

## D4.5 EU Cybersecurity and Privacy cluster engagement report.

### 2<sup>nd</sup> Report

Author(s)	M. Ramirez, CITIC
Status	Draft
Version	V1.0
Date	26 <sup>th</sup> June 2019

#### 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)

#### **Abstract:**

This document provides an overview of the Cybersecurity and Privacy clusters in Europe and an engagement plan to involve them in the activities organized by the cyberwatching.eu project. The document details the process and methodology to keep a constant channel of collaboration. The report also describes the actions implemented so far and others that have been foreseen to reinforce the collaboration with clusters as intermediate actors that can provide access to numerous SMEs.



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

**Document identifier: Cyberwatching.eu – WP4 – D4.2**

Deliverable lead	<b>AEI Ciberseguridad</b>
Related work package	<b>WP4</b>
Author(s)	M. Ramirez CITIC
Contributor(s)	-
Due date	30/06/2019
Actual submission date	11/07/2019
Reviewed by	Nicholas Ferguson & Niccolò Zazzeri, Trust-IT & Justina Bieliauskaite, DSME
Start date of Project	<b>01/05/2017</b>
Duration	<b>48 months</b>

**Revision history**

Version	Date	Authors	Notes
0.1	20/06/2019	M. Ramírez (CITIC)	First version
0.2	21/06/2019	J. Bieliauskaite (DSME)	First review
0.3	26/06/2019	Nick Ferguson & N. Zazzeri (Trust-IT)	Second review
0.4	26/06/2019	M. Ramirez (CITIC)	Changes integration
0.5	28/06/2019	M. Ramirez (CITIC)	PMB review
1.0	09/07/2019	Nick Ferguson, (Trust-IT)	Final version

## Executive Summary

Clusters are groups of specialized companies, many SMEs, and other related actors, such as Universities and public administrations, that cooperate closely together in a particular sector and geographical location. In D4.2 cyberwatching.eu reported on how it has identified and interacted with clusters actively working in Cybersecurity and Privacy (CS&P) across Europe and a catalogue of these clusters published on the cyberwatching.eu website<sup>1</sup>. The next step, which is reported in this deliverable, is to consolidate the relationship and aggregate a few more clusters to extend the area of influence of cyberwatching.eu. However, involving relevant and collaborative clusters is not an easy task, and it requires perseverance and adapt the strategy to the potential success of the actions carried out, and the new variables discovered in the process.

Another big issue is to monitor closely ongoing and new initiatives that may modify the way Cyberwatching.eu interact with clusters, like clusters changing or growing (i.e. Info Security Ireland becoming cyberireland) or the future actions of the European Cybersecurity Competence Center and Network. The project would like to avoid duplicating efforts on tasks that are already being developed by others.

With 56 relevant CS&P clusters identified across Europe, cyberwatching.eu identified a targeted group of clusters to ignite real interaction. Three clusters in particular, are already engaged and very committed to interacting with cyberwatching.eu and we will continue to strengthen ties with them. Webinars are one of the most successful activities carried out, and the power that they have to reach potential attendants among their members has to be taken advantage of, by reinforcing this activity.

For the coming months, efforts must focus in going on with the activities defined in D4.2 first report, and starting new joint actions with clusters. These new actions will be oriented to face the main challenges for CS&P clusters and their members, beginning with the three major challenges identified in the previous report (Excellence, Internationalization and Emerging Industries) and continuing with the new challenges that will be identified during the project through the contact with the clusters.

Collaborative work should lead to the confluence of research and industry objectives, to make this tandem a differential value that allows European companies to compete in any market.

---

<sup>1</sup> <https://www.cyberwatching.eu/clusters>

## Table of Contents

---

<b>1</b>	<b>The current EU CS&amp;P Cluster Landscape .....</b>	<b>5</b>
1.1	Introduction .....	5
1.2	Synergies with ongoing initiatives of reference .....	7
<b>2</b>	<b>Activity report M15-26 .....</b>	<b>8</b>
2.1	Work carried out with clusters .....	8
2.2	Evaluation of the planned activities for M15-M26 .....	11
<b>3</b>	<b>Next Steps .....</b>	<b>14</b>
3.1	Dedicated activities .....	14
3.2	Timeline and responsibilities .....	16
<b>4</b>	<b>Conclusion .....</b>	<b>16</b>
<b>Annex A.</b>	<b>Clusters classification .....</b>	<b>18</b>

## LIST OF FIGURES

Figure 1	Promotion of “cluster of the month” in cyberwatching.eu site .....	11
Figure 2	Relevant Cyber Clusters distribution .....	14
Figure 3	Timeline of activities and responsibilities .....	16

## LIST OF TABLES

Table 1 –	Net EU Contribution by country in cybersecurity and privacy topics .....	7
Table 2 –	Summary of contacts with clusters .....	9
Table 3 –	Summary of activities with clusters involved .....	10
Table 4 –	Summary of “cluster of the month” activity .....	11

# 1 The current EU CS&P Cluster Landscape

## 1.1 Introduction

In the first report of the Cluster Engagement strategy, Cyberwatching.eu established the motivations and objectives of involving European Cybersecurity and Privacy (CS&P) clusters in the project. Due to their multiplier effect in the impact of the project over the different stakeholders, as they work with multiple entities in a daily basis, incubating new projects and assisting in the commercialization of the results, clusters are the perfect link to the enterprise landscape.

From the first year of Cyberwatching.eu, we have known that Clusters working in the CS&P sector are not specifically targeted by any of the former EU cluster initiatives. Therefore, there is space for improvement and Cyberwatching.eu started by identifying the clusters working in CS&P.

The first set of clusters were identified by the consortium through the [European Cluster Collaboration Platform](#) and the UK Cybersecurity Clusters Forum, which are the leading European hubs for international cluster cooperation, with public information from the majority of the clusters. During the first year, after filtering from 850 clusters, Cyberwatching.eu selected 66 clusters from 24 EU countries with an alignment of mission, scope and strategy with the Cybersecurity and Privacy sector, to be added to the cyberwatching.eu cluster catalogue.

This catalogue has a key role in the Cybersecurity and Privacy ecosystem. The goal of this catalogue is to make it easier for clusters to be found as well as to reinforce their reputation and showcase their events, projects and initiatives. In addition, clusters have a variety of opportunities to collaborate and create research and partnership with multiple actors in the space.

The information of these clusters was manually added to the catalogue by the consortium. Thereafter, in February 2018, these first 66 clusters were contacted via email to inform about the cyberwatching.eu project and announce their inclusion in the catalogue of clusters, giving them the option to modify the data if they consider it necessary. In a second round, by the end of 2018, new interesting clusters were identified, analysed and most of them contacted.

From this point, cyberwatching.eu has been working with some of the clusters in different activities.

Nevertheless, in the M1-M18 review, the consortium was advised by the EU reviewers to focus on especially **relevant clusters in CS&P**, no more than ten, which could collaborate with the project in a closer way. Moreover, this has been the goal of the last months, to try to identify and engage these relevant clusters, taking also into account the geographical distribution, to cover all the European area. To identify them, besides the criteria defined in D4.2 first report, cyberwatching.eu has taken into account these considerations to determine if a cluster is relevant:

- **The core activity of the cluster:** CS&P should be its core activity or one dedicated activity specified in the cluster goals.
- **The number of members:** if a cluster is ICT but not specifically in CS&P, will be consider of relevance if it has more than 500 members. This can be assumed since cybersecurity and privacy is a critical issue on ICT sector, so a large ICT cluster will be always of interest from either the supply or demand side.
- **Current collaborators:** clusters that are already actively participating in cyberwatching.eu activities are considered as priority.

- **Greek clusters:** from the task T2.2, we have observed that there are many R&D projects coordinated from Greece, so cyberwatching.eu considers Greek clusters of potential interest, due to the knowledge that they can provide to add value to Cyberwatching.eu deliverables.
- **Clusters from areas with less R&D funded projects under H2020.** From the Implementation figures of [Horizon Dashboard](#), filtering by “cybersecurity” and “privacy” related topics we can see that main participants are from Italy, Spain, Germany, Greece or France (in the top5), and among the less participative countries are Croatia, Hungary, Latvia or even Denmark. In order to increase the impact of the project we will consider of interest engaging clusters from these countries.

Country	H2020 Net EU Contribution	H2020 Participations
Italy	€ 51.027.928	165,00
Spain	€ 43.920.057	145,00
Germany	€ 48.478.597	126,00
Greece	€ 40.082.469	123,00
France	€ 40.518.548	108,00
United Kingdom	€ 28.654.837	83,00
Belgium	€ 18.979.755	56,00
Netherlands	€ 17.572.936	48,00
Portugal	€ 10.205.205	37,00
Austria	€ 13.308.003	34,00
Switzerland	€ 6.691.493	31,00
Cyprus	€ 8.152.814	29,00
Romania	€ 5.730.191	24,00
Ireland	€ 7.072.555	23,00
Israel	€ 10.803.337	22,00
Bulgaria	€ 4.222.326	22,00
Poland	€ 5.948.802	21,00
Luxembourg	€ 5.935.613	18,00
Slovenia	€ 4.880.313	18,00
Norway	€ 8.179.316	17,00
Estonia	€ 5.763.449	15,00
Sweden	€ 5.345.340	14,00
Finland	€ 5.060.606	12,00
Czech Republic	€ 3.483.819	12,00
Denmark	€ 3.354.299	10,00
Lithuania	€ 1.970.571	7,00
Serbia	€ 918.444	4,00
Slovakia	€ 747.729	3,00
Latvia	€ 454.750	3,00
United States	€ 67.300	3,00
Turkey	€ 556.063	2,00
Ukraine	€ 248.000	2,00
Gibraltar	€ 443.750	1,00
Hungary	€ 396.375	1,00

Country	H2020 Net EU Contribution	H2020 Participations
Croatia	€ 184.800	1,00
Moldova (Republic of)	€ 90.000	1,00
Taiwan	€ 0	1,00

Table 1 – Net EU Contribution by country in cybersecurity and privacy topics

In Annex A, there is a classification of clusters according to the rules, and if they are or not in the catalogue, and if they have been already contacted or not. All this information is periodically updated in a spreadsheet shared by the consortium to know exactly what kind of contacts cyberwatching.eu has with the clusters.

In this deliverable, cyberwatching.eu presents the report on the performed activities with clusters from M15 to M26, and the next steps to be addressed.

## 1.2 Synergies with ongoing initiatives of reference

With the aim of creating a **network of CS&P clusters**, Cyberwatching.eu started focusing on the [European Cluster Collaboration Platform](#), the leading hub for international cluster cooperation, with public information from the majority of the clusters and access to the latest actions organized by or targeted for clusters. It contains information from the majority of the other initiatives, present and past, and a description of many of the active clusters in Europe, but also abroad.

Deepening the knowledge of the clusters, we found different initiatives of cybersecurity networks grouping several clusters active in CS&P from the same country or region:

- [Cyber Wales Ecosystem](#): a network of five cyber related Clusters with over 800 members across Wales. One of our assiduous collaborators, South Wales Cybersecurity cluster, is one of them.
- [UK Cyber Security Forum](#): It is a social enterprise representing sole traders and small & medium companies (SMEs) who are actively working in cyber security. 37 clusters across UK are part of this network (including Wales clusters). Again, South Wales Cybersecurity cluster is one of them.
- [3B ICT - Balkan and Black Sea ICT Clusters Network](#): A network of clusters with the main goal to create framework to intensify collaboration of ICT Clusters and ICT organizations in the Balkan and Black Sea region aiming to meet common challenges affecting SMEs growth, innovation and business environment. Cyberwatching.eu has identified at least 14 CS&P relevant clusters that are members of this network. One of our assiduous collaborators, ClujIT, is one of them.

Cyberwatching.eu has established a solid collaboration relationship with the representatives of these networks, prioritizing the effort of communication with the network to minimize the effort of individual communication with each and every one of the clusters.

Another initiative to take into account is the future **European Cybersecurity Industrial, Technology and Research Competence Centre, the Cybersecurity Competence Community and the Network of National Coordination Centres**, that is being promoted by the European Commission to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market. This initiative will help to create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem. Cyberwatching.eu is working side by side with the four pilots that are paving the way, since all the Cyberwatching.eu stakeholders have a place in the future Cybersecurity Competence Community.

Moreover, the work with clusters can play a key role in adding actors to this Community.

The activities carried out with clusters under Cyberwatching.eu projects must complement these ongoing initiatives to establish the basis for the development of the **European network of CS&P clusters**.

## 2 Activity report M15-26

### 2.1 Work carried out with clusters

Currently the Cluster Catalogue<sup>2</sup> includes 68 clusters coming from 24 EU countries; each cluster has a dedicated space describing its mission, the benefits for its members and some contact data. The clusters can update the information shown by filling in the web form. This form is received by the web administrators that will update the page according to the request. The web form also includes the possibility that the clusters register themselves through a web form at <https://www.cyberwatching.eu/submit-your-csp-cluster>, although before making this information public, it must be reviewed by the web administrator. The Cluster Catalogue can be filtered by Vertical market and Country.

Another way of identifying new clusters for the catalogue has been through the contact with the National Contact Points (NCPs). **104 NCPs for ICT and/or Security from 30 countries** have been contacted to ask for information in their countries about clusters of interest working in CS&P (among other information requested).

From the links and references provided by the NCPs as well as from direct search on the Internet, a new set of clusters was identified in a second round. This new set has 149 clusters related to ICT, but only 39 of them can be considered as priority regarding the rules mentioned in the introduction section. In a first stage of this second round, 31 of these clusters have been contacted via email to invite them to join the catalogue of clusters using the cluster registration form available on the project website. In a next stage, the remaining 8 clusters will be contacted until the list is completed, but it is necessary a previous work of gathering the proper contact. Two clusters completed this form and were included in the web, making a sum of **68 clusters in the catalogue**.

Not all the clusters in the catalogue are considered priority cluster. Even when in D4.2 Cluster engagement first report cyberwatching.eu identified 22 clusters as priority, applying the criteria listed in section **Error! Reference source not found.** the number was reduced to 18. However, there is still work to be done to get to know these clusters and engage the actual interesting actors, and this will be described in section 3. Annex A contains the details of the priority and non-priority clusters, specifying whether they are in the catalogue or not, and contacted or not yet.

The following table shows a summary of all contacts made with clusters to date.

<sup>2</sup> <https://www.cyberwatching.eu/clusters>



#Emails	To	Subject	#Answers
72	Clusters	Check cluster data in catalogue	2
146	NCPs	Request for information	20
72	Clusters	Invitation to webinar “Cybersecurity as an opportunity in a changing market”	6
41	Clusters	Register using web form	2
103	Clusters	Invitation to webinar “Privacy & Trust: How to ensure management and control of identities and rights”	N/A <sup>3</sup>
8	Clusters	Invitation to be Cluster of the month	4
24	Clusters	Invitation to “Second concertation meeting”	0

Table 2 – Summary of contacts with clusters

The first row shows the number of emails sent to the clusters identified in the M1-M14, to check that their data in the catalogue were correct. Although there were 66 clusters in this group, 72 emails were sent since some clusters had more than one contact person. As for the second row, some of the 104 NCPs were contacted several times, making a total of 146 emails sent. Of these emails, only 20 responses were obtained with information (links or references to organizations). The third row shows the emails sent to invite the clusters to the webinar “Cybersecurity as an opportunity in a changing market”. The fourth row corresponds to the second round of contacts with the clusters and the two that have used the web form. The fifth row shows the number of emails sent to invite the clusters to the webinar “Privacy & Trust: How to ensure management and control of identities and rights”. The sixth row shows the number of clusters contacted to propose them for the “cluster of the month”. Even being a free promotional action for them, only 50% replied to the email. The last row shows the emails sent to invite the priority clusters to the “Second concertation meeting”.

It is important to mention that all communications with the clusters have been used to also do tasks of dissemination of the Marketplace and the SME end-user-club.

In June 2018, the 66 clusters from the catalogue were invited by email to join the webinar [“Cybersecurity as an opportunity in a changing market”](#). The invitation was complemented with a phone call to the 22 clusters identified as priority in the D4.2 first report. Again **ClujIT** and **GAIA** were invited to participate as speakers, and again they accepted the invitation. From the other clusters, there were answers showing their interest from 5 of them (South Wales Cyber Security Cluster, Silicon Alps Cluster GmbH, Clúster Canarias Excelencia Tecnológica, Startup Estonia and SIIT Scpa). There were also expressions of interest from 2 companies from 2 clusters that had forwarded the invitation-email to their members (Clúster Canarias Excelencia Tecnológica and ITL - Estonian Association of Information Technology and Telecommunications).

In October 2018, a new webinar [“Cyber risk management from the SME point of view”](#) was organized. This time, the topic was very oriented to SMEs, so there were no massive invitations to clusters to participate in the webinar. Nevertheless, **South Wales Cyber Security Cluster** was invited to participate as speaker, and John Davies accepted.

In addition, this same month cyberwatching.eu organized the first annual workshop in Krakow, under the Cybersec Forum 2018, and **South Wales Cyber Security Cluster** was invited and they accepted to participate in the Panel discussion on approaches to readiness for projects moving from proof of concept to realization.

<sup>3</sup> The registration to the webinar was through a web form, so no email was received.

In June 2019, the Second Cyberwatching.eu Concertation Meeting took place in Brussels. Cyberwatching.eu sent invitations emails to 24 clusters identified as priority, but there were no answer. The following table summarizes the activities carried out with clusters.

Date	Type of Event	Title	Clusters
<b>April 2018</b>	Concertation Meeting	First Concertation Meeting	<ul style="list-style-type: none"> <li>GAIA (Spain)</li> <li>ClujIT (Romania)</li> </ul>
<b>June 2018</b>	Webinar	Cybersecurity as an opportunity in a changing market	<ul style="list-style-type: none"> <li>GAIA (Spain)</li> <li>ClujIT (Romania)</li> </ul>
<b>October 2018</b>	Annual Workshop	Aligning and prioritising EU and international Cybersecurity and Privacy	<ul style="list-style-type: none"> <li>South Wales Cyber Security Cluster (United Kingdom)</li> </ul>
<b>October 2018</b>	Webinar	Cyber risk management from the SME point of view	<ul style="list-style-type: none"> <li>South Wales Cyber Security Cluster (United Kingdom)</li> </ul>
<b>December 2018</b>	Webinar	Privacy & Trust: How to ensure management and control of identities and rights	<ul style="list-style-type: none"> <li>5 invitations sent but no positive answer</li> </ul>
<b>June 2019</b>	Concertation Meeting	Second Concertation Meeting	<ul style="list-style-type: none"> <li>24 invitations sent to priority clusters but no positive answer</li> </ul>

**Table 3 – Summary of activities with clusters involved**

Another of the activities that have been launched within the project is the selection of the **cluster of the month** in order to offer a direct highlight to the most active clusters among the different events or activities organized. The selected cluster is contacted via email and is asked to answer a small interview, in order to better explain its activities and the benefits that the cluster brings to its members. This interview is published in a special section of the website and a promotion in the home.



Figure 1 Promotion of “cluster of the month” in cyberwatching.eu site

This activity started in the month of November and the following table shows the clusters that have participated:

Month	Cluster
November 2018	<a href="#">South Wales Cyber Security Cluster</a>
December 2018	<a href="#">GAIA</a>
January 2019	<a href="#">Cluj IT</a>
April 2019	<a href="#">Bavarian IT Security and Safety Cluster</a>

Table 4 – Summary of “cluster of the month” activity

This activity was not always easy, as relevant clusters do not always respond to the information request. In addition to this, cyberwatching.eu site is in a transformation period to adapt the content to the EC recommendations from the M1-M18 review, with different access profiles.

## 2.2 Evaluation of the planned activities for M15-M26

With the aim of improving the work developed with clusters, it is necessary to evaluate the level of compliance with the planned activities.

From the D4.2 first report, the status of the planned activities can be assessed as follows:

- **Online catalogue maintenance:** the catalogue has been periodically updated and a web form has been developed to enable clusters to register in the site. **Lead partner: Trust-IT & AEI**
- **Questionnaire:** to send a questionnaire was an activity planned to gather needs from the clusters, and to get to know how they deal with the Cybersecurity and Privacy themes internally. However, as the cyberwatching.eu site is in a transformation process, there is still place to think about the role of clusters in the new site, and what kind of questions must be asked to know how cyberwatching.eu can be useful for them. **Lead partner: AEI**
- **Webinars organization:** clusters have actively participated in 2 webinars. **Lead partner: AEI & Digital SME**
- **Events:** clusters have actively participated in the first and second concertation meeting and the annual workshop. **Lead partner: AEI, DSME & Trust-IT**
- **Newsletter preparation:** the definition of the newsletter is still in progress. **Responsible: Trust-IT**
- **Cluster of the month:** Four clusters have been promoted as “cluster of the month”. This activity is under assessment. **Responsible: AEI**
- **Surveys:** no specific surveys for clusters were sent yet. Aligned with the different activities carried out for SMEs with clusters involved, such as webinars or events, very light surveys will be shared with them to know the cluster managers’ point of view in relation to the specific activity topic, in order to gather information that allows Cyberwatching.eu to improve the collaboration and assistance to them, and also to prepare useful information for SMEs to be shared through Cyberwatching.eu site. **Responsible: Digital SME & other partners**
- **SMEs end-user club membership:** AEI and CITIC disseminated among clusters the importance for their members to join the SMEs end-user club. Nevertheless the process to be patron is still under development. It is important to remind that by this patronage, clusters will be able to propose issues and matters that will be treated in the club in order to find the response for the needs of their members. Cyberwatching.eu will look for the experts that could provide the appropriate answers, which will be shared with the community of SMEs. **Responsible: Digital SME & AEI**
- **Marketplace partnerships:** AEI and CITIC disseminated among clusters the benefits of joining the Marketplace as a buyer or provider, but there is still a lot of work to do to involve clusters in the marketplace operation. Again, it is important to remind that during the publication of supply and demand profiles, the Cybersecurity and Privacy clusters collaborating with the project will have a “shorter way” from the submission of the information to the publication. The publications from the clusters will be “pre-validated”, which means that they have already made a first check that the demand or supply profile is sound and it is within the context of the marketplace. Anyway, Cyberwatching.eu will make a final validation to ensure that the information provided and the description of the request has enough quality to be included in the marketplace. The cluster that was referred during the submission will appear as contact, and when the project ends and ensures its sustainability by the charge of royalties from the marketplace, the clusters that collaborate with the marketplace will receive a percentage of the total operations funnelled in the marketplace. A Memorandum of Understanding will be signed by the responsible of the marketplace with every cluster interested during the project. **Responsible: AON & Digital SME**

Because of the work developed together with the clusters, Cyberwatching.eu has achieved loyalty of three key clusters:

- **Cluj IT:** Founded in October 2012, Cluj IT is an innovation based value chain network of Romanian IT companies and related organizations with the purpose of increasing the competitiveness and growth of IT services and products on international markets and of forging a strong sustainable public – private partnership in order to improve the life quality of the community we are part of. Cluj IT Cluster also strives towards the enhancement of innovation capabilities of our members, in particular, and of the Romanian IT industry in general. Its focus is on:
  - Creating a collaborative culture based on trust and reliability
  - Fostering entrepreneurship
  - Promoting Romanian IT solutions and services abroad and become known as a centre of excellence in IT
  - Forging strong and long lasting partnerships for the mutual benefit of our members and society in general
  - Support and create opportunities for Cluj IT members to work on large international projects.

The representative of this cluster is **Andrei Kelemen**, who has actively collaborated with cyberwatching.eu. Cluj IT is also a member of the - 3B ICT - Balkan and Black Sea ICT Clusters Network, so he can be the facilitator to get to all the cluster in the network.

- **South Wales Cyber Security Cluster:** The South Wales Cyber Security Cluster has been formed, under the umbrella of the UK Cyber Security Forum, by a number of cyber security focused businesses in the Cardiff area including Pervade Software Ltd, Wolfberry IT Security and Urquhart-Dykes & Lord LLP. The aims of the Cluster are two-fold:
  - To support the members of the cluster by communicating National and International initiatives and trade opportunities, providing a networking platform to share ideas and best practice, encouraging collaboration and identifying partnership opportunities so that small cyber security specialist businesses in Wales can find new ways to grow.
  - To support the Welsh Government's commitment to Cyber Security (and UK Government's Cyber Security Strategy) by building cyber security knowledge, skills and capabilities in the Region, to make businesses more resilient to cyber attacks and the Region one of the most secure places in the world to do business.

The representative of this cluster is **John Davies**, who has actively collaborated with cyberwatching.eu. John Davies is also the representative of the Cyber Wales Ecosystem, so he can be the facilitator to get to the five clusters in the network.

- **GAIA:** GAIA is the Association of Electronic and Information Technologies in the Basque Country, a private and professional non-profit organisation, established in 1983, currently made up of 260 companies that offer products and services in the field of electronics, information technology and telecommunications. GAIA's mission is to boost the development and growth in the Electronics-IT and Telecommunications sector, and to favour the assimilation and efficient usage of the sector's technologies, with the aim of collaborating in the development of the Information and Knowledge Society.

The representative of this cluster is **Jokin Garatea**, who has actively collaborated with cyberwatching.eu. GAIA is also a member of CONETIC (Confederación Española de Empresas de Tecnologías de la Información, Comunicación y Electrónica) – one of the Spain's biggest ICT SME associations.

The following illustration shows the geographical distribution of the **56 priority clusters** and, highlighted in red, these three loyal clusters together with the AEI in Cybersecurity and Advanced Technologies, while highlighted in green 7 potential loyal customers according to the mentioned criteria



Figure 2 Relevant Cyber Clusters distribution

## 3 Next Steps

### 3.1 Dedicated activities

The project must continue and reinforce the activities defined in D4.2 first report and carried out for M15-M26. Specifically cyberwatching.eu will keep working in the following tasks focusing on the specific target clusters:



- Online catalogue
- Involvement of clusters in cyberwatching.eu periodic webinars
- Cluster of the month
- Events (invitation to clusters representatives to participate as attendants or speakers)
- Surveys: distribution of cybersecurity and privacy related surveys to clusters in order to gather information for cyberwatching.eu deliverables
- Newsletter
- Promotion of cyberwatching.eu marketplace opportunities in terms of promoting companies in the clusters and their services

Nevertheless, cyberwatching.eu needs to accomplish some complementary activities to strengthen relationships with clusters:

- **List of 10 loyal clusters:** review the priority cluster list and assign a number in order of priority following the criteria defined in this and the previous report. The final goal will be to have ten relevant and collaborative clusters. To get to this goal, it will be necessary emails, phone calls, and face to face meetings (in one of the events organized by cyberwatching.eu, by any of the cluster or by a third organizer).
- **Define clusters area in cyberwatching.eu site:** define, together with the 10 loyal clusters the type of information that should be published in cyberwatching.eu site that is of interest for clusters, including space for clusters' activities promotion. It also may include legal and policy issues, funding opportunities, EC cluster-oriented activities, etc.
- **Analysis of clusters:** to analyse the 10 loyal clusters to identify common points, differences, strengths and weaknesses. Through personal interviews, questionnaires and additional documentation facilitated by the clusters representatives, the goal is to have a radiography of clusters ecosystem.
- **Define joint actions:** after the clusters analysis, and with the objective of promoting cyberwatching.eu services among clusters members, joint actions will be defined, with individual clusters or a subgroup of them, and ideally with all of them. The results from these joint actions can be promoted among all the cyberclusters identified from the beginning of the project to reach as many final users as possible. To start with, these common actions could be oriented to address the three major challenges for clusters identified in D4.2 first report:
  - Excellence: High quality cluster management is a key element of successful world-class clusters. Dedicated webinars on cluster management skills could be organised. The creation of a best practices guide for cluster management could be promoted from cyberwatching.eu, where clusters could contribute with their experience.
  - Internationalization: The mission of many clusters is to support their members to create new market opportunities. For this challenge, cyberwatching.eu has to convey the importance of the Marketplace as a feasible access to international markets.
  - Emerging industries: To face the speed with which technology evolves, Technology Radar and SME End User Club are the appropriate tools to be up to date with the latest technological innovations and emerging industries.
- **Engage with competence centre pilot network projects** to act as a facilitator for Clusters in order to be involved in those projects. For example Cyberwatching.eu could leverage its contacts and role in order to facilitate:
  - *Cluster inclusion in the SPARTA Catalogue of Cyber Range Providers.* SPARTA is actually developing a fully labelled catalogue of

organisations providing cyber range solutions in order to realize a European collaborative effort to develop methods and solutions for prediction and awareness and knowledge-based cybersecurity management. Clusters or individual organisations inside the clusters could benefit from this inclusion not only on a visibility level but also on an operational level, for example being able to know innovative way of handling the complexity of cybersecurity threats and to improve their cyber security skills.

- Cluster participation in ECHO Federation of Cyber Range. The ECHO project will enable interconnecting and pooling cyber range capabilities in Europe. The solution will foster unprecedented cooperation between different range providers by facilitating the delivery of multi-sector exercises with complex and distinct technological requirements. Clusters or individual organisations inside the clusters joining ECHO could therefore benefit from sector-specific hands-on skills development and knowledge sharing.

### 3.2 Timeline and responsibilities

In order to achieve the objectives of the work with the Cybersecurity and Privacy clusters it is very important to schedule and define the responsibilities of each partner participating in the task. The next illustration shows the planned timeline for the activities and their responsible.

	jul-19	ago-19	sep-19	oct-19	nov-19	dic-19	ene-20	feb-20	mar-20	abr-20
<b>Online catalogue maintenance</b>										
Responsible: TRUST-IT & AEI										
<b>Periodic webinars</b>										
Responsible: AEI & Digital SME										
<b>Cluster of the month</b>										
Responsible: AEI & TRUST-IT										
<b>Events</b>										
Responsible: AEI, DSME & TRUST-IT										
<b>Surveys</b>										
Responsible: DSME & all										
<b>Newsletter</b>										
Responsible: TRUST-IT										
<b>SMEs end-user club patronage</b>										
Responsible: DSME & AEI										
<b>Marketplace partnerships</b>										
Responsible: AON & DSME										
<b>List of 10 loyal clusters</b>										
Responsible: AEI										
<b>Define clusters area in cyberwatching.eu site</b>										
Responsible: AEI & TRUST-IT										
<b>Analysis of clusters</b>										
Responsible: AEI										
<b>Define joint actions</b>										
Responsible: AEI & all										
<b>Engage with competence centre pilot network projects</b>										
Responsible: AEI & all										

Figure 3 Timeline of activities and responsibilities

## 4 Conclusion

During the last 14 months, the project has worked to start collaboration with the clusters and to identify a reduced group of relevant clusters to establish a symbiotic relationship with cyberwatching.eu. The organizational structure of clusters usually shows some weaknesses, mainly due to the fact that the majority of cluster directors have to manage their own companies, besides to rule the cluster. This condition limits the available time to address requests from third parties like cyberwatching.eu. Hence



the need to transmit the clear and concise message that cyberwatching.eu will benefit them when managing their cluster, and will benefit their members in achieving their goals. Nevertheless, with three success stories of already engaged clusters, the objective seems reachable.

An important point is to get a deeper knowledge of CS&P clusters and their members' needs, especially those needs that can hardly be covered by the cluster limited resources and cyberwatching.eu could complement. The Marketplace and the End User Club must be seen as useful tools for cluster members to be competitive in the Digital Single Market, and at the same time, they must be the main subscribers to improve these assets.

In the next months, cyberwatching.eu must define and organize joint actions with clusters, specially focusing on the next research programme Horizon Europe, and the new industry-oriented Programme, Digital Europe, and their challenges. New opportunities will open up for researchers and SMEs to cooperate in both programmes and cyberwatching.eu, together with the clusters, will be act as facilitators to integrate both worlds as successfully as possible.

By crossing technology trends (through the R&D projects analysis and the Technology Radar implementation) and industry needs (through the close contact with clusters), it will be possible to set out guidelines for industry and the public sector to comply effectively with standards and regulations.

If clusters are the gateway to European cybersecurity main players, cyberwatching.eu must become the gateway for those players towards success in the Digital Single Market.

## ANNEX A. CLUSTERS CLASSIFICATION

### A.1. CLUSTERS ALREADY IN THE CATALOGUE, IDENTIFIED AS PRIORITY (18)

Name	Country	Region	Description
<b>AEI Ciberseguridad y Tecnologías avanzadas</b>	Spain	Castilla y León	The Spanish Cybersecurity Innovation Cluster (AEI Ciberseguridad y Tecnologías Avanzadas) brings together companies, Research Centres, Universities, public and other private organizations interested in promoting new technologies, the industrial sector and other related stakeholders, wishing to contribute to the objectives of the Association regarding Security Technologies, at national and international level. The National Cyber Security Institute (INCIBE) promotes the Association, with the aim of providing an operational structure to all companies interested in the promotion and development of a Business Technological Pole linked to INCIBE's mandate.
<b>BICCnet - Bavarian Information and Communication Technology Cluster</b>	Germany	Bavaria	The cluster, BICCnet works to assure the growth of information & communication technology (ICT) in Bavaria. BICCnet – the Bavarian Cluster for Information & Communications Technology – furthers the inter-networking of ICT enterprises, as well as the networking with research institutions and the Bavarian Digitalization Center promotes the reciprocal transfer of knowledge. Here focus is placed on innovative technologies and topics, such as blockchain, data analytics, and AI. In addition, the cluster supports ICT enterprises with their positioning in an increasingly global context. Thus, the cluster should provide assistance – also for small and medium-sized business in particular – in taking advantages of growth opportunities. Here BICCnet concentrates on the topic of smart systems for smart cities within the framework of the Smart City Tech Partnership (SmartCityTech.eu).
<b>bwcon - Baden Württemberg: Connected</b>	Germany		Baden-Württemberg is one of the strongest economic regions in Germany and Europe. A network of excellent research institutions and powerful industrial clusters at global level are the base of the region's global competitiveness. Baden-Württemberg: Connected e.V. (bwcon) is the leading business initiative for the promotion of the high-tech sectors in the region with offices in Stuttgart, Freiburg, Horb and Villingen-Schwenningen. With its approximately 600 members since 1997, the main goal is to foster key-technologies in order to strengthen the region's economic development. The focus is on information and communication technologies (ICT) as drivers of innovation in the fields

			of mobility, production, health and energy. bwcon creates a unique platform for cross-sector collaboration between developers, users and investors.
<b>Cap Digital</b>	France		<p>Cap Digital was created as a result of a public policy for the development of economic sectors with strong growth potential located in the same geographical area. Since 2009, the cluster has been implementing the Paris Region's strategy for digital content and services, supporting innovative SMEs in this field.</p> <p>Our 1000 members are primarily innovative SMEs but also major universities, higher education establishments, research labs, and corporations focused on a specific technology-driven industry (Triple helix cluster).</p> <p>Our members represent French digital industry's most active players.</p>
<b>Cluj IT Cluster</b>	Romania		<p>Founded in october 2012, Cluj IT is an innovation based value chain network of Romanian IT companies and related organizations with the purpose of increasing the competitiveness and growth of IT services and products on international markets and of forging a strong sustainable public – private partnership in order to improve the life quality of the community we are part of. Cluj IT Cluster also strives towards the enhancement of innovation capabilities of our members, in particular, and of the Romanian IT industry in general. Our focus is on:</p> <ul style="list-style-type: none"> <li>* Creating a collaborative culture based on trust and reliability</li> <li>* Fostering entrepreneurship</li> <li>* Promoting Romanian IT solutions and services abroad and become known as a centre of excellence in IT</li> <li>* Forging strong and long lasting partnerships for the mutual benefit of our members and society in general</li> <li>* Support and create opportunities for Cluj IT members to work on large international projects.</li> </ul>
<b>Consumer Affairs at ZD.B</b>	Germany	Bavaria	<p>In the name of the Bavarian government the Center Digitisation.Bavaria (ZD.B) performs a bundling function for already existing activities in the areas of digitisation and develops them further in a sustainable manner.</p> <p>With its business office in Garching the Center Digitisation.Bavaria acts as a coordinator for numerous actions. They especially include</p> <ul style="list-style-type: none"> <li>* Thematic platforms: Networking between companies and scientists concerning key themes of digitisation</li> <li>* Junior Research Groups: Encouragement of scientific junior researchers in the thematic fields relevant for digitisation</li> <li>* Innovation labs: Bringing together companies and students in order to work at innovative prototypes</li> </ul>

			<p>The office for Consumer Affairs of the ZD.B has the goal of implementing solutions to consumer issues right into the process of digital transformation.</p> <p>Working with companies, research organisations and consumer organisations, we will identify and anticipate consumer issues. Those issues will then be tackled together with companies, and incorporated into political frameworks.</p> <p>A key topic currently is „Privacy by Design“, where we help companies to understand the requirements of the Data Protection regulation, and provide best-practice examples to technically implement it.</p>
<b>Digital League</b>	France	Auvergne-Rhône-Alpes	<p>Digital League is the cluster of companies in the digital sector in Auvergne-Rhône-Alpes. With +500 members, our goal is to foster economic growth and employment in the regions.</p> <p>Digital League offers all companies, whatever their size, actions in the service of 3 missions: federate, grow together and radiate.</p> <p>On a daily basis, Digital League promotes the exchange of good practices between entrepreneurs, schools, laboratories, investors and institutions to create winning synergies.</p>
<b>GAIA - Association of Knowledge and Applied Technologies industries in the Basque Country</b>	Spain	Basque Country	<p>GAIA is the Association of Electronic and Information Technologies in the Basque Country, a private and professional non-profit organisation, established in 1983, currently made up of 260 companies that offer products and services in the field of electronics, information technology and telecommunications.</p> <p>GAIA's mission is to boost the develop and growth in the Electronics-IT and Telecommunications sector, and to favour the assimilation and efficient usage of the sector's technologies, with the aim of collaborating in the development of the Information and Knowledge Society.</p>
<b>HSD - The Hague Security Delta</b>	Netherlands		<p>The Hague Security Delta forms partnerships and creates knowledge bridges with the main global security clusters in the USA, Canada, Singapore and South Africa. Besides, It has strong ties to the main European security regions and Brussels, making the Netherlands the secure gateway to Europe.</p>
<b>ISIN - Irish Software Innovation Network</b>	Ireland		<p>Technology Ireland Innovation Forum will drive transformational, innovative, and impactful collaboration throughout the digital technology cluster by supporting organisations to scale.</p> <p>Mission Statement:</p> <ul style="list-style-type: none"> <li>* Support SMEs to engage with SMEs and SMEs with MNCs to leverage synergies and create new collaborative opportunities.</li> <li>* Support the design and implementation of technology roadmaps to assist the scaling of companies in and out of Ireland.</li> </ul>

			<ul style="list-style-type: none"> <li>* Support Research to Innovation to Commercialisation (R-I-C Model).</li> <li>* Support the emergence of new value chains through cross cluster collaboration.</li> </ul>
<b>ITL - Estonian Association of Information Technology and Telecommunications</b>	Estonia		<p>Estonian Association of Information Technology and Telecommunications (officially abbreviated as ITL) is a voluntary organisation, whose primary objective is to unite the Estonian information technology and telecommunications companies and organisations, to promote their co-operation in Estonia's development towards information society, to represent and protect the interests of its member companies and to express their common positions. The main priorities for 2017-2019 are:</p> <ul style="list-style-type: none"> <li>- Digital economy</li> <li>- E-state and information society policy</li> <li>- Education, labour and R&amp;D</li> </ul>
<b>LSEC - Leaders in Security</b>	Belgium		<p>LSEC is an international IT - &amp; Information Security cluster, a not for profit organization that promotes Information Security and the expertise in Europe. Founded by the University of Leuven, supported by European Commission FP7 and leading a PAN European Private partnership that interacts with Public Institutions, LSEC connects security experts, research institutes and universities, government agencies, end users, funding bodies and technical experts who are driving European research agendas. LSEC activities aim to raise cyber security awareness, support innovation and improve the competitiveness of the IT- Security market.</p>
<b>Secured Communicating Solutions cluster</b>	France	Provence Alpes Côte d'Azur	<p>SCS is a world-class competitiveness cluster dedicated to digital technologies. Created in 2005 in the Provence Alpes Côte d'Azur region in the South of France, it brings together an ecosystem of more than 300 industrial players, large multi-national groups, SMEs and startups, research laboratories and leading universities in their fields. They are working together to develop and market products and innovative services to generate growth and jobs in high growth markets.</p>
<b>SIIT Scpa</b>	Italy	Liguria	<p>SIIT SCpA was founded in 2005 with the aim to create an integrated system among large industries, small and medium-sized businesses, the University of Genoa, public institutions, research and finance, with particular attention to the development of industrial research and technology transfer activities. By that logic, the Region of Liguria, the Ministry of Economy and the Ministry of Universities and Scientific Research have entered into an agreement in which the six lines of implementation of the District's operations have been identified. SIIT SCpA is a non-profit consortium company, which represents an aggregation of a regional</p>

			nature, whose main aim is to promote and favor production competitiveness in the areas of interest.
<b>Silicon Alps Cluster GmbH</b>	Austria	Carinthia and Styria	The Silicon Alps Electronic Cluster is a public-private partnership that brings together Austrian players from industry, science and public authorities to develop and position the electronics and microelectronics sector with a regional focus on the locations Carinthia and Styria. The Silicon Alps cluster regards itself as a long-term strategic alliance and a tool for cooperative, efficient and business-oriented location development.
<b>South Wales Cyber Security Cluster</b>	United Kingdom	South Wales	The South Wales Cyber Security Cluster has been formed, under the umbrella of the UK Cyber Security Forum, by a number of cyber security focused businesses in the Cardiff area including Pervade Software Ltd, Wolfberry IT Security and Urquhart-Dykes & Lord LLP. The aims of the Cluster are two-fold: * To support the members of the cluster by communicating National and International initiatives and trade opportunities, providing a networking platform to share ideas and best practice, encouraging collaboration and identifying partnership opportunities so that small cyber security specialist businesses in Wales can find new ways to grow. * To support the Welsh Government's commitment to Cyber Security (and UK Government's Cyber Security Strategy) by building cyber security knowledge, skills and capabilities in the Region, to make businesses more resilient to cyber attacks and the Region one of the most secure places in the world to do business.
<b>Systematic Paris-Region</b>	France		With its Open Innovation focus, the Systematic Paris-Region international competitiveness cluster is there to bring together and promote an ecosystem of excellence that counts over 800 members. Systematic connects stakeholders from software, digital and industry, and boosts digital projects through collaborative innovation, SME development, networking and business sourcing, across a range of future growth sectors: energy, telecoms, healthcare, transport, information systems, factory of the future, digital city, and security. The cluster is also there to promote its members, its region and its innovation projects, with the aim of raising their profile and enhancing the attractiveness of the geographical territory and ecosystem.
<b>tech UK</b>	United Kingdom		techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. More than 950 companies are members of techUK. Collectively they employ approximately 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium-sized businesses.

## A.2. CLUSTERS ALREADY IN THE CATALOGUE, BUT NOT IDENTIFIED AS PRIORITY (50)

Name	Country	Region	Description
<b>AEI del Conocimiento de Asturias</b>	Spain	Asturias	The "AEI del Conocimiento de Asturias" is established to promote technological development, innovation, knowledge management and applied research in the knowledge society sector, and may also carry out other activities related to the previous ones. To this end, the AEI aims to contribute to the growth and expansion of its partners, by adopting collaborative strategies aimed at fostering research, the implementation of new technologies and the implementation of innovations within the scope of their respective business activities, to increase their productivity and improve their competitiveness, enhancing their economic viability and projection in the national and international market.
<b>Aerospace Valley</b>	France	South-Western France (Occitania and Nouvelle Aquitaine)	Created in 2005, Aerospace Valley is the most significant innovation "pôle de compétitivité" in France in the fields of aeronautics, space and embedded systems, counting with over 840 members from both the industry and the academia. With offices in Toulouse (HQ) and Bordeaux, the innovation cluster covers the two geographically adjacent regions of South-Western France, Occitania and Nouvelle Aquitaine. With 124,000 industrial employees, Aerospace Valley represents around 1/3 of the French aerospace workforce. Similarly, 8,500 researchers and scientists are active within the Aerospace Valley territory, thus representing 45% of the French national R&D potential in the aerospace sector. As of June 2016, Aerospace Valley has obtained funding for 475 R&D projects representing an accumulated value of 1.2 billion Euro covering most scientific and technical fields related to the various sectors of aerospace. Within the framework of the general French "pôle de compétitivité" program, which aims to stimulate employment by fostering local and regional competencies in technical and economic areas, Aerospace Valley strives to create an ambitious 35-40,000 new jobs by the horizon year 2025.
<b>AITA - Albanian ICT Association</b>	Albania		The Albanian ICT Association was established in 2007 as an initiative of Albanian enterprises working to address the needs of the IT sector; as well as to transform the association into the most important representative body of the Albanian IT domain. AITA is focused on generating projects and implementing activities that have direct impact on the members and on the wider IT community in Albania, aiming also at a sustainable growth and development of the association itself.

<b>Alliance Cluster</b>	Hungary		The objective of the Cluster is to develop unique, up-to-date and marketable products within the scope of the info-communications industry. Previously software products were mainly sold independently and were implemented to make the processes of various industrial sectors more effective. By contrast, the intention of the Cluster is to put the ICT achievements to work for the development of professional processes of different sectors, as well as creating and fulfilling new user demands. In this way, new systems will emerge with new functions. The penetration of advanced technology and methods into traditional industries is incessant all over the world and market success may only be achieved with this same approach. New emphases, as well as previously unknown services and product groups, are thus created; e.g. in the field of environmental protection, health care or diagnostics. In these sectors, ICT techniques have been present from the beginning and constitute the driving force of development.
<b>ALPHA RLH - Laser and Microwaves French Cluster</b>	France	Bordeaux, Limoges and La Rochelle	<p>The ALPHA-RLH competitiveness cluster works with companies and laboratories in setting up, evaluating and funding innovative projects.</p> <p>The cluster is based in Bordeaux, Limoges and La Rochelle, and brings together talents in Photonics and Microwave technologies. It facilitates progress and innovation at the service of the economic development of the Nouvelle-Aquitaine region.</p> <p>ALPHA-RLH is structured around two key Strategic Fields of Activity: Photonics-Lasers (laser sources and procedures, optical components, instrumentation) and Microwaves-Electronics (integrated circuits, radiocommunication systems, radar systems), with the support of digital tools (Digital Solutions &amp; the Factory of the Future Cross-Disciplinary Field of Activity), and promotes the notion of collaborative innovation for the purposes of four markets (applied Strategic Fields of Activity):</p> <ul style="list-style-type: none"> <li>* Health (Medical Devices and Autonomy) : techniques for imaging, diagnosis and treatment, technological solutions for people suffering from a loss of autonomy</li> <li>* Communications-Security : components or systems for data transfer, data and network security</li> <li>* Aeronautics-Space-Defense : embedded optic/optronic systems, innovative solutions for making materials, communication, navigation, lighting</li> <li>* Energy-Smart Buildings : solar technologies, lighting solutions, energy efficiency, energy storage, communicating or connected devices for buildings.</li> </ul>
<b>Brainport Development - High Tech</b>	Netherlands		The High Tech Software Cluster takes care of recognizability and visibility of her member companies nationally and abroad, and offers a platform on which new products & services that meet the conditions of the present and future markets (from manufacturing to Smart Industry



<b>Software Cluster</b>			4.0) are very rapidly and innovatively developed. These new products and services create value for companies that are active within the HTSM sector (High Tech Systems & Materials) and contribute to strengthening competition and innovation power of her customers.
<b>BrainsBusiness - ICT North Denmark</b>	Denmark	North Denmark	BrainsBusiness is a unique platform for ICT innovation in North Denmark through the interaction of industry and university and the link to public authorities - a strong platform which does not have its equal other places in Europe. The overall aim of BrainsBusiness is to contribute to the North Denmark ICT cluster becoming recognised as one of the most attractive and competitive ICT clusters in Europe.
<b>Bydgoszcz IT Cluster</b>	Poland		BKI is an organisation of IT industry companies and universities based in Bydgoszcz. Mission of the association is to take measures in order to further cooperation between entrepreneurs and research institutions, as well as increase competitiveness and innovation. Moreover, its members take actions in order to create systems supporting entrepreneurs, promote IT as a key industry for the region, build up the prestige and development of higher education, and activate the labor market in the ICT sector.
<b>Canarias Excelencia Tecnológica</b>	Spain	Canary Islands	Founded in July 2008, Canarias Excelencia Tecnológica is an ICT Cluster that arises from the need to create in the Canaries a private and independent institution, committed to developing the sector and that leads the economic diversification of our islands, for it, our activities focus on the promotion and dissemination of Information Technology and Communications as key to economic and social progress in our archipelago.
<b>Clúster Digital de Catalunya</b>	Spain	Catalonia	The Cluster TIC Digital's mission is to catalize the resources of ICT catalan sector, by multiplying their individual capabilities and taking profit of the sinergies existing between the agents, contribute to the development of the companies by increasing their competitiveness and turnover with new products and intensives services of knowledge and high added value, as well as positioning the Cluster and its members as a reference of collaborative innovation at local and internacional level.
<b>Cluster TIC Galicia</b>	Spain	Galicia	The Galician ICT Cluster, known as Cluster TIC Galicia, is a private non-profit business association led by Industry and founded in 2008 to bring together companies, business associations, professional associations and other stakeholders from the Galician ICT sector. It is active in the whole value chain of the ICT macro sector and works closely with the Galician Universities and Research Centres. Cluster TIC Galicia main mission is to bring together all Galicia ICT sector stakeholders to

			boost competitiveness, innovation, new market opportunities, internationalisation and the effective cooperation between Public Administrations, Businesses and Research Institutions.
<b>Compare Competence area ICT</b>	- Sweden	Värmland	<p>Our main focus is to find a way to match our ICT companies with small- and midsized enterprises that wants to develop their business through digital transformation. This is also a challenge in the public sector in which we are working closely with the municipality of Karlstad and the county of Värmland to find ways to have the ICT companies support the public sector when implementing digital technology in their organizations.</p> <p>We also work for the need of support of competens for the companies in our cluster. We do this by collaboration with the university in Karlstad, other schools with IT education and networks around the region. We are focusing on a way to integrate the refugees, with a university degree or great experience in IT, into the Swedish ICT companies to increase the diversity and create new business opportunities through new networks and new knowledge.</p>
<b>Control &amp; IT Cluster</b>	Romania		<p>Par excellence, the professional and business activity of Control &amp; IT cluster, has its main focus, without being exclusive, in the field of processes guidance and control, associated services of any kind, respectively, in Technology Information and Communications, Electronics, High Tech as well as Key Enabling Technologies. Considering the smart specialisation in IT, the cluster envisages primarily the following directions: e-Energy, e-Government, eHealth, eClimate, e-Creative Industries, e-Agriculture etc.</p> <p>The main objective of the cluster is to provide a general framework for industry specific projects, products and services development through cooperation, collaboration, partnerships and any other form of effective support, know-how creation with minimal cost, development of modern technologies, environmentally friendly verification and implementation, both within the cluster and throughout the economic environment.</p>
<b>Cool Silicon</b>	Germany		<p>Cool Silicon, established in the framework of the "Spitzenclusterwettbewerb" (Leading-edge cluster competition) of Germany, is located within "Silicon Saxony" and deals with R&amp;D in the field of energy-efficient ICT, covering the entire value chain of micro-/nanoelectronics from automated production equipment up to energy efficient sensor networks.</p> <p>Our mission is to create new solutions for the Internet of Things, supporting in particular SMEs in establishing (also international) R&amp;D collaborations. Key members are the Technical University of Dresden, several institutes of Fraunhofer as well as large industry players such as Infineon or Globalfoundries.</p>

<b>CyberForum</b>	Germany	Baden-Wurtemberg	<p>CyberForum is a non-profit organization based in Karlsruhe. Our activities are mainly based in the Technology Region Karlsruhe.</p> <p>“From the network, for the network” is the guiding principle which inspires CyberForum. The exchange of experience, knowledge, contacts and ideas takes centre stage. Exciting business ideas start here, entrepreneurs meet like-minded people; scientists and technology enthusiasts make contact with economists, creative minds and business angels.</p> <p>Our members come from various branches such as software development, e-commerce, IT consulting, social media, gaming, IT security, software architecture and media agencies and the creative industry.</p>
<b>Dataföreningen i Norr</b>	Sweden		<p>Skelleftea shall be a leading actor regarding digitization of society. Digitization will be the region's main growth engine based on close cooperation with business, research, government and citizens.</p> <ul style="list-style-type: none"> <li>- Strive for increased recruitment to the industry by increasing young people's interest in ICT and helping universities to develop existing and new programs.</li> <li>- Work with business development, internationalisation and innovation - cross-fertilization between members and other lines of business by taking part in development projects and collaboration with municipality, region and other clusters.</li> <li>- Create publicity for the ICT industry by promoting the industry locally and putting Skellefteå and its ICT industry on the European map.</li> <li>- Develop existing resources within the industry by organising joint training, inspiration lectures, seminars and conferences.</li> </ul>
<b>Different Angle Cluster</b>	Romania		<p>Promote and support research, innovation and education in order to develop and implement solutions and projects for smart city area.</p>
<b>DITEK - Artificial Intelligence Technology Cluster</b>	Lithuania		<p>DITEK is created with the intention to develop and improve the products based on artificial methods with the help of joint knowledge, technical experience and scientific expertise as well as their most recent achievements both in Lithuania and abroad. Objectives:</p> <ul style="list-style-type: none"> <li>* To earn profit for all Partners participating in the Cluster by taking advantage of the variety of tools maintained by the including but not limited to the knowledge base, know-how, professional competence and sales platform;</li> <li>* To store the knowledge base necessary for the expansion of the Cluster, research and development (R&amp;D) activities as well as different other joint operations and share the said knowledge base within the Cluster;</li> <li>* To accumulate all sorts of professional competence and share it within the Cluster during</li> </ul>

			<p>meetings, seminars and consulting sessions;</p> <p>* To increase the competitive ability of the Cluster participants in the market by taking advantage of the accumulated knowledge base, diversified competencies, engaging in internal projects and using other tools available in the Cluster;</p> <p>* To create additional value added through development of new products and services or through improvement of the existing ones by taking advantage of the know-how and competence accumulated in the Cluster.</p>
<b>DSP Valley</b>	Belgium		<p>DSP Valley is an independent cluster of excellence in smart electronic systems and embedded technology solutions. DSP Valley groups 100+ members: universities, research institutes and companies, from small start-ups, over SMEs to large international groups with a local R&amp;D activity.</p> <p>DSP Valley offers its members a networking platform that allows them to explore each other's expertise and that stimulates innovation by exploiting complementarities.</p> <p>With its extensive offer of high quality activities DSP Valley is one of the top clusters in Europe in the area of smart electronic systems and embedded technology solutions. Its activities include for example regional and international inter cluster B2B forums, Academia-to-Business forums, a shared group booth at international exhibitions, custom matchmaking events, technical seminars, a bi-monthly newsletter and brokerage services for participation in European ICT programs.</p>
<b>High Tech NL</b>	Netherlands		<p>High Tech NL is the sector organisation by and for innovative Dutch high-tech companies and knowledge institutes. High Tech NL is committed to the collective interests of this sector with a focus on long term innovation and international collaboration. Members share their knowledge, look for ways to cooperate and use the powerful network to become successful innovators.</p>
<b>i2CAT</b>	Spain	Catalonia	<p>Brings together engineering, manufacturing (OEM and TIER1), technology providers, associations, investigation centers, universities, and the Administration with the clear objective to identify, develop and promote best practices around Industry 4.0 (also known as Industrial Internet).</p> <p>Companies and the whole value chain actively participate in an open innovation process, detecting need that can hardly be solved by themselves alone. Therefore, multidisciplinary groups are created to design and build collaborative solutions that help organization achieve their business needs.</p>

<b>ICT Technology Network Institute</b>	Slovenia		<p>Our mission is to develop and manage the digital transformation ecosystem in the region and connect ICT industry to vertical and traditional industries in order to create new value chains and support innovation.</p> <p>ICT Technology Network (ICT TN) was established in 2003 as a consortium of leading Slovenian companies and research institutions in the field of ICT. Today, it brings together app. 40 partners; its activities are coordinated by the ICT TN Institute. By joining together companies, R&amp;D institutions, technology developers, technology users, service providers and governmental agencies, ICT TN forms an ecosystem (Triple Helix cluster with a bronze cluster management excellence label) for establishment, organization, implementation and dissemination of collaborative national and international projects focusing on joint R&amp;D, cluster and intercluster development, technology transfer, innovation management, infrastructure and competence building, policy enforcements, living labs and pilot activities. In 2010, ICT TN established the Competence centre “OpComm” which activities are related to Future Internet and Internet of things.</p>
<b>IDM Ecosystem ICT &amp; Automation</b>	Italy	South Tyrol	<p>The ICT &amp; Automation ecosystem concentrates on establishing the “SMART Green Region South Tyrol”, in which entrepreneurs, researchers and citizens use and develop digital technologies in order to improve the quality of life. The ecosystem supports firms in all sectors to make use of the opportunities offered by digitalisation. To achieve this, the ecosystem is especially focussed on the use of “open technologies”, as these in particular allow for investment in the competences of the workers. At the same time, international opportunities available to firms through the internet will be investigated.</p> <p>The ecosystem is striving for the digitalisation of all sectors, in particular by the use of open technologies. The aim is to improve the quality of life using information technology and automation.</p>
<b>IKT Telemark</b>	Norway		<p>IKT Telemark helps member businesses to grow through collaboration and joint resources in a) competence and knowledge development, b) innovation and business development and c) sales and marketing.</p>
<b>INEO</b>	Spain	Galicia	<p>Ineo: three ideas, one aim: INEO's main aim is to develop Galician ICT business by strengthening its innovative and technological profile. This requires close co-operation between partners, which is the base of our association. Ineo believes in PROXIMITY, which gives us sound knowledge of daily needs of the market and places us in a privileged position to be able to offer ADDED VALUE services for the companies to be more competitive. This enables our members to reach quality and success. SUCCESS based on professionalism and</p>

			well-thought-out work. We serve everybody who is striving for excellence in everything they do, just like us!
<b>INFOPOLE Cluster TIC</b>	Belgium	Wallonia	<p>INFOPOLE Cluster TIC is the business cluster that brings together and unites professionals from Information and Communication Technologies (ICT) in order to promote business and innovation through partnership.</p> <p>Several application areas are the foundation of our actions : Industry 4.0, health (eHealth), intelligent transports, Internet of Things (IoT), Serious Game, Big Data, Open Data, Transmedia, Cyber Security, Web, ecommerce.</p> <p>Through its network of more than 100 companies, INFOPOLE can help you find the ideal partner whatever your IT project!</p> <p>INFOPOLE, a cross-sectorial cluster that is a major player in the Digital Wallonia strategy.</p>
<b>InnoZent OWL e.V.</b>	Germany		<p>InnoZent OWL e.V., founded in 1998, has made it its core task to network different competences of and with companies, science and research, politics and administration. Likewise, organisation of market places and projects, as well as contributions to the development of competences, are part of the network portfolio.</p>
<b>International Security Cluster</b>	Lithuania		<p>International Security Cluster promotes informational and physical security as the top priority of any business and science activities. We focus on the following physical and informational security sectors:</p> <ul style="list-style-type: none"> <li>* Strategic Communications (at the state and corporate level)</li> <li>* Protection from psychological manipulation and physical influence (information technologies, research, education (and training), the products, process evaluation)</li> <li>* Cyber-security (Internet, telecommunications and mobile security software)</li> <li>* Command, control, communications and computer network security systems</li> <li>* Creative and innovative strategic decisions</li> </ul>
<b>IT CLUSTER SERBIA</b>	Serbia		<p>Vision of IT Circle Cluster is coordination and integration of methods and resources to create an organization that can appear on the market as an authority and a regional leader and to accomplish more complex projects in Serbia and the EU. Our vision also is to become the most reliable supplier of innovative IT services, products and organizational support systems. Mission of IT Circle Cluster is a common appearance in the market with the aim of achieving greater competitiveness of its products and achieving synergy effects for the benefit of all members and the local and regional community. The mission includes making Belgrade and</p>

			Serbia more attractive for investors and young people by building strong and visible brand of IT Circle Cluster.
<b>IT&amp;C Cluster "Lower Danube"</b>	Romania		<p>The IT&amp;C CLuster was founded in 2015 and aims to:</p> <ul style="list-style-type: none"> <li>* Increase the capacity of research - development (R &amp; D), stimulating cooperation between institutions of research - development and innovation (RDI) and enterprises and increase access of companies to CDI</li> <li>* Identify and promote initiatives that generate innovative products and services.</li> <li>* Generate research, development and innovation projects</li> <li>* Organize trainig programs, qualification and improvement open for the specialized cluster memebbers and also for all that are interested.</li> <li>* Represent the IT&amp;C interests in front of any state institution.</li> </ul>
<b>Klaster B+R&amp;I</b>	Poland		<p>Mission: Building an innovative knowledge-based economy through the intelligent management of research and development.</p> <p>Primary goal: Mutual cooperation of enterprises, business associations, non-profit organizations, research institutes and the other for the implementation of joint projects and ventures.</p> <p>Cluster of Research and Development and Innovation (Cluster R+D&amp;I) has been reorganized at the beginning of August 2014. Cluster dating back to 2011 as a grassroots initiative of companies introducing innovations to the Polish Economy. The coordinator of the Cluster is the Foundation for the Development of Science and Business in the Area of Medical Sciences and Strict (Fundacja Rozwoju Nauki i Biznesu w obszarze Nauk Medycznych i Ścisłych).</p>
<b>Klaster.info</b>	Poland		<p>The mission of Klaster.info is competes with international companies and the desire to systematically enlarning domestic and foreign markets by raising competitiveness. We want our offer brings you the alternative. Our Cluster creates the conditions to make a strong ICT Development of Industry, encourages innovation, stimulates the development of cooperation, pursues common objectives of members of the association. We want to develop international cooperation, especially in the region (understood primarily as the eastern and southern part of Europe and the Baltic States ) , but also in more remote areas , such as Israel or South America. Therefore implemented by the Coordinator of the Cluster project assuming optimization Business processes Polish SME Cluster members work closely together in the field of Business Advisory and Information for more than five hundred small and medium enterprises across the country.</p>

<b>Košice IT Valley</b>	Slovakia		The vision of Košice IT Valley cluster is creating regional partnership of IT companies, education institutions and regional authorities that will contribute to extension and quality increase of educational programs, creation of broad portfolio of job opportunities for qualified work force and the elaboration of a common strategy necessary for achieving prosperity of the region of Eastern Slovakia and thus ensuring gradual increase of quality of life of its citizens. The main objective of Košice IT Valley cluster is to create conditions for the development of the IT industry and thus improving the quality of life in Eastern Slovakia.
<b>Kyiv IT Cluster</b>	Ukraine		KYIV IT Cluster is a non-profit organization, whose aim is to unite and develop the whole IT community of Kyiv, the capital of Ukraine and the area with the most IT potential in the country. We have several projects aimed both on educating the community, building relationships with our local authorities and also - on helping local companies to promote and establish partnerships with abroad companies.
<b>Latvian IT Cluster</b>	Latvia		Latvian IT Cluster vision is to create a value network of Latvian companies, providing reliable IS development and application services for export. Latvian IT Cluster mission is to increase competitiveness and growth of IS and IT services export through promotion of collaboration between companies on the basis of the shared vision. The Latvian IT Cluster is looking for cooperation partners in other regions with an aim to share knowledge, know-how, and professional experience, to expand business borders and find cooperation partners for companies and common international projects.
<b>Mazovia Cluster ICT</b>	Poland		The mission of the Mazovia cluster ICT is to bridge the gap between the action and conditions for SME's development in the metropolitan area and the rest of the Voivodship. Cluster accomplishes this mission by establishing and developing cooperation between sector of computer science enterprises, telecommunication, telecommunication and electronic media R&D units, universities and business institutions and local authorities in the area of Warsaw and outside metropolitan area.
<b>Minalogic</b>	France	Auvergne-Rhône-Alpes	Minalogic is a global innovation cluster for digital technologies serving France's Auvergne-Rhône-Alpes region. The cluster supports the region's leading innovators by facilitating networking, fostering collaborative R&D, and providing companies with personalized assistance throughout all phases of business growth. The products and services developed by our members address all industries, from ICT and healthcare to energy and advanced manufacturing.



<b>Mobile Heights</b>	Sweden		Mobile Heights is an industry driven networking community founded by Ericsson, Sony Mobile, Telia Company and the Regional council of Skåne and the universities of Lund, Malmö and Blekinge. Today a large number of companies and organizations from multiple industries cooperate to boost the business within the area of connected technologies. By investing in research, open innovation and entrepreneurship, the common vision is to maintain and strengthen the region as an international hotspot for connected technologie
<b>NiCAT Cluster</b>	Serbia		In today's world the IT and high technologies are the driving force of development. Our region is marked as a region with engineering culture. We believe that there is a huge potential and opportunity for success. An experienced cluster manager, committed board and active SMEs pursue 5 strategic directions leveraging all the potentials of regional stakeholders with the support of the City , and at the same time establishing links and cooperation with Regional and national agencies (RAS...), Development agencies (USAID, GIZ, EEN, SIPO....We believe in systematic approach and create systematic solutions.
<b>onGranada - Asociación Cluster Granada Plaza Tecnológica y Biotecnológica</b>	Spain	Andalusia	onGranada Tech City is the brand that represents the Asociación Clúster Granada Plaza Tecnológica y Biotecnológica. It is an initiative of the CGE – Granada Business Confederation that includes among its members and governing bodies with: Granada City Hall, Granada Council Office, University of Granada, Board of Andalusia, Granada Chamber of Commerce, ICT Business Associations – Andalusian, national and European Business Associations. Its purpose is to locate technology- and biotechnology-based projects and companies in Granada and Andalusia, taking advantage of the major advantages offered by Andalusia in this type of industry, thereby boosting the local business fabric and creating quality jobs, as well as increasing the sector's turnover. onGranada aims to position companies in the areas such as ICT, Electronics, Biotechnology, Biotechnology, BioICT and Science and Technology applied to Health in a leading position at national and international level, as well as contributing to the development of Andalusia's Technology Based Industry.
<b>ProcessIT Innovations</b>	Sweden		Bring together actors focused on the 4th industrial revolution in challenge oriented research and innovation collaborations
<b>Service Innovation Clust-ER (antes ASTER TIC)</b>	Italy		The Service Innovation Clust-ER is an association of public and private bodies: companies, research centres and training institutions that share skills, ideas and resources to support the competitiveness of the sector. The Emilia-Romagna Region has found in the Clust-ERs the subjects capable of multiplying

			<p>innovation opportunities through a collaborative approach, as they focus their activity in R&amp;D strategic sectors.</p> <p>Together with the Technopoles and the High Technology Network laboratories, they are one of the key players in the regional innovation ecosystem coordinated by ASTER, the Emilia-Romagna consortium for innovation and technology transfer.</p> <p>The Service Innovation Clust-ER focuses on its action on 5 strategic lines of research and innovation enabled through 5 working groups, or Value Chains, representative of the Emilia-Romagna service innovation system:</p> <ul style="list-style-type: none"> <li>* IOT</li> <li>* Big Data</li> <li>* Cybersecurity</li> <li>* Intelligent IT services</li> <li>* Goods Logistics</li> </ul>
<b>Silesia Cluster</b>	<b>ICT</b>	Poland	<p>Cluster's mission is the formation of a strong and stable organization in Silesia Voivodeship being able to meet any need pertaining the fields of informatization, telecommunication and project engineering.</p> <p>Strategic goals:</p> <ul style="list-style-type: none"> <li>- Facilitation of access to domestic and European sources of funding;</li> <li>- Aggregation of informational and material resources and creation of consortia for R&amp;D and application projects;</li> <li>- Support in the area of marketing and promotion;</li> <li>- Development of cooperation between members of the Cluster and other domestic and foreign entities.</li> </ul>
<b>Silicon Saxony</b>		Germany	<p>Silicon Saxony was founded as a network for the semiconductor industry in Dresden in 2000. Since then, this initiative, having started with 20 partners, has grown into a huge network. Today Silicon Saxony is one of Europe's most successful trade association for the semiconductor, electronic, microsystems and software industries. The number of members has risen to 330 at present. Silicon Saxony connects manufacturers, suppliers, research institutes, universities and public institutions along the ICT value chain.</p> <p>In order to create effective and efficient networks the association enables vibrant forums for its members and specialists. These work groups are an essential driving force in the development of new technologies and procedures, e. g. cyber-physical-systems</p> <p>With the objective of strengthening the sustainability of the business region as a location for</p>

			information & communication technology (ICT) at both the national and international level, the association sees itself as a communication and cooperation platform for its members.
<b>System Science Innovation Cluster</b>	Hungary		The primary aim of our Cluster is to connect research institutes, universities, enterprises and the industry as well as to create partnerships in Hungary and enable our members to enter international markets. System Science Innovation Centre Private Company Limited by Shares managing the Innovation Centre in Balatonfüred is our partner in delivering our strategy and aims. Our strategic goal is to establish a Centre for Research and Training Professionals through the combination of three key activities (Project Management + Research + Training) carried out at the Innovation Centre.
<b>TECNARA</b>	Spain	Aragon	The Aragón's ITC, Electronics and Telecommunications Companies Cluster, TECNARA, is the cluster initiative created in april 2011 in order to give answer to the requests of his associates for having better performances in competitiveness and internationalisation process.
<b>TICE.PT Associação para o Pólo das Tecnologias de Informação, Comunicação e Electronica</b>	Portugal		<p>The National Portuguese ICT Cluster - TICE.PT was created in 2008, with headquarters in Aveiro. It engages and mobilizes relevant actors throughout Portugal, and in particular in the regions of Braga, Porto, Coimbra and Lisbon, covering the entire value chain in the area of ICT. The concertation platform TICE.PT ensures and promotes the interfaces between the academic world, represented by universities and institutes R&amp;D, the business world, represented by the affiliates and also through networks, in particular of Smes, represented by their associations.</p> <p>The National Portuguese ICT Cluster TICE.PT, Site of Information Technologies, Communication and Electronics, was formally recognised by the Portuguese Government in August 2009, within the framework of Collective Efficiency Strategies of NSRF.</p> <p>The TICE.PT aims to promote and leverage networking strategies for the sector. Network between companies and R&amp;D centers, in order to induce a renewal active in national economic context, producing positive effects on national offering, enhanced by innovation and knowledge, creating export capacity and added value in domestic products.</p>
<b>UK IT Association</b>	United Kingdom		Our services revolve around our themes of: More Business For You – Helping Businesses Make Better Tech Buying Decisions – Driving up Standards in our Sectors

<b>Vojvodina ICT Cluster - VOICT</b>	Serbia		<p>The vision of Vojvodina ICT Cluster is Digital Serbia!</p> <p>On one hand, we want to mobilize resources of different stakeholders and use Serbian ICT sector international success, results and expertise to create conditions that will foster further development of ICT and bring about spillover effects on other industry sectors and society in general.</p> <p>On the other, we strive to increase visibility of Serbia as a very interesting alternative location for the development of sophisticated software, and put Novi Sad on the regional and European map as the hotbed for software solutions and products in this part of the world</p>
<b>Wielkopolska ICT Cluster</b>	Poland		<p>1. To boost collaboration and ICT research driven projects A) Number of successful project consortia created, B) Number of projects launched.</p> <p>2. To build strong and valuable relations within the cluster A) Number of events engaging the cluster members.</p> <p>3. To internationalize the brand of Poznan and Wielkopolska region and associated with ICT innovations A) Number of international and domestic alliances, B) Growth of export.</p>

### A.3. CLUSTERS NOT IN THE CATALOGUE, BUT IDENTIFIED AS PRIORITY AND ALREADY CONTACTED (30)

Name	Country	Region	Description
<b>Bristol &amp; Bath Cyber</b>	United Kingdom	South West of England	<p>Bristol and Bath Cyber is the UK Cyber Security Forum's regional Cyber Security Cluster for the Bristol and Bath area. We facilitate networking, sharing of best practice and research collaboration between small cyber security companies and larger Academic, Corporate and Government organisations. This enables advancement of cost effective and innovative cyber products and services in addition to boosting the regional economy.</p> <p>Through its members Bristol and Bath Cyber support regional education and awareness sessions relating to Cyber Security issues for the general SMEs, charities and individuals. We are also finding new ways to bridge the skills gap through an innovative new program "Do Cyber".</p>
<b>CAST - Competence Center for Applied Security Technology</b>	Germany	Hesse	<p>CAST e.V. offers a variety of services in the field of secure modern information technology and is a contact for all questions regarding IT security. Its network of competencies imparts knowledge of IT security technology on all educational levels - from supporting specialization in IT security at the TU Darmstadt, to career-accompanying education. Informational seminars, consultation, workshops and tutorials are how CAST supports the user when choosing the right security technology.</p> <p>The goal of CAST e.V. is to provide and develop the necessary competencies for the growing importance of IT security in all branches of business and public administration.</p>
<b>CINI - Laboratorio Nazionale di Cyber Security</b>	Italy		<p>The National laboratory of Cybersecurity aims to coordinate this network and to introduce National and International activities to help the country in better facing the cyber threats, improving the service continuity of the critical systems, increasing the society awareness, improving the protection toward the cyber attacks of the public administration and of the companies and supporting standard definition processes and methodological national frameworks. The national and international's coordination work done by the National Laboratory of Cybersecurity, will allow us to keep the Italian scientific excellence in this field alive thanks to joined initiatives and to continuous information flow we'd like to achieve among members, real and academic world.</p>
<b>CLUSIB - Club de la Sécurité Informatique Belge</b>	Belgium		<p>The widespread use of computer systems exposes companies to a series of new risks of different kinds, be it accidents (e.g. destruction of equipment through fire), errors (e.g. data transmission errors, file erasures) or malevolence (e.g. viruses, fraud, data theft). These risks may cause substantial losses and even be dangerous for the survival of the organization.</p> <p>In order to make organizations aware of this and enable them to develop the means to prevent and efficiently manage these risks, the Federation of Belgian Enterprises (FEB Asbl) created the Belgian Computer Security Club (CLUSIB Asbl) in 1989, with the support of some of its members with a keen interest in this matter.</p>

Name	Country	Region	Description
			The main objective of CLUSIB is to take any initiative aimed at fostering the security of information systems and networks.
<b>CLUSIF - Club de la Sécurité de L'Information Français</b>	France		The CLUSIF, French Information Security Club, is a professional club set up as an independent association. Open to all businesses and communities, this club brings together suppliers and users from all sectors of the economy. The main objective of CLUSIF is to promote the exchange of ideas and feedback through working groups, publications and thematic conferences. The topics covered in relation to information security vary according to the news and the needs of the members of the association.
<b>CLUSIL - Club de la Sécurité de l'Information</b>	Luxembourg		CLUSIL develops cooperative actions with public authorities, semipublic authorities for the security of information. With about 200 members from all economic sectors, it is a well-established and independent actor among the Information Security Landscape of Luxembourg and the “Grande Region”. In just 20 years, we have come a very long way and are very proud.
<b>CLUSIS - Association suisse de la sécurité de l'information</b>	Switzerland		The Clusis, Swiss Association for Information Security, is dedicated to all aspects of cybersecurity. Not-for-profit association was founded in 1989. Originally, the founders of Clusis are aware that companies must be aware of the risks to which they are now exposed. Information technology is booming and businesses have begun to operate without being able to protect their sensitive data. The players in the economy also need a competent interlocutor to answer their questions.
<b>CLUSIT - Associazione Italiana per la Sicurezza Informatica</b>	Italy		The awareness, the training, the continuous professional updating and the exchange of information are the most effective tools to face the problems of information security. CLUSIT arises from the experience of other European cybersecurity associations such as CLUSIB (B), CLUSIF (F), CLUSIS (CH), CLUSIL (L) which are a point of reference for cyber security in their respective countries for over 20 years, plus APSIT - CLUSI Tn, CLUSICI, CLUSIQ. CLUSIT is open to any person and organization that shows an interest in computer security. The objectives are: <ul style="list-style-type: none"> <li>* To spread the information security culture in companies, public administration and citizens.</li> <li>* Participate in the development of laws, rules and regulations that involve information security, both at the community level and in Italy.</li> <li>* Contribute to the definition of training paths for the preparation and certification of the various professional figures operating in the ICT security sector.</li> <li>* Promote the use of methodologies and technologies to improve the level of security of the various realities.</li> </ul>

Name	Country	Region	Description
<b>CSA Italy - Cloud Security Alliance Italy</b>	Italy		CSA Italy is aimed at professionals and companies who believe in the success of the Cloud Computing model and in sharing experiences and best practices to promote their use in safety. CSA Italy is a non-profit association established under Italian law in October 2011, the Italian chapter of the Cloud Security Alliance, an international association that was created with the aim of promoting the use of best practices for the security of cloud computing, together with training and raising awareness of the safe use of all forms of computing. CSA today has more than 330 member companies, 20 affiliated organizations and is followed by a community of more than 73,000 professionals interested in knowing, contributing and being an active part in the cloud security market. CSA has already activated more than 30 cloud security research initiatives and coordinates more than 80 chapters at regional and national level.
<b>ECC - The European Cybersecurity Cluster</b>	Europe		ECC4iu is the European cluster dedicated to the cybersecurity of the industrial and urban systems. On July 11th, 2017 in Lyon, ECC4iu association was created. This association has the role to support any type of projects and initiatives related to the industrial and urban systems security. This cluster gathers in the form of colleges: <ul style="list-style-type: none"> <li>* Industrial and urban system operators</li> <li>* Assistance with contracting and project management</li> <li>* Hardware and software providers for cybersecurity of the industrial and urban systems</li> <li>* Solution integrators of industrial and urban systems</li> <li>* Services companies (consulting, insurances, legal, etc.)</li> <li>* Academic &amp; research organizations</li> </ul>
<b>EDEN Cluster</b>	France	Rhône-Alpes	EDEN, the first French national Defence, Security and Safety SME cluster, has developed a model for the exchange and pooling of strengths that offers its members greater visibility, enhances their know-how and improves their competitive positioning in the French and international markets. EDEN's objectives are to make French product provision more consistent and reduce costs to facilitate access to global markets, make it easier for SMEs to access Research and Technology and improve knowledge of their respective markets in order to strengthen their competitive position. The EDEN model was created on the initiative of six Rhône-Alpes businessmen, with the support of the Lyon Chamber of Commerce and Industry (CCI) and the General Directorate for Armament (DGA) and is now widely deployed across France and internationally, through partnerships signed with clusters in other countries.
<b>EUCYBSEC - European Cyber Security Excellence Center</b>	Czech Republic		Our vision is to create a communication space to share the newest findings in the field of cybersecurity and cyber-defense, where the people from commercial, state, and academic fields communicate and interact with each other. Our mission is to continuously aim our professional potential in the field of cyber-defense and to

Name	Country	Region	Description
			become the main mediator of catering the highest possible standards of cyber-defense and cyber-security for all our members.
<b>FISC - Finnish Information Security Cluster</b>	Finland		Finnish Information Security Cluster is an organization established in 2012 by major Finnish information security companies to promote their business and operations in national and international context. We believe that cyber security involves everyone. It requires extensive public-private-partnership cooperation models.
<b>HMAC - Hellenic Association of Mobile Application Companies</b>	Greece		"The Hellenic Association of Mobile Application Companies (HAMAC), is a non-profit organization comprised of high-tech companies whose business activities include the development of added value mobile applications, the provision of added value services for telecommunication providers, the provision of innovative communication, content and application services.
<b>CyberIreland (former INFO SECURITY IRELAND)</b>	Ireland		"InfoSecurity Ireland (ISI) is an industry-led organisation that facilitates collaboration, marketing and research for the Irish information security sector. ISI supports the interaction of technology firms, research institutes and third level colleges to contribute to the development of Ireland as a centre of excellence in information security . ISI also promotes the industry globally by creating an awareness about Ireland's track record and capabilities in the field.
<b>ISMS Forum - Asociación Española para el Fomento de la Seguridad de la Información</b>	Spain		The Spanish Association for the Promotion of Information Security, ISMS Forum Spain, is a non-profit organization founded in January 2007 to promote the development, knowledge and culture of Information Security in Spain and act for the benefit of all the community involved in the sector. Created with a plural and open vocation, it is configured as a specialized discussion forum for companies, public and private organizations, researchers and professionals to collaborate, share experiences and learn about the latest developments and developments in Information Security. All its activity is developed based on the values of transparency, independence, objectivity and neutrality. ISMS Forum Spain already has more than 175 associated companies and more than 1000 associated professionals. The Association is already, therefore, the largest active network of organizations and experts committed to Information Security in Spain.
<b>ITSECURITY - Bavarian IT Security &amp; Safety Cluster</b>	Germany	Bavaria	The Bavarian IT security cluster employs companies from the IT industry, companies that use IT security technologies, universities, other research and education institutions and lawyers to achieve common goals. Key topics in the area of IT security are IT security and functional safety. The association has set itself the task of increasing the competitiveness and market opportunities of its member companies. The areas of expertise of the Bavarian IT security cluster e.V. develop from



Name	Country	Region	Description
			the competencies and interests of the individual members as well as from the public-security IT security topics.
<b>Malvern Cyber Security Cluster</b>	United Kingdom	Worcestershire	<p>We are a group of more than 80 small cyber security companies centered around Malvern in Worcestershire. We cooperate on a range of initiatives to grow our cyber security businesses, improve the cyber security of local enterprises, and also raise awareness of cyber security amongst young people.</p> <p>For an SME active in the cyber security and information assurance sector, it is free to join this cluster. For other organisations, there are different kinds of Cluster membership available.</p> <p>If you work in Cyber Security but are not based in our region (Herefordshire, Worcestershire or Gloucestershire) you may be interested in joining the UK Cyber Security Forum which coordinates numerous clusters around the UK, and of which Malvern Cyber Security Cluster is one. Through this organisation, you may also find a cluster closer to you through this Forum.</p>
<b>NI Cyber</b>	United Kingdom	North Ireland	<p>The Northern Ireland Cyber Security Cluster promotes international business, innovation and collaboration opportunities. The cluster consists of companies developing world-leading cybersecurity technologies from Northern Ireland, across a diverse range of sectors including finance, banking, insurance, legal, telecoms, threat intelligence, defence, security and healthcare.</p> <p>Regular meetups provide opportunities for networking, and learning on industry challenges and new technologies.</p>
<b>Norfolk Cyber Security Cluster</b>	United Kingdom	Norfolk	<p>The aim of the Cluster is to support the membership by communicating National and International cyber security initiatives as well as providing trade opportunities between member businesses in Norfolk.</p> <p>The cluster will also provide a networking platform to share ideas and best security practice within the county of Norfolk and also encouraging collaboration and identifying partnership opportunities so that SME's in Norfolk can find new ways to grow and be secure</p> <p>Supporting Norfolk County Council's commitment to Cyber Security (and UK Government's Cyber Security Strategy) and local businesses by building and sharing cyber security knowledge, skills and capabilities in the region, to make businesses more resilient to cyber-attacks and attract inward investment to the County.</p>
<b>North East Cyber Security Cluster</b>	United Kingdom	North East of England	<p>We are a group of small cyber security companies situated in the North East of England. We cooperate on a range of initiatives to grow our cyber security businesses, improve the cyber security of local enterprises, and also raise awareness of cyber security amongst young people.</p> <p>It is free to join this cluster and, as long as you are actively working in the cyber security or information assurance markets, we would be very pleased to welcome you to this group.</p> <p>There are different kinds of Cluster membership available. All membership is free of charge. Click</p>

Name	Country	Region	Description
			<p>here to see more about membership options.</p> <p>If you work in Cyber Security but are not based in the north east region you may be interested in joining the UK Cyber Security Forum, which is also free of charge, and may also find a cluster closer to you through this Forum. The North East Cyber Security Cluster is one cluster within the UK Cyber Security Forum.</p>
<b>North Wales Cyber Security Cluster</b>	United Kingdom	North Wales	<p>The North Wales Cyber Security Cluster has been formed, under the umbrella of the UK Cyber Security Forum, by a number of cyber security focussed organisations in and around North Wales including Hashtag Marketing Ltd and Glyndwr University.</p> <p>The aims of the Cluster are two-fold:</p> <ul style="list-style-type: none"> <li>* To support the members of the cluster by communicating National and International initiatives and trade opportunities, providing a networking platform to share ideas and best practice, encouraging collaboration and identifying partnership opportunities so that small cyber security specialist businesses in Wales can find new ways to grow.</li> <li>* To support the Welsh Government's commitment to Cyber Security (and UK Government's Cyber Security Strategy) by building cyber security knowledge, skills and capabilities in the Region, to make businesses more resilient to cyber attacks and the Region one of the most secure places in the world to do business.</li> </ul>
<b>North West Cyber Security Cluster</b>	United Kingdom	North West of England	<p>The North West Cyber Security Cluster, founded in 2014, is a group of SMEs from the cyber security and IT industry across Lancashire, Cumbria and Merseyside. The cluster currently involves and liaises with North West businesses, government bodies, nuclear and CNI, police and other notable departments with a wide range of strengths and services, all with a common goal to raise standards across the industry and provide first class services to protect businesses from cyber threats.</p>
<b>nrw.units</b>	Germany	North Rhine-Westphalia	<p>The network nrw.uniTS forms an organizational core for all actors of IT security in NRW. In addition to small and medium-sized companies, this also includes numerous researchers and multipliers. The focus of the project is on promoting cooperation.</p> <p>nrw.uniTS organizes, coordinates and promotes contacts, knowledge, projects and also actions in the field of IT security, which are useful for individual companies and others, but which they alone can not handle. The cooperation between university and industry guarantees the linking of application-oriented top-level research with action-oriented entrepreneurial spirit. With our wide-ranging expertise, we create short paths to potential business partners, develop markets, promote technologies and product innovations. Our more than 130 members are also committed to raising awareness of other important industries and areas for the important topic of IT security. With events, checklists and much more, we inform you about current IT threats or give you tips on how best to protect yourself.</p>

Name	Country	Region	Description
<b>Oxford Cyber Security Cluster</b>	United Kingdom	Oxfordshire	<p>The cluster is one of eighteen across the country, operating under the umbrella of the UK Cyber Security Forum. The Forum and its member clusters bring together over five hundred businesses involved with cyber security. The Oxford cluster itself has over fifty member organisations from business, business support organisations and academia.</p> <p>The Oxford cluster's objectives are:</p> <ul style="list-style-type: none"> <li>* Promote the need for increased information security / resilience</li> <li>* Signpost assistance available locally</li> <li>* Bring together businesses with an interest in information security</li> <li>* Link local specialists to wider UK community through UK Cyber Security Forum</li> <li>* Connect the commercial and academic worlds to explore research opportunities</li> </ul>
<b>Pôle d'excellence cyber</b>	France		<p>Initiated in 2014 by the Ministry of the Armed Forces (cyber defense pact) and by the Regional Council of Brittany (pact of the future) with a national scope and a goal of international outreach, the cyber center of excellence is based on the academic fabric and regional industrialists, as well as national partners or other territories.</p> <p>The mission of the Cyber Excellence Center is to stimulate the development of:</p> <ul style="list-style-type: none"> <li>* The cyber training offer (initial, continuous, superior),</li> <li>* Cyber academic research,</li> <li>* The industrial and technological base of cybersecurity, with particular attention to innovative SMEs-SMIs, including export.</li> </ul>
<b>SBA Research</b>	Austria		<p>SBA Research was founded in 2006 as the first Austrian research center for information security by the TU Wien, the Graz University of Technology and the University of Vienna. In recent years, the Vienna University of Economics and Business, the AIT Austrian Institute of Technology and the University of Applied Sciences St. Pölten joined as academic partners.</p> <p>Within a network of more than 70 companies, 15 Austrian and international universities and research institutions, and many additional international research partners we jointly work on research challenges ranging from organizational to technical security to strengthen Europe's Cybersecurity capabilities.</p> <p>Through scientific research of information security we develop practical and applicable solutions, while focusing on current issues like cyber security. SBA Research employs approx. 100 people and is by now the largest research center in Austria which exclusively addresses information security. The center is part of the Austrian COMET excellence program (COMET – Competence Centers for Excellent Technologies).</p>

Name	Country	Region	Description
<b>SEPE</b>	Greece		SEPE, the Federation of Hellenic Information Technology & Communications, Enterprises was founded in February 1995 and is the sector's representative for the digital technology industry, aiming at the development of the Greek economy and society. Approximately, 4,500 small, medium, large, local and multinational companies operate in the Information and Communications Technology and Consumer Electronics Industry sectors in Greece, with more than 230,000 employees. The country's turnover in the digital technology sector in turns represents 4% of the GDP.
<b>South West Cyber Security Cluster</b>	United Kingdom	South West of England	Supported by the police, leading universities, industry experts and business organisations, the Cluster exists to raise the profile of cyber security issues and help the region's businesses and organisations take steps to counter the threats
<b>UK Cyber Security Forum</b>	United Kingdom		The UK Cyber Security Forum is a social enterprise representing sole traders and small & medium companies (SMEs) who are actively working in cyber security. As a qualifying SME, it is completely free to join the Forum, and we now have more than 500 such Core Members across the country.

#### A.4. CLUSTERS NOT IN THE CATALOGUE, IDENTIFIED AS PRIORITY BUT NOT CONTACTED YET (8)

Name	Country	Region	Description
<b>Cluster IT Mitteldeutschland</b>	Germany	Saxony-Anhalt	<p>Coordinating and making visible the activities of the Central German IT industry - this is the core concern of the cluster IT Mitteldeutschland e. V. The industry network was founded in 2009 by seven regional IT companies and takes care of the interests of the IT industry in Saxony, Saxony-Anhalt and Thuringia. The Cluster IT now has around 50 members and partners. The association includes both large, renowned companies and small, young companies. Institutions and universities are also part of the industry network. The Cluster IT Mitteldeutschland is committed to strengthening the regional IT landscape - by making innovations visible, designing modern structures and by encouraging favorable conditions for IT companies. In addition, the cluster IT makes the know-how and the innovative strength of the local IT companies more transparent. He creates the basis for cross-company activities. The goal is to create a size and a radiance that is respected in the national and international context.</p> <p>Another central focus of work is the acquisition and safeguarding of the skilled labor potential in central Germany. For this purpose, the cluster IT Central Germany works intensively together with the universities in Saxony, Saxony-Anhalt and Thuringia and shows employment potential in the central German IT industry.</p> <p>Many members of Cluster IT Mitteldeutschland are involved in working groups on industry-relevant topics such as "Energy 4.0", "IT Security", "Personnel Marketing" or "Software". In doing so, they develop ways of solving the current problem and advocate their becoming known in business and the public.</p>
<b>CyNam - Cyber Cheltenham</b>	United Kingdom	Cheltenham	<p>CyNam, (Cyber Cheltenham) is a new non-profit making organisation based in the heart of the UK's cyber security community in Cheltenham. The goal of CyNam is to bring together the best technology minds from local SME's and Startups to fully harness the rich cyber security ecosystem that flourishes around Cheltenham, the home of the National Technical Authority for Information Security, GCHQ.</p> <p>CyNam is now a Community Interest Company with a Board of Directors incorporating technical leaders from the local community, with backing from local and national government.</p>
<b>DANISH CYBERSECURITY CLUSTERS</b>	Denmark		<p>Danish Cyber Security Clusters is a joint project between the Innovation Network for Finance IT, CenSec/Inno-Pro, and InfinIT - three Danish innovation networks engaged in the cyber security agenda. The innovation networks are a part of the Danish innovation infrastructure and is funded by the Ministry of Higher Education and Science.</p>

Name	Country	Region	Description
<b>Midlands Cyber</b>	United Kingdom	Midlands	<p>The Midlands is one of the fastest growing and economically important areas within the UK. The Midlands Engine is home to numerous Cyber Security and Defence organisations, including those providing service to the UK Government. It is also home to several universities providing exceptional cyber training and education.</p> <p>Midlands Cyber is a partnership organisation for cyber businesses across the Midlands Engine geography, supporting businesses with growth and attracting direct foreign investment.</p> <p>Our Vision:</p> <ul style="list-style-type: none"> <li>-To be globally recognised as the UK's Leading Region for Cyber Innovation</li> <li>-Promoting a connected community of Disruptive Technology Expertise across the region</li> <li>-Creating a commercial bridge linking future business protection with first class cyber capabilities</li> </ul>
<b>North European Cybersecurity Cluster</b>	Finland		<p>"The North European Cybersecurity Cluster (NECC) promotes information security and cybersecurity-related cooperation and collaboration in the Northern European region in order to enhance integration into the European Digital Single Market.</p>
<b>NSM Cluster - Network Security Monitoring Cluster</b>	Czech Republic	South Moravian	<p>Network Security Monitoring Cluster (NSM Cluster) is co-operative industrial cluster focusing on the network security and security in ICT.</p> <p>Our activities are:</p> <ul style="list-style-type: none"> <li>* projects in terms of technical innovative infrastructure;</li> <li>* scientific and research projects;</li> <li>* designing and complex solutions integration in network security monitoring field;</li> <li>* cluster promotion;</li> <li>* networking, know-how sharing;</li> <li>* education and training about network security monitoring;</li> <li>* actual network security trends and information sharing;</li> <li>* creating and comment draft bills concerning the dilemma of network security monitoring and security in ICT;</li> <li>* the representation towards other associations and international organizations related to the network security monitoring and security in ICT topic (e.g. ENISA, IT Security in Germany).</li> </ul> <p>NSM Cluster has 21 members together with Masaryk University in Brno and is open for other members. It was founded in South-Moravian Region and most of current members</p>

Name	Country	Region	Description
			ale held in South Moravia but clusters ambition is to become interregional grouping in Czech Republic (and also to Europe).
<b>si-Cluster</b>	<b>Greece</b>		"The Hellenic Space Technologies and Applications Cluster (si-Cluster) is an emerging, industrially-led and user-driven innovation cluster in Greece, with a sizeable potential to compete worldwide in the challenging and fast-growing sector of space technologies and applications.
<b>SSV - Security Systems Valley</b>	France		<p>Increased threats (terrorism, cybercrime, environmental disasters ...), technological and numerical changes, multiplication of interdependencies ... Any new event reveals the inadequacy of the solutions adopted, often too partial and compartmentalized.</p> <p>The issues of safety and security need to be understood in a transversal and innovative way, considering all the parameters in their complexity and comprehensiveness in an objective: to face the challenges of resilience. This new approach to risk must involve the mobilization of all skills by promoting synergies and collaborations between the civilian and military worlds, public and private, while optimizing the convergence of areas of expertise, as well as citizen mobilization.</p> <p>From these observations came the Val d'Oise department's initiative for a "global security" by favoring the urban level of proximity and affirming as a major strategic axis the renewal of the secure local socio-economic fabric: the territory of trust. This new territory remains to be conquered.</p> <p>This Systems Security Valley approach benefits from numerous industrial, institutional, associative and academic supports. It is intended as a testing ground, a real test bed of new replicable solutions across the country.</p>