D4.6 EU Cybersecurity and Privacy cluster engagement report.

3rd Report

Author(s)	M. Ramirez, CITIC
Status	Final
Version	V1.0
Date	30/10/2020

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 organised 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	**AEI Ciberseguridad**
Related work package	**WP4**
Author(s)	M. Ramirez (AEI Ciberseguridad)
Contributor(s)	N, Ferguson, Trust-IT & Justina Bieliauskaite, DSME
Due date	31/08/2020
Actual submission date	30/10/2020
Reviewed by	N, Ferguson, Trust-IT & Justina Bieliauskaite, DSME
Start date of Project	**01/05/2017**
Duration	**48 months**

Revision history

Version	Date	Authors	Notes
0.0	27/08/2020	M. Ramírez (AEI)	First version
0.1	28/09/2020	N. Ferguson (TRUST)	First internal review
0.2	07/10/2020	J. Bieliauskaite (DSME)	Second internal review
0.3	19/10/2020	M. Ramírez (AEI)	Final version
1.0	30/10/2020	M. Ramírez (AEI) & N.Ferguson (Trust)	Final version approved by PMB

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 the first of three EU Cybersecurity and privacy cluster engagement reports[1] published in July 2018 (M27), 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[2]. In D4.5[3] the second of the reports published in June 2019 (M26), Cyberwatching.eu reported on how to consolidate the relationship with a targeted group of clusters to ignite real interaction. Three clusters in particular, were already engaged and very committed to interacting with Cyberwatching.eu.

In the following months (M26-41), efforts have focused on consolidating the relationship with the relevant clusters and going on with the activities defined in D4.5 second report. Now a consolidated group of eight clusters engage with Cyberwatching.eu and a memorandum of understanding has been drafted and shared with them.

Cyberwatching.eu aims to impact positively on the clusters and their members by promoting project assets such as the GDPR temperature tool, providing networking opportunities with the R&I community, and raising awareness of emerging technologies and opportunities for businesses, and best practices during the COVID-19 pandemic. A key channel for this support is the provision of joint webinars which is being carried out.

Future activities will focus on guaranteeing the sustainability of project assets to be defined in D5.3 (Sustainability plan). The services offered by Cyberwatching.eu have companies as end users, especially SMEs, and clusters are the instrument to reach them. With the involvement of a few relevant clusters it is possible to give visibility by the “call effect”. Clusters form a key target stakeholder group for this sustainability activity and by cementing further our alliance with them, we hope to achieve greater impact and sustainability

[1] https://www.cyberwatching.eu/d42-eu-cybersecurity-and-privacy-cluster-engagement-report-1st-report

[2] https://www.cyberwatching.eu/clusters

[3] https://www.cyberwatching.eu/d45-eu-cybersecurity-and-privacy-cluster-engagement-report-2nd-report

Table of Contents

LIST OF FIGURES

1 Cyberwatching.eu's CS&P Cluster Network

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.

After 40 months of Cyberwatching.eu, we have found that Clusters working in the CS&P sector are not specifically targeted by any of the former EU cluster initiatives. Rather, there are different cybersecurity network initiatives which group several clusters that are active in CS&P and from the same country or region (Cyber Wales Ecosystem, UK Cyber Security Forum, 3B ICT - Balkan and Black Sea ICT Clusters Network).

In order to realise effective and real collaboration which can impact positively on clusters, Cyberwatching.eu has established synergies with a small number of clusters. This includes the consolidation of engagement with the three clusters (CLujIT, CyberWales and GAIA) and to expand this to a further five which also takes into account the geographical distribution, to cover all the European area.

In this deliverable, Cyberwatching.eu presents the report on the performed activities with clusters from M27 to M40, and the next steps to be addressed.

1.2 Engaged clusters

The following table provides details on the clusters that Cyberwatching.eu has established synergies with. The information has been gathered during analysis of the clusters that was carried out to identify the focus of the clusters and to define possible activities and themes for collaboration.

As can be seen in figure 1, engagement is primarily in Central and Western Europe although one of our key collaborations is with ClujIT in Romania.

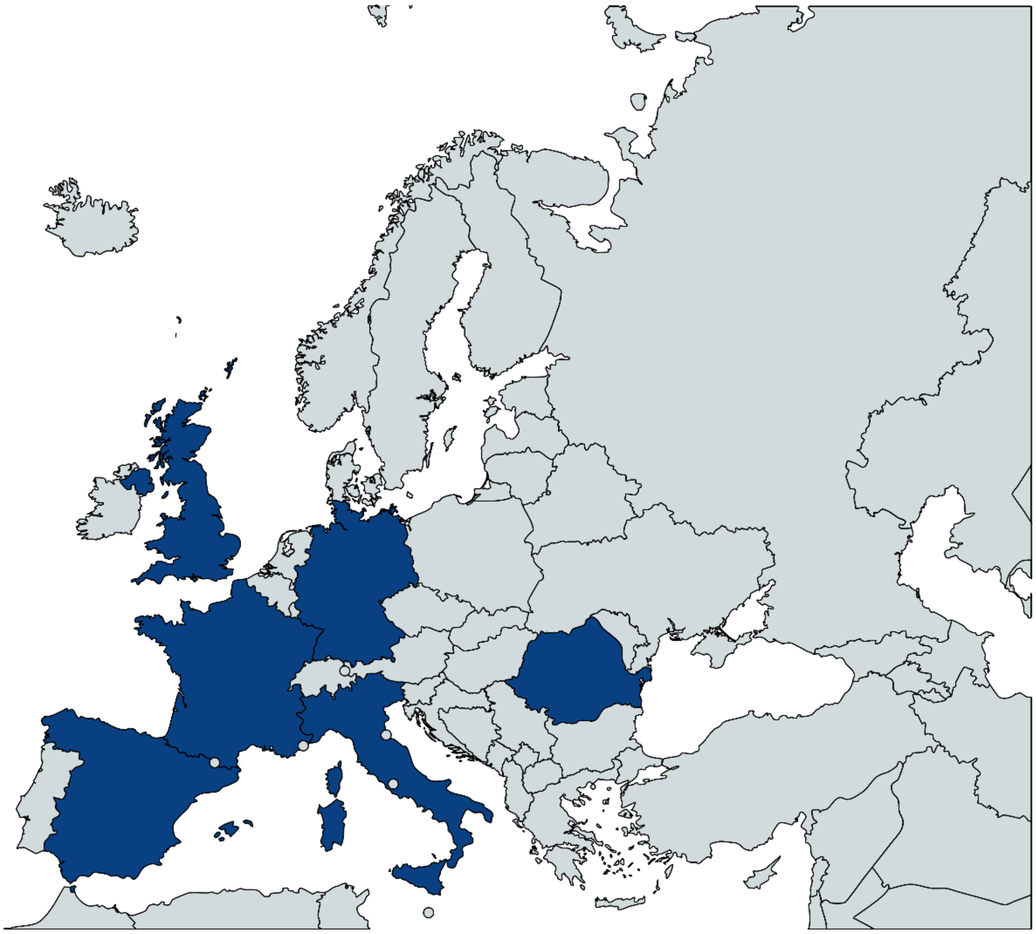


Figure 1 Engaged Cyber Clusters distribution

ClujIT

- **Country**: Romania
- **Website**: https://www.clujit.ro/
- **Number of members:** 82
- **Mission / Vision:**
    - Becoming one of the most credible suppliers from Central and Eastern Europe.
    - Members able to be competitive on national and international markets.
    - Innovative IT services and products as well as of organizational support systems.
    - Founding lasting public-private partnerships for the mutual benefit of the cluster's members and of the society in general.
    - Promote innovation in processes, design of products and services to increase competitiveness on international level.
    - Creation of a partnership culture based on trust and dependability. Promotion of the Romanian IT market
- **Working Groups / Main interests:**
    - Data Intelligence
    - Learning and Development
    - Smart City
    - Marketing
    - Internationalization

- **Synergies with Cyberwatching.eu**:
  - Speaker at Concertation meeting April 2018
  - Speaker at webinar "Cybersecurity as an opportunity in a changing market" June 2018
  - Speaker at webinar "Teleworking and cybersecurity in times of Covid-19: challenges and risks for SMEs" July 202

GAIA - Association of Knowledge and Applied Technologies industries in the Basque Country

- **Country**: Spain
- **Website**: http://www.gaia.es
- **Number of members:** 255
- **Mission / Vision:**
  - Its objective is to be a benchmark in Collaborative Innovation for the creation and implementation of globally competitive solutions based on own Knowledge and Technology (Consulting, Engineering, Electronics, Computing, Telecommunications and Gamification).
- **Working Groups / Main interests:**
  - Talent
  - Knowledge and Technology
  - Alliances
  - Internationalization
- **Relation with Cyberwatching.eu**:
  - Speaker at concertation meeting April 2018
  - Speaker at webinar "Cybersecurity as an opportunity in a changing market" June 2018

CyberWales

- **Country**: United Kingdom
- **Website**: https://cyberwales.net/
- **Number of members:** +2.000
- **Mission / Vision:**
  - Cyber Wales is a representative body with the aim of being the Heart and the Voice of the cyber Communities in Wales.
  - It's a network of 9 cyber-related clusters.
  - Help cyber companies to grow by communicating initiatives & trade opportunities, providing a networking platform to share ideas & best practice, encouraging collaboration and identifying partnership opportunities.
  - Help make businesses more resilient to cyber-attacks by building cyber security knowledge, & skills and making Wales a hub for cyber security expertise in Europe.
- **Working Groups / Main interests:**
  - Education & Training cluster
  - Women in Cyber
  - Capture the Flag
  - Critical National Infrastructure
  - Data Privacy
  - South Wales Cluster
  - North Wales Cluster
  - IP Wales Cluster
- **Relation with Cyberwatching.eu**:

  - Speaker at webinar “Cybersecurity as an opportunity in a changing market” June 2018
  - Speaker at Annual Workshop October 2018
  - Speaker at webinar “Cyber risk management from the SME point of view” October 2018
  - Speaker at webinar “Teleworking and cybersecurity in times of Covid-19: challenges and risks for SMEs” July 2020.

AEI Ciberseguridad

- **Country**: Spain
- **Website**: https://www.aeiciberseguridad.es/
- **Number of members:** 71
- **Mission / Vision:**
  - To provide an operational structure to all companies interested in the promotion and development of a Business Technological Pole linked to INCIBE’s mandate
- **Working Groups / Main interests:**
  - Innovation and Development (R&D)
  - Training. Leadership
  - International: cPPP
  - International: Cybersecurity Seal.
- **Relation with Cyberwatching.eu**:
  - Partner of Cyberwatching.eu

The Hague Security Delta (HSD)

- **Country**: Netherlands
- **Website**: https://www.thehaguesecuritydelta.com/
- **Number of members:** 299
- **Mission / Vision:**
  - To form partnerships and create 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.
  - HSD took the initiative in 2016 to collaborate with other 5 relevant security cluster in Europe (France: SAFE Cluster, Denmark: CenSec, Finland: Safety and Security Cluster, Germany: KIT, Germany: Security Cluster), so we considered them a relevant cluster to collaborate with.
- **Working Groups / Main interests:**
  - Data forensics
  - Data Diode: Data traffic that can only go one way
  - Critical infrastructures
  - Talent
  - Training
  - Cybersecurity awareness
  - Artificial intelligence (their research institutions were focused in what to do in AI from the stakeholder view)
- **Relation with Cyberwatching.eu**:
  - In November 2019, we had a virtual meeting with Bert Feskens, from HSD, and they were keen to collaborate with us, especially interested in SMEs, because their two main goals, as a cluster, are developing cybersecurity solutions and increase economic development.

- HSD promoted GDPR Temperature Tool, and other useful Cyberwatching.eu resources for SMEs (like SMEs guides).
- In December 2019, we had a virtual meeting with Herman Hartgers, from SME Connect (helpdesk of HSD). Interested in in fraud and cybercrime and Digital SME presented the Twenty2x event and the opportunities that brings to SMEs.

ITSECURITY - Bavarian IT Security & Safety Cluster

- **Country**: Germany
- **Website**: https://www.it-sicherheitscluster.de/
- **Number of members:** 134
- **Mission / Vision:**
  - To initiate and promote collaborations, particularly between the scientific and economic community
  - To further the development of IT security research and training
  - To provide information about security risks and their technical and organisational solutions
  - To present the Cluster's members and their security expertise
  - To launch and mentor company start-ups
- **Working Groups / Main interests:**
  - 'IT Security' includes all issues of IT or information security which are concerned in the broadest sense with protection against intelligent, strategic attack.
    - Data protection
    - Cloud Security
    - Industrial IT Security
    - Information security management
  - 'IT Safety' applies to the technical/functional issues of information security and is primarily concerned with protection against harmful influences.
- **Relation with Cyberwatching.eu**:
  - On 8-10 October DSME organised SME Delegation & SME workshop at the it-sa cybersecurity fair. SMEs that participated had a chance to meet the Bavarian Cluster, and they were informed about the Cyberwatching.eu project. A follow-up call identified that the cluster is interested in participating in H2020 projects and were using Cyberwatching.eu as a reference.

DIGITAL SME France

- **Country**: France
- **Website**: https://www.digitalsme.eu/digital-sme-france-membership/
- **Number of members:** 5
- **Mission / Vision:**
  - As a member of the European DIGITAL SME Alliance, DIGITAL SME France promotes a European oriented approach towards the development of French SMEs active in Information and Communication Technologies (ICT).
- **Working Groups / Main interests:**
  - Not specified.
- **Relation with Cyberwatching.eu**:
  - On 25 May, Cyberwatching.eu, in collaboration with DIGITAL SME France, organised an SME online workshop to raise SMEs' awareness about the cybersecurity issues when teleworking. The workshop was held in French and allowed to reach the target audience of French-speaking SMEs, mainly located in Eastern France and Luxemburg. Besides being informed about the Cyberwatching.eu and its key offers for the SMEs, the participants got an introduction to cybersecurity and cyber-attacks. The experts then raised the risk awareness of the participants, describing the specific risks and cyber threats related to teleworking: phishing, ransomware, data theft, Business Email Compromise (BEC) scam, etc. and explaining what kind of vulnerabilities might be exploited by cyber criminals. Finally, the participants got security recommendations from the experts.
  - On 22 July, Cyberwatching.eu and DSME France signed a Memorandum of Understanding based on their common goals with some commitments from both parties.

Italian DIGITAL SME Alliance

- **Country**: Italy
- **Website**: https://www.digitalsme.eu/digital-sme-italy-membership/
- **Number of members:** 16
- **Mission / Vision:**
  - Representation of the interests of Italian SMEs in the ICT sector at national and European level.
  - Information and news on European policies and regulatory updates.
  - Promote the exchange of know-how and expand possible working collaboration between members in Europe.
  - A direct channel of communication with the European institutions through bilateral meetings, participation in conferences and inclusion in expert groups.
  - Dissemination and support to members for participation in projects funded by the European Union.
  - Enhancing its members' sectoral skills by participating to European trainings and workshops.
- **Working Groups / Main interests:**
  - EU funding.
- **Relation with Cyberwatching.eu**:
  - Cyberwatching.eu is still defining activities with Italian DIGITAL SME Alliance.

1.3 Work carried out with clusters

In this section, we look at the work carried out with the clusters since June 2019.

1.3.1 Engaging with clusters during the COVID-19 pandemic

In March 2020, due to the **outbreak of covid-19**, many companies were forced to implement teleworking. Cyberwatching.eu partners identified an opportunity to impact positively on the clusters by organising **webinars** on how to guide these companies to make sure their business remains GDPR compliant and secure at the same time.

Through a dedicated meeting Cyberwatching.eu facilitated clusters to share their experiences and to look at how each one were supporting their members. GAIA, CyberWales, ClujIT and HSD have created dedicated activities to help companies to face this new situation:

GAIA cluster launched this initiative: https://www.dw4all.eu/

Currently available in Spanish or Euskera, the platform provides resources for teleworking: technological solutions, advanced services and a learning centre for SMEs and the self-employed.

A marketplace with products and services exclusively for teleworking, and also some guides with good practices is also available.

CyberWales launched a support & mentoring service in collaboration with the Cambridge Judge Business School and the Behavioural Insights Team to determine the impact of mentoring on digital tech businesses.

As part of this project, CyberWales were able to offer the opportunity for free mentoring to any digital tech SME with more than five employees. More information here.

Cluj IT Cluster supported the SME-led campaign “Digital Solutions in times of COVID-19″. The campaign was led by Cyberwatching.eu partner Digital SME and ClujIT is very collaborative with Cyberwatching.eu.

The **Hague Security Delta** implemented different measures outlined here: https://www.thehaguesecuritydelta.com/news/newsitem/1552-hsd-office-activities-concerning-covid-19-pandemic

Cyberwatching.eu published its own COVID-19 questionnaire in August 2020 which focused on working practices during the pandemic. This was promoted to the clusters and analysis of results will be included in D3.5.

1.3.2 Webinar series

With the success of the Cyberwatching.eu webinar series, a meeting was held with the clusters to identify potential topics for joint webinars. With the various COVID-19 activities taking place at a regional level, Cyberwatching.eu brought the clusters together with the objective of providing EU-wide perspectives on the COVID-19 pandemic and cybersecurity challenges, best practices and support for SMEs.

In addition, the clusters identified other topics that would be of interest to their networks such as **Cybersecurity risks in disruptive technologies** (such as Cyber Range, AI, IoT and Blockchain). The key focus of these webinars will be to focus on how companies can use these technologies to improve their cyber posture and respond to CS challenges. In addition, the webinars will provide a unique deep dive into the potential of these technologies. The activity will be combined with the R&I project cluster webinars being carried out in WP2 thus facilitating projects in reaching out to companies while raising awareness of cybersecurity challenges and future solutions.

Teleworking during COVID-19 – Good practices and tips for cybersecurity[4] – 25 May 2020

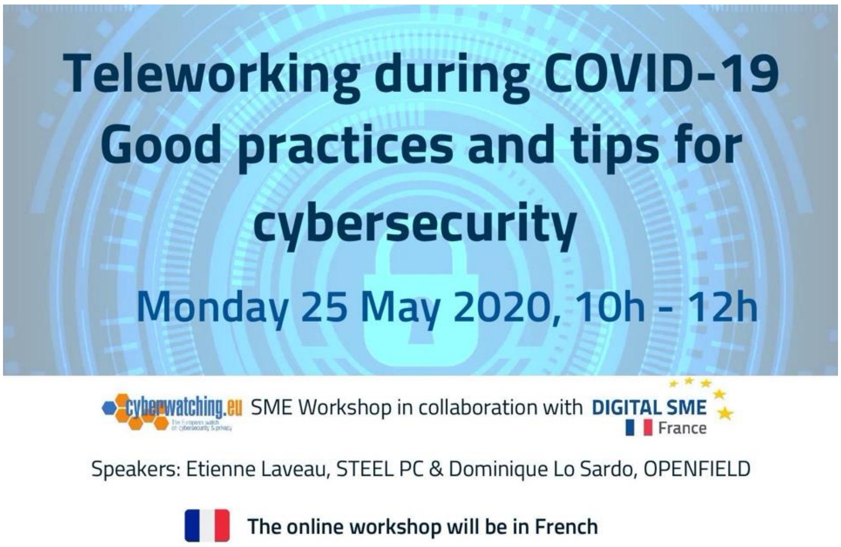

Teleworking during COVID-19
Good practices and tips for cybersecurity
Monday 25 May 2020, 10h - 12h
cyberwatching.eu
SME Workshop in collaboration with DIGITAL SME France
Speakers: Etienne Laveau, STEEL PC & Dominique Lo Sardo, OPENFIELD
The online workshop will be in French

Figure 2 Teleworking during COVID-19 webinar organised together with DIGITAL SME France

In collaboration with **DIGITAL SME France**, Cyberwatching.eu, organised an online SME workshop to raise SMEs' awareness about the cybersecurity issues when teleworking.

This workshop was held in French and allowed to reach the target audience of French-speaking SMEs, mainly located in Eastern France and Luxemburg.

Besides being informed about the Cyberwatching.eu and its key offers for the SMEs, the participants got an introduction to cybersecurity and cyber-attacks. The experts then raised the risk awareness of the participants, describing the specific risks and cyber threats related to teleworking: phishing, ransomware, data theft, Business Email Compromise (BEC) scam, etc. and explaining what kind of vulnerabilities might be exploited by cyber criminals. Finally, the participants got security recommendations from the experts.

[4] https://www.cyberwatching.eu/news-events/events/teleworking-during-covid-19-good-practices-and-tips-cybersecurit

Teleworking during COVID-19: Good practices and tips for cybersecurity[5] - 23 July 2020

WEBINAR
TELEWORKING DURING COVID-19
Good practices and tips for cybersecurity
23 July - 11AM CEST
cyberwatching.eu
The European watch on cybersecurity & privacy
In collaboration with
CLUJ IT
Cyber Wales
European DIGITAL SME Alliance

Figure 3 Teleworking during COVID-19 webinar organised together with ClujIT and CyberWales

COVID-19 has meant that company staff are now working remotely. Telework will go on for an indefinite period and could even become the new standard for companies. The pandemic has forced many small and medium enterprise (SME) to implement a quick transition to a more digitalised workflow. This rapid and, in many cases, involuntary modernisation of small and medium companies obviously carries with it many cybersecurity risks.

It is therefore fundamental for SMEs to increase their knowledge of the cybersecurity area, as their unpreparedness can easily lead to the exposure of sensitive information on the internet and the loss of critical assets, also causing brand damage.

This webinar saw presentations from two of the collaborating clusters ClujIT and CyberWales, provide practical risks and best practices for SMEs that are coping with the pandemic.

‘Impact and mitigation measures of COVID-19’ (impact on the digital market, data protection issues, tracking apps and privacy risks, impact on Security R&I programmes, funding opportunities in the wake of COVID – December 2020

This webinar will focus on the actual impact of COVID-19 10 months since its outbreak effected European companies directly. Data from the Cyberwatching.eu COVID-19 questionnaire will be analysed and reported on. Clusters will be invited to also contribute to the webinar.

[5] https://www.cyberwatching.eu/news-events/events/teleworking-during-covid-19-good-practices-and-tips

1.3.3 Memorandum of understanding

Following the M1-18 review recommendation to focus on engagement with a smaller number of key clusters, we discontinued work on the **cluster catalogue and** the "**cluster of the month**" activity.

To cement collaboration work focused on developing a **Memorandum of Understanding** for clusters, which is included in Annex A.

The focus of this collaboration agreement was centered on the following commitments:

Cyberwatching.eu commits to involve clusters in:

- access to the Cyberwatching.eu Marketplace and Catalogue;
- access to the SME end-users' club and its services (for the Cluster's members);
- additional visibility (through the Cyberwatching.eu website and social media channels);
- information on the project development, main results and project deliverables;
- early access to the project results and tools;
- networking opportunities;
- invitation to the Cyberwatching.eu events.

Clusters commit to:

- supporting Cyberwatching.eu goals and vision;
- involving its members to the marketplace and/or SME end-users' club;
- promoting and disseminating Cyberwatching.eu results.

Digital SME signed this MoU with DIGITAL SME France last 22 July and the consortium has offered the cluster to sign it with the same goals.

1.3.4 Other activities

Another initiative carried out with GAIA, CLujIT, The HSD and ClujIT was the involvement in the Pan-European Hackathon held on 24-26 April.

We informed them about the Industrial Cluster Response Portal developed by the Cluster collaboration Platform, in collaboration with the **European Cluster Alliance (ECA)** and promoted by DG GROW, to support the efforts of industrial clusters to address the challenges posed by the COVID-19 epidemic in Europe. We also informed them about the Pan-European Hackathon and the survey to submit challenges.

Despite the main concern of the hackathon being the health emergency, there were also other aspects that had to be addressed: economy/business and social challenges. And in those 3 aspects, cybersecurity and ICT were very important. We therefore tried to involve the 4 engaged clusters in this initiative to form groups for the challenges. At the beginning they all showed interest in participating, but finally the prizes were not clearly defined and clusters declined the invitation.

We have maintained communication with the 4 clusters over time to inform them of the updates related to Cyberwatching.eu: the launch of the GDPR temperature tool, the launch of Cybersecurity self-assessment for SMEs and the Cyberwatching.eu information notice tool. We also asked them to promote a newspiece about our Marketplace.

Through the **AEI de Ciberseguridad**, as a European cybersecurity cluster, we have promoted the Cyberwatching.eu assets, as well as the different surveys that have been launched from the consortium, in addition to communicating the progress of the project through monthly newsletters, as well as in the meetings of the Board of Directors.

Although Cyberwatching.eu have focused on knowing better and collaborating more closely with a small group of clusters, the work of gathering information on European cybersecurity and ICT clusters has not been in vain, since thanks to this list of contacts collected from public web pages, we have been able to launch some more extensive communication campaigns when we needed to reach a larger number of companies.

In this way we have managed to send to more than 200 contacts, improving the impact of the Cyberwatching.eu activities:

- Invitations to register for the webinar: “Teleworking during COVID-19: Good practices and tips for cybersecurity”
- Invitations to promote the use of Cyberwatching.eu information notice tool.
- Invitations to promote the survey “Cybersecurity and Privacy in Covid-19”

1.4 Evaluation of the planned activities for M27-M40

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 D4.5 second report, the status of the planned activities can be assessed as follows:

- **Involvement of clusters in Cyberwatching.eu periodic webinars**: Given the COVID-19 pandemic, the webinar series is now the main means for collaboration with the clusters. To strengthen the reach of this we plan to combine some R&I project webinars with these which focus on emerging technologies, a topic of interest to a number of the clusters. .
- **Surveys: distribution of cybersecurity and privacy related surveys to clusters in order to gather information for Cyberwatching.eu deliverables:** As mentioned above, we have sent more than 200 emails to reach companies across the clusters in promoting the survey “Cybersecurity and Privacy in Covid-19”. The results will be collected and analysed in the deliverable 3.5 (Risk and recommendations on cybersecurity services).
- **Online catalogue maintenance:** Due to the new approach of closer contact with the relevant clusters, Cyberwatching.eu has ruled out maintaining and updating the cluster catalogue, although the link to the catalogue still exists today.
- **Cluster of the month:** As with the catalogue, this activity is no longer promoted as our goal is not to establish close ties with all clusters.
- **Newsletter:** As we are focusing on a more personalized relationship, we have not created a specific newsletter for clusters, and instead we maintain periodical direct contact with them.
- **Promotion of Cyberwatching.eu marketplace opportunities in terms of promoting companies in the clusters and their services**: We have promoted the Cyberwatching.eu marketplace to the clusters and their members.
- **Define clusters area in Cyberwatching.eu site**: A new website section highlighting our engagement with the clusters listed in section 1.2 will be published.
- **Periodic meetings**: We have held virtual meetings with the clusters, individually (HSD) and collectively (for the series of webinars), with the aim of knowing their interests and adapting the activities to their preferences.
- **Define joint actions**: Although we have carried out some collaborative activities and more are in the offing, after knowing better the preferences of the

clusters, we have made the decision to base these activities on those preferences, abandoning the initial idea of excellence, internationalization and emerging industries identified in D4.5 as key concepts.

- **Engage with competence centre pilot network projects:** This aspect is being widely covered in other tasks of the project, and the linking of cybersecurity clusters in pilot projects is not so relevant within their preferences.

2 Next Steps

2.1 Dedicated activities

The project must continue and reinforce the activities defined in D4.5 second report and carried out for M27-M40. Specifically, Cyberwatching.eu will keep working in the following tasks focusing on the specific target clusters:

List of 10 loyal clusters	Cyberwatching.eu will prioritize on identifying and covering actual needs of the current loyal clusters listed in section 1.2
Analysis of clusters	Cyberwatching.eu will continue the work of getting to know the clusters and their interests in depth in order to jointly define the cluster section on the web, as well as to define joint actions and invite them to participate in webinars and other events. Depending on each cluster interest, we are considering language specific webinars as we have done for the DSEM France. To date GAIA and AEI were interested in a Spanish language webinar. HSD and ClujIT did not see this as necessary.
Define clusters area in Cyberwatching.eu site	
Events	
Involvement of clusters in Cyberwatching.eu periodic webinars	
Define joint actions	
Surveys	In this case, Cyberwatching.eu will continue to use the expanded list of clusters to promote not only the marketplace, but also the rest of the useful tools and services for companies (GDPR temperature tool, Cybersecurity self-assessment for SMEs, Cyberwatching.eu information notice tool). It will also use the same channel to disseminate surveys that can be used for our deliverables.
Promotion of Cyberwatching.eu marketplace	

Nevertheless, Cyberwatching.eu has identified some complementary activities to strengthen relationships with clusters:

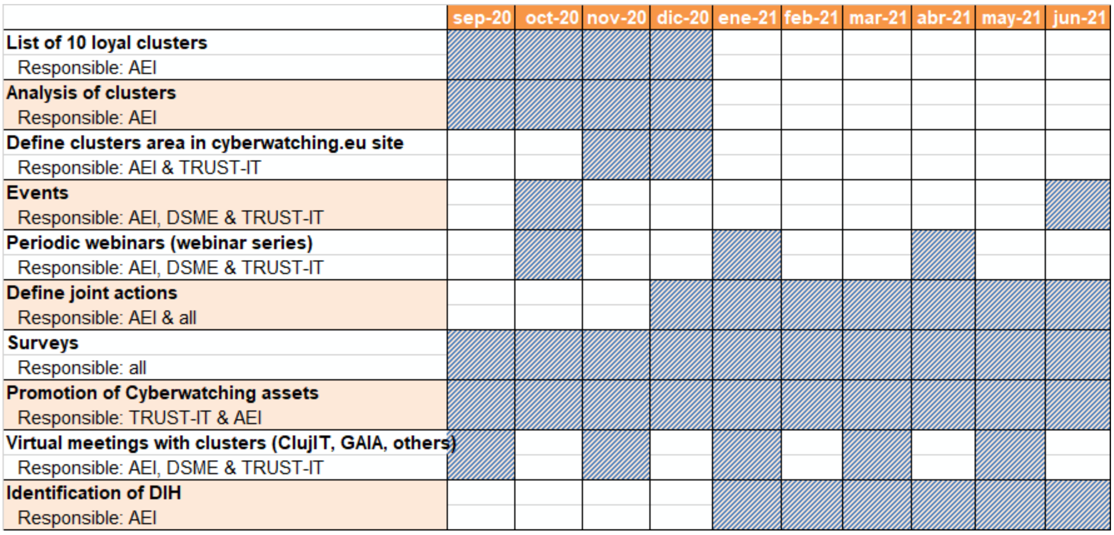
- **Webinar series:** We will work on fine tuning the topics of the webinar series, to determine the approach and the target audience and we will involve relevant speakers who could catch the attention of the SMEs. We will start from a less technological approach, for a broader audience, and then will deep into more technical topics that will be identified through surveys to attendees of the first webinars. Regarding future webinars, like **Cybersecurity risks in disruptive technologies** (such as Cyber Range, AI, IoT and Blockchain) we will:

  - better target the audience from cluster members
  - offer a more in depth look at these technologies having specific webinars on each of them (for example webinar #3 could be entirely on Cyber Range, webinar #4 entirely on AI and so on)
  - recruit as speaker experts coming from R&I projects but also important European initiatives such as ECSO.
  - Highlight Cyberwatching.eu assets such as the GDPR temperature tool and risk management tool and gather feedback on them.

- **Virtual meetings with clusters:** In the same way that we organize a virtual meeting with HSD, we will keep encouraging this direct contact with all the engaged clusters, to complement email communications and identify their interest to define joint actions. One of the common interest of clusters is Talent and Digital Skills in cybersecurity, so this could also be a key topic for joint activities.
- **Italian DIGITAL SME Alliance**: Through Digital SME, Cyberwatching.eu is preparing a workshop with their members. This will most likely cover the topic of EU funding, and will show how Cyberwatching.eu can help them - e.g., by highlighting trends in cybersecurity and privacy research and innovation; demonstrating best practices from the EU projects and also from SMEs that exploit EU research results and so on. Another activity that is being planned, together with one of Italian Digital SME Alliance members - Assintel - is to feature an article about Cyberwatching.eu in their magazine on cybersecurity.
- **Identification of Digital Innovation Hubs with a strong focus on cybersecurity**: The European Commission has proposed the creation of the first-ever Digital Europe Programme which will invest **€8.2 billion** to align the next long-term EU budget 2021-2027 with increasing digital challenges and European Digital Innovation Hubs (EDIHs) will be implemented within this programme. Grant opportunities will focus on improved hub facilities and employment of personnel. This will allow EDIHs to deliver services that stimulate a broad uptake of Artificial Intelligence, HPC and **Cybersecurity**, in both industries (in particular SMEs and midcaps) and public sector organisations. The first restricted call for EDIHs is expected to be launched in the 1st Quarter of 2021 so that the selected d EDIHs can start their operation in 2021. Given that Cyberwatching.eu is scheduled to end in June 2021, it will have scope to contact EDIHs and promote their services to be integrated as part of the services offered to SMEs. This will contribute to the sustainability of the project. This task will be carried out in alignment with Task 4.2, leaded by Digital SME. Digital SME has organised the event “Making EDIHs work for SMEs” on Monday, October 26, to analyse the role of existing industry ecosystems within EDIHs and the European added value of the EDIHs. Mr. José Lucio González Jiménez, vice-president of AEI de Ciberseguridad participated as speaker.
- **European Digital Innovation Hub (EDIH) networking event**: Cyberwatching.eu will attend this event, co-organised by Luxembourg, with the support of DIHNET and the European Commission. It will gather Digital Innovation Hubs (DIHs), designated EDIHs, regions and Member States, and various representatives of EEN, Clusters, SME associations, public sector organisations and vocational training institutes.

2.2 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.



	sep-20	oct-20	nov-20	dic-20	ene-21	feb-21	mar-21	abr-21	may-21	jun-21
List of 10 loyal clusters Responsible: AEI	▨	▨	▨	▨						
Analysis of clusters Responsible: AEI	▨	▨	▨	▨						
Define clusters area in cyberwatching.eu site Responsible: AEI & TRUST-IT			▨	▨						
Events Responsible: AEI, DSME & TRUST-IT		▨								▨
Periodic webinars (webinar series) Responsible: AEI, DSME & TRUST-IT		▨			▨			▨		
Define joint actions Responsible: AEI & all				▨	▨	▨	▨	▨	▨	▨
Surveys Responsible: all	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Promotion of Cyberwatching assets Responsible: TRUST-IT & AEI	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Virtual meetings with clusters (ClujIT, GAIA, others) Responsible: AEI, DSME & TRUST-IT	▨		▨		▨		▨		▨	
Identification of DIH Responsible: AEI					▨	▨	▨	▨	▨	▨

Figure 4 Timeline of activities and responsibilities

3 Conclusion

During the last 14 months, the project has worked to continue the collaboration with the engaged clusters and to add some other relevant clusters to stablish a symbiotic relationship with Cyberwatching.eu.

Cyberwatching.eu is facing its last year of execution, so dissemination efforts must be increased to try to guarantee the sustainability of the project. The services offered by Cyberwatching.eu have companies as end users, especially SMEs, and clusters are the instrument to reach them.

With the involvement of a few relevant clusters it is possible to give visibility by the “call effect”. If we can establish clear alliances with key clusters, the word will spread and the rest of the clusters will want to take part in the project activities and promote Cyberwatching.eu assets among their members.

SMEs have been the most affected due to the COVID-19 crisis, and more than ever clusters must support their companies to put at their disposal all the tools that facilitate the path to a risk-free digital transformation.

In these circumstances, the providential figure of EDIH arises, in the form of connected ecosystems that seek to offer digital transformation services to companies, with a strong focus on cybersecurity services. For this reason, Cyberwatching.eu must, on the one hand, consolidate the relationship with the clusters in this last mile of the project, and on the other, identify and establish synergies with the new emerging figures of EDIHs.

The role of Cyberwatching.eu as an integrator of innovative solutions (providers in the marketplace) and R&D projects (project radar) can become the key to offering services to EDIHs, as an instrument to bring together and connect Europe in a digital and cybersecurity environment.

In the next months, Cyberwatching.eu must define and organise joint actions with clusters and EDIHs, 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 and EDIHs, will be act as facilitators to integrate both worlds as successfully as possible.

ANNEX A. CLUSTERS MEMORANDUM OF UNDERSTANDING

cyberwatching.eu
The European watch
on cybersecurity & privacy

Memorandum of Understanding

THIS Memorandum of Understanding is made and entered into force as of _____ 2020

by and between

Cyberwatching.eu consortium (*Consortium*), represented by _______, ____________,

and

____________________________ (*Cluster*), represented by ___________,

(together called The Parties)

WHEREAS

The Parties see cyber-risks among the most serious global risks and acknowledge the need for a comprehensive and organic view to face the growing cybersecurity & privacy challenges;

The parties share common goals of securing European Digital Society against cybersecurity threats, of fostering and promoting EU cybersecurity and privacy in research and innovation (R&I), of maximizing synergies between R&I actions at EU and national levels;

The Parties recognize the importance of better uptake and understanding of cutting-edge cybersecurity and privacy services which emerge from Research and Innovation initiatives across Europe**.** They agree on a need of better cooperation and coordination between the European and national research initiatives and business in the field;

The parties wish to set forth their current understanding and agree to cooperate under the conditions established in the following articles.

In consideration of the mutual rights and obligations hereto, the Parties hereby agree:

1. Objective

The main objective of this Memorandum of Understanding (MoU) is to strengthen the collaboration between The Parties with an objective of promoting the uptake and understanding of cutting-edge cybersecurity and privacy services which emerge from Research and Innovation initiatives across Europe.

2. By signing this MoU, the Consortium commits to provide the Cluster with[6]:

- access to the Cyberwatching.eu Marketplace and Catalogue;
- access to the SME end-users' club and its services (for the Cluster's members);
- additional visibility (through the Cyberwatching.eu website and social media channels);
- information on the project development, main results and project deliverables;
- early access to the project results and tools;
- networking opportunities;
- invitation to the Cyberwatching.eu events.

3. By signing this MoU, the Cluster commits to support the Consortium by:

- supporting Cyberwatching.eu goals and vision;
- involving its members to the marketplace and/or SME end-users' club;
- promoting and disseminating Cyberwatching.eu results.

4. Confidentiality

The Parties agree not to disclose privacy protected information to any third party, unless expressly agreed by the concerned Parties in written.

5. Legal Nature

The Parties expressly affirm that this MoU is not a legally binding contract, but it is intended to confirm the basic settings agreed upon and the goodwill of the Parties to materialise a fruitful collaboration.

6. Duration

This MoU enters into force from the date of its signature. It will terminate when either Cyberwatching.eu is ended or when one of the Parties gives notice of termination to the other.

IN WITNESS WHEREOF, the Parties hereto have caused this Memorandum of Understanding and to be executed as of the date stated above.

Cyberwatching.eu consortium, represented by
Date

[6] The Consortium reserves the right to introduce charges for its services at any stage of the project life-spam or after its conclusion. However, the Cluster will be informed about such charges in advance, and it always retains the right to terminate the MoU.