in 2011, while from March 2012 to March 2013, the figure rocketed 614% to 276,259 total malicious applications. Cisco reports[29] that mobile malware that targets specific devices made up just 1.2% of all web malware encounters in 2013. Though this is still not a significant share, clearly evidences an emerging target for malware developers. By March 2013, Android was the target of 92% of all known threats. Cisco indicates a 99% during the entire 2013. This represents a significant threat given than 1 billion Android-based smart phones are anticipated to be shipped in 2017.

The Bring-Your-Own-Device (BYOD) paradigm complicates the situation even more. BYOD means the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged company information and applications. A Gartner survey [25] states that nearly two-thirds of all working adults (62%) now regularly use a personal device for business activities. This trend is significantly stronger in emerging markets, where "bring your own device" practices are mostly driven by necessity and not by personal preference. Gartner also predicts by 2017 that half of employers will require employees to supply their own device for work purposes[31] .

Although BYOD may be a convenience to employees and create a positive experience, this has a clear impact on corporate security models. These mobile devices designed for consumers have new, innovative technology, yet they lack business-grade security and management features organisations require. As reported by SANS [32] ,less than 10% of organisations are “fully aware” of the devices accessing their network. It’s difficult to manage all of these types of equipment, especially with a limited IT budget.

Software as a Service.

Software as a Service or SaaS is a technology that is attracting many business customers looking for new paradigms in order to source software functionality in new ways. In the 2012 Gartner Hype Cycle’s (see **Figure 4**), SaaS is reaching the “plateau of productivity”, which can be interpreted as the market acknowledging that there are truly useful SaaS based business tools being deployed in real life. Although SaaS represented only 4.9% of total software revenues in 2011, a consistent and significant shift towards SaaS is occurring. Perpetual license revenue has been shrinking since 2004 while subscription revenue (including SaaS) is forecast to grow at a 17.5% compounded annual rate, reaching 24% of total software revenue by 2016. Software companies are now closely evaluating aspects of their business models, including delivery methods, pricing strategies and sales compensation options

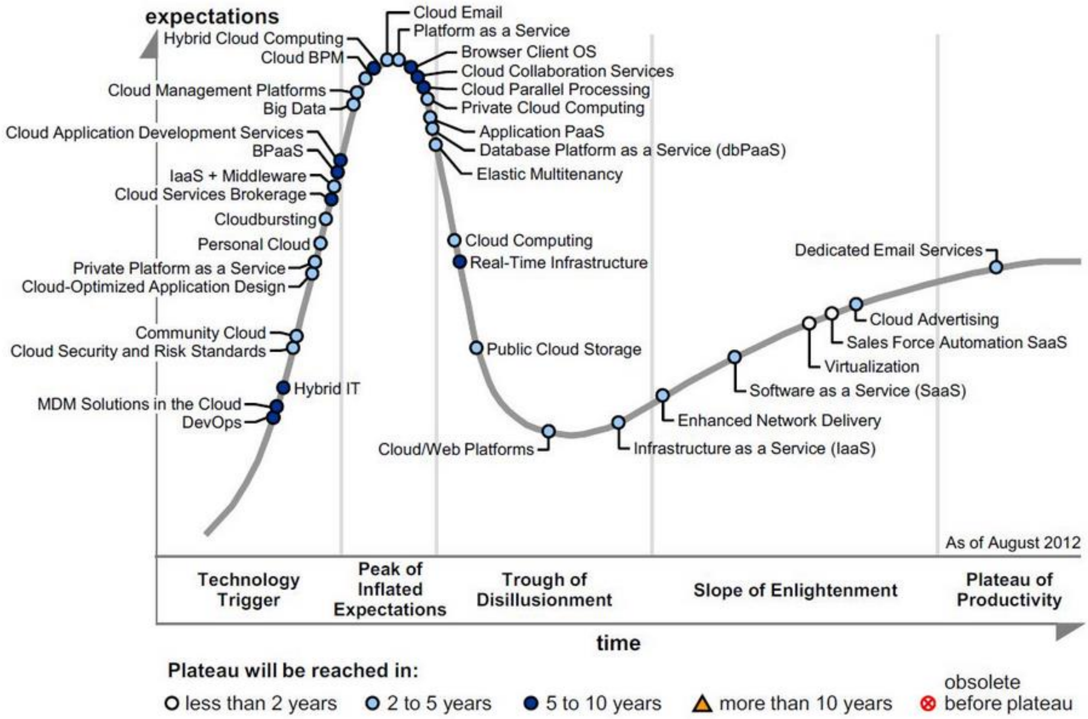


Figure 4: Gartner Hyper Cycle for Cloud Computing 2012

Internet of Things (IoT)

The term Internet of Things refers to an scenario where every day physical objects will be connected to the Internet and be able to identify themselves to other devices and to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction.
Though the Internet of Things is still only in its early stages, the number of Internet-enabled devices is beginning to explode. According to Cisco[34] , there are currently more than 10 billion connected devices on the planet. The highest connection growth is expected at the end of this decade due to decreasing connectivity costs. The number of connected devices is expected to reach 1.8 trillion in 2020, growing 3% annually.
As machines get smarter and start automating more human tasks, humans will need to trust the machines and feel safe. Since business processes are concerned, a high degree of reliability is needed. But the gargantuan amounts of devices and data involved are imposing several security challenges. Privacy, data security and regulation are the topics of concern when related to IoT, but it is also expected that cyber attackers will shift their normal targets to these devices and exploit their vulnerabilities to launch any attack. Thingsbots[4] is one example of this situation, but other are also imaginable, for instance, the control of cameras for industrial espionage or hacking any medical instrument to change its parameters.

3.1.1.4. Societal

Digitally connected society

The fast development and diffusion of ICT today has generated a digital society where habits and lifestyles have been significantly transformed i.e. our daily lives increasingly rely on the use of technology, especially social networks and their applications. This is enabling people to share information easily and consult each other on any number of issues, such as product information, instead of relying on professional critics. In line with this, social networks are also turning into a primary source of news and information. The emergence of smartphones with integrated apps makes this trend even stronger. As users connect more frequently and for longer periods, the need for cyber protection increases.

According to recent figures there are two billion Internet subscriptions, so roughly a third of the world's population is connected. It has been predicted that by 2020 between 70 -80% of the world's population will be connected, thanks to support of local governments in developing countries.

Cyber awareness

Citizens should understand threats for end-users and their impact. They need to understand how to adopt safe behaviour online for the secure use of ICT resources, and be cyber security-aware. However in accordance to the 2012 Eurobarometer on Cyber security [24] , most EU citizens say they have seen or heard something about cybercrime in the last 12 months (73%), and this is most likely to have been from television (59%). Most EU citizens do not feel very or at all well informed about the risks of cybercrime (59%). There is a clear link between being well informed and feeling confident online. Internet users express high levels of concern about cyber security: 74% agree that the risk of becoming a victim of cybercrime has increased.

In relation to the users' experience with cybercrime, more than a third of Internet users across the EU (38%) say they have received emails fraudulently asking for money or personal details. This is by far the most common type of cybercrime experienced by respondents. In addition, 15% of Internet users say that they have accidentally encountered material which promotes racial hatred or religious extremism, while 13% have not been able to access online services because of cyber-attacks, and 12% have experienced online fraud. Across the EU, 8% of Internet users say they have experienced identity theft.

3.2. Market description

The ACDC solution shows a dual behaviour, as it combines two aspects: botnet information sharing and botnet disinfection. Therefore this section explores the situation of both areas from a market point of view.

3.2.1. End-point Security Protection

In the first place, ACDC's market targets include the Endpoint Security Industry. The endpoint security market encompasses products and services that are designed to monitor, manage and protect all the endpoints on a network from attack or to directly protect information residing on endpoints.

These products provide malware (virus, spyware, rootkits, trojans and worm) detection and cleaning, a personal firewall and/or some form of host intrusion prevention (such as application control, buffer overflow protection, behavioural monitoring and enforcement, and heuristics) capability for devices. Endpoint security is used to detect and remove computer viruses, prevent the implanting of spyware, protect the computer from hacking attacks while connected to the Internet, and provide data protection with encryption.

The endpoint security industry is characterized by strong competition, fuelled by relatively high technology spillover and economies of scale. Endpoint security is a traditional, mature technology, but vendors continue to improve security technologies to keep up with the complex threat environment. To succeed in this competitive market, vendors need to offer competitive pricing and value-added features. In this way, the market is evolving from Antivirus-only to one that favours multiple functions in an integrated suite[36] . IT security experts see the benefits of consolidated management and reporting from a single console. Other related functions, such as endpoint encryption, web security, reporting, and data loss protection (DLP), are also being pulled into this kind of suites for simplified management and integrated visibility.

The term endpoint security is also being used in association with antivirus in the cloud. In this SaaS delivery model, the host server and its security programs are maintained remotely by the vendor.

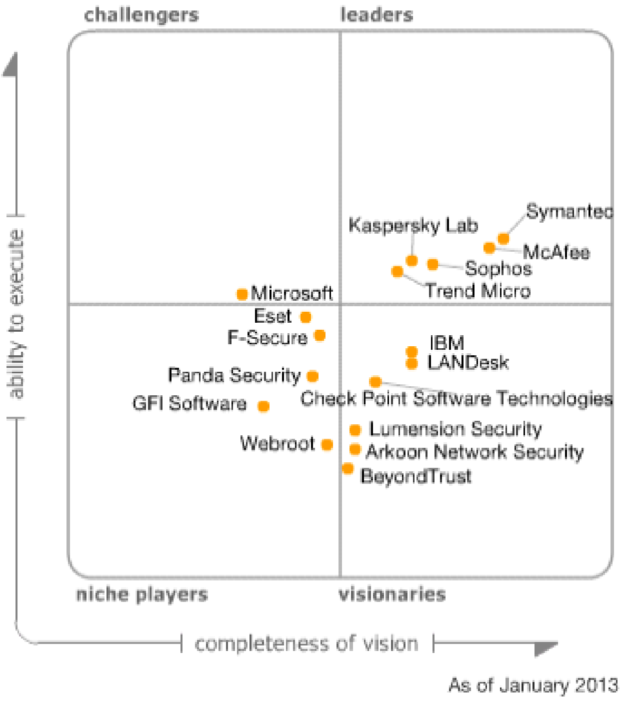
The global Endpoint Security market in 2011 was worth $63.7 billion, and is expected to grow to about $120.1 billion by 2017. The analysts forecast its growth at a compounded annual growth rate (CAGR) of 10.19% over the period 2013-2018 [37] . One of the key factors contributing to this market growth is the growing compliance regulation. The market has also been witnessing the adoption of SaaS-based security solutions. However, the growing complexity of network infrastructure could pose a challenge to the growth of this market.

North America, Western Europe, and Asia-Pacific (APAC) regions are emerging markets, whereas Latin America, Middle East & Africa, and Eastern Europe regions are considered as high growth markets. Western Europe is estimated to contribute $28.1 billion of the global revenue by 2017; at a CAGR of 10.1% from 2012 to 2017 [38] .

The industry's heterogeneous customer segments are often faced with significant switching costs, and pay attention to the brand of the security product's vendor. At the macro level, the market is segmented into those products that are purchased by consumers (B2C segment) and those that are acquired by corporations (B2B segment) and other organisations. Products and services vary at each segment. The distribution channels are manifold. The endpoint security providers can act as direct market resellers (DMR), but they have also developed partnerships with technology partners (original equipment manufacturers' (OEM) or value-added resellers (VAR)) to deliver security products in an embedded fashion or to build security services. An example is the partnering with Internet Service Providers (ISPs) or Telecoms, due to their direct relationship with mass consumers.

According to Gartner [39] , in 2013, the large enterprise endpoint security market was dominated by the companies Symantec, McAfee and Trend Micro[39] , together they represent approximately 68% of the total revenue of Magic Quadrant participants, as shown in **Figure 5**. The quadrant is based on an assessment of a company's ability to execute and completeness of vision in the endpoint security market. Sophos and Kaspersky Lab were the two other global leaders that were competitive across multiple functions and geographies, and push the combined Leaders quadrant market share to 85%. Other vendors included in the report are Microsoft, highlighted as major challenger to the leaders, IBM [41] or Panda Security [42] . Other mentioned companies are F-Secure[43] , GFI Software[44] , Check Point[45] , Eset[46] , Bitdefender[47] , LANdesk [48] , Webroot[49] , Arkoon Network Security[50] , and Lumension Security[51] .

IDC also provides a vendor assessment in the Western European market for 2012 called marketscape [52] , as shown in **Figure 5**. This shows vendors' positions with a strategic axis, representing a three to five-year span, and a capabilities axis, representing the current product and go-to-market execution. Each vendor's market share is indicated by the size of the bubble. In this case, Symantec owns the largest market share, followed by McAfee. Symantec and Kaspersky Labs are positioned as leaders. Trend Micro, McAfee, Sophos and F-Secure are positioned as major players. This is not very different from the Gartner's assessment.



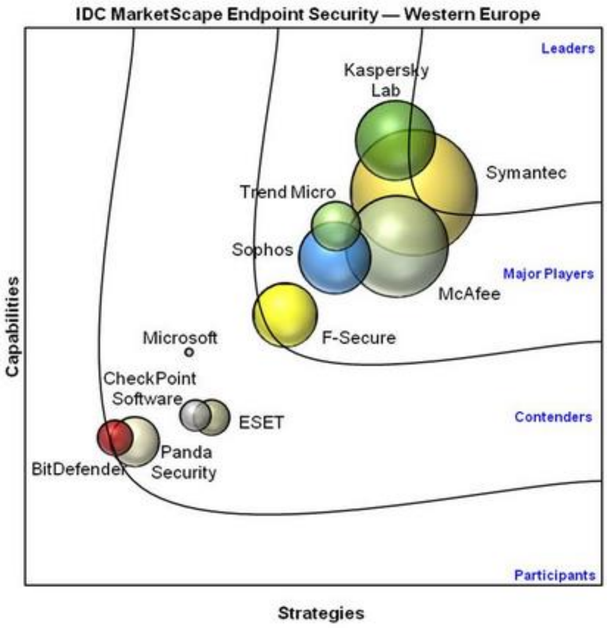


Figure 5: Endpoint security vendor landscape

Source: Gartner[39] , IDC[52]

The following sections intend to catch a glimpse of some of the competitors. Our survey is limited to the four main vendors (Symantec, McAfee, Sophos and Kaspersky), therefore it should not be considered as exhaustive. The features described in this document are based on the documentation provided by the vendors and/or third party analyser.

Symantec. https://www.symantec.com/

Symantec has a broad portfolio of security and management capabilities for enterprises and consumers. Symantec's core endpoint security solution is Symantec Endpoint Protection (SEP), currently in version 12 [53] . SEP 12 provides a full-featured Endpoint Protection Platform (EPP) solution, including anti-malware protection, device control and its Sonar engine for behavioural heuristics.

Symantec Endpoint Protection is built on multiple layers of protection against new and unknown threats. It includes the latest features for improved security, performance and management.

McAfee® http://www.mcafee.com

McAfee (an Intel company) offers a broad portfolio of information security solutions for business and customers. The endpoint protection suites include the ability to manage in-house, remote, virtual and mobile endpoints. The suites add defence in depth against the full threat spectrum from zero-day exploits to hacker attacks.

At the core of all McAfee products is the McAfee ePolicy Orchestrator platform enabling unified control and security status across organisations' security and compliance products. This is one of its differentiators. It can manage most common endpoints, such as workstations, virtual machines, file servers, exchange servers, tablets, mobile phones, clustered servers and employee-owned devices. Apart from controlling the endpoint security, it provides DLP tools.

McAfee offers professional consulting to select software and to create policies, as well as training McAfee offers security consulting as well as industry-specific packages so that businesses obtain the security that best suits their unique needs. It also provides specific training on advanced security topics.

SOPHOS http://www.sophos.com

Sophos sells exclusively to business, both midmarket and enterprise. The vendor primarily appeals to buyers who want simplified administration and management.

Sophos's endpoint security products combine endpoint, data, email, web, server and mobile protection all in one license. One license includes 24/7 support and free updates.

It provides endpoint protection for Unix, Linux, Exchange and SharePoint servers, as well as mobile phones. It can also protect Windows, Apple and virtual machines through a single management console.

In terms of DLP, Sophos provides a few encryption tools with the ability to encrypt disks, folders, email attachments and files. Full disk encryption includes secure pre-boot authentication, password tools and recovery abilities. If you add the Sophos Email Appliance or Virtual Email Appliance, it will provide email encryption, data loss protection, antispam and antiphishing for the mail gateway. The software can lock and control mobile devices and email access, and remotely lock and wipe data from devices that have been lost or stolen.

KASPERSKY lab http://www.kaspersky.com/

Kaspersky Lab offers broad endpoint platform support, including an agentless VMware vShield solution with an intrusion prevention system/intrusion detection system (IPS/IDS) using VMware Network Extensibility technology.

Kaspersky Endpoint Security for Business, called SELECT, combines signature-based, proactive and cloud-assisted technologies to deliver anti-malware protection.

Every feature within SELECT can be managed and controlled from the Kaspersky Security Centre, a centralised management console. This enables granular IT security management across the entire IT network. This console supports the management of a wide range of operating systems and platforms – including servers and desktops running Windows, Linux or Novell Netware, and includes Mobile Device Management (MDM) for mobile devices running Android, iOS, BlackBerry, Symbian, Windows Mobile and Windows Phone.

The table below compares the above-mentioned solutions according to the following features:

- Endpoint protection refers to the ability to manage the most platforms possible.
- Security refers to those features used to block malware, scanning emails and managing passwords.
- Data Loss Protection (DLP) refers to tools for preventing intentional or unintended data loss. The best endpoint solutions can stop employees from sending blocked files via email, instant chat or Internet upload. Some also provide endpoint encryption.
- Deployment refers to the different possibilities (on premise, virtualized environments, cloud-based or service provider)
- Management features refers to the existence of a centralized management console that facilitates the endpoints' software deployment, control and monitoring.
- Customer support

Table 2: Comparison of Endpoint security vendors' solutions

Vendor	Endpoint protection	Malware detection rating	Security	DLP	Deployment options	Mgt features	Customer support
Symantec.	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓	✓✓
McAfee	✓	✓✓	✓✓	✓	✓✓✓	✓✓✓	✓✓
SOPHOS	✓	✓✓	✓✓	✓	✓✓✓	✓✓	✓
KASPERSKY lab	✓✓	✓✓✓	✓✓✓	✓✓	✓	✓	✓✓

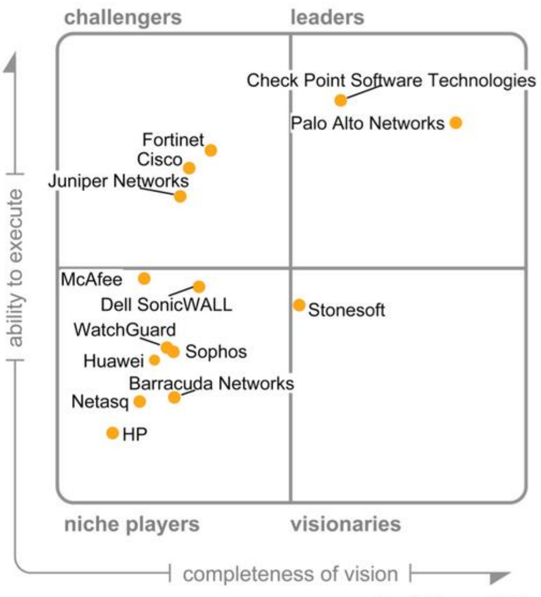
Source: based on [55] [56]

3.2.2. *Enterprise Network Firewall*

As a second area of interest, the Enterprise Network Firewall market emerges. This market is composed primarily of purpose-built appliances and virtualized models for securing corporate networks. Products must be able to support single-enterprise firewall deployments and large global deployments, including branch offices. These products are accompanied by highly scalable management and reporting consoles, products, and a sales and support ecosystem focused on the enterprise. The firewall market has evolved to next-generation Firewalls (NGFWs), incorporating full-stack inspection to support intrusion prevention (including malware prevention), application-level inspection and granular policy control. Malware prevention builds on a robust prevention feature set by adding one or more components focused specifically on the eradication of viruses, spyware, and other forms of malware.

The global enterprise firewall market is expected to grow by 11.1% CAGR, to a consolidated $34.7 billion over the 2012-2018 period [55] [68] . According to Gartner, less than 10% of Internet connections today are secured using next-generation firewalls (NGFWs). By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs.

The key vendors dominating this market space are Checkpoint [44] and Palo Alto[58] ., but there are other significant players such as Cisco[59] , Fortinet[60] , or Juniper Networks[61] , as main challengers. This is show in **Figure 6**.



As of February 2013

Figure 6: Enterprise network firewall landscape
Source: Gartner [57]

3.2.3. *Information Sharing*

A second aspect of ACDC relies on information sharing about botnets.
The concept of Information Sharing and Analysis Centre (ISAC) was introduced in 1998 in the US Presidential Decision Directive 63[62] . This directive recognized the potential for the critical infrastructures to be attacked either through physical or cyber means with the intent to affect the military or economic power of the US. The ISACs are sector specific and were established by the critical infrastructure owners and operators. The Information Technology Sharing and Analysis Centre (IT-ISAC) [63] was founded in 2000. The goal of ISACs is to provide users with accurate, actionable and relevant information. Services provided by ISACs include risk mitigation, incident response, alert and information sharing.

The Multi-State (MS-ISAC) [64] was founded in 2003 as the ISAC for state, local, tribal and territorial (SLTT) governments. The MS-ISAC launched its new cyber security operations in November 2010 and supports the Department of Homeland Security National Cyber Security Division.

In the EU, ENISA published in 2006 a feasibility study [65] about a European Information Sharing and Alert System for citizens and SMEs (EISAS). This defined an information sharing concept and infrastructure and an accompanying organisational structure (based on national structure) to support the Member States. It aimed at disseminating appropriate and timely information on Network and Information Security (NIS) vulnerabilities, threats, risks and alerts, as well as sharing good practices. This study acknowledged the crucial role of CERTs in the provision of both reactive and proactive services. In 2011, upon request of the EU Commission [66] , ENISA also published roadmap [67] for further development and deployment of the EISAS in 2013.

In the private sector there are also information sharing initiatives, such as the Microsoft's Cyber Threat Intelligence Program (C-TIP)[69] , a new system that uses a cloud computing platform to fight botnets and malware. The system will allow Microsoft to share information on computer virus infections with ISPs and CERTs in near real-time. Similar initiatives are the HP Threat Central security intelligence platform[70] .

3.3. *ACDC Positioning*

3.3.1. *ACDC offering*

The ACDC offering consist of those foreground assets developed by one or more partners that can be exploited after the project. This offering can be classified into tangible and intangible outcomes, consistent with its nature.

3.3.1.1. Tangible results

As tangible results of the project we can mention the following:

The ACDC facility
This is an online infrastructure that provides solutions to target users to fight botnets, and to build up through data collection an analysis capability of botnets occurrence and behaviour to also provide early detection of emerging botnets. **Figure 7** introduces a conceptual overview of the solution.

The core of the infrastructure is the Central Data Clearing House (CCH). The CCH is able to collect and store data feeds about botnet-behaviour by means of sensors deployed over a monitored system. The CCH is able to integrate different data streams with different data type and to filter out all information relevant to research, clearing or detection. These feeds are transferred to the analysers in order to detect vulnerable or potentially infected websites, emails, computers etc. The information

and knowledge gained from this analysis can be reported on-demand access to interested stakeholders by means of the community platform https://acdc-project.eu
This reporting feature is linked to the access policy which defines which data is available to which users.

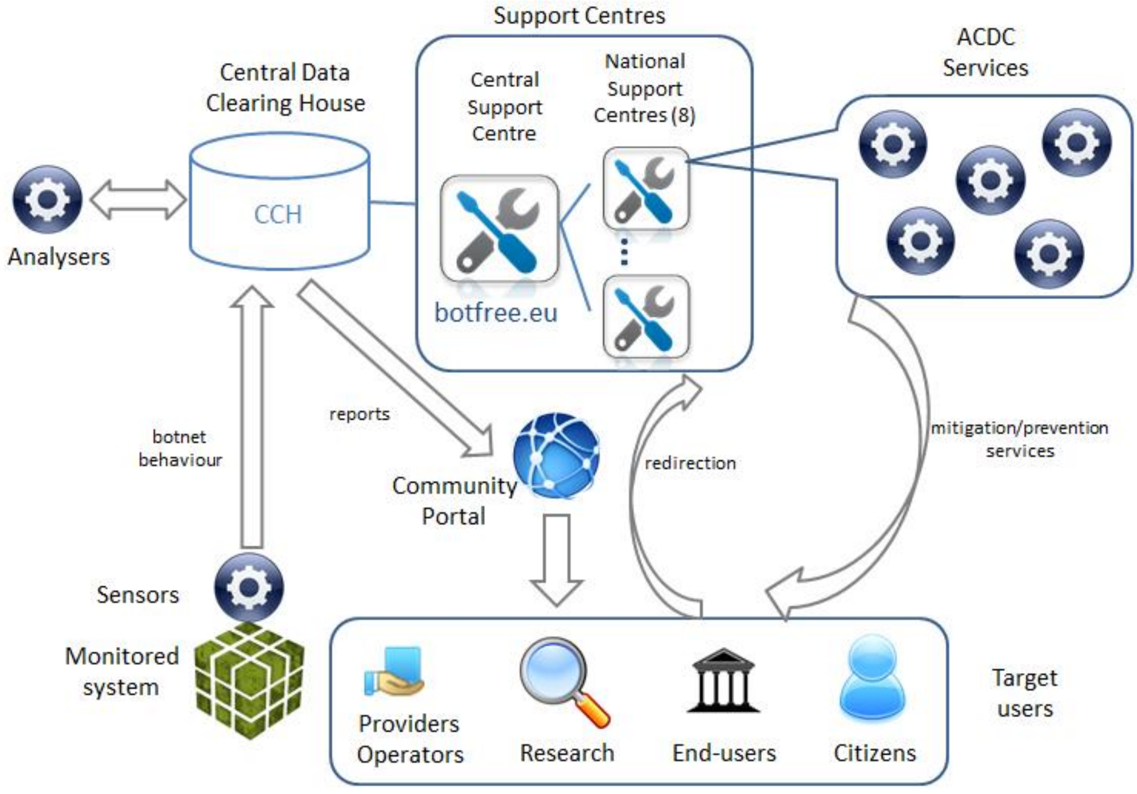


Figure 7: ACDC solution – conceptual view

While the botnet detection occurs at the CCH, the ACDC botnet mitigation and prevention services are located at the Support Centres. There is a Central Support Centre (also called the Pan-European Support Centre), accessible through the website https://www.botfree.eu. This centre is owned by ECO.

In addition, there are several national centres with local websites. For example, the German Support Centre is accessible through the website https://www.botfrei.de. Botfrei.de is an initiative from ECO supported by the Federal Office for Information Security (BSI)[71] . These national support centres are linked to the central support centre. Initially such national support centres are deployed in eight member states: Belgium, Croatia, France, Germany, Italy, Portugal, Romania and Spain. The Central Support Centre takes the role of a national support centre in the case of those member states that do not run their own centre – also supporting the setting up of additional centres through the ACDC community members interested to expand.

The community portal

The community portal (CP) is deployed as the single front-end to access the ACDC data clearing house, as well as a support to the ACDC members as a knowledge management tool and as an activity support tool. The community portal together with the ACDC data clearing house propose an advanced policy access control enabling providers of data and solutions to tailor the type of access allowed for their contribution – and for users wishing to access the data to have a clear visibility of what are their rights and obligations with respect to the data. The information about the community portal is provided in more details in deliverable D6.2.1 while the different models for users to interact are detailed in D6.3.1.

The table below summarizes the list of tangible results of the project and the corresponding ownerships.

Table 3: Ownership of ACDC tangible assets

Asset	Owner
Central Clearing House	ECO
Central Support Centre	ECO
Belgium Support Centre	LSEC/KUL
Croatian Support Centre	CARNET
French Support Centre	SignalSpam
German Support Centre	ECO
Italian Support Centre	ICSTI
Portuguese Support Centre	FCCN
Romanian Support Centre	CERT.ro
Spanish Support Centre	INTECO
Community portal	EII
Project portal	ECO

3.3.1.2. Intangible results

The intangible results of the project are mostly based on the knowledge and experience gained through the course of the project. In this sense the following can be mentioned:

Information about infected users and botnets

The most significant knowledge asset is the information about infected users, malware and its distribution services and methods, which is stored in the Central Data Clearing House. This information comes from sensors deployed over specific infrastructures (called monitored systems in **Figure 7**) and handled based on different trust levels and other defined criteria. Trust levels include various types like reputation, provider, source, volume, or frequency.

The access to this information is managed through the community platform, according to the type of member category, legal requirements, and other kind of possible restrictions expressed by the owners of the information. For example, a data source may restrict the access of a specific ISP to a range of IPs. In addition, basic reports and statistics on detection and performance can be made available on the community platform.

This can be considered as an information services provided by ACDC.

Deliverables

Another relevant knowledge asset is the project deliverables, which contain the know-how generated during the project. The topics of deliverables include:

- The architecture of the ACDC system.
- Components and technology development.
- Experiment methodology (planning, integration and deployment).
- Evaluation and validation of interoperability and effectiveness.
- Botnet measurements, metrics and other quantitative indicators.
- Legal requirements.
- Community identification of stakeholders
- Community building and animation.

ACDC will issue a total of 49 deliverables, of which 37 are defined as for public dissemination (PU), 4 restricted to other programme participants (PP), 7 restricted to a group specified by the consortium (including the Commission Services) (RE) ,and 1 as Confidential (CO). As a reference, Annex II of this deliverable provides a list of those deliverables labelled as PU.

Methodology

ACDC will develop an experimentation methodology. This methodology will be designed based on three phases: experiments design and planning, test and run the experiments and analysis (including metrics) and reporting. The methodology also proposes different roles and generic responsibilities for participants. These details will be available in D3.1 - Planning reports of the experiments, D3.2 - Design report of each experiment, as well as in auxiliary documentation to be developed during the design and planning phase to support the deployment, test and execution, and reporting phases.

Services

In the context of ACDC, the word “Service” has two meanings. In the first place, this word refers to the traditional meaning of IT services; this is an activity resulting from the use of something. As of now, they will be called “Support services”. These services can consist of services for customers, but also can refer to internal services between facility and services providers.

On top of that, the ACDC solution offers a set of tools that are also called “services” in other deliverables (e.g. D2.3). These services are categorized as “ACDC services” (e.g.: sensors, analysers, or CCH services) and “Technical services” (e.g: security, data translation or communication, among other). The deliverable D2.3 provides a wide description of both ACDC Services and Technical Services, outlining the basic models for integration and delivery principles. As a reference, Annex I. provides a catalogue of them ACDC services categorized in line with the service taxonomy defined in the mentioned deliverable D2.3.

Having said that, there list of ACDC services include:

- In relation to the support centres, ACDC will offer botnet detection and mitigation services.
- In relation to the central clearing house, ACDC will generate reports based on the feeds collected by sensors and processed by the analyser tools.
- In relation to the community portal, ACDC will offer support services for the community, for example training services ranging in scope from general skills development (e.g. with regard to botnet mitigation) to dedicated modules on the application of specific software.

The user community

The creation of a community of stakeholders related to fighting botnets is one of the major work lines of the ACDC project. As detailed in deliverable D6.1.2, 426 stakeholders have been identified and 90% of these have already been contacted. Creating and animating this community is a major output of ACDC on which to build exploitation plans.

Brand

The project brand could be considered as a valuable intangible asset. A strong brand can establish a distinct image and differentiate ACDC from other solutions in the market place.

The most identifiable element of this brand is the ACDC logo (see **Figure 8**), as any end-user is going to associate it to the project solutions and services. The ACDC logo design brings together the three key aspects of the solution: "end to end approach”, “fighting against botnets” and “infrastructure”. All aspects related to the project image are taken into consideration in D5.1.1.

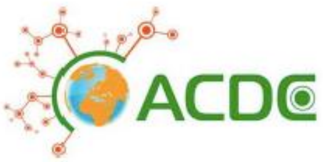


Figure 8: ACDC logo

3.3.2. *Target users*

To define the ACDC target users we will merge the classical participants' role of EU project with the cyber security positioning defined in the deliverable D6.1.1. Following this criteria, the target users can be divided into three groups, namely:

- Industrial users. This category can be split in two general groups (though a finer granularity is possible) :
  - Critical infrastructure operators vulnerable to threats from Internet (SCADA systems).
  - Providers of applications and services that can be vulnerable to attacks and therefore compromised (user perspective). But also those that provide solutions to fight botnets (contributor/provider perspective). This category comprises a wide range of stakeholders, including storage providers (data centres, cloud operators), security solutions providers (for example, endpoint security providers), providers of integration services, Internet service providers (ISPs), and mobile network providers.

- Research users. This category consists of any organisation or group conducting research related to the cyber security field. This category includes universities, research institutes, information security labs or EU research projects.

- End-users. This category can be split into three:
  - "Policy makers" refers to those organisations dealing with regulations related to cyber security. This includes institutions or agencies involved in the definition of regulations impacting the cyber security field, citizens' associations or relevant ministries from national governments concerning the mitigation of online threats.
  - "Operational stakeholders" refers to those organisations fighting against cyberattacks on a daily basis. This group encompasses national or international centres relating to cybercrime and security, Computer and Emergency Response teams (CERTs) and Computer Security Incident Response Team (CSIRT), Public prosecutors and law enforcement agencies (LEA).
  - "Intermediaries" refers to those organisations bringing together interests of particular groups on topics related to cyber security. This covers end-users and citizens' organisations, industry associations and sector federations or focus groups (such as trade associations).

3.3.3. *Competitive advantage and initial SWOT Analysis*

Table 4: ACDC initial SWOT analysis

Initial SWOT	
Strengths	**Weaknesses**
• Existing operative model for CCH and Support centre. • Breadth of services offering: connection of existing heterogeneous technologies and services into one system. • Wider participation of the stakeholders' community. • Engagement with Law Enforcement Agencies.	• Dependency on the partners' investments and solutions. • Low brand reputation. It can be easily confused with the famous Australian rock band. • Customer satisfaction needs to be tested.

Initial SWOT	
Opportunities	**Threats**
• ACDC can be the European centre of reference for fighting anti-botnets. • Possibility to expand the portfolio of services. • The facility can extend the geographical coverage. • Increasing demand for cybersecurity solutions and products • ACDC solution can act as an add-on in other anti-botnet solutions. • ACDC gives direct support to ISPs.	• Strong and tested endpoint security products with large installed client bases, backed by reputable companies, are difficult to compete with. • There may be a lack of parties willing to invest in sustaining the solution after the end of the project. • Many stakeholders can perceive ACDC as a threat: ISPs, CERTs, Hosting providers • End users that do not care. • ISPs that fail to cooperate/lack of (governmental) support • A lack of profile against existing initiatives.

3.3.4. Value Proposition and expected impact

3.3.4.1. Differentiation

These are the key differentiation aspects of ACDC with regard to other anti-botnet initiatives:

- ACDC provides detection and analysis of malicious activity in multi-domain infrastructures and a large variety of end-points, including mobile devices. Unlike other current anti-botnet solutions, ACDC goes beyond the mere C&C take-down to combat the infestation at the end-user's system, and analyses of data will better information positions on those creating and using botnets.
- ACDC integrates a complete set of heterogeneous solutions accessible online ranging from detection to protection against on-going attacks.
- Tailored access to the botnet fighting solutions depending on the customer's profile.
- ACDC offers custom-made step-by-step guidance to owners of infected machines for removing malware.
- The solution is built bringing a large community of diverse target-users on-board and involving them through concrete activities.
- ACDC provides an extensive sharing of information with the stakeholders' community without borders.
- ACDC strives to break down silos and have different entities share knowledge and cooperate in fighting botnets.
- The ACDC legal framework is fully consistent and relies on European cyber defence directive.

3.3.4.2. Expected impact

ACDC effectively contributes to increase the European cyber security by its holistic approach.

ACDC directly addresses the EU directive by means of the set-up of an infrastructure fostering the information sharing across Member States. As starting point, 8 countries will have their own national support centre and 28 partners from 14 countries will set-up the ACDC information sharing approach. These countries include Austria, Belgium, Bulgaria, Croatia, Czech Republic, France, Germany, Italy, Netherlands, Portugal, Romania, Slovenia, Spain and United Kingdom, which represents a 51% of the EU.

ACDC deals not only with the direct removal of a botnet and reduction of malware distribution, but also contributes with improved botnet measurements, the increase in intelligence, and better understanding of the legal implications.

Another relevant pillar is the participation of the end-users, by provisioning tools to fight and detect botnets, as well as increasing the level of awareness and understanding of the citizen in cyber security risks, and in particular this type of cyber-attack. By means of getting access to training and getting exposed to experiences in dealing cyber security issues, end-users can become more aware but also involved in what they can do to limit the propagation of botnet and to support early detection and incident reporting. Through this involvement, ACDC aims to move from the "this is happening to me" approach to "I can protect myself directly".

Finally, ACDC contributes to a robust information sharing model with the stakeholders' community that yield a level of the botnet situational awareness in order to empower operational and strategic decisions about how to better protect and respond. This model is based not only in sufficient detail to be valuable, but also takes into account the profile and need of the recipient. The most novel aspect of the approach is the collaboration with law enforcement agencies that can benefit directly from this feature.

3.3.4.3. Benefits for the target users

Furthermore ACDC is expected to provide the following benefits:

- For European end users:
  - Greater knowledge of and access to advanced anti-botnet tools and technologies.
  - Greater interoperability between internal software solutions and with external collaborators.
  - New frameworks for learning and collaboration.
- For security and services providers, as well as researchers:
  - Greater access to a growing and increasingly important customer base.
  - Greater interaction with trusted and key end-users.
  - Opportunities for networking and collaboration.
  - Scalability and improved resource utilization.
  - Availability of data specifically related to the European context by collecting data sets from ISPs operating in one or more Member States (current data bases reflect the American and Asian continents).
  - Proactive support for the integrity and security of services to customers.

3.3.4.4. Value Chain

The following figure shows the overall ACDC value chain[72] . The core of the chain consists of value activities relating to service and infrastructure provision. For simplicity, these activities are not broken down. The service provision activities are related to the ACDC and technical services, while the infrastructure provision activities are related to the CCH, the support centres and the CP. Below the core, supporting activities are indicated, such as the governance of the ACDC solution (facility and services), its maintenance and upgrade, and business development (including marketing and sales). Above the core the supporting services are indicated (consultancy, training or support).
Upstream value activities include the parallel chains of service, hardware and infrastructure creation. Downstream activities are focused on the service consumers, consisting of a large amount of the ACDC community (target users). For simplicity, this chain is not broken down.

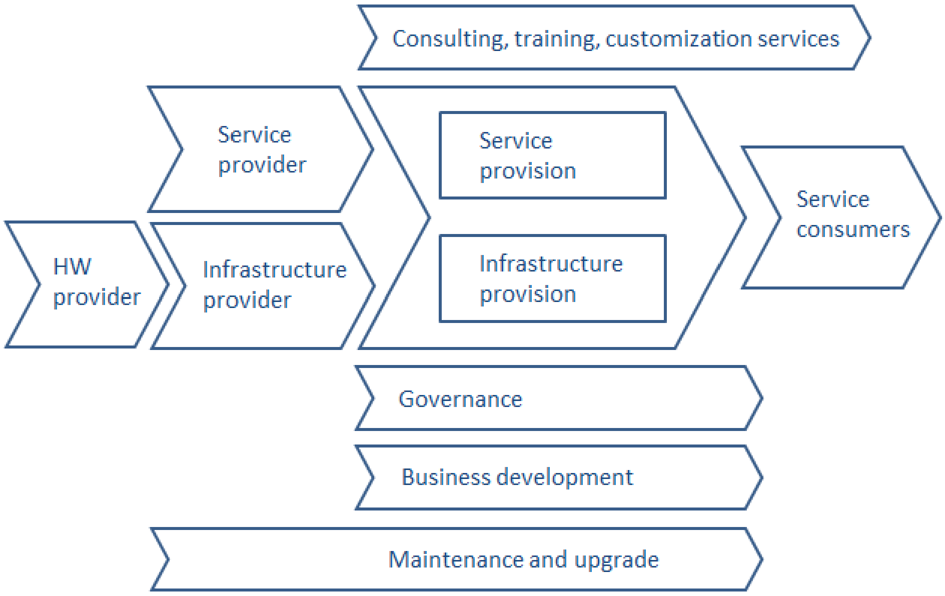


Figure 9: ACDC value chain

3.4. *Offering strategy*

3.4.1. *Sustainability*

Sustainability is one of the major goals of the ACDC project and it is related to the exploitation activity. This section approaches the sustainability aspects of the project, providing some considerations about the possible business model, actors, business structures and revenue models around the ACDC solution.

3.4.1.1. 5 year plan

This section provides an insight of the exploitation timeline to achieve the sustainability of ACDC.

ACDC 5-year exploitation plan	Y1 - 2013				Y2 - 2014				Y3 - 2015				Y4-2016	Y5- 2017
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4		
	Seed										Start-up			Growth
Definition of ACDC technical concept	■	■	■	■										■
Solution set-up			■	■	■	■	■	■	■					
Experiments run						■	■	■	■					
Evaluation and validation							■	■	■					
ACDC offering definition and business plan									■	■				
Ramp-up												■	■	
ACDC offering diversification														■
Identification of target-users	■	■												
Community set-up and animation		■	■	■	■	■	■	■	■					
Promotion		■	■	■	■	■	■	■	■	■	■	■	■	■

Figure 10: ACDC 5-year plan

The figure above represents a 5-year plan for ACDC exploitation. It consists of three phases that matches the initial stages of the business life cycle. These are the “Seed”, “Start-up” and “Growth” phases. The first phase, called “Seed”, spreads over year 1, year 2, and half of year 3. It covers the duration of the ACDC project, funded by the European Commission. For that reason, the time granularity is finer here, so that the dependencies with the project are perceived. It is worth noticing that this Gantt chart is aligned with the project’s one, but it is simplified to only consider the most relevant aspects influencing the exploitation activity. These aspects are the definition and set-up of the technical solution (related to the activity within WP1, WP2), the experiments (WP4), the evaluation (WP3) and the offering definition (WP1-WP6).

The second phase, called “Start-up”, starts in mid-year 3 and extends to year 4. The transition between “seed” and” start-up” phases should occur in the first half of year 3, when all project activities would converge into the final specification of ACDC. The start-up phase considers the ACDC business structure is already settled. The offering coming out of the “Seed” phase is in production and there is an initial client’s portfolio. At the same time this is most critical phase of the plan, as it will put the business idea to the test.

Around the beginning of year 5, the phase “Growth” is expected to happen. At this point revenues and customers are expected to increase and new opportunities arise. Though the initial offering can be maturing, this is the moment to consider new exploitation lines.

3.4.1.2. Operational model

The most general ACDC operational model is represented in **Figure 11**.
In this model there are different roles that can be played by the ACDC stakeholders:

- The ACDC customers, who consume the ACDC offering. Most of these customers are expected to come from the ACDC community of stakeholders (WP6).
- The ACDC facility providers, consisting of those partners who provide an environment for the ACDC services, acting as a kind of catalogue or marketplace in which different service providers offer services. These actors consist of the owner of the CCH, the owners of the support centres and the owner of the community platform.
- The service providers, consisting of those partners who bring the ACDC and Technical services into the ACDC facility. This group could eventually be enlarged with members of the community acting as providers.
- The data providers, consisting of those stakeholders sharing information collected from their systems with ACDC CCH.

In this model several flows are identified:

- The grey arrows in the picture represent the service flow towards the customers. These services comprise the ACDC, technical and support services provided through the facility side.
- The purple arrows represent possible internal services between service providers and facility owners on one side, and between facility owners on the other side.
- The orange arrows represent possible revenue flows associated to the services.

The final proposition for ACDC will consist of an instantiation of this picture, according to the decisions taken by partners and the remaining elements in the model. This will be discussed in a later section.

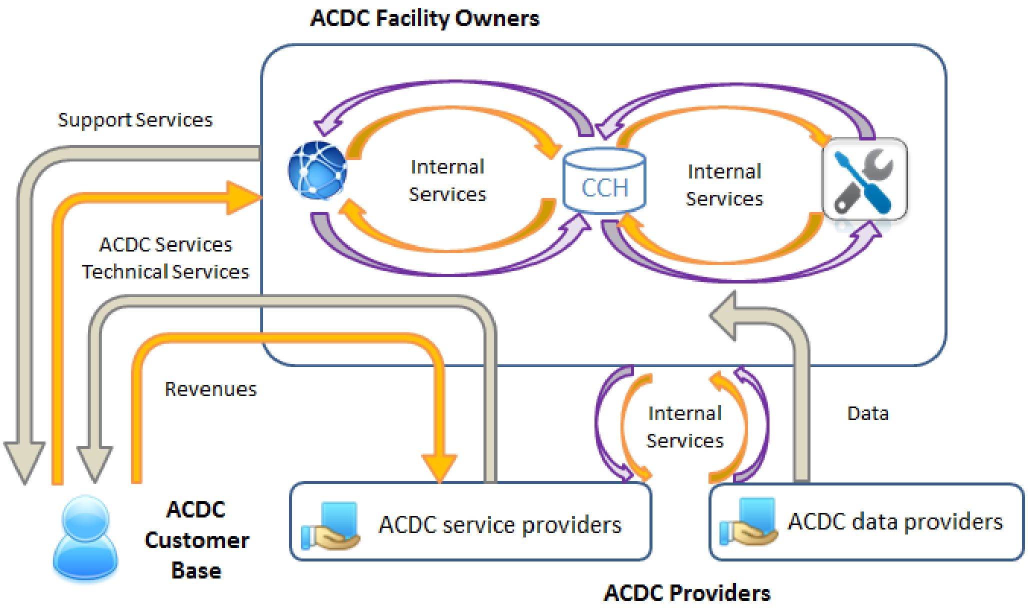


Figure 11: ADCD operation model

During the “Seed” phase of the 5-year plan, all exploitation efforts will be oriented to the accurate and final definition of this operational model. In particular, the effort should be placed on the following aspects:

- Definition of the final ACDC offering (as of M30), presumably consisting of:
  - The Central Data Clearing House
  - A Central Support Centre
  - Eight National Support Centres (possibly more if other MS set-up their support centre).
  - Service portfolio, consisting of
    - ACDC services
    - Technical services
    - Support services
- Final business plan D5.2.2, defining aspects such as:
  - The business structure that will be operated
  - The governance model in terms of resources, operation and maintenance.
  - Definition of the cost structure and the revenue model.
  - Definition of a marketing-mix strategy
- To define how the community (WP6) and related activities can transition into sustainable for profit or not-for profit initiative and the necessary steps. The natural path would be that part of community becomes the client’s portfolio and the community animation a business development department. A subset of the community, consisting of service providers could join the service offering, especially if they participated in the experiments.
- To define how the dissemination activity (WP5) can transition into marketing activities. A possibility could be a marketing department.

During the “Growth” phase, the ACDC offering can consider a diversification strategy. A possible technology roadmap could include:

- A roadmap for additional support centres in further MS.
- To enhance the botnet detection and mitigation services portfolio with new solutions not considered in the initial offering.

- To enhance the service portfolio to include tools fighting other cyber threats currently out of scope.
- To enhance the current support services portfolio with additional services. This could include:
    - Configuration services to support the integration of new support centres or tools to the facility.
    - Consultancy services to select relevant services for the customers. This could include aggregation or composition of services to offer new solutions or legal advice (e.g: data sharing, user notification, privacy, barriers for information sharing)
    - Experimentation services leveraging both the ACDC platform and knowledge gained during the project.
    - Advisory services to public and private sector end-users.

3.4.1.3. Legal structure

In order to further progress with the consolidation of a viable sustainability plan, it is necessary to create a legally binding partnership between a critical set of partners necessary to continue ACDC operations beyond the lifetime of the project. This section describes a number of legal structures in which the ACDC project could turn into at the end of the project.

The objective of this section is neither to decide at this point the final legal structure of ACDC nor constrain the outcome of the project, but to provide a synopsis of the possibilities in order to understand how ACDC could be operated. Moreover, the final legal structure cannot be discussed in isolation of existing partners' business models and strategies. In section 3.6 partners described these models.

That said, there are three legal structures to consider in the ACDC context:

I) New Legal Entity or Foundation

This option is to develop a new legal entity responsible for a commercial ADCD operation to which the foreground is passed. Issues the new entity would need to establish are:

- Legal basis (type of entity)
- Legal base (country)
- Business model, business plan
- Ownership model for the entity (who owns how many shares)
- Governance model (how partners control it)

IPR would be assigned to the company by the owners in return for shares, or licensed to it in return for a fee. The company then trades as an independent entity and shares profit with shareholders. ACDC project partners can largely participate in one or both of two ways:

1. As a shareholder in the company, with its shareholding being related to the ownership of assets assigned to the company, and
2. As an active participant in the new organisation in relation to activities such as: management, sales, development, marketing, consulting and delivery of infrastructure resources.

An alternative to this model would be a "foundation" approach with participation of multiple organisations.

II) Joint Venture (JV)

A joint venture is a business agreement in which two or more partners acting together and sharing resources in pursuit of a business or in relation to a specific project. The partners each make different contributions to the joint venture whether by way of assets, investment or skills, share the benefits and risks, and may take different levels of responsibility. One partner may take on the responsibility for managing the project and its finances, while other may also provide staff and handle product branding. Personnel and other resources are seconded to the project office from partners. Foreground must be cross-licensed, or a shared ownership or access model adopted. Revenue sharing and liability sharing is described in the joint venture agreement.

A JV agreement should describe:

- the scope of the JV
- the management of the JV
- financial and strategic objectives of the JV
- the decision making process
- responsibilities of each partner
- how to avoid and resolve disputes
- how to add or remove entities from the JV
- partners' rights and obligations (including, but not limited to, financial matters)
- the value of non-cash contribution (e.g. time, software, facilities)
- how to share benefits and losses

A governing board is responsible for key decisions such as strategic planning and budgeting. It should be made clear where the decision making authority lies, as this can be uncertain in a joint venture with several partners.

A lighter format of this model would be closer to a collaborative project where there is no central office, and participants are assigned on a full or part time basis.

III) Supply Chain

A supply chain consists of a number of partners that contribute to delivering a component of product or service. There is no central structure and may be no agreement covering all of the consortium partners.

In this model a partner would focus on its core competency. Each partner acts as supplier/customer to next partner to build the supply chain. There is a set of companies with an offering to sell and any partner who wishes to contract a service of another is free to do that on terms agreed between the two. Anyone can participate, if they provide a service, facility or capability that is of interest to others in the chain.

Foreground must be cross-licensed, or a shared ownership or access model adopted.

3.4.1.4. Commercial vs non-commercial approach

The following section tries to discuss these two approaches, a commercial and a non-commercial model, putting up pros and cons according to three dimensions: financial, acceptance and trust factors. The objective is to consider some major barriers to ACDC.

I) Financial sustainability.

Sustainability is a question of cost. The ACDC operational model will incur in a set of costs that have to born to ensure the continuity of the solution. The ACDC cost structure could be broken down into the following types:

- Operating costs, which comprise maintenance, support, quality (including service level issues), security, insurance and compliance.
- Services update/upgrade costs.
- Staff costs.
- Management costs.
- Sales and marketing costs.

In both approaches, commercial and non-commercial, the heart of the matter is the source of funds to cover this structure. Three possible sources can be taken into account, but they are not mutually exclusive. They contribute to the revenue flows depicted in **Figure 11**.

- The ACDC tenants. This would imply that most or all costs are born by the owners of the solution.

- The customers' base. This would imply charging customers for the service.
  In this option, ACDC could also adopt a profit-oriented model, aiming at generating Return on Investment (ROI). This is, if revenues would eventually go beyond the break-even point in order to both maintain the solution and generate profit to be reverted into the owners.
  In this model it is important to consider the variety of customers' profiles and their different needs. The value of the offering depends on what's important to any of these groups, and therefore the pricing model can influence how they perceive the added-value of ACDC.
  This could lead to a complex model of pricing.
  The Table 5 provides an overview of possible pricing mechanisms for ACDC for consideration. Fixed pricing mechanisms produce prices that do not differentiate in function of customer characteristics, are not volume dependant, and are not based on real-time market conditions. Differential pricing refers to pricing mechanisms that produce prices that are either based on customer or product characteristics, are volume dependant, or are linked to customer preferences, but not based on real-time market conditions.

- External sources. One option could be public funding, though it is not realistic to assume continued public funding for full operational capability. Another option could be on-line advertisement on the community portal, but this could be perceived as malicious adware.

Table 5: Pricing mechanisms

Category	Pricing model	Description
Fixed pricing	Pay per use	Customer pays in function of metered usage of service (time or quantity)
	Subscription/ flat pricing	Customer pays a flat fee in order to access the use of a product or to profit from a service.
Differential pricing	Service feature dependant	Price is set according to service configuration. Includes also bundling of different services
	Service feature dependant	Price is tailored to the characteristics of every single customer.
	Value-based	The final price will strongly depend on the customer's valuation of a value proposition.
	Tiered-pricing	Pricing is based on package of services.
	Freemium	Part of the offering is provided free of charge, but a premium is charged for advanced functionality, capacity or support.

II) Acceptance.

Sustainability is a question of stakeholders' acceptance of solution. This acceptance has to be considered at external and internal level.

In a commercial model, the pricing model can influence how the target users perceive the added-value of ACDC, which could result in an acceptance barrier. In addition, this model will probably create no differentiation from other existing, more mature, and more trustworthy solutions.

On the other hand, a non-commercial model would put all the cost pressure in the solution tenants. In a multi-tenancy model like ACDC costs can be shared among owners, but not all of them will be bearing the same quantity. This means that the perceived indirect benefit (e.g: networking, access to stakeholders) must be really attractive to really accept bearing costs as an investment.

III) Trust.
Sustainability is also a question of trust. Building trust is a very slow process, done in small steps, in a closed, secure environment. This fragile aspect can be damaged in sight of a commercial model.
The ACDC solution is based on the assumption that providers will voluntarily share date. Adopting a commercial model can make security providers perceive the solution as pure competition and therefore refuse any information sharing. This would represent a very high risk for the solution survival, especially for the CCH.

3.4.1.5. Branding considerations

The exploitation of the ACDC brand only makes sense in the framework of a joint exploitation. Branding is much related to trade marks, as intellectual property. Due to the European character of the solution, it would be advisable to seek for a Community trade mark (CTM), which offers protection throughout the EU.

In a first analysis, the ACDC brand is clearly distinctive and fanciful but not descriptive therefore it would not be rejected for such registration. The NICE class would be 42 - IT security, protection and restoration. In a first search in the Office for Harmonization in the Internal Market (OHIM)[73] , no CTM was found for ACDC, but twenty local results appeared in the search: 7 registered trademarks in France, Germany, Italy, Norway, Portugal, Russia, Spain; 3 filed in US and Bulgaria; 1 expired in Germany; and 9 ended in Turkey, US and Europe.

The registration of a Community trade mark cost has to be considered in the cost structure of ACDC. The CTM is about €900 and this would be paid over a 10-year time span with no possible alteration. Therefore, as part of the later marketing strategy, it is suggested an early measurement of the customers’ perception of the brand in order to introduce any change in the graphical identity attributes.

Finally, the CTM registration can be done either on a company or an individual basis. This is another decision to be made at the end of the project.

3.4.2. Other exploitation lines

Even though sustainability is the main exploitation objective of the project, the ACDC can leverage other important aspects of the project. As secondary exploitation line, each organisation will individually follow particular plans in accordance with the roles played within the project (industry, research or end-user) and the different interest, expectations and priorities in relation to the project outcomes. The different exploitation routes are explained in the following sections. In addition, the partners’ preliminary position in light of exploitation results is introduced in the section 3.6.

3.4.2.1. Exploitation of the ACDC facility

This refers to the exploitation of the different tangible results by their natural owners in a different fashion of that explained in the previous chapter (this is individually). The national support centres could run on their own outside the ACDC context and keep offering some detection and mitigation services, as well as support to users of infected systems, as some of these tools and services are owned by the same organisations that run the centre. The German support centre would constitute one of the most representative cases of this kind of exploitation, as it would also integrate in the same facility the central clearing house and the tools provided by ECO. At the same time, the Italian centre could integrate the services from the community portal.

The community portal itself could be also exploited for other cyber-security communities, leveraging the experience gained in ACDC, or adapted to other non-cyber domains. It could also be exploited as training facility, depending on the definition of supporting services.

3.4.2.2. Knowledge exploitation

Knowledge dissemination

This line refers to pure dissemination actions, such as the participation in related conferences or in platforms of high-visibility in order to raise awareness of the project or to communicate the project results. The following list indicates some relevant forums for ACDC activity according to the partners' involvement in such organisations.

- The European Network and Information Security Agency (ENISA) [12]
- The WG3-botnet working group within the European Public-Private Partnership for resilience (EP3R).[14]
- The Task Force of Computer Security Incident Response Team (TF-CSIRT) within the Trans-European Research and Education Networking Association (TERENA). [75]
- the International Forum of Incident Response and Security Teams (FIRST)[77]
- the Anti-phising working group (APWG)[76]
- The Réseaux IP Européens (RIPE) Anti Abuse working group [74]
- The European Cybercrime Centre (EC3)[78]
- European Cybercrime Task Force (EUCTF)
- Message Anti Abuse Working Group (MAAWG)[79]
- London Action Plan (LAP)[80]
- Interpol[81]
- Council of Europe[82]
- Financial Information Sharing and Analysis Centre (FI-ISAC)[83]

Knowledge transfer

This line refers to transfers to both industry and academia. Knowledge can be considered a tool to increase the competitiveness of ACDC stakeholders. As particular actions we can mention:

- The diffusion of the project deliverables and other supporting material, which can contribute to foster the ACDC openness to a broader audience, enhancing the linkage to other research initiatives, as well as to reduce the fragmented expertise.
- The knowledge gained during the project can be applied to partners' existing services in order to enhance its effectiveness and quality, therefore improving the customers' experience.
- Seek for synergies with other research initiatives or communities, for example research projects from the FP7 program or H2020, or the working groups indicated in the previous point.

  The easiest way of participation could be by joining the stakeholders' community and participating in the defined activities. In some other cases, it could be to define alternative collaboration agreements between parties (e.g: memorandum of understanding, terms of reference) in order to define the scope, duration and termination of the collaboration, confidentiality and IPR issues.
- Training programs on particular aspects of the project, such as botnet mitigation, botnet measurements, legal aspects or even other cyber security topics. This can be done on the platform community or internally in the partners' organisations.
- Set-up of academic programs at universities (e.g: PhD Theses).

3.4.2.3. Standardization

The ACDC consortium shall consider the following types of contributions to standardization activities:

- Identification of relevant standardisation activities to stimulate the project participation within them. Table 6 provides an initial assessment of potential relationships with relevant standardization bodies for ACDC standardization activity in line with the partners' involvement in such organisations.
- Dissemination activities within the target standardization bodies. This can be seen as part of the dissemination activity, but definitely can be considered as a first step towards awareness creation and influencing the standardization initiatives.
- Use and adoption of existing standards. This is very related to the CCH, aiming at supporting a wide-spread of data formats, such as X-ARF (Extended Abuse Reporting Format) [84] , Structured Threat Information eXpression (STIX)[85] , Trusted Automated eXchange of Indicator Information (TAXII)[86] , or Cyber Observable eXpression (CybOX)[87] .
- Monitor changes or updates in the current standards or any new standard relevant to the project in order to assure that project incorporate the most-to-date standardization framework.
- Identify and disseminate the potential contributions of ACDC of the current standards and specification (suggestion of improvements, extension proposal or complete new standards) showing the scope and impact of these contributions. This task will be executed mainly in the final part of project depending of the project results. For example, the technical deliverables will report the experiences with the use and adaptation of current standards and specifications. Some impact on current standard can also be derived from the ACDC work on feed formats to and from the central data repository. The list of standards that could receive such impact includes: X-ARF, STIX, RFC-5070 (Incident Object Description Exchange Format - IODEF)[90] , or RFC 5965 (An Extensible Format for Email Feedback Reports)[91] .

Table 6: Standardization bodies relevant for ACDC

Standardization body	Standardization Groups	Involved ACDC partners
International Organisation for Standardization (ISO)	ISO 27000 series - ISO 27002 [93]	LSEC
Industry Consortium for Advancement of Security on the Internet (ICASI)	CVRF (Common Vulnerability Reporting Framework) [92]	LSEC
Internet Engineering Task Force (IETF)	Managed Incident Lightweight Exchange (MILE) [94]	TID CyCEF DE-CIX IF(IS)
Spanish Association for Standardisation and Certification (AENOR) [95]	CTN 139: Information Technology and Communications for Health. SC 8 – Systems and Devices for Third Age Groups and Disability. SC 3 - Security, privacy and quality. CTN 133: Telecommunications. GT2 Digital Television. GT3 Accessibility. CTN 71: Information Technology. SC 7 - SW Engineering and Information Systems. SC 27 - Information Technology Security Techniques.	INTECO

3.4.2.4. Development of competences

Because ACDC is a multi-faceted project, it can contribute to the development of some competences within the participating organisations. In general, most partners can increase their knowledge, expertise and skills in the anti-botnet field. The project also focuses on community aspects, such as recruiting and animating, and business development, such as exploitation and sustainability. According to the European e-Competence Framework [96] , these are the ICT competence areas that can be reinforced (proficiency levels not considered):

- A.1 Business Strategy Alignment
- A.3 Business Plan Development
- A.4 Product or Project Planning
- A.5 Architecture Design
- A.8 Sustainable Development
- B.2 Systems integration
- B.4 Solution deployment
- C.3 Service delivery
- D.10 Information and knowledge management
- E.2 Project and portfolio management
- E.4 Relationships management
- E.9 IT Governance

3.4.2.5. Mainstreaming Legal compliance

The legal evaluation and validation of ACDC pilots will provide a set of lessons learnt in terms of compliance with legal requirements. This will identify some existing legal barriers and shortcomings and help to formulate policy recommendations for public authorities at European level to ensure the wide deployment of the ACDC solution. These recommendations will be reflected in the deliverable D5.4 – Policy recommendations (M30).

3.5. Business impact drivers

This section presents those factors that have an impact in the effectiveness of the exploitation strategy. Two temporal dimensions are considered. The short-term refers to the project execution, aligned with the “Seed” phase, while long-term would relate to the “Start-up” phase and beyond.

3.5.1. In the short term

3.5.1.1. Technology readiness of the solution

The business impact of ACDC will be driven by the technology readiness of the entire solution. This readiness depends on the technical progress regarding the deployment of the CCH, the set-up and operation of each support centre, the set-up and operation of the community platform, and the integration of the services, especially ACDC services and Technical services. This readiness will result into the expected added value to the customers (the community), as well as in the customers’ experience and therefore in the perception of the ACDC brand.

3.5.1.2. Promotion

The promotion of the ACDC solution is instrumental for its take-up, therefore dissemination and exploitation activities have to be aligned. In this sense, the dissemination activity should include:

- To create awareness of the ACDC solution.
- To communicate the differentiation aspects of the ACDC solution.
- To approach and involve target users (regular networking and lobbying activities can be instrumental in this sense).

- To stimulate the take-up.

In ACDC the promotion task lies within the dissemination activity, planned and reported within the respective deliverables.

3.5.1.3. Community

The participation of target users in the different activities of the project can be very beneficial for the final solution, as it will integrate and reconcile different perspectives.

At the same time, this participation can be seen as an opportunity for ACDC to generating demand and a "business need" by demonstrating the value of its services to European end users over the course of the project.

Moreover, the participation of key players (especially on the providers' side) in the community can contribute to make the platform sufficiently attractive to other participants to join, contributing in this way to a multiplication effect of the ACDC solution.

At this stage of the project, the following participation has been proposed (as defined in D6.3.2):

- Participation in experiments
- Contribution to regulations
- Sharing data (provision of data / usage of data)
- Becoming a member of the ACDC External Consultative Board

But to reach this level of participation, enough levels of trust must be developed.

3.5.2. In the long term

3.5.2.1. Participation beyond ACDC

Sustainability can be only achieved if a sufficient number of stakeholders are committed at the end of the "Seed" phase to support the following phases. This commitment is very dependent on strategic decisions within the partners' organisations, which can tremendously change within a 3 years frame. Therefore it is important to check the participants' interest and try to preserve the engagement or to look for alternatives that could fill a potential gap.

Several scenarios can be envisaged at the end of the project:

1. Best-case scenario. All consortium partners commit to the ACDC solution. The final offering is complete in terms of infrastructure (CCH, support centres and community portal) and of services. Some target-users from the community participate as service providers.
2. Average-case scenario. Not all partners commit to the joint ACDC solution. The offering results incomplete in terms of:
    a. Services. The absence of one of these services in the offering could be replaced by another similar solution provided for the remaining partners or by a new provider joining ACDC. An easy replacement would depend of the availability of substitutes and their fast integration in ACDC.
    b. Community Portal.
    c. National Support Centres. The absence of one of these centres could be taken up by the central support centre. As an alternative, the ownership of the national support centre could be transferred to (an)other organisation(s) interested in running the centre.
    d. CCH. As core functionality, the absence of this element would be critical for the ACDC functionality. The replacement of this element would incur additional R&D investments that cannot be acceptable by the group.
3. Worst-case scenario. There are no partners committed to the joint ACDC solution and the offerings consist of a collection of individual solutions.
4. Out-of-the-box scenario. ACDC is sustained by members who pay for the maintenance of ACDC in exchange for relevant data to their business and for data supplied to enforcement agencies and academia.

3.5.2.2. Other critical success factors

In the long term it is necessary to consider the following ACDC abilities:

- Ability to keep service relevant for customers.
- Ability to expand capacity according to customers' needs.
- Ability to defend against competition.
- Ability to maintain expertise within the organisations.
- Ability to alter service providers on the fly conforming to changes in the market.

3.6. Preliminary individual exploitation plans

The present section provides the initial ACDC partners' individual exploitation plans. Organisations are sorted per role, considering three major roles: industrial partners, academic and research partners and CERTs.

Each plan consists of four sections: a description of the organisation's business model, the relevance of the project ACDC for the organisation (the motivation for participation or the expected benefits from the project), an overview of the provided tools and their licenses, and a short description of the individual exploitation plan along the project execution. For this description the following consideration is taken: short term, ranging from M12 to M24 of the project; medium term, covering M25-M30; and long term, as of M30.

3.6.1. Industrial partners

3.6.1.1. Association of the German Internet Industry (ECO)

3.6.1.1.1.Organisation business model

ECO, with around 700 member organisations, is the largest Internet industry association in Europe. Since 1995, we have been instrumental in the development of the Internet in Germany, fostering new technologies, infrastructures and markets, and forming framework conditions. In the Competence Network, all important specialists and decision makers of the Internet industry are represented, and current and future Internet themes are furthered, together with a team of more than 40 staff.

Special ECO services [97] help to make the market more transparent for providers and users. Our seal of approval ensures quality standards; our consultations for members and our services for users provide support in questions of legality, security and youth protection.

As an association, one of our most important tasks is to represent the interests of our members in politics, and in national and international committees. As well as our headquarters in Cologne, we have our own office in the German capital Berlin, and are represented at all relevant political decision-making processes in Brussels.

ECO is a founding member of EuroISPA [98] , the umbrella organisation for European Internet associations, eco also represents the German industry with a seat on the Council of the Generic Names Supporting Organisation (GNSO)[99] at the Internet Corporation for Assigned Names and Numbers (ICANN) [100] , and is a driving force behind the Internet Governance Forum[101] – in short: We are shaping the Internet.

3.6.1.1.2.ACDC relevance in the current business model

As a non-profit organisation, eco plans to spread the word on his members, making them aware of the project and evaluating possibility to involve them in the project and further outcomes.

Special services can be offered for a fee like Initative-s par example.
AV products can be offered on an affiliate basis within the support centre pages.

3.6.1.1.3.Licensing arrangements

Eco provides ACDC with following tools

- The central clearing house (CCH). The core component of ACDC. All sensor information will be send to the CCH, stored and
- EU Cleaners from AVIRA and Surfright will be offered for free, to clean infected end-user PC.
- Initiative-S a service to monitor websites for malware. Domain owners can enlist their domain to be regularly checked for malware or dive by exploits.
- The German User Support Centre. A Place, where end-users can find help in cleaning infected PC´s. The support centre includes a website, a blog, a community board and possibly mail and telephone support.
- The acdc-project.eu website is hosted by eco.
- Botfree.eu – the landing page for the national support centres.

3.6.1.1.4.Initial plan

Eco already spreads the word about ACDC on his members to shape the awareness for the project.

Short term
Eco is already offering AV products on the German support centre as a founding for it.

Medium term
Eco is evaluating the possibility to offer services for industrial and financial partners within initiative-s. Also the central Clearing House can offer feeds to interested partners and organisations as a paid early-warning-system

3.6.1.2. Technikon Forschungsgesellschaft gmbH (TEC)

3.6.1.2.1.Organisation business model

Technikon is an independent, privately owned company in Austria which provides research services and technology based consultancy to high-tech companies across Europe. Technikon develops usable and cost effective hardware entangled security measures and develops individual trustworthy security concepts and solutions. The technological focus is trustworthy and privacy preventing authentication; reconfigurable security systems with usable key creation, storage and deletion; and software-hardware binding as protection against cloning and reverse engineering.

3.6.1.2.2.ACDC relevance in the current business model

The ACDC project perfectly meets Technikon’s technological focus being trustworthy and privacy preventing authentication; reconfigurable security systems with usable key creation, storage and deletion; and software-hardware binding as protection against cloning and reverse engineering.

3.6.1.2.3.Licensing arrangements

The Fast-Flux detection tool developed by TEC within ACDC takes a list of domain names or URLs as input and generates an output-file that indicates if a respective domain has been suspected to use Fast-Flux or not. The basic idea behind this tool is that, when a coarse physical location on the globe is associated with each IP-address of a corresponding domain, the IP-addresses of Fast-Flux domains

will be more arbitrarily distributed in space than those of a non-Fast-Flux domain and can thus be used as an indicator for Fast-Flux activity. The tool is provided Licensing free to other ACDC partners.
The System Fault Detection Tool Technology developed by TEC within ACDC is a FPGA based prototyping technology to detect system misbehaviour. The technology utilizes Physically Unclonable Functions (PUF) embedded in Hardware. The idea is to integrate the technology, such that misbehaviour (e.g. caused by inserting a SW/HW fault) can be detected and appropriate measures taken (e.g. put device in safe mode). PUF technique is used to store and safeguard secrete keys. Currently most of the services are purely software measures and the hardware is not regarded. This novel technology is based on hardware components and aims to detect failures in a cost effective and secure way. The technology developed can be licensed to other partners based on fair and reasonable conditions.

3.6.1.2.4.Initial plan

The project results will be exploited by using Technikon's "Trusted knowledge suite" to run the IT infrastructure and to improve the features and the handling of the tools. Our capability to manage national and international RTD projects will increase due to the experience gained out of the project. The reputation gained from the project will have a positive influence on our future reputation activities.
As Technikon's contribution on security requirements is concerned it will profit from the expertise gained in the collaboration with the scientific and industrial partners on development of novel security technologies. This will also positively influence TEC's activities in supporting and establishing start-up IT companies. Technikon as the national representative of the Women in Science, Engineering and Technology (WiTEC) network [102] , will also use the project to promote the objectives of WiTEC.

Short term
The short-term exploitation perspective of our development of core security technology is limited. The knowledge gained during the RTD activities is highly beneficial for our mid business development. Cooperation with partners within the ACDC consortium have already been established and will be extended.

Medium term
Our mid-term perspective of the development results within ACDC are to create patents in the field of security hardware technologies. The ACDC environment is very helpful to correlate our assumption of our costumer's needs and their pathway towards the implementation of novel security technologies.

Long term
In the long-term perspective we assume that parts of our technologies are integrated in state-of-the Art security technologies and are used within Network equipment world-wide.

3.6.1.3. Atos Spain (Atos)

3.6.1.3.1.Organisation business model

Atos is focused on business technology that powers progress and helps organisations to create their firm of the future. Serving a global client base, Atos delivers solutions and services, across five market sectors: Manufacturing, Retail & Services, Public Sector, Healthcare & Transports, Financial Services, Telecoms, Media & Technology, and Energy & Utilities.
Atos has also a horizontal offering of solutions and services for four service lines: Atos Consulting & Technology Service, Systems Integration, Managed Services, and Hi-Tech Transactional Services &

Specialized Businesses. This offering consists of Priority Offerings, Global Key Offerings (GKOs) and Common Offerings.

The GKOs are a set of solutions developed and tested in specific business environments to solve specific problems. Particularly there is a GKO on Identity, Security and Risk Management Services (ISRM) [103] .This GKO aims at offering together risk management, regulatory compliance and digital security for its customers.

The vision of the Research & Innovation group of Atos (ARI) is mainly focused on applying the latest research outcomes to real world situations where Atos' clients need solutions that go beyond what current products provide. In this sense, ARI can contribute to develop and growth the ISRM GKO, as well as developing proofs of concept for innovation topics. The ACDC project is perfectly aligned with this vision. Atos general business model is represented in **Figure 12**.

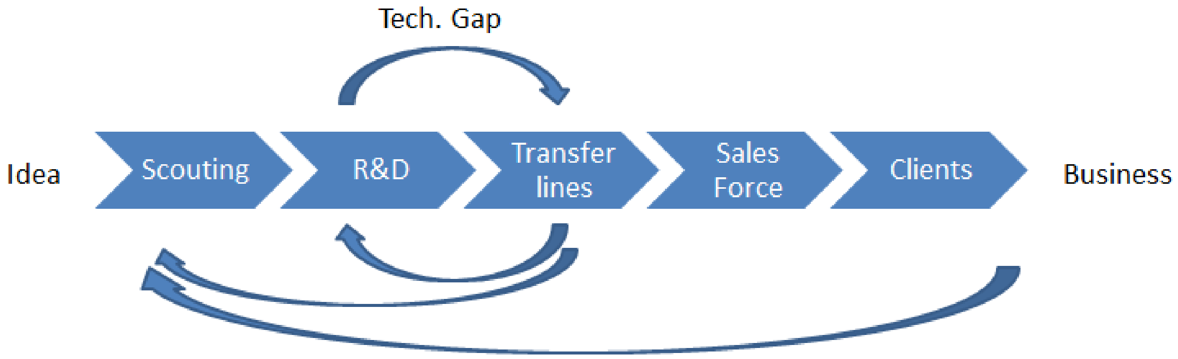


Figure 12: Atos business model

3.6.1.3.2.ACDC relevance in the current business model

As security service provider, Atos needs to respond to the new security challenges imposed by the environment and the market. Therefore the participation in a project such as ACDC can contribute to generate knowledge and experience that can be used for further improvements.

Atos provides the ACDC project with the solution "Atos High Performance Security" (AHPS), which is one of the solutions of the ISRM GKO portfolio. It provides a range of services from log management to real-time security and compliance monitoring for business applications, perimeter security devices, servers, users and business processes. During the project it will be extended to the STIX format and it is expected to improve its functionality by means of its direct participation in the project experiments.

Moreover, the ISRM GKO offers additional managed services to customers that can be benefit from the ACDC project. The following services can be highlighted: data encryption, endpoint protection, malware scanning, vulnerability management, and managed Business Partner Access.

3.6.1.3.3.Licensing arrangements

One of the AHPS versions is based on an open source security information and event management system that can be used for experimental purposes in ACDC. A commercial version will be available under specific agreements based on time and scope constraints.

3.6.1.3.4.Initial plan

Atos intends to follow several exploitation routes. In the first place, the main activity is to explore the commercial opportunities of ACDC within the ISRM GKO. The goal is to check the business alignment of ISRM with the final ACDC entity in order to participate in the future sustainability (in the long term). Atos has already established contact with the ISRM transfer line in order to raise awareness of the project motivation and of the solutions proposed. Other transfer lines and sales force teams will be also contacted in the medium term for informational purposes.

In line with this route, the ISRM service portfolio will be further analysed in the medium term in order to identify possible services enhancements based on the ACDC findings.

In the second place, Atos will explore the opportunities of using the testbed facility for internal research. The possibility of designing and running experiments over ACDC could be an interesting aspect to further develop security solutions. This aspect will be considered in relation to the results obtained from the experiments with the AHPS solution (expected in the late medium term).

Another route is the synergies with other research projects. Atos can acts as a bridge between the ACDC project and projects coming from the FP7 program or the Horizon 2020 in order to establish collaboration between them in the short-medium term. One good candidate is the project NECOMA (Nippon-European Cyberdefence-Oriented Multilayer threat Analysis)[104] , also participated by Atos, which targets three related aspects: data collection, threat data analysis and development of new cyber defence mechanisms.

Finally Atos will contribute to different promotion and transfer actions. The internal focus is important here. The expertise gained during the project can be transferred by mean of workshops practical sessions to security teams within Atos, especially the Atos Research & Innovation.

3.6.1.4. Bulgarian Post PLC (BGPOST)

3.6.1.4.1. Organisational Business Model

Bulgarian Posts PLC is a modern and fast-developing company with history and traditions that date back to 1879. The company is the designated postal operator on the Bulgarian market and has a leading position in a highly competitive market. It is a commercial organisation offering a broad range of services: postal services; money orders and payments services; courier services; subscription for periodical editions; collection of fees for electricity, water supply, telephone, mobile services; hybrid mail, direct mail; customs services. The network of the company consists of around 3000 post offices with more than 5 000 PC's, 5 185 post boxes for letter collection and 43 972 post boxes for letter delivery across the country which means that we reach Bulgarian citizens in every town and village. The company is also one of the biggest employers in Bulgaria with more than 11,000 employees. The postal sector is going under major changes as a result of the liberalization of the market, the changing demand and the development of information and communication technology (ICT). On the one hand, electronic substitution and the new means of communication have led to significant decrease in the traditional letter mail volumes. On the other hand, with the development of ICT, the postal sector is experiencing an increase in the e-commerce segment as well as in financial services. Having in view the aforementioned, optimization of business processes and implementation of new services based on ICT is of great priority for Bulgarian Posts PLC. For this purpose the strategy of the company covers aspects such as: development of the online communication network of all postal offices; implementation of systems for complete automation of processes (automated counter, migration to "thin clients", introduction of e-services); information security improvement (implementation of quality system – БДС EN ISO 27001); introduction of an ERP system; training of staff.

3.6.1.4.2.ACDC relevance in the current business model

The ACDC project is in line with the business plan of the company as the development of new services and business processes based on ICT is a top priority for the company. Thus information security is of paramount importance.
The implementation of the project at our company goes through several stages. First, a testbed environment was created. Second, the anti-botnet tools will be installed and tested, and the results will be evaluated. The third stage is related to the company's participation in the ACDC community and the dissemination of the results at a national level.

3.6.1.4.3.Licensing arrangements

Not applicable.

3.6.1.4.4.Initial Plan

BGPOST will adhere to the dissemination plan in line with D6.1.1, published on the workspace. BGPOST will work to disseminate and promote the ACDC project and its results among the stakeholders at the national level. The company aims to involve companies of various sectors in Bulgaria, including public institutions. Besides, BGPOST will work to extend the ACDC community and to attract new users of the anti-botnet instruments of the project.

3.6.1.5. CASSIDIAN (CSD)

3.6.1.5.1.Organization business model

Cassidian CyberSecurity (CSD) is a subsidiary of Airbus Group focused on CyberSecurity solutions. The entity is composed of 600 employees, mostly engineers, located in France, United Kingdom and Germany. It aims at delivering capabilities through products and services. Research & Innovation projects can be associated with any technical business line as long as it brings long term added value to the company.

3.6.1.5.2.ACDC relevance in the current business model

ACDC is an ambitious project and being part of it is a real benefit for the company relating to business impact it could have in the future. When the company proposed to develop an Operational Intelligence Center based on malware analysis, it was a fantastic opportunity to engage into something we really believe. It is a heavy program including:

- dynamic malware analysis based on an internal sandbox
- Static malware analysis based on an internal tool to disassemble a code
- Unpacking engine based on internal solution
- Correlation engine on associated malware markers

The solution is intended to be delivered as a commercial service at the end. ACDC offered the opportunity to contribute to the development of this solution.
The Operational Intelligence Center provides intelligence based on malware analysis. During the experiment phase of ACDC, the solution will be fed with malware from ACDC partners. Therefore, the more partners will provide malware, the more the solution will deliver added value.

3.6.1.5.3.Licensing arrangements

The solution will be used as a service. During the experiment phase of ACDC, the service will deliver intelligence for each ACDC submission.

3.6.1.5.4.Initial plan

Short term
The Operational Intelligence Center is already used by Cassidian Cybersecurity Incident Response Team to analyze malware and collect information about it.
The team is using and developing the Operation Intelligence Center and therefore is regularly adding features to the solution that makes sense for operational activities.

Medium term
In the medium term, the Operational Intelligence Center will be directly plugged into Cassidian Cyber Defence Center in order to deliver value to our products and solutions in a worldwide perspective

Long term
In the long term, the Operational Intelligence Center will be offered as a commercial solution for our customer with a pricing depending on features and volume.

3.6.1.6. DE-CIX

3.6.1.6.1.Organisation business model

Founded in 1995, DE-CIX in Frankfurt is the leading operator of Ethernet-based carrier and ISP interconnection worldwide. DE-CIX facilitates the exchange of IP traffic between networks through a distributed, failsafe and scalable infrastructure in various metro markets across Germany and in the Middle East. This includes broadband networks, hosting providers, content providers and cloud computing players.
Almost 600 ISPs from about 60 countries use DE-CIX to handle a large fraction of their Internet traffic and make DE-CIX the world's largest interconnection facility that supports peering. DE-CIX's customer base includes the world's leading players, such as 1&1, Akamai, China Telecom, Facebook, Google and Telefonica.
The company began its international growth with the takeover in 2012 of the operations of UAE-IX in Dubai, United Arab Emirates, the country's first carrier-neutral interconnection and peering platform. DE-CIX is a wholly owned subsidiary of eco e.V., the world's largest Internet industry association.

3.6.1.6.2.ACDC relevance in the current business model

DE-CIX has lots of experience in running high-speed networks and operating high-speed network equipment. DE-CIX will contribute to definition of requirements, architecture and standards of the centralised data clearing house. Due to its exposed position in the Internet landscape DE-CIX has the potential to host the centralised data clearing houses data bases and servers and to integrate this into the existing data exchange platform Also DE-CIX hosts and participates in a multitude of industry events like RIPE, Nanog and European Peering Forum. DE-CIX will use these forums to spread the word to its customers and to the community at large.

3.6.1.6.3.Licensing arrangements

Software developed source code may be shared with project partners.

3.6.1.6.4.Initial plan

DE-CIX is already spreading the word about ACDC to its customers.

3.6.1.7. Engineering Ingegneria Informatica (EII)

3.6.1.7.1.Organisation business model

Engineering is the major Italian Information Technology Group and a leading IT multinational in Italy, Europe and Latin America. It is ranked as the fifth Company in its sector over the Italian Market according to annual revenues.
In 2012, revenues reached 770 M€, of which close to 7% came from the international market and EBITDA totalized 96.0 M€. The company employs 7,000 professionals, of which 2,800 are external resources. It operates across 40 sites in Italy and abroad, including Belgium, Argentina, Brazil and the US.
Its revenue is split across different markets as shown in the figure below.

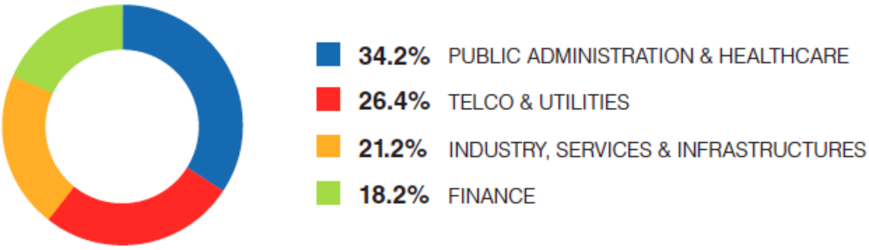


Figure 13: Engineering's revenues split across markets

Within this organisation, Engineering has a research task force of 250 employees active across 6 laboratories – this large dedication to research has created a culture of technology transfer from research to business that is in line with the ACDC goals.
In terms of business model, Engineering operates by delivering services and in-house solutions as well as bringing in outside technologies to cater to all the needs of its customer base; examples of this approach include an SAP customisation activity and the managed services (refer to next section).
Engineering also operates its own training facility, with The Engineering IT Academy "Enrico Della Valle" which provides on-site and residential certified training courses. Over 300 courses are available and during 2012, 19.200 man days of classes have been provided.

3.6.1.7.2.ACDC relevance in the current business model

ACDC directly addresses the focus of Engineering in the market of managed services. Indeed, the company operates an integrated network of Data Centres located in Pont Saint Martin, Turin, Milan, Padua, Vicenza and Rome. This infrastructure manages 15.000 servers and 230.000 workstations, catering to the needs of development, security and control of the business in all market sectors.
Thanks to "state of the art" enabling infrastructures and technologies, these data centres guarantee the highest international standards of safety, reliability, efficiency of business continuity services. In this context, ACDC directly supports an important part of the company's market.
The other aspect in which ACDC is fully relevant is the Engineering training approach in which ensuring that all professionals are aware of botnets and of possible solutions is of utmost important in order to serve its customer base.

3.6.1.7.3.Exploitation dimensions

Engineering intends to exploit ACDC's results in three dimensions.
The first dimension is the extension of the managed services capabilities in cyber-security and more specifically in early detection of any botnet related activities across its different centres.

The second dimension is the provision of services to its customer base to enhance the customers' level of protection against botnets, through training, through enhancing access control policies to key assets to decrease the vulnerabilities and through a better identification of networks and data resources at risk both internally and externally.

The third dimension is the exploitation of the community portal (built on a background asset provided by Engineering) as a knowledge management centre for cyber-security communities, and as the base to support the evolution of legislations in Europe.

3.6.1.8. G Data Software AG (GDATA)

3.6.1.8.1.Organisation business model

Non-public stock company.
GData develops and distributes IT-security products and services. The core business is based around anti-virus solutions for both consumers and enterprises. GData develops own detection technologies and maintains rulesets and databases for these technologies. These comprise signature based detection and removal, URL- and file blocklists, special tools for dedicated malware (e.g. banking Trojans).

3.6.1.8.2.ACDC relevance in the current business model

Botnets are a core infrastructure of the cybercrime economy. It is absolutely necessary to combine the forces of all relevant parties. Fighting malware in general and botnet in particular is a fundamental goal of GData. GData's main task in the project is to create interfaces to the data of the data warehouse in order to make it accessible in AV products. GData considers the ACDC data warehouse as one of the most interesting data sources for detecting botnets and mitigating its impact.

3.6.1.8.3.Licensing arrangements

GData provides two kinds of deliverables: a) tools for detecting and removing botnet-related malware and b) programs and interfaces to data. For a) tools will be made publicly available but source code will not be shared. As to b) the source code will be shared to project partners.

3.6.1.8.4.Initial plan

In the short run GData will provide tools for the removal of botnet related malware. The mid-term goal is to provide interface to data. Once the interfaces are established GData will create new detection methods based on the shared data in the ACDC data warehouse.

3.6.1.9. Signal Spam (SignalSpam)

3.6.1.9.1.Organisation business model

Signal Spam is a non for profit organisation aiming at building a trustworthy network of players to tackle spam and related cybercrime issues, such as botnets. The association welcomes Law Enforcement Agencies, Public Authorities, ISPs, Senders, Security Vendors and professional organisations. Signal Spam collects reports of spam from French citizens, qualifies them, and redistributes a useful data to its members matching their needs and capacities to tackle the specific spam the end user reported.
Therefore, Signal Spam operates data feeds and feedback loops in compliance with personal data protection policy (the CNIL – the French Data Protection Agency – is member of the Board of Signal Spam), and is also a major point of entry for end users wanting information or to take actions against spam.

This data is a valuable resource for the members of Signal Spam in their respective mission while emanating from end users, giving them the opportunity to take an active part in global protection.

3.6.1.9.2.ACDC relevance in the current business model

Signal Spam operates spambots feeds. The data indicates an IP address is corrupted (sending spam) and belongs to a Botnet. This data has the specificity of being legally usable in the court or during investigations by Law Enforcement officers.
ADCD can centralize spambot reports for European countries, enabling Signal Spam to push useful data to other lawfully accredited agencies in European countries through a centralized clearing house. On the other hand, the CCH can be a deposit for reports matching French IP space coming from other countries, accessible for Signal Spam its members.
Signal Spam has technology in place, notably for end users reporting tools, that can be used in other European countries. We see ACDC as a toolbox in which each country can retrieve the technology it needs to establish a comprehensive spambots reporting and mitigating system (by merging initiative such as Signal Spam or Botfree).
Therefore, ACDC is relevant as :

- A centralized clearance house where to share and access data (metrics or reports) on botnets;
- A toolbox for missing technologies in European countries.

3.6.1.9.3.Licensing arrangements

Signal Spam put at the disposal of ACDC's members spam reporting plugins for e-mail clients in open source.

3.6.1.10.Telecom Italia (TI)

3.6.1.10.1.Organisation business model

Telecom Italia Group operates across the entire advanced telecommunications services supply chain: fixed line, mobile, Internet, multimedia & TV, office & system solutions, IT services and R&D.
The TI Group is present as a major player in Italy and Latin America (Brazil).
Technological innovation, competence and reliability are the main features of TI Group companies, which provide products, services and solutions for the needs produced by the advancement of the digital society.
The main drivers of TI business model are:

- Fixed communications
- Mobile communications
- Service for operators
- International services
- Media
- Research and development
- IT services and product

The transformation of traditional services, especially the voice segment, into a commodity has drove TI to innovate its offering, increasing ADSL penetration, fiber access infrastructures and fostering the diffusion of voice, broadband and services bundles.
In this context TI major investments are oriented to broadband and development (reinforcing existing networks - HSDPA and LTE in mobile, Superinternet and ultrabroadband/fiber in fixed - extending coverage). In the last years TI has rethought also its traditional business model by developing value-added services in a multi-device scenario: mobile payment, VoIP, Cloud services,

App Store. The extension of the business from voice to fixed / mobile connectivity, end-to-end device management and IaaS (Internet as a Service) is a vital step forward which the Group is taking with its 3-tier cloud computing proposal: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The company has already launched cloud offerings that allow customers to save and share multimedia content, and it continues to work in this direction, coupling technological excellence with quality of service.

3.6.1.10.2.ACDC relevance in the current business model

Telecom Italia Information Technology is TI company in charge to manage all the Information technology aspects and the structure of cyber security which works daily to protect Italian customers (consumers and businesses) from telematics scams and theft of sensitive information.

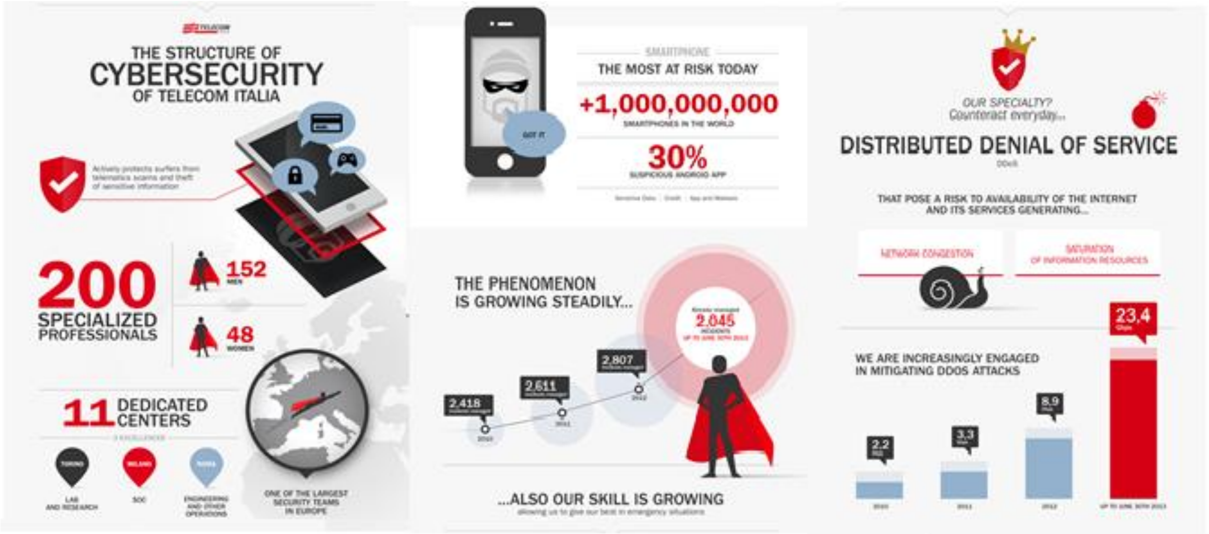


Figure 14: The structure of cyber security of Telecom Italia

As Service Provider TI has the responsibility to offers reliable and safety services and connections to its customer by protecting its network infrastructure and advising its users about possible infection.
The ACDC take a relevant role for TI in achieving and assuring these objectives in providing the results of data and botnet analysis and in identifying mitigation tools and techniques. On the other hand TI contributes to the ACDC project through the sharing of the data collected from the deployed honeynet infrastructure.

3.6.1.10.3.Licensing arrangements

TI no license arrangements

3.6.1.10.4.Initial plan

In the short medium term TI will collaborate to the creation of Italian CERT organisation under the Ministero dello Sviluppo Economico (Ministry of Economic Development) of Italy with the intent to build up a National Support Centre. In this context TI will provides guidelines for the construction of a central website from the Italian support centres, from which TI will provide appropriate advice, recommendations and giving at the same time competent support in removing the malware. Obviously the intent is to provide and encourage also other SPs in using the Support centre as a means to support their customers and increase the security awareness of the Italia communities. At the same time, the results of the ACDC Pilot will be used also internally to increase even more the security awareness and culture of the TI operations and IT designers.

In its role of ISPs, TI is probably the best positioned to support customers in, at least, detecting infections and advising the users whose machines have been compromised. However some legal concerns regarding the data sharing and the user notification will arise. For example, there may be legal issues (privacy concerns) that arise with the transfer and sharing of IP addresses of machines suspected of being compromised by some form of malwares/bots. TI intends to examine legal implication in order to remove legal barriers to information sharing. In the war against the botnets TI has already encounter part of the legal problems by choosing and implementing, as tool for malware and botnet detection, a honeynet infrastructure to avoid to adopt other instruments (e.g. the monitoring or inspection of users traffic) that can breach data protection's laws. Anyway the handling of IP address is a more complex issue. In the short medium term TI will use ACDC to analyse legal issues with the intent to understand whether a user's IP address constitutes personal data, if there are implication on its sharing and so on. In the perspective to notify the infected customers TI will also investigate the most correct and legal way to provide a user's advice to avoid that it can be considered by the recipients as an unwelcome message (e.g. spam or other kind of privacy violation). Such information and experienced will be used to set up and offer "advanced" commercial security services to the customers.

In the long term TI plan to improve its internal network protection by extending the use of honeypot as tools to detect anomalies within internal network infrastructures (e.g. intranet). The highest concentration of sensitive data and critical business applications makes the data centre more vulnerable to cyber-attack and malware infection. The intent is to use a honeynet as a simple and effective sensor to be used within an internal infrastructure as a way to trigger alerts in case of potential malware infection. That can be viewed as a warning system able to discover that someone is trying to access critical applications and sensitive data and to enforce preventive and appropriate security controls.

3.6.1.11.Telefónica I+D (TID)

3.6.1.11.1.Organisation business model

Telefónica Group is one of the world leader integrated operator in the telecommunication sector, with presence in Europe and Latin America. It operates in 24 countries. As of September 2013, Telefónica's total number of customers amounted to 320.3 million [105] .In Europe, on top of the Spanish operations, the Company has operating companies in the United Kingdom, Ireland, Germany, Czech Republic and Slovakia, providing services to more than 101.9 million customers as of the end of September 2013.
Organisational structure is design in a integrated management model where different Europe operational units are grouped inside "Telefónica Europe". Moreover a global operational business unit exists called "Telefónica Global Resources" and the unit "Telefónica Digital" focused in seizing the opportunities within digital word.

"Telefonica Investigación y Desarrollo" (TID) as a part of the Telefónica Group is in charge of innovation and strategic vision of emerging network and security technologies. TID's focus is applying new ideas, concepts and practices in addition to developing advanced products and services.

Thanks to this operational capacity Telefónica can provide different business solutions related with communication, information and entertainment solutions. Some of the relevant Global services Telefónica offer with different brands includes:

- "Movistar": Offer Fixed/ FFTH, and Mobile, Internet access, TV and voice in Spain and America
- "VIVO": Integrated operator for Brazil.

- “O2”: Offer Fixed and Mobile Internet access, TV and voice in Europe.
- “Telefónica Digital Services”: Video & Media provider, Cloud, M2M, eHealth, Applications and Security.
- “Telefónica Security Engineering” offering Integrated Security Technology: Fraud prevention, physical and electronic security.
- “Telefónica Global Solutions”: Focus on Multinationals, Wholesale and roaming companies delivering an end-to-end managed communication service: voice, data, Satellite, IT solutions, Tier-1 internet transit, managed security, etc.

3.6.1.11.2.ACDC relevance in the current business model

In general terms all information and results obtained in the project will expand the knowledge to protect Telefónica customers and will improve their quality of service reducing the security threats on the network. This is possible because one of the benefits expected, as a direct result of the project, is valuable information about botnets presence or activity in Telefónica networks, e.g. infected users by a bot.

Other relevant aspect is Telefónica internal infrastructure protection in Spain. Telefónica keeps a continuous monitoring and early alerts related to end user SPAM generation, and other Malware activities (DDoS Attacks, phising campaigns, etc.) through Operational and Security units. This monitoring has the objective to alert the client about the problem and protect the user and the network blocking this malicious traffic only when exist enough legal evidence. The integration in ACDC network could increase detection capacity and the volume and quality of evidences, and ultimately enhance user experience.

Also Between above mentioned different services offered by Telefónica business model, we can highlight a sample set of Security focused commercial services that have a clear relevance in relation with ACDC project:

- Movistar “Redes Limpias” (Clean Network) [106] . Navigation Security Service for SME and corporations in Spain clients to protect network access against security threats, some related with botnets (anti-SPAM, antivirus,anti-DoS).
- Telefónica Digital Cyber-security intelligence [107] . Enable companies to protect themselves from cyber-attacks they may be subjected to. It is a detection and analysis service whose main value lies in digital intelligence. The service focuses on two main areas: Reputation and protection of the brand and disruption of business avoidance due to leaks of information, activism, online hacktivism, DDoS attacks, breaching of security mechanisms and theft of credentials.
- Telefónica Global Solutions Anti-phising & anti-fraud service [108] . Provide a strong defence against the growing number of economically motivated attacks on business infrastructures.

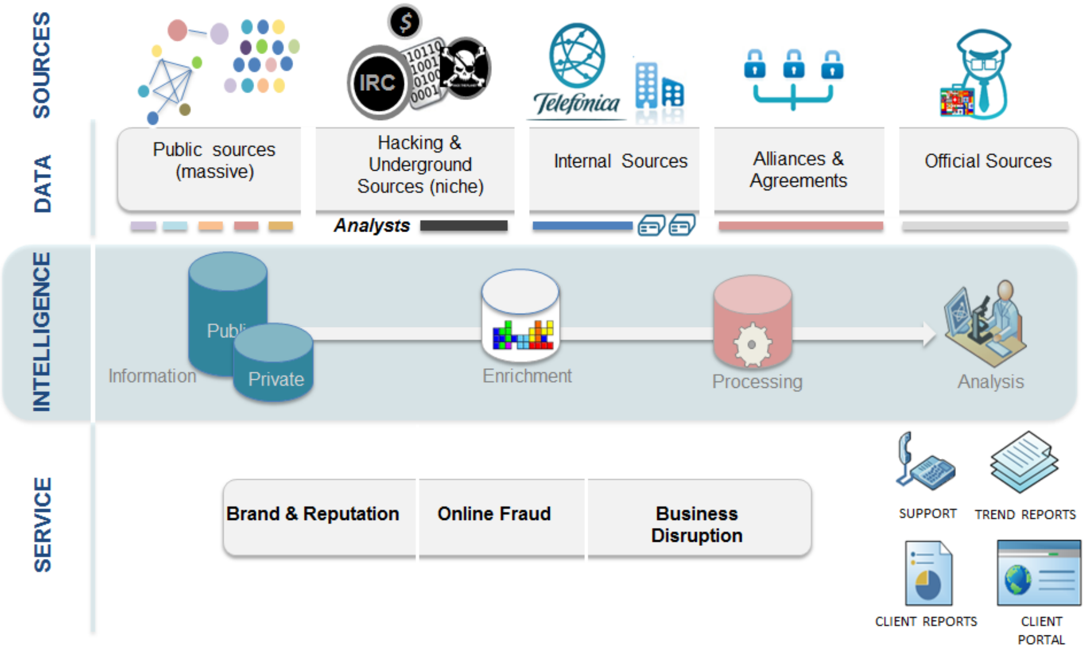


Figure 15: Telefónica Cyber security Service

3.6.1.11.3.Licensing arrangements

TID offer several tools mainly related to Deep packet Inspection (DPI), SpamBot detector and DNSbot Detector. These tools are pre-commercials tools, deployed internally in Telefónica network but currently, they are not offered by any vendor o service product. Licensing model is not yet defined but it will be available under specific agreement conditions that will be discussed with interested stakeholders or partners.

HP Sentinel is a product developed and sold by Hewett-Packard based in a commercial license. TID has tested in his own company's Network and also is developing integration with ACDC in an ad-hoc solution limited by the moment to the project lifetime.

Any other TID tools are specific designed for Telefónica, and will be not licensed.

3.6.1.11.4.Initial plan

TID initial plan will be compromise by several actions throughout project live and after that.

In short-term, TID will be engaged in several activities of internal Telefónica dissemination and discussion, mainly between different business unit of Telefónica with interest in fight against malware and Botnet. Between these activities one objective is obtain a feedback from legal departments in Telefónica Units, trying to clarify what kind of information is feasible to share with ACDC from Telefónica Network.
Additionally one of the Telefónica activities interest is to try to start some kind of small pilot inside Telefónica and feed information (anonimysed if necessary) to ACDC as part of the experiments. One option is look for a Honeypot tool in a Telefónica Unit Datacentre's. Other option is extend HP Sentinel tool to another TID premise and feed ACDC network. This way TID will contribute to extend the detection network and improve experiments goals.

In Medium-term horizon TID will be focus on offer a ACDC deployment in a Telefónica networks unit, where legal constrains allow it, since project's evolution will reach a certain level of maturity in CCH and detection's tools. TID is working with HP and their SDN technology with the objective to deploy it in some kind of Telefónica Clients or premises that include by default ACDC integration.

Long-term period will be focused in integrating ACDC as part of some commercial Security Services of Telefónica, like some of services mentioned in business model. TID and HP discussion will be kept to incorporate TID developments for ACDC integration to the HP Sentinel commercial product.

Finally in long-term TID also expect that knowledge and technology obtained in the project will allow extend cooperation and information exchange between national network operators and CERT, extending ACDC model, now that two Spanish organisations (TID and INTECO) have been active partner of ACDC project.

3.6.1.12.XLAB Razvojprogramskeopreme in svetovanjed.o.o. (XLAB)

3.6.1.12.1.Organisation business model

XLAB[109] is a Slovenian based SME, focusing on research and development in the field of distributed systems, cloud computing, big data and cyber security. XLAB's research group is known as the strongest Slovenian research group outside academia and helps bridging the gap between academia and industry.

XLAB promotes the use of the computation as a commodity for addressing general needs, e.g., in the field of the high-performance computation. Additionally, the company strongly promotes solutions for specific custom problems XLAB can implement with elastic and highly available services, backed by the cloud computation, and security frameworks (identity management, authorization frameworks). Externally, XLAB has close ties to the Slovenian Cloud Competence Centre and to the Slovenian branch of the EuroCloud initiative[111] . XLAB is actively promoting all its products and projects to its business and project partners and therefore ensuring awareness and hopefully their uptake in businesses.

The XLAB's ISL Online[110] products stemming from this area are known world-wide and have been recognised as one of the best products in the niche. On the other hand, due to the nature of the products, we have expertise in firewall penetration technology, required for the operation of the products. XLAB works also as a supporter to start-ups such as Koofr [112] , 8memo[113] , Olaii[114] , SmartHousKeeping [115] and several others. Security and privacy by design is our main concern when building new systems, even if they are not critical for the organisation.

3.6.1.12.2.ACDC relevance in the current business model

Device Monitor (mobile sensors) that is delivered by XLAB is an entity consuming events and data provided with these events submitted to the CCH instance. Currently we gather data from STIX Aggregator, but we foresee to use CCH's feed of the information. Eventually, the data is used to detect malicious events on Android devices. Users are informed whether they are accessing (un)trustworthy content on the Internet (by examining outgoing connections). Moreover, the mobile sensor is able to detect SMS hijacks and monitors other security-relevant metrics on the device. By reusing technology provided by the ACDC project we will be able to extend and upgrade our current products and provide additional functions to end-users users of our existing customers. Licensing arrangements

XLAB provides ACDC with the following tools:

- Suricata IDS (with extensions)
- GCMServer (interface between devices and CCH / STIX Aggregator)

- Device Monitor (mobile sensors)

Suricata IDS is licenced as GNU GPL meaning that derived work is distributed only under the same licence. GCM Server and Device Monitor have Business licences.

3.6.1.12.3.Initial plan

XLAB's intention of exploitation lines within ACDC is in three viable time-dimension plans. In the short-term (M13-M24) we see more adoption of the Bring Your Own Device concept (BYOD) within enterprises where security of mobile devices is of utmost importance. By adopting ACDC mobile sensors with support of the self-evolving ACDC framework that provides information about malware activities from the outside world, will gain considerable benefit on the security side of adopters. In the short-term plan we wish to adopt the ACDC framework within our organisation to support security-related actions and decisions.

Medium-term exploitation plan (M25-M30) extends the short-term plans by promoting the technology with our business connections/academia contacts. The true effort will be given after the first release, when components are put together and system can be explained and demonstrated.

In the long-term (beyond M30), positioning ACDC as product on the market may prove problematic as it is a product of plethora of partners (academia and SMEs). These long-term goals will extend the ones from medium-terms by supporting early adopters and giving more effort in the dissemination and exploitation of developed components.

Moreover, XLAB plans to exploit ACDC in commercial and non-commercial ways. Commercially we will try to transfer the innovation into commercialization of ACDC and transferring the innovations into current services. The non-commercial exploitation will be done through synergies with other research initiatives (e.g. already exploiting within MACCSA [117] initiative being established). However, as XLAB is also a research performing SME, we will transfer the know-how and academic findings of the project to the PhD candidates in XLAB and thus continuing the research on the topic.

3.6.1.13.Montimage(MI)

3.6.1.13.1.Organisation business model

The monitoring tool (MMT) allows the detection, analysis and mitigation of attacks. MMT's formal models allow specifying security properties denoting security rules and/or attacks. These security properties rely on the identification of specific events occurrences coupled with performance indicators and are based on deep package inspection (DPI) techniques. The tool is composed of several independent modules that include: MMT_Probe for the classification of communication flows and data extraction; MMT_Security for the analysis of events and behaviour; MMT_Report for the generation of custom reports; and MMT_Operator for deploying distributed network probes and correlating results obtained from the different probes to produce overall analyses. The tool can be used on-line or off-line (e.g., to analyse files containing structured information such as pcap files). The tool can be distributed as a software turn-key solution, integrated software and hardware turn-key solution or integrated to an existing platform as software libraries.

The targeted users of MMT are Network operators, network equipment manufacturers, network administrators (public and private organisations), and research. The following figure shows the business model where Montimage acts as Tool Vendor, providing software libraries or a turn-key solution to the Integrator and support & maintenance to the integrator and/or the end user.

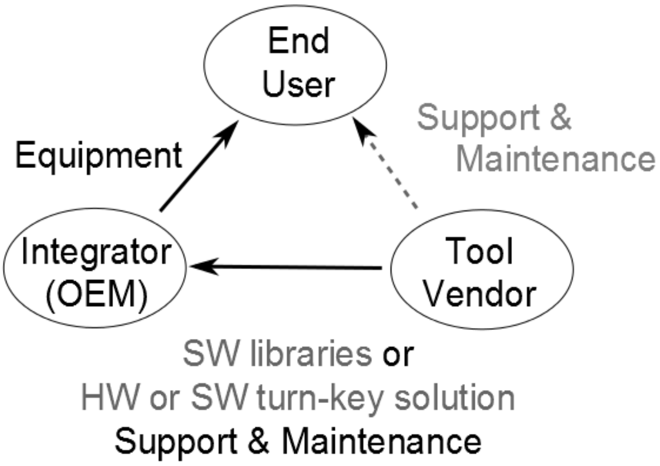


Figure 16: MI business model

3.6.1.13.2.ACDC relevance in the current business model

Probes and analysis modules can be deployed in the network to detect predefined sequence of events and behaviours. Operators can thus deploy these probes to analyse live network traffic or use them off-line to analyse captured files. In this way the probes can provide results of their analyses to the Centralised Data Clearing House of the ACDC project in an agreed format. Currently the tool can produce alerts in STIX format. The probes can also be used to trigger automated mitigation actions in response to a sequence of events.

3.6.1.13.3.Licensing arrangements

Montimage provides ACDC with the following tools:

- MMT_Probe: A version of this classification and extraction toolisavailable as freeware.
- MMT_Security: A version of thisanalysistoolisavailable as Open source.
- MMT_Report: ademonstration web service isavailable on-line
- MMT_Operator: not yetavailable

Commercial versions of MMT_Probe, MMT_Security and MMT_Probe are available and depend on usage (deployment, throughput, and required support (training, technical support, configuration/installation, integration and deployment, specific plugins...).

3.6.1.13.4.Initial plan

Short term
A collaboration has been established with another ACDC partner, CyberDefCon, to set up hardware appliances based on Montimage's and CyberDefCon's tools. These appliances will allow detecting and eliminating bad or unwanted traffic using different techniques. They will be able to provide information to the ACDC Clearing House and obtain information from it by using, for instance, the STIX format. A first demonstration version will be available by March 2013.

Medium term
Together with CyberDefCon, a project will be set up to develop a commercial version of the different appliances. This project will include several ACDC partners and other organisations (operators, research institutions, SMEs).

Long term

A company has been created for commercially exploiting the different appliances.

3.6.2. *Academic and research partners*

3.6.2.1. Fraunhofer (FKIE)

3.6.2.1.1.Organisation business model

The Fraunhofer-Gesellschaft is the leading organisation for institutes of applied research in Europe, undertaking contract research in behalf of industry, the service sector and the government. The Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) (former FGAN) has embodied excellence in applied research in the field of defence and security technology for more than 50 years. Fraunhofer FKIE conducts application-oriented research in the area of information and communication technology for public authorities and organisations from the defence and security sectors. The Cyber Defence Research Group (CDRG) of Fraunhofer FKIE (comprised of 5 senior/ post-doctoral and about 30 junior researchers) develops efficient solutions for the protection of data transmissions in critical environments and for heterogeneous network architectures.

To capture malware and bot samples the CDRG runs and develops sensors like honeypots and honeyclients. The CDRG applies reverse engineering techniques to analyse the captured malware and bots to gain deep knowledge of their functionality. This deep knowledge is used to develop and run botnet detection techniques. To identify critical events, identify dependencies, and obtain a high level overview of the security situation, a concept of model-based situational awareness is being developed. It offers domain experts an intuitive, compact, and visual representation of the security situation. The model correlates information about functional resource dependencies, business processes and information flows with information about the protected network infrastructure. An intuitive picture of the current situation can be derived from the initial state of the model and the state transitions triggered by incoming messages from different security components.

3.6.2.1.2.ACDC relevance in the current business model

ACDC is a relevant part of Fraunhofer FKIE’s anti-botnet activities. Information provided by the CCH or partners like CARNet allows refining Fraunhofer FKIE’s competences in botnet detection as well as botnet information processing. Thus, ACDC provides valuable input particularly to the CDRG in order to succeed in current and future cyber defence related research projects.

3.6.2.1.3.Licensing arrangements

All tools provided by Fraunhofer FKIE will be published under an open source license.

3.6.2.1.4.Initial plan

There are three fields of activities in which the information and sensors from this pilot will be extremely useful for Fraunhofer FKIE. Thus, FKIE will use the outcomes of the project to enrich its research and activities. The first field is deep malware analysis. To be able to analyse the really severe malware, there is an urgent need to a) know which malware families are most severe and b) get a sample of that malware. For both of these purposes the pilot will be extremely helpful. The second field of exploitation is the exchange of information regarding cyber threats. This will enable FKIE to operate its analysis on a better data basis, find collaboration partners and increase the overall cyber security. The latter is especially true for the third field, i.e. development, publication and running of new sensors. By exchanging data and experience with partners on a European level, FKIE will be enabled to develop better sensors and detection methods matching both, the threat posed by cyber-attacks and the needs of people fighting cyber threats. Especially the publication of these improved sensors and detection methods will increase cyber security.

3.6.2.2. Institute for Internet Security, Gelsenkirchen University of Applied Sciences (IF(IS))

3.6.2.2.1.Organisation business model

As IF(IS) is a research institute and there are no commercial transfer lines. The use of ACDC for if-is could be found in non-commercial exploitations like bachelor and master thesis. IF(IS) also wants to make new contacts across the borders to find new partners. Therefor ACDC with its 28 partners from 14 countries is a good platform to make new connections.

3.6.2.2.2.ACDC relevance

ACDC is the main part of botnet research done by the institute for internet-security. The knowledge we have gathered over the past years is something we want to share with others. As ACDC is a project not only for the users but for the botnet fighting institutions too. IF(IS) hopes to benefit from information provided by other partners to get new ideas for our research.

3.6.2.2.3.Licensing

The DDoS monitoring tool is not for public use as it is for research purposes only. The Information gained will be shared with all Partners via the CCH.

3.6.2.2.4.Initial Plan

IF(IS) already shares IP-addresses of known DDoS C&C servers with the CCH. This could be used by all partners to improve their black lists or help to identify infected hosts. In the future if-is will further improve its DDoS monitoring tool and integrate informations shared by ACDC partners

3.6.2.3. KU Leuven (KUL), as coordinator of the Belgian Cybercrime Centre of Excellence for Training, Research and Education

3.6.2.3.1.Organisation business model

The Interdisciplinary Centre for Law & ICT (ICRI) is a research centre at the Faculty of Law of KU Leuven [118] dedicated to advance and promote legal knowledge about the information society through research and teaching of the highest quality. ICRI is also among the founding members of The LEUVEN Center on Information and Communication Technology (LICT)[119] and iMinds [120] . It is the coordinator of the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE)[121] .

ICRI is committed to contribute to a better and more efficient regulatory and policy framework for information & communication technologies (ICTs). Its research is focused on the design of innovative legal engineering techniques and is characterised by its intra- and interdisciplinary approach, constantly aspiring cross-fertilisation between legal, technical, economic and socio-cultural perspectives. Within the ACDC project, ICRI-KU Leuven analyses the legal implications and obstacles to the successful deployment of the ACDC anti-botnet tools, which includes examining the application of the Data Protection Directive (95/46/EC), e-Privacy Directive (2002/58/EC) and upcoming European legislation, such as the General Data Protection Regulation. The objective of ICRI-KU Leuven is to advance the already existing knowledge on ICT-law and to examine compliance of new technologies with the European legal framework on data protection and electronic communications.

The Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) is the main platform for collaboration and coordination with regard to cybercrime matters in Belgium. It combines expertise of academic research groups, industry players and public organisations into a broad knowledge network. B-CCENTRE coordinates research teams at various universities that collaborate across disciplines on specific cybercrime, cybersecurity and cyber forensics related topics in both fundamental and applied research activities.

Together with experts from public sector and industry partners, the academic B-CCENTRE partners design and teach basic and advanced trainings on specific cybercrime topics and develop and implement awareness raising initiatives. B-CCENTRE also engages in the fight against cybercrime beyond the Belgian borders through numerous contacts with similar centres and expert organisations abroad.

B-CCENTRE regularly organises training, workshops, seminars as well as larger conferences for different target audiences. It has co-authored the Belgian Cyber Security Guide, outlining 10 key principles and 10 key actions to ensure/increase cyber security in companies and organisations. Via its website, the B-CCENTRE provides a one stop shop for information related to cybersecurity and cybercrime issues in Belgium and beyond, reaching out to different interested audiences.

3.6.2.3.2.ACDC relevance in the current business model

KU Leuven will benefit from ACDC through building internal knowledge on privacy aspects and net neutrality surrounding information sharing platforms. This created knowledge will be used in connection with other projects carried out inside KU Leuven by different researchers and applied in the academic courses taught in Dutch and English on various aspects of ICT-law and through which the obtained knowledge will be further exploited. Furthermore, the knowledge gathered through ACDC will be converted into academic papers and workshops, contributing to the exposure and promotion of the research centre. KU Leuven researchers will present the knowledge gained at international conferences and seminars.

B-CCENTRE will provide support for the establishment of the Belgian Cyber Security Centre, a governmental agency coordinating the activities of the Belgian public authorities dealing with cybersecurity, which will be created in the course of 2014. Its activities will include the further enhancement of the Belgian CERT as well as the development of public-private cooperation in the field of cybersecurity.

3.6.2.3.3.Licensing arrangements

ICRI-KU Leuven does not provide any tool to the project.

3.6.2.3.4.Initial plan

The legal knowledge and expertise developed with ACDC will be used in different stages and for different purposes on the activities performed by ICRI-KU Leuven. Other areas such as botnet metrics and the functioning of the community platform are also interesting sources for KU Leuven and are expected to be integrated to our new areas of knowledge and experience. Because ICRI-KU Leuven is a non-profitable and public funded institution, the goals to be pursued are based on public interest and promotion of education.

In the short term, the examination of legal and policy issues will contribute to the development of our staff and to generate academic publications. This will reinforce our expertise in the field of ICT-law and contribute to the state-of-the-art regarding data protection studies and concepts.

In the medium-term , the ACDC experience will be turned into a contact point to reach stakeholders involved in the network of the B-CCENTRE. This will be translated into training and education sessions to improve the level of network information security and information sharing. Also, the creation of the national support centre, in which ICRI and the B-CCENTRE are involved, will result in further cooperation between our institutions and the private and public sector.

In the long-term, participation in ACDC will contribute to reinforce the resilience of the Belgian public and private sectors and to promote the role of the B-CCENTRE. Moreover, this has the potential to enhance the EU capabilities to fight cyber menaces. ICRI and B-CCENTRE aim to have a real impact on the functioning and scholarship of information sharing platforms on cybersecurity and on future policies addressing this matter. Finally, we aim to be a key player in the fight against botnets.

3.6.2.4. Fundació Privada Barcelona Digital Centre Tecnològic (BDIGITAL)

3.6.2.4.1.Organisation business model

Barcelona Digital Technology Centre (BDigital) is an advanced technology centre specialized in the application of Information and Communication Technologies (ICTs) in the fields of healthcare, security, mobility, energy, and food and environment. As a technology transfer centre BDigital has several objectives:

- To promote the growth of the ICT sector and business transformation to the new digital society through the research and development of new knowledge-intensive and high added value products and services.
- To improve the competitiveness of the Catalonian economy.
- To be leading technology center in the ICT field for Catalonian companies, and an international point of reference for our excellence in research and development in the specific areas of ICT in which we operate.

3.6.2.4.2.ACDC relevance in the current business model

Barcelona Digital provides security services to CaixaBank. The idea is to create a service to collect all the malware obtained by partners and save it in the "Data clearing house". The idea is to get the malware and extract which is the affected entity. BDigital will create an automated solution and offer it to the ACDC group.

3.6.2.4.3.Licensing arrangements

Not applicable.

3.6.2.4.4.Initial plan

In the short term, BDigital will focus on the following worklines:

- Creating Data connectors for the "clearing house"
- Starting with the first tests, collecting samples of some families retrieved from the malware database
- Identifying the first affected entities from malware

In the medium term, BDigital will focus on

- Automating the collection of samples of the database
- Creating an automatic report for the affected entities found in malware
- Add intelligence analysis to find more useful data.

In the long term, BDigital will continue to offer the part of malware analysis. In addition, will support analyzing traffic, offering intelligence knowledge to detect new patterns.

3.6.3. Public Community Emergency Response Team and Institutional Organisations

3.6.3.1. Croatian Academic and Research Network – CARNet and Croatian National CERT (CARNet)

3.6.3.1.1.Organisation business model

Croatian Academic and Research Network – CARNet is a government agency founded in 1995 and operating as an independent part of the Croatian Ministry of Science, Education and Sports. Following a mission to develop advanced ICT infrastructure for the educational and scientific community including a fast and secure network infrastructure, diverse content and services, CARNet's activities are divided into four primary areas: providing ICT infrastructure and connectivity to the Croatian academic, scientific and other educational institutions, fostering the development of information society, supporting the development of a modern education system and running national services – National CERT and .hr Domain Registry.

Croatian National CERT [122] was established in accordance with the Information security law and its main task is processing of incidents on the Internet, i.e., preservation of the information security in Croatia. Its constituency are all Internet users in Croatia. National CERT is hosted by CARNet and organized as a department. All services provided by the National CERT are free of charge as this is government-funded organisation. National CERT cooperates with different commercial entities: hosting providers, ISPs, banks, etc. Activities of National CERT include receiving and disseminating information on incidents from and to its constituency, being Croatian national point of contact for incident reporting.

3.6.3.1.2. ACDC relevance in the current business model

ACDC project is quite relevant as several project objectives are in line with activities and mission of both CARNet and National CERT, as follows:

- fostering the development of information society
- preservation of the information security in Croatia
- handling different types of security incidents:
  - Denial of Service attacks
  - Compromised servers hosting malware or phishing web sites
  - Bots and botnet control centres, flux domains
  - Spam
  - Suspicious or not allowed network activities, information system compromises
- receiving and disseminating info on incidents relevant to Croatia, i.e. Croatia national point of contact for incident reporting.

The following table shows significant overlap between results derived by ACDC and taxonomy of incidents related to policy of National CERT.

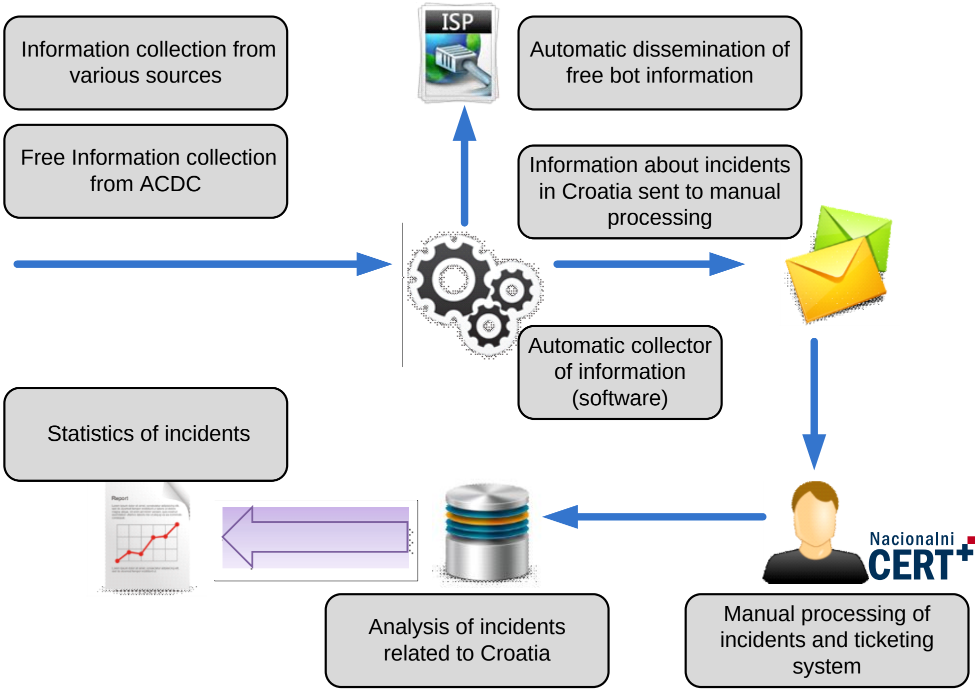
Table 7: CARNET map of interests

ACDC result	National CERT taxonomy of incidents which are processed
Fast-flux	Botnet Command and Control, proxy bots
Malicious web sites	Compromised servers: • Servers hosting Malware,

ACDC result	National CERT taxonomy of incidents which are processed
	• Servers hosting Phishing web sites • Servers hosting Ads propagated by spam • Other compromise types
DDOS	Any type of denial of services
Spambots	Spam
-	Unwanted network activities like brute force, vulnerability scans e.t.c
Mobile bots	Bots
-	Network abuse

Information on infected systems disseminated by ACDC is considered very valuable for National CERT and thus might be included in standard dissemination procedure as shown on the picture:

Incident processing in National CERT


Information collection from various sources
Free Information collection from ACDC
ISP
Automatic dissemination of free bot information
Information about incidents in Croatia sent to manual processing
Automatic collector of information (software)
Statistics of incidents
Report
Nacionalni CERT
Analysis of incidents related to Croatia
Manual processing of incidents and ticketing system

3.6.3.1.3. Licensing arrangements

CARNet provides several tools to ACDC. Info on licensing for a particular component is given, as follows:

- **Spamtrap sensor** – distributed in OVA format to ACDC project members and can be used only for ACDC project purposes. Spamtrap software has open source licence as well as used components
- **Honeypot sensor** – distributed in OVA format to ACDC project members and can be used only for ACDC project purposes. Honeypot software has open source licence as well as used components

- **Passive DNS sensor** – distributed in OVA format to ACDC project members and can be used only for ACDC project purposes. pDNS sensor software has open source licence as well as used components
- **NIRC**-the software component is integrated in Mediation server - the software can be used strictly within the framework and for the purposes of the ACDC project. CARNet reserves the right to modify the software and terms of service without prior notification at any given moment. The software runs only in CARNet collecting information related to incidents in all EU-members IP space.
- **Mediation server** - the software can be used within the framework and for the purposes of the ACDC project. Use of the software is only possible with the prior knowledge and written approval of CARNet. Distribution and modification of the software is prohibited. CARNet reserves the right to modify the software and terms of service without prior notification at any given moment.

3.6.3.1.4. Initial plan

Since CARNet is public institution with activities based on non-for profit basis, the initial exploitation plan is non-commercial. Initial plan aims to identify potential users (stakeholders), contact them through the priorities and user groups, inform them about the ACDC project and potentially actively involve them in project.

As far as short term is concerned, interest for collaboration has been expressed on behalf of Croatian Telecom, University of Zagreb and BGPOST. ACDC member BGPOST already installed spamtrap and honeypot sensors in their networks and University of Zagreb did the same. CARNet is negotiating with Croatian Telecom to install fast-flux sensor at their premises that would enable ACDC to detect large number of fast-flux domains due to the fact that Croatian Telecom is the largest ISP in Croatia. In this way detection of fast-flux domains accessed by majority of bots in Croatia would be detected. CARNet already deployed in its network all three sensor types. The results of all sensor types except fast-flux detection are sent to STIX aggregator.

In medium term, CARNet will concentrate on sensor exploitation in Croatia and using data received from Central Clearing House. This data would be analysed and free data will be sent by existing dissemination channels to ISPs, hosting providers and end-users. This process will be automated by software in the same way as National CERT disseminates information to constituency currently. Besides dissemination, National CERT will act on information on incident in Croatia received from ACDC .

In long term National CERT will continue to receive free information on malicious URLs, bots, fast-flux domains and botnet C&C related to Croatia and will deal with such incidents on Internet. CARNet will liaise with stakeholders willing to use commercial results of ACDC. CARNet also plans to host national anti-botnet support centre (domain antibot.hr) as well as maintain and run its network sensors software. CARNet as a service provider has plans to improve the security of its services using results of ACDC project as well.

3.6.3.2. CERT-RO & Romanian Partners

3.6.3.2.1.Organisation business model

Romanian National Computer Security Incident Response Team (CERT-RO) is a public institution, designated as a national contact point regarding cyber-security incidents, in charge with preventing, analysing, identifying and reacting to cyber-security incidents at national level.

CERT-RO was founded in 2011, and its activity is based on a Government Decision (494/2011). CERT-RO constituency is composed of all users, systems and networks from Romanian cyber-space; this includes commercial, government and research/education oriented teams as well as service providers and ISPs. In order to maintain the security of the RO cyber-space we do cooperate with a large number of entities, both from RO and abroad, including public authorities, CERTs, ISPs, security vendors etc. A part of these partners, especially the public authorities, are implied also in the ACDC project.

Among the services that CERT-RO offers we can find: **proactive** (Alerts on new threats and vulnerabilities that may affect national cyberspace, Notices regarding the possibility of major cyber security incidents occurrence, Study guides and documentation on recent developments in the field of IT & C security, Security assessment for partners (audits, network and application pentests etc.).), **reactive** (Alerts and warnings on the occurrence of major attacks preceding activities, Alerts and warnings related to cyber security incidents occurrence, Management of a database with national cyber security incidents, Security incidents investigation and results dissemination), **support** (Awareness activities for the government and partners, Risk assessments, Support the partners in development of their own CERT teams, Consulting services for securing critical infrastructures, Development of the national policy and security strategy with partners).

3.6.3.2.2.ACDC relevance in the current business model

The activities and objectives within the ACDC project, are in accordance with our long and medium term policies, regarding the handling of botnet activities or other related cyber-security incidents within Romania.

Responding to botnet related incidents occupies a great part of our activity, as over 90% of the alerts that we receive monthly are related to this phenomenon. Taking care of this great number of botnet alerts, means having the proper tools, having access to information related to the subject and having a great number of external partners that can provide help and support in case needed. These all requirements are accomplished by the ACDC project.

3.6.3.2.3.Licensing arrangements

CERT-RO develops the following tools within the ACDC project:

- **HoneyNetRO** – based on multiple open-source solutions, in-house customized and developed after our needs and after ACDC requirements. The solutions can be as a service or as a solution by other ACDC partners but only within the project activities.
- **NoSQL Big Data Storage Tool** – based upon MongoDB open-source solution used for storing large volumes of information. The solution is customized after our needs. We can provide support in installation and operation if needed.
- **Spam Analysis Tool** – In-house developed solution that can provide correlation of spam emails into clusters. Clusters of IPs which send similar spam, allegedly form the same botnet. The solution can be provided as a service for the ACDC partners, since the source code is proprietary and cannot be provided.

3.6.3.2.4.Initial plan

Since CERT-RO is a public non-profit institution, the initial plan regarding exploitation is totally non-commercial.

On the short and medium term we plan on developing and improving the solutions that we proposed in the project, in order to develop a large national network of sensors, able to detect botnet related activities. Other tools provided by other partners in the project can also be used in order to improve the detection rate. The data collected will be sent to CCH in order to be used by partners.

On the medium term we also would like to extend the network of sensors, implement as many sensors as possible within key national players (ISPs, universities etc.) and extend collect data that can be provided to the CCH.
On the long term we plan on sustaining and improving the infrastructure developed within the project. Collected data will be used for disinfection within our constituents and for our partners. We also plan on using the info provided by the ACDC CCH for alerting and disinfecting our constituents.

3.6.3.3. DFN-CERT

3.6.3.3.1.Organisation business model

The DFN-CERT, which was historically the CERT of the German Research Network only, nowadays provides key security services to industry as well. Due to a long term role in helping other CERTs to establish or become more mature, the DFN-CERT builds on a trusted network of contacts throughout Europe and beyond.

Based in Hamburg, the DFN-CERT is responsible for a constituency of several hundred universities and research institutions throughout Germany. It has a long term relationship in international, European and national fora and groups related to fighting cyber crime and helping the victims of attacks and incidents. Preparing proactive steps through focused research in the IT security field enables the DFN-CERT to promote best practices. This is done both in writing and in educational courses. Most recently a software based threat management was added to the service portfolio.

The DFN-CERT provides managed services in terms of DDoS detection/mitigation, incident management, vulnerability management as well as early warning to key players in Government and industry.

3.6.3.3.2. ACDC relevance in the current business model

Being a CERT, DFN-CERT exchanges incident data as well as early warning data on a day to day basis. This is an integral part of the services provided to the constituency. The benefit of participating in ACDC is thus twofold. DFN-CERT will use the data obtained from the ACDC Pilot to enhance the services for its customers in incident handling and automatic warning where applicable. Furthermore DFN-CERT will profit by supporting the data formats established in the Pilot for sharing data with other partners. This will also be aided by the outcomes of the Pilot's legal tasks concerning exchange of incident or other security related data on a European level.

Beyond that the DFN-CERT has a strong research interest in the needed technical fields of measurement (e.g., honeypots) and data distribution (e.g., one-to-many or many-to-many incident distribution platforms) and further data enhancement and aggregation to provide early warning measures for new rising threats.

3.6.3.3.3.Licensing arrangements

DFN-CERT does not provide any tool to the project.

3.6.3.3.4.4.3.3.4.4. Initial plan

DFN-CERT initially plans to use the ACDC mechanisms, especially the distribution mechanisms attached and maintained by the central clearing house. DFN-CERT plans to use these mechanisms to enhance its own current channels and benefit from the centralized maintenance instead of increasing in-house maintenance efforts, which would be necessary without ACDC.

In the short-term DFN-CERT plans to use ACDC as a resource to distribute incident data towards ISPs on a much larger scale than today. In addition DFN-CERT would be able to hand over data involving end customers and other relevant parties for which it today does not have an established trusted communication channel that could be utilized. This will extend the outreach making it possible for more potential and actual victims to benefit from the improved sharing activities.

DFN-CERT's medium-term plans call for full integration of data provided by the central clearing house into its own data processing facilities. By doing this, DFN-CERT can also enhance its services directed towards the German research community as the primary constituency.

Also in the mid-term DFN-CERT would be highly interested in Botnet metrics as a tool of qualifying network security measures on an ISP or organisational basis, allowing for the development of more adaptive alerting services based on much improved situational awareness.

In the long-term DFN-CERT will re-engineer all its communication and distribution channels to be compatible with the established technical and organisational standards as demonstrated by ACDC. This will allow DFN-CERT to benefit from more information sources, invest less in proprietary software and be fully integrated in the trusted sharing communities, both directly as an active contributor and indirectly as a beneficiary of all data submitted to ACDC by organisations and parties that have no direct relationship with DFN-CERT.

The feasibility of this will certainly depend on the rights management for submitted data, the data formats, and the availability of a minimum guarantee of follow-up data handling inside ACDC as well as further agreements covering important operational aspects necessary to build the underlying trust fabric. With DFN-CERT as a leading partner concerning the data formats handling during the project duration, DFN-CERT hopes to be able to make this plan successful and convincing.

3.6.3.4. National Institute of Communication Technologies (INTECO)

3.6.3.4.1.Organisation business model

The National Institute of Communication Technologies (INTECO) is a state owned company attached to the Spanish Ministry of Industry, Energy and Tourism through the State Secretariat for Telecommunications and for the Information Society.

INTECO is the responsible, through its CERT, to managing the defence of the cyberspace and serve as preventive and reactive security support to Spanish entities and citizens. INTECO has the ability to act in response to security incidents ranging from the citizen to the business sector, especially strategic and critical infrastructure sectors, and the specific area of academic network.

At present, the government of Spain has several agents working from different perspectives in order to achieve a secure cyberspace. INTECO is a leading figure in the panorama of national cyber security, both from the point of view of providing services to different target audiences, and in the exercise of awareness and communication needs and current challenges of cyber security.

The commitment with cyber security of the Ministry of Industry, Energy and Tourism is translate in building strategies and pooling of actions, as well as the establishment of collaborative spaces with all agents nationally and internationally.

Last February was published the Spanish Digital Agenda [123] , with specific objectives for the development of the economy and the digital society.

The last March was approved the National Security Strategy [124] which provides current security needs and includes in its own the cyber security, ensuring representation of the points of view corresponding to the requirements, resources and activities relevant about cyber security.

In the same way, last June were published the seven plans that articulate the Spanish Digital Agenda, INTECO had been reflected in one of them; the Plan of Trust in the Digital Domain [125] .

The Trust in the Digital Domain Plan makes its own the joint mandate of the Spanish Digital Agenda, the European Cyber Security Strategy and the National Security Strategy to advance in the objectives of building an environment of trust that contributes to the development of the economy and the digital society, have an open, safe and secure cyberspace, ensure the safe use of networks and information systems, and respond to international commitments on cyber security.

One of the main measures to strengthen confidence in the digital domain is consolidate INTECO as centre of excellence in digital trust, subject to the following lines:

- Extend their participation at all levels of trust in coordination with other entities in the digital trust domain.
- In the domain of cyber security, place it as a reference entity for strategic sectors, companies and citizens.
- Establish the necessary skills to study emerging risks and to anticipate needs and take preventive measures.

Those lines and Plans define, therefore, INTECO's business model, that is based on the following activities, with non-commercial objectives:

- **Services:** INTECO promotes services in the area of cyber security that allow the use of ICT and increase the digital trust. Specifically, INTECO works to protect the privacy of users, encourages the establishment of mechanisms for preventing and responding to security information incidents, minimizing their impact if they occur, and promotes the progress of security information culture through awareness and training.
- **Research:** INTECO has a strong ability to tackle complex projects of different nature and with a strong innovative component. The dynamic of its operations is oriented to research, allowing INTECO has the capacity to generate intelligence about cyber security to approach its application in new technologies and mechanisms which also reversed in improving services.
- **Coordination:** INTECO participates in collaborative networks that facilitate immediacy, comprehensiveness and effectiveness when deploying an action in the field of cyber security, always with a perspective based on experience and information exchange. Therefore, coordination and collaboration with other organisations, public and private, national and international, across the field of cyber security is an essential factor for the INTECO activity.

3.6.3.4.2.ACDC relevance in the current business model

ACDC proves to be relevant in the current INTECO business model, through the alignment of several ACDC project objectives with the measures covered by the Trust in the Digital Domain Plan, in which INTECO takes part as state instrument for cyberspace defence management, in particular, the following:

- Implementation of a neutral incident management point: Implementation during 2014 of the technical and customer support centre, to support the security incident management code of conduct, stated in the amendment of the Information Society Services Law (LSSI), to be established as the national support centre for priority response in the fight against botnets.
- Deployment of a new technological platform for early warning and technological surveillance services: That includes new cyber security intelligence services, by means of the establishment of agreements with leading international institutions, and research and innovation work, constituting a core of knowledge and evolving service for proactive threat detection, early warning and support in strategic decision making regarding to cyber security in Spain.

- Development of new communication channels for digital trust: By means of the implementation of a new Website offering specialized security contents to the distinct public targets, to achieve greater impact and efficiency in the dissemination and early warning activities.
- Development of a new awareness plan: To strengthen the awareness and training actions in digital trust INTECO develops, by incorporating the public and private sector, and including among others the implementation of actions in line with the European Strategy for Cyber security.

3.6.3.4.3.Licensing arrangements

INTECO provides to ACDC different information that is not affected to need licensing arrangements, nonetheless could be necessary some agreements about privacy and confidentiality.

As public entity without economic purposes, in the case that INTECO provides to ACDC partners some of its tools and source code, like Skanna and Evidence Seeker, a specific usage policy or license should be defined (not yet defined).

3.6.3.4.4.Initial plan

In the short term ACDC contribute to INTECO as a useful source of information and knowledge about botnets mitigation. This information will allow INTECO mainly in the following actions:

- Develop and contribute to the Spanish National Antibotnet Support Centre offering Spanish end users new tools or services to detect, disinfect and prevent botnet infections.
- Develop and/or deploy new tools or services to detect and analyse new botnets and infection channels.
- Create awareness campaigns for citizens.

In the medium term INTECO pretends to obtain the following objectives:

- Consolidate Spain as a leader in cyber security aspects.
- Reduce the level of infections caused by botnets.
- Increase on citizens the level of knowledge of the threats associated with botnets.
- The INTECO recognition as the national governmental reference centre in the fight against botnets.
- Improve cooperation and coordination at national and European level to take effective measures against botnets.
- Increase the protection provided to European citizens and helps prevent fraud.
- Increase cyber security in Europe, decreasing the level of botnets and their impact.

In the long term INTECO aims to impact on the standards and specifications in the fight against botnets and formalize valuable partnerships with companies of the public and the private sector around the world to work together in the fight for the botnets detection, with the objective of increased the cyber security and the cooperation with others areas of the world in anti-botnet actions.

3.6.3.5. IstitutoSuperioredelleComunicazioni e delleTecnologiedell'Informazione (ISCTI)

3.6.3.5.1.Organisation model

The Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI), founded in 1907, is a technical/scientific body within the Italian Ministero dello Sviluppo Economico, Dipartimento per le Comunicazioni. Its activity is focused on regulation, experimentation, basic and applied research, training, specialized education and dissemination in the field of electronic communications and services. In addition, ISCTI ensures technical support to private organisations, public institutions and citizens through laboratories and specialized personnel.

The ISCTI supports Italian Public Administration within international organisations like ITU (International Telecommunication Union) [126] , CEPT (Conference Europeenne del Administrations del Postes et Telecommunications)[127] and ETSI (European Telecommunications Standards)[128] . Through the CONCIT (Comitato Nazionale di Coordinamento per l'Informatica e le Telecomunicazioni), formed by the ISCTI, CEI –Comitato Elettrotecnico Italiano [129] and UNI – Ente Nazionale Italiano di Unificazione[130] and recognized at a European level), the ISCTI carries out the translation of the European regulation into the National regulation.

In the cyber security sector ISCTI is committed in the development of the Italian National CERT to be provided by Ministero dello Sviluppo Economico through a joint effort among public CERTS, national private network operators and other stakeholders.

ISCTI also collaborates with ENISA (European Network and Information Security Agency) participating to the Management Board and to a number of technical working groups including implementation of guidelines of Article 13a of the Directive 2009/140/EC [131] .

It participations to the Cyber Security Exercises organized at European and extra-European level, and has contributed to the planning and execution of Cyber Europe 2010 and 2012 and to the planning of Cyber Europe 2014 [132] , first, second and third European cyber exercise. It has also contributed to the planning and execution of Cyber Atlantic 2011 [133] , first joint EU-US exercise.

In the sector of the Computer Science Security Certification, the ISCTI hosts OCSI expert team which participates to the CCRA (Common Criteria Recognition Arrangement)[134] international treaty as Italian Information Security Certification Body. OCSI is also member of SOGIS (Senior Officials Group for Information Systems Security) for mutual acknowledgement of ICT security certifications at European level. OCSI security certifications are then acknowledged at international level on the basis of CCRA and SOGIS agreements.

In addition, ISCTI hosts its own security certification laboratory for classified products, i.e. CE.VA (Centro Valutazione).

3.6.3.5.2.ACDC relevance in the current model

ACDC project represents for ISCTI an opportunity for public-private cooperation at European level and of implementation of European Digital Agenda programme. Namely, the participation in the project will result into increased know-how and access to new instruments and capabilities to counter botnet threats. As for the latters, ISCTI, in cooperation with the organisations of the ACDC Consortium, will build the Italian Support Centre, which will be hosted in the ISCTI location and realized with the help of EII and TI. This will be a national focal point for information, prevention and dissemination on botnet threats in cooperation with the other Support Centres in Europe. In the medium-long term, it will be also an instrument to help define guidelines and procedures for the telecommunication operator in order to prevent and tackle botnets as well as to support infected users. In addition to providing support to users, the centre will carry out detection of threats with the help of GARR, national telecommunication operator for research institutions in Italy and will be open to contribution from other national operators. The centre will be focused on collection of statistics on botnet at national level for sharing with the European centralized clearing house. It will be also open for contributions from academy, enterprises providing security solutions and analysts at national and international levels.

3.6.3.5.3.Licensing arrangements

The Support Centre infrastructure to build in ISCTI location will be owned by ISCTI. Ownership and utilization rights of tools applied to the Support Centre will be regulated among contributing partners according to provisions of the ACDC Consortium Agreement. In the development and utilization of tools open-source SW will be privileged.

3.6.3.5.4.Initial plan

The initial plan for the development of the support centre includes basic services according to the ACDC approach for support centres mainly focused on information, prevention and dissemination of botnet threats and relevant international activities with special focus on the ACDC project activities. A longer term plan, based on the acquired results of the project, will follow to envision potential support to users in cooperation with national internet service providers and network operators.

4. Conclusions and future work

This deliverable has defined an initial exploitation plan for the ACDC project. The plan defines strategic actions necessary to deliver business insight across a range of exploitation options, with specific focus on the sustainability of the ACDC solution at the end of the project. This relies on the joint exploitation of the following elements: the central data clearing house, the central support centre, the national support centres, a wide portfolio of services (information, detection, mitigation, technical and support),and a methodology for experiments (including metrics).

Since the technical results are still in a preliminary stage, the objective is to provide a reference to ensure that the technical dimension is oriented to the future market opportunities and to prepare an effective launch upon completion of the project. At the same time, the plan considers how to leverage the on-going work of dissemination and community building in order to lay the foundations for the future rollout of the solution.

Apart from the sustainability perspective (supported by the technological dimension), the project ACDC also showed its impact at knowledge, technical and social level, as commented. Exploitation activities have been addressed in detail, with a common framework being used by all project participants. Additionally preliminary Individual exploitation plans have been outlined to identify an initial list of business and transfer opportunities.

During the second period of the project, ACDC will consolidate the technical work and enter the experimentation and validation phases. The outcomes of each phase will be taken into consideration to review and refine the exploitation strategy and to develop the final exploitation plan. All final considerations will be included in the deliverable D5.2.2 at M30 (July 2015).

5. References

[1] Symantec. Grappling with the ZeroAccess Botnet. http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet

[2] Securelist. http://www.securelist.com/en/

[3] BBC. Microsoft disrupts ZeroAccess web fraud botnet. http://www.bbc.co.uk/news/technology-25227592

[4] Proofpofing. “Proofpoint Uncovers Internet of Things (IoT) Cyberattack”. http://www.proofpoint.com/about-us/press-releases/01162014.php

[5] Taskforce Bestuur Informatieveiligheid en Dienstverlening. http://www.taskforcebid.nl/

[6] European Union. The Stockholm Program. http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_en.htm

[7] European Commission. Digital Agenda for Europe. http://ec.europa.eu/digital-agenda/

[8] Europol. EuropeanCybercrime Centre. https://www.europol.europa.eu/ec3

[9] Eur-Lex. “Joint Communication to the European parliament, the council, the European economic and social committee and the Committee of the regions. Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace”. http://eur-lex.europa.eu/JOINByRange.do?year=2013&min=1&max=25

[10] Eur-Lex. “Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union”http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:HTML

[11] ENISA. NIS platform. https://resilience.enisa.europa.eu/nis-platform

[12] ENISA. Homepage. http://www.enisa.europa.eu/

[13] ENISA. Press release. “New Regulation for EU cyber security agency ENISA, with new duties”http://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cyber security-agency-enisa-with-new-duties

[14] ENISA. European Public-Private Partnership for Resilience. https://resilience.enisa.europa.eu/ep3r

[15] European Cyber security Month. http://cyber securitymonth.eu/

[16] European Commission. Horizon2020. Security. http://ec.europa.eu/programmes/horizon2020/en/area/security

[17] European Economic Forecast. Autum 2013. http://ec.europa.eu/economy_finance/publications/european_economy/2013/pdf/ee7_en.pdf

[18] OECD Economic Outlook, Volume 2013 Issue 2.November 2013. ISBN: 9789264200951. http://www.oecd-ilibrary.org/economics/oecd-economic-outlook-volume-2013-issue-2_eco_outlook-v2013-2-en

[19] Forrester."A Better But Still Subpar Global Tech Market In 2014 And 2015". http://www.forrester.com/A+Better+But+Still+Subpar+Global+Tech+Market+In+2014+And+2015/fulltext/-/E-RES104903

[20] Eurostat. Real GDP growth rate – volume. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tec00115

[21] Trading Economics. Euro Area GDP Growth Rate. http://www.tradingeconomics.com/euro-area/gdp-growth

[22] Block Chain. http://blockchain.info/

[23] Littlecoinblog. Bitcoin’s Market Cap have just hit $10 Billion. http://litecoinblog.org/bitcoins-market-cap-just-hit-10-billion/

[24] European Commission. 2012 Eurobarometer. http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

[25] McAfee. McAfee Threats Report: First Quarter 2013. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf.

[26] Project Syssec. RED BOOK. A Roadmap for Systems Security Research. http://www.red-book.eu/m/documents/syssec_red_book.pdf

[27] The Enterprise Strategy Group. "Malware and the State of Enterprise Security". http://cdn.blog.malwarebytes.org/wp-content/uploads/2013/07/ESG-Brief-Malwarebytes-Jul-2013-1-1.pdf

[28] IDC. "IDC Forecasts Worldwide Tablet Shipments to Surpass Portable PC Shipments in 2013, Total PC Shipments in 2015".http://www.idc.com/getdoc.jsp?containerId=prUS24129713

[29] CISCO. "Cisco 2014 Annual Security Report". https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[30] Canalys. "Over 1 billion Android-based smart phones to ship in 2017".http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017#sthash.P3oAg9Wq.dpuf

[31] Gartner. “User Survey Analysis: Is Bring Your Own Device Job Essential or a Personal Preference?” March 2013. https://www.gartner.com/doc/2395315?pcp=itg

[32] SANS institute. “SANS Mobility/BYOD Security Survey”. March 2012. https://www.sans.org/reading-room/analysts-program/mobility-sec-survey

[33] Juniper Networks. “Mobile Threats report”. http://www.juniper.net/us/en/forms/mobile-threats-report/

[34] Cisco. Connections Counter: The Internet of Everything in Motion. http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342

[35] Price-Waterhouse. ”PwC Global 100 Software Leaders. Converging forces are building that could re-shape the entire industry”. May 2013.http://www.pwc.com/en_US/us/technology/publications/assets/pwc-global-software-100.pdf

[36] C.Wang, C. Shereman. “The Forrester Wave™: Endpoint Security, Q1 2013”. January 2013. https://www.m3corp.com.br/wp-content/uploads/2013/09/1-L43Z9O.pdf

[37] Global Endpoint Security Market 2014-2018. http://www.researchandmarkets.com/research/d7f3mw/global_endpoint

[38] Markets and Markets. “Cyber Security Market”. June 2012. http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

[39] P. Firstbrook, J. Girard, and N. MacDonald. “Magic Quadrant for Endpoint Protection Platforms”. 2013. Gartner. https://www.gartner.com/doc/2292216

[40] Trendmicro. http://www.trendmicro.com/

[41] IBM. http://www-01.ibm.com/software/

[42] Panda security. http://www.pandasecurity.com/spain/

[43] F-Secure. http://www.f-secure.com/

[44] GFI software. http://www.gfisoftware.com/

[45] Checkpoint. http://www.checkpoint.com/

[46] ESET. http://www.eset-la.com/

[47] Bitdefender. http://www.bitdefender.com

[48] LANdesk. http://www.landesk.com/

[49] Webroot. http://www.webroot.com/us/en/

[50] Arkoon. http://www.arkoon.net/en/

[51] Lumension. https://www.lumension.com/

[52] IDC Marketscape. “Western European Enterprise Endpoint Security 2012 Vendor Analysis”. http://www.idc.com/getdoc.jsp?containerId=IS01V

[53] Symantec End-Point protection. http://www.symantec.com/endpoint-protection

[54] McAffee Endpoint protection suites. http://www.mcafee.com/uk/products/endpoint-protection/endpoint-protection-suites.aspx

[55] Top Ten Reviews. “2014 Best Endpoint Protection Software”. http://endpoint-protection-software-review.toptenreviews.com/

[56] AV-comparatives. “Whole Product Dynamic. Real-World Protection Test”. December 2013. http://www.av-comparatives.org/wp-content/uploads/2013/12/avc_prot_2013b_en.pdf

[57] Young. G. “Gartner Magic Quadrant for Enterprise Network Firewalls”. February 2013. https://www.gartner.com/doc/2329815

[58] Palo Alto Networks. https://www.paloaltonetworks.com/

[59] Cisco Sysmtems Inc. http://www.cisco.com/

[60] Fortinet Inc. http://www.fortinet.com/

[61] Juniper Networks Inc. http://www.juniper.net/us/en/

[62] IT Law Wiki. “Presidential Decision Directive 63”. http://itlaw.wikia.com/wiki/Presidential_Decision_Directive_63

[63] The Information Technology - Information Sharing and Analysis Center. http://www.it-isac.org/

[64] Multi-State - Information Sharing and Analysis Center. http://msisac.cisecurity.org/

[65] ENISA.”EISAS- European Information Sharing and Alert System. A Feasibility Study”.2006/2007. http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf

[66] European Commission. “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”. March 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[67] ENISA.”EISAS- European Information Sharing and Alert System. A Roadmap for further development and deployment”. February 2011. http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap

[68] Market Info Group. “Robust Growth for Global Enterprise Firewall Market”. http://www.marketinfogroup.com/robust-growth-for-global-enterprise-firewall-market/

[69] Microsoft. “Microsoft Takes Botnet Threat Intelligence Program to the Cloud; Provides Near Real-Time Data” May 2013. http://www.microsoft.com/government/ww/safety-defense/blog/Pages/post.aspx?postID=312&aID=98

[70] Hewlett Packard. “Announcing HP Threat Central security intelligence platform”. September 2013. http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/Announcing-HP-Threat-Central-security-intelligence-platform/ba-p/6186875

[71] Federal Office for Information Security. https://www.bsi.bund.de/EN/Home/home_node.html

[72] D. Field. "Identification of Business Models Through Value Chain Analysis - A Method for Exploiting Large Technology Projects - A Whitepaper". September 2011.

[73] Office for harmonization in the internal market (OHIM). https://www.tmdn.org/tmview/welcome

[74] Réseaux IP Européens (RIPE). Anti-Abuse working Group. http://www.ripe.net/ripe/groups/wg/anti-abuse

[75] TERENA. Task Force Computer Security Incident Response Teams (TF-CSIRTs). http://www.terena.org/activities/tf-csirt/

[76] Anti-Phising Working Group (APWG). http://www.antiphishing.org/

[77] Global Forum for Incident Response and Security Teams (FIRST). http://www.first.org/

[78] Europol. European Cybercrime Centre (EC3). https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837

[79] Message Anti Abuse Working Group (MAAWG).http://www.maawg.org/

[80] London Action Plan (LAP). http://londonactionplan.org/

[81] Interpol. http://www.interpol.int/

[82] Council of Europe. http://hub.coe.int/

[83] Financial Information Sharing and Analysis Centre (FI-ISAC). https://www.fsisac.com/

[84] X-ARF Network Abuse Reporting. http://www.x-arf.org/

[85] Structured Threat Information eXpression (STIX). http://stix.mitre.org/
[86] Trusted Automated eXchange of Indicator Information (TAXII).http://taxii.mitre.org/
[87] Cyber Observable eXpression (CybOX). http://cybox.mitre.org/
[88] Malware Attribute Enumeration and Characterization (MAEC). http://maec.mitre.org/
[89] Common Attack Patterns Enumeration and Classification (CAPEC).http://capec.mitre.org/
[90] The Internet Engineering Task Force. RFC-5070 Incident Object Description Exchange Format. http://www.ietf.org/rfc/rfc5070.txt
[91] The Internet Engineering Task Force. RFC 5965 An Extensible Format for Email Feedback Reports.http://tools.ietf.org/search/rfc5965
[92] Industry Consortium for Advancement of Security on the Internet (ICASI). Common Vulnerability Reporting Framework http://www.icasi.org/cvrf
[93] The ISO 27000 series. ISO 27002 http://www.27000.org/iso-27002.htm
[94] Internet Engineering Task Force. Managed Incident Lightweight Exchange. (MILE) https://datatracker.ietf.org/wg/mile/charter/
[95] Spanish Association for Standardisation and Certification (AENOR). Comités Técnicos de Normalización (CNT). http://www.aenor.es/aenor/normas/ctn/ctn.asp
[96] European e-Competence Framework. http://www.ecompetences.eu/site/objects/download/5983_EUeCF2.0framework.pdf
[97] Association of the German Internet Industry (ECO). Services. http://international.eco.de/services.html
[98] European association of European Internet Services Providers Associations. http://www.euroispa.org/
[99] Council of the Generic Names Supporting Organisation. http://gnso.icann.org/en/
[100] Internet Corporation for Assigned Names and Numbers (ICANN).http://www.icann.org/
[101] Internet Governance Forum. http://www.intgovforum.org/cms/
[102] European Association for Women in Science Engineering and Technology (WiTEC).http://www.witec-eu.net/
[103] Atos. Identity Security and Risk Management. http://atos.net/en-us/home/we-do/identity-security-and-risk-management.htm
[104] NECOMA project. http://www.necoma-project.eu/
[105] Telefónica. Corporate Profile. http://www.telefonica.com/en/shareholders_investors/html/informaciongrupo/perfil.shtml
[106] Movistar. Redes limpias. https://www.movistar.es/empresas/para-tu-oficina/seguridad/ficha/empresas-redes-limpias)
[107] Telefónica. Cyber Security intelligence. http://blog.digital.telefonica.com/?press-release=telefonica-cyber-security-latch-cyber-detect-threats
[108] Telefónica. Global Security Services.http://www.multinationalsolutions.telefonica.com/media/55614/global_security_services_t8970.pdf
[109] XLAB. http://www.xlab.si
[110] XLAB. ISL Online. http://www.xlab.si/products/isl-online/
[111] EuroCloud. http://www.eurocloud.org/
[112] Koofr. http://koofr.net/
[113] 8memo. http://8memo.com/
[114] Olaii. http://olaii.com/
[115] SmartHousKeeping. http:// smarthousekeeping.com
[116] GNU GLP. http://www.gnu.org/licenses/gpl.html
[117] Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA). http://www.federatedbusiness.org/mne7
[118] KU Leuven - Faculty of Law. http://law.kuleuven.be/
[119] LEUVEN Center on Information and Communication Technology (LICT). http://www.esat.kuleuven.be/LICT/

[120] iMinds. http://www.iminds.be/

[121] Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE). http://www.b-ccentre.be

[122] Croatian National CERT. http://www.cert.hr

[123] Spanish Digital Agenda. www.agendadigital.gob.es

[124] Spanish National Security Strategy. http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/256935/20131332EstrategiadeCiberseguridadx.pdf

[125] Plan of Trust in the Digital Domain. http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaconfianza/Plan/Plan-ADpE-5_Confianza.pdf

[126] International Telecommunication Union. http://www.itu.int/es/Pages/default.aspx

[127] Conference Europeenne del Administrations del Postes et Telecommunications (CEPT). http://www.cept.org/cept/

[128] European Telecommunications Standards Institute. http://www.etsi.org/

[129] Comitato Elettrotecnico Italiano. http://www.ceiweb.it/it/

[130] Ente Nazionale Italiano di Unificazione. http://www.uni.com/

[131] EUR-Lex. Directive 2009/140/EC. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

[132] ENISA. Cyber Europe. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe

[133] ENISA. Cyber Atlantic. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic

[134] Common Criteria Recognition Arrangement (CCRA). http://www.commoncriteriaportal.org/ccra/

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

6. Annex I.ACDC Services

This section includes the catalogue of ACDC tools provided by the partners. The categorization of services follows the taxonomy of services described in D2.3. A wider description of each, stating their readiness level and how they contribute to the ACDC solution, is also available in the mentioned deliverable D2.3.

Table 8: ACDC tool classification per solution

Sensors and detection tools for networks	Systems infections – infected web-site analysis	Device detection and mitigation – multi-purpose tools for end-users	Centralized Data Clearing House
• Wildfire • Spamtrap and low interaction honeypot(s) multipurpose appliance • Passive DNS replication appliance • Mediation server for sensors and near real-time drive by download component • HoneyNetRO • Spam Analysis Tool • SPAM-BOT detection • DNS-based BOT detection • Smart BOT Detector • SDN Malware Detector • MonitoringHub and Accounting Manager • Suricata Engine • KB-IDS for Android • AHPS • Montimage Monitoring Tool • Honeynet Network • Operational Intelligence Centre • Cyber threat detection	• WebCheck • SiteVet • HoneyUnit • PDF Scrutinizer • HoneyclientDispatcher • Skanna • Initiative-S	• DDoS Monitoring Tool • Flux-Detect 2.0 • HitmanPro • DE-Cleaner • Conan Mobile • System Fault Detection	• NoSQL "BigData" Storage Tool • Correlation Server • ISP Data Adaptor • Whois • Evidence Seeker • AHPS • Centralized Data Clearing House

Table 9: ACDC services

Sensors	Analysers	Mitigation	Lookup	Remediation	Prevention	CCH
• Suricata Engine • KB-IDS for Android • Spamtrap • DarknetRO • Low interaction honeypot(s) multipurpose appliance • HoneyNetRo • Honeynet Network • HoneyUnit • PDF Scrutinizer • HoneyclientDispatcher • Cyber threat detection	• Wildfire • Passive DNS replication appliance • Fortigate • SPAM-BOT detection • DNS-based BOT detection • Smart BOT Detector • Suricata Engine • KB-IDS for Android • Montimage Monitoring Tool • IBM QRadar • sflow/netflow analysis • WebCheck • HoneyUnit • Skanna • Initiative-S • AHPS • Montimage Monitoring Tool (MMT) • Evidence Seeker • Conan Mobile • System Fault Detection • Operational Intelligence Central • Spam Analysis Tool • Mediation server for sensors and near real-time drive by download component • PDF Scrutinizer • DDoS Monitoring Tool • Flux-Detect 2.0 • Mediation server for sensors and near real-time drive by download component • PDF Scrutinizer	• HitmanPro • DE-Cleaner	• SiteVet • Whois	• WebCheck		• NoSQL "BigData" Storage Tool • Centralized Data Clearing House

Table 10: Technical Services

Security	Messaging	Loggin	Data Access Services	Data Transformation
-	• Mediation server for sensors and near real-time drive by download component. • Correlation Server	• IBM QRadar	• MonitoringHub and Accounting Manager • ISP Data Adaptor	• AHPS

Table 11: ACDC tools per consortium partner

Partner	ATOS	CARnet	CASSIDIAN	CERT.RO
Provided Solution	• AHPS	• Spamtrap • Low interaction honeypot(s) multipurpose appliance • Passive DNS replication appliance • Mediation server for sensors and near real-time drive by download component	• Operational Intelligence Central	• DarknetRO • HoneyNetRo • Fortigate • Spam Analysis Tool • NoSQL “BigData” Storage Tool
Partner	**CyDef**	**DE-CIX**	**ECO**	**FKIE**
Provided Solution	• WebCheck • SiteVet	• sflow/netflow analysis	• Cyber threat detection • Initiative-S • HitmanPro • DE-Cleaner • Centralized Data Clearing House	• HoneyUnit • PDF Scrutinizer • HoneyclientDispatcher • Correlation Server
Partner	**IF(IS)**	**INTECO**	**LSEC**	**MI**
Provided Solution	• DDoS Monitoring Tool	• Skanna • Evidence Seeker • Conan Mobile • Flux-Detect 2.0 • Whois	• Wildfire • IBM QRadar	• Montimage Monitoring Tool
Partner	**TEC**	**TI**	**TID**	**XLAB**
Provided Solution	• System Fault Detection	• Honeynet Network	• SPAM-BOT detection • DNS-based BOT detection • Smart BOT Detector	• Suricata Engine • KB-IDS for Android • MonitoringHub and Accounting

			• Suricata Engine • ISP Data Adaptor	Manager

7. Annex II. ACDC Public Deliverables List

Deliverable no.	Deliverable title
D1.1.1	Overall Software Architecture Description
D1.1.2	Overall Software Architecture Description (refinement)
D1.2.1	Specification of Tool Group Centralised
D1.2.2	Specification of Tool Group Centralised (refinement)
D1.3.1	Specification of Tool Group Support Centre
D1.3.2	Specification of Tool Group Support Centre (refinement)
D1.4.1	Specification of Tool Group Malicious or Vulnerable Websites
D1.4.2	Specification of Tool Group Malicious or Vulnerable Websites (refinement)
D1.5.1	Specification of Tool Group Network Traffic Sensors
D1.5.2	Specification of Tool Group Network Traffic Sensors (refinement)
D1.6.1	Specification of Tool Group End Customer Tools
D1.6.2	Specification of Tool Group End Customer Tools (refinement)
D1.7.1	Data Formats Specification
D1.7.2	Data Formats Specification (refinement)
D1.8.1	Legal requirements
D1.8.2	Legal requirements (refinement)
D2.3	Technology Development Framework outlining basic models for integration and delivery principles
D2.4	Executable Service Code
D4.1	Documentation of botnet metrics methodology and development
D4.2	Statistical evaluation of the impact of the Pilot
D4.3	Legal validation of the prototype tested during the Pilot
D4.4	Publicly accessible database of botnet metrics
D5.1.1	Dissemination plan
D5.1.2	Intermediate Dissemination Report
D5.1.3	Intermediate Dissemination Report
D5.1.4	Final dissemination report
D5.2.1	Conception Exploitation plan

D5.2.2	Final Exploitation plan
D5.2.3	Sustainability Plan
D6.1.1	User profiles and categorization
D6.1.2	Identified user list across the different selected organisations
D6.2.1	ACDC Social Platform deployed, Online platform
D6.2.2	ACDC Social Analytics tool, Online tools
D6.3.1	Involvement model for users in ACDC
D6.3.4	Final report on ACDC user community - lessons learned, proposals for future involvements
D7.1	Project internal IT communication infrastructure.
D7.2.1	Periodic report according to EC regulation of the model contract
D7.2.2	Periodic report according to EC regulations of the model contract