D7.3

Dissemination strategy and activities, engagement and business opportunities - P1

Project number	883275
Project acronym	HEIR
Project title	A secure Healthcare Environment for Informatics Resilience
Start date of the project	September 1st, 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Report
Deliverable reference no.	D7.3
Workpackage	WP7
Due date	02-2022 – M18
Actual submission date	25/02/2022

Deliverable lead	IMT
Editors	Hervé Debar
Contributors	Konstantinos Lampropoulos, Eftychia Lakka (FORTH), Apostolis Zarras (TUD), Konstantina Koloutsou (STS), Michalis Smyrlis (STS), Panagiotis Rodosthenous (ITML), Celia Nilssen (NSE)
Reviewers	Michalis Vakalellis (AEGIS) Matthias Pocs (STELAR)
Dissemination level	PU
Revision	1.0
Keywords	Communication, dissemination, social networks, website, visual identity, external advisory board

Abstract

This deliverable describes the dissemination strategy put in place in the HEIR project, to facilitate the execution of the dissemination activities and maximize their impact. It provides tailored actions for several types of public, scientific, healthcare, cybersecurity and general public. It provides additional strategic information in engaging the CERT/ISAC community, which is a fast-growing set of bodies in Europe, and how to address other EU projects. It then provides ongoing and upcoming dissemination activities of particular importance for the progress of the project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275

Executive Summary

This deliverable describes the dissemination strategy put in place in the HEIR project, to facilitate the execution of the dissemination activities and maximize their impact.

It provides tailored actions for communication and dissemination towards several types of scientific, healthcare, cybersecurity communities and the general public. Scientific dissemination takes the form of publications and workshops, and is well known to the scientific community. We have specific actions for the healthcare community, which is less engaged in ICT and cybersecurity aspects. We also have specific actions towards the cybersecurity community, which is less knowledgeable about the medical sector. Finally, we have a significant dissemination effort towards the general public, to raise awareness of these issues.

It provides additional strategic information on engaging the CERT/ISAC community, which is a fast-growing set of bodies in Europe, and ways to address related EU projects. This aims at supporting this community with new methods and tools to better understand and fight cyber attacks.

It then provides ongoing and upcoming dissemination activities of particular importance for the progress of the project. In particular, we intend to speed up industry-oriented dissemination, as events are reopening in Europe.

Table of Contents

List of Figures

List of Tables

1. Introduction

This deliverable paves the way for reporting the structuration of activities in task 7.2, "Communication strategy triggering awareness and new business opportunities", and task 7.4, "Exploitation and standardization activities and links to CERTS and CSIRTS".

The proposed communication and dissemination strategy aims at developing actions that will help HEIR reach the following program goals and KPIs presented in the description of action.

Table 1 HEIR Impact and KPIs

HEIR Impact	Current implementation	KPI	Target
HEIR aims to contribute the development of the solid CSIRT Network with its technological tools and modules that can be used to raise levels of the overall security and resilience in health sector across the EU.	Establishment of links to CSIRTS and CERTS and feedback gathering on the architecture	iKPI1: Number of health sector related entities/ stakeholders	>20
HEIR will advance state of the art in the fields of (i) cyber threats identification, monitoring and protection, (ii)data exchange and protection; and machine learning – facilitated threat detection, mitigation and real-time response; (iii) a multiple-level visualisation and awareness raising mechanism	Scientific publications	iKPI4: Number of publications in the specific fields	> 5
Via HEIR Observatory module the project will construct a solid, automated information sharing network among all involved actors in the health sector.	Establishment of links to CSIRTS and CERTS and feedback gathering on the RAMA score	See iKPI1	
HEIR will focus on raising cybersecurity awareness to executives and employees in healthcare sector, defining the duties, responsibilities and communication procedures and protocols of all the members ensuring at the same time alignment with current directives and legislations; thus, significantly advancing Security Governance in health sector	Involvement of healthcare partners and EAB members	iKPI9: Number of executive members of healthcare institutions engaged to security governance practices through HEIR platform	>5

In order to successfully engage the community, the HEIR project has developed a communication strategy, that is reported in section 2. Given the specific focus of the project, section 3 explicitly addresses the issue of CERTs and CSIRTs, and of liaison with other interested parties. Section 4 reports on the progress so far in terms of deploying this strategy.

2. Communication and dissemination strategy

The communication strategy of HEIR is developed in three domains. The first domain concerns the scientific communication, where the objective is to communicate to the appropriate venues scientific advances made in the project. The second domain is health-care partners, where we need to engage the healthcare community in understanding the impact of cyberthreats and the proposed solutions included in HEIR.

2.1 Project communication and dissemination phases

Disseminating HEIR activities, progress and outcomes is of paramount importance for the consortium. HEIR's project dissemination strategy (see Figure 1) constitutes of three main phases

- The initial phase, 'Raise Awareness', included activities that would make sure that the vision, objectives and outcomes of the project will be widespread and understood both in the scientific and related stakeholder communities.
- The second phase, 'Diffuse knowledge', aims to present the initial results of the HEIR project, by demonstrating the use of the HEIR platform as well continuously update the targeted groups through HEIR's website and social media channels.
- Lastly, the 'Intensify communication' phase will be realized during the last year of the project. Its main target is to present the mature HEIR ecosystem to relevant conferences and promote the exploitation of project outcomes outside the HEIR consortium.

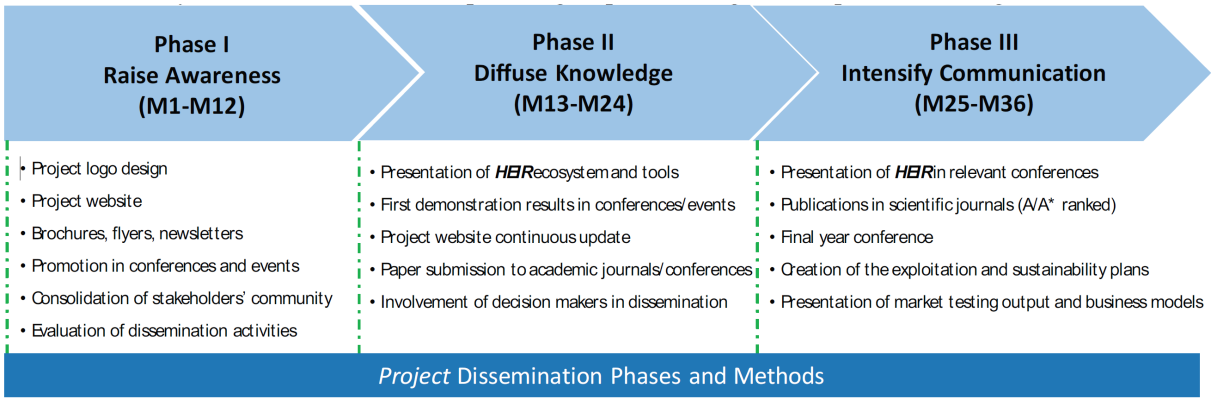

Figure 1 Project dissemination phases and methods

2.2 Dissemination and communication target groups

One of the main purposes of HEIR dissemination and communication strategy is to make the stakeholders aware of the project's new ideas, services and results and probably adopt and exploit them.

The main strategic stakeholder groupings have been identified for the dissemination and communication of the project and are:

- Key actors
  - Public/private hospitals
  - Health care institutions
  - Medical centres clinics
  - Health policy/authority and decision makers
  - European and global organisations
  - Academic and research institutions
- International networks
  - Health care networks
  - IT security associations/organizations
  - eHealth service providers
  - Technology providers
- Potential end-users
  - Medical IT/non-IT personnel
  - Hospital managers
  - Doctors
- Policy makers
  - National and EU Health Authorities
  - Health Care Decision Makers
- Other
  - Universities
  - General Public

2.3 Communication Channels

2.3.1 Project Website

The site is a key place to disseminate the research results of the project. To that end, a dedicated web site has been created for the HEIR project sharing information regarding objectives, results, partners and events.

2.3.1.1 Website Creation

The HEIR website was created at the stages of the HEIR project and it is being updated with new content so to achieve an up-to-date interaction with the public. Through this website basic information regarding the project and the relevant activities of partners are being shared to the public. In this way, key messages, and non-confidential deliverables (sharing technical and non-technical work) can be accessed by the interested third parties. Aspects such as the project architecture, work plan and innovations are described (Figure 4). The use cases considered in the project are presented. The consortium of project is also presented, acknowledging the partners that participate in the project. Apart from the non-confidential deliverables, the publications and dissemination materials are available online (Figure 3). Finally, the news of the project are posted regularly and the past or upcoming events are included (Figure 5). The aim of the website is to enhance the dissemination and communication activities within the project, fostering the further recognition of the project and its objectives.

The following subsections present several pages of the HEIR website.

2.3.1.2 Content

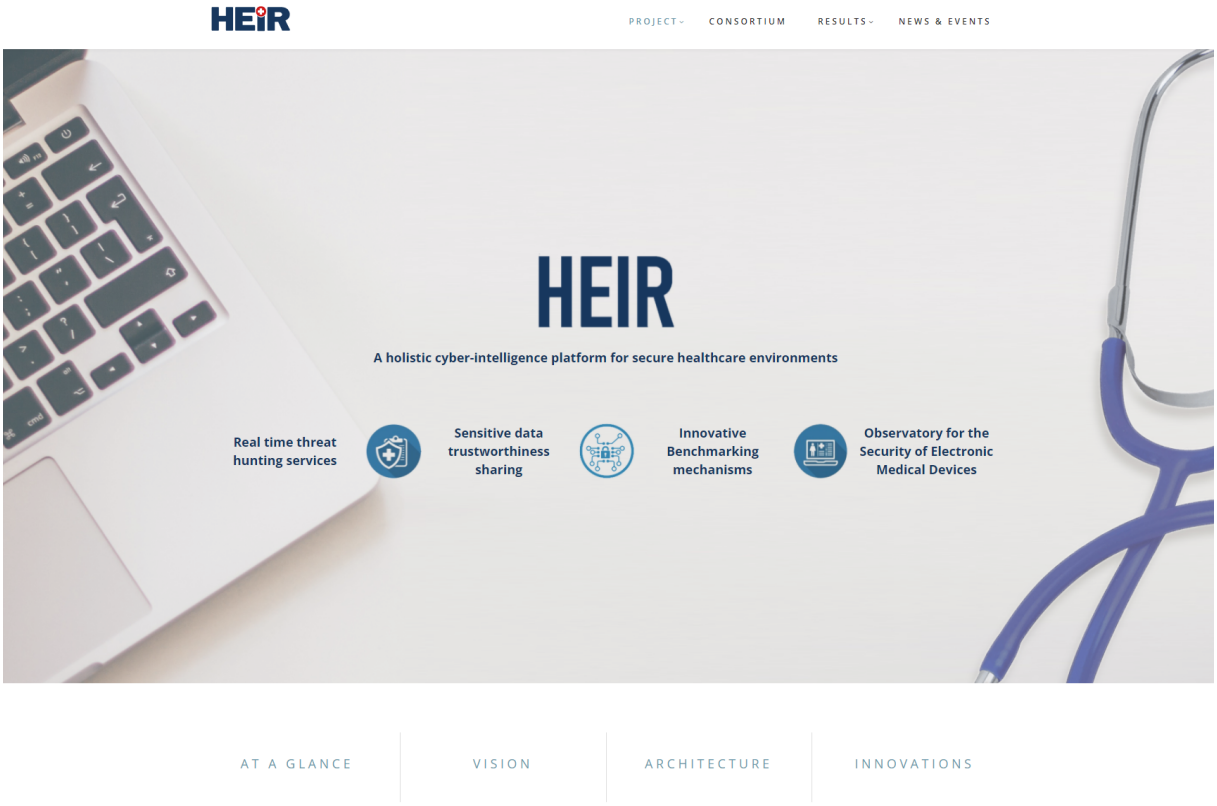

Figure 2 HEIR website landing page

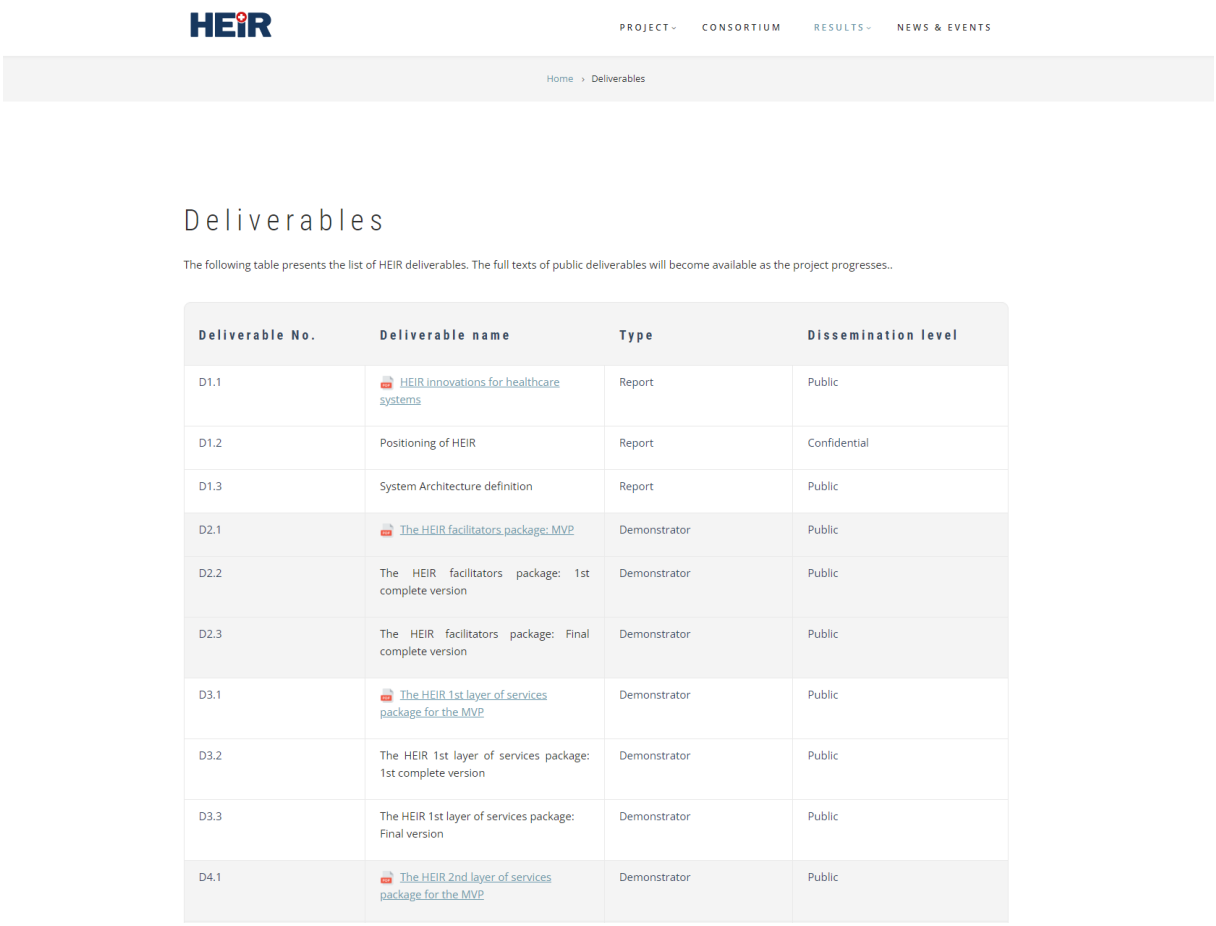

Figure 3 HEIR website deliverable page

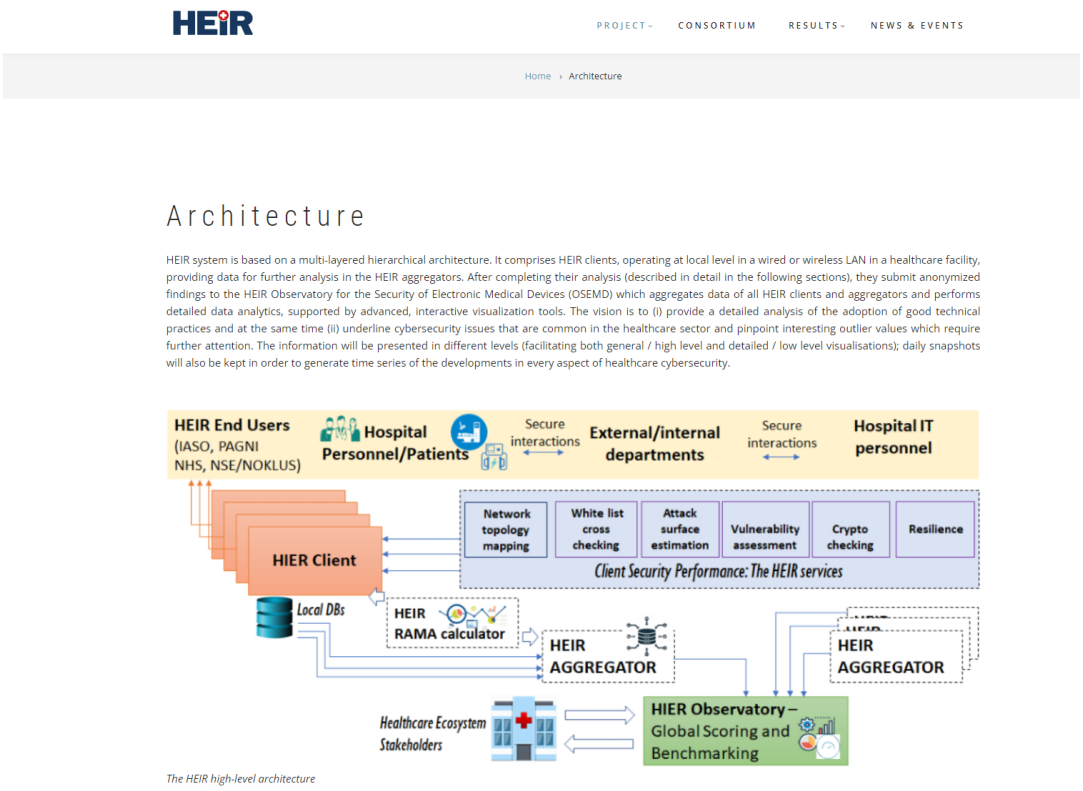

Figure 4 HEIR website technical content

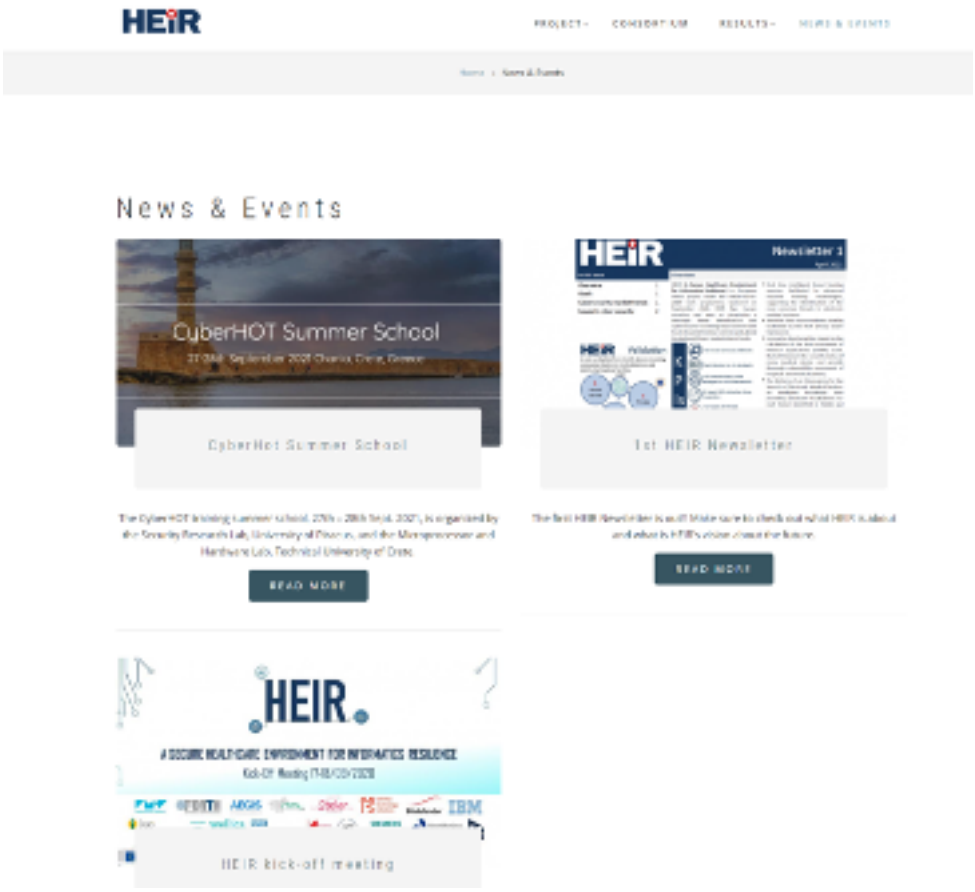

Figure 5 HEIR website news page

2.3.2 Social media channels

Social media channels play a critical role in disseminating the projects' results. HEIR considers the active presences and participation in the social media and networking streams (e.g., Twitter and LinkedIn) of utmost importance for the success of the project. Having said that, HEIR created a dissemination strategy that involves all partners. Through the dissemination of the progress and the results of, at least on a weekly basis, we aim at sharing its advancements and at steadily increasing the number of our followers, thus enhancing the impact of the project in the scientific field, as well as the industry.

In order to disseminate the results, we have created a Twitter, LinkedIn and YouTube account from where public important information will be disseminated.

2.3.2.1 Twitter account

Twitter has a million of engaged user every month from around the world. This creates an opportunity for HEIR to disseminate its results to these users. In the framework of HEIR's dissemination plan, HEIR's twitter account[1] has been created, as presented in Figure 6.

[1] https://twitter.com/h2020_heir

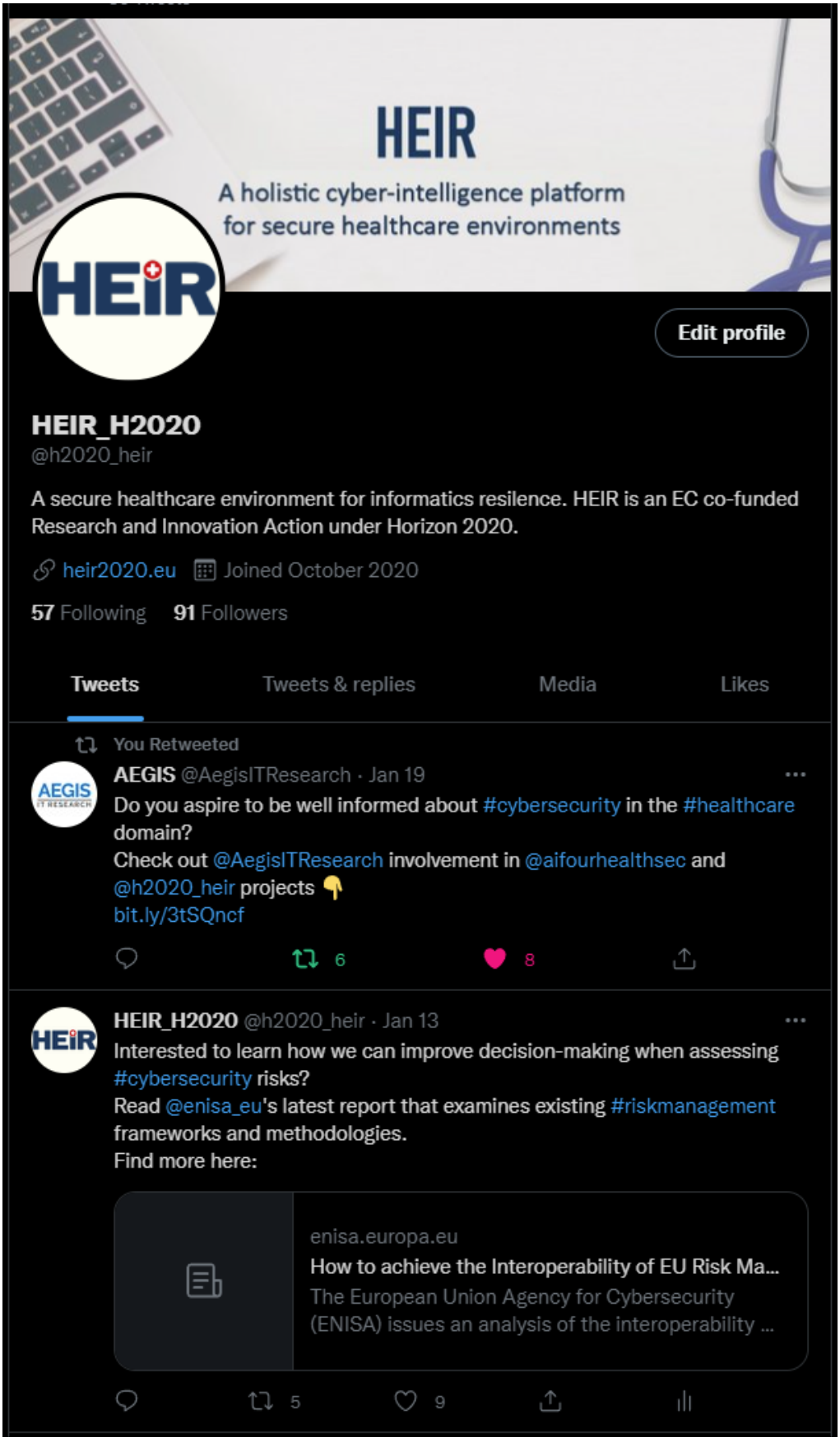

Figure 6 Twitter account

2.3.2.2 LinkedIn account

There's no better place to connect with business professionals than on LinkedIn. With almost over 690 million users and 45% of them being active every month[2], LinkedIn is the perfect place for HEIR to disseminate its results. In the framework of HEIR's dissemination plan, HEIR's LinkedIn account[3] has been created, as presented in Figure 7.

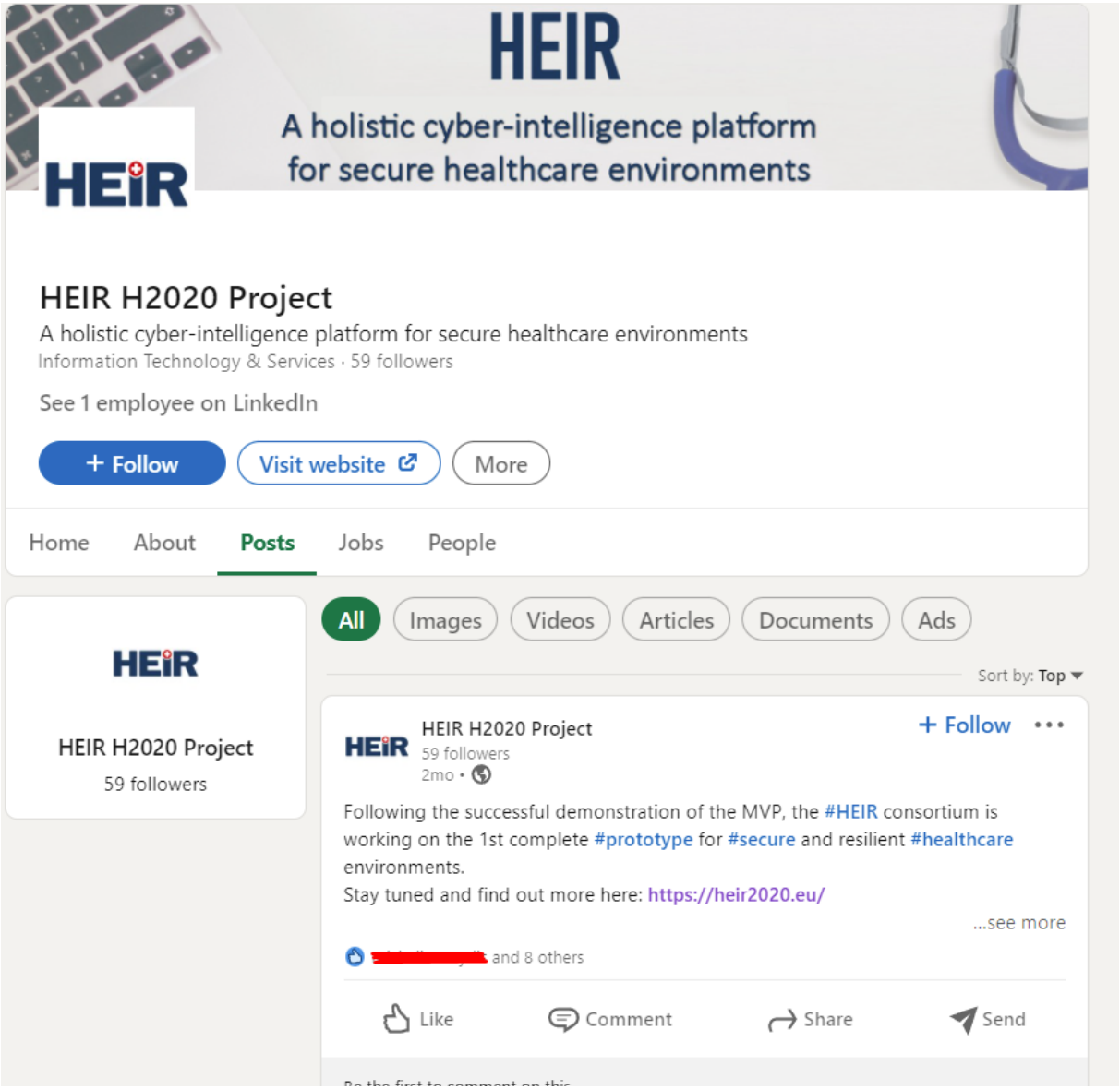

Figure 7 LinkedIn account

[2] https://tinyurl.com/linked-in-stats
[3] https://www.linkedin.com/company/heir-h2020-project/

2.3.2.3 YouTube account

Lastly, HEIR will utilise a YouTube account in order to demonstrate its platform, as well as short videos that explains the pilots scope involved within the project. In the framework of HEIR's dissemination plan, HEIR's YouTube account[4] has been created, as presented in Figure 8.

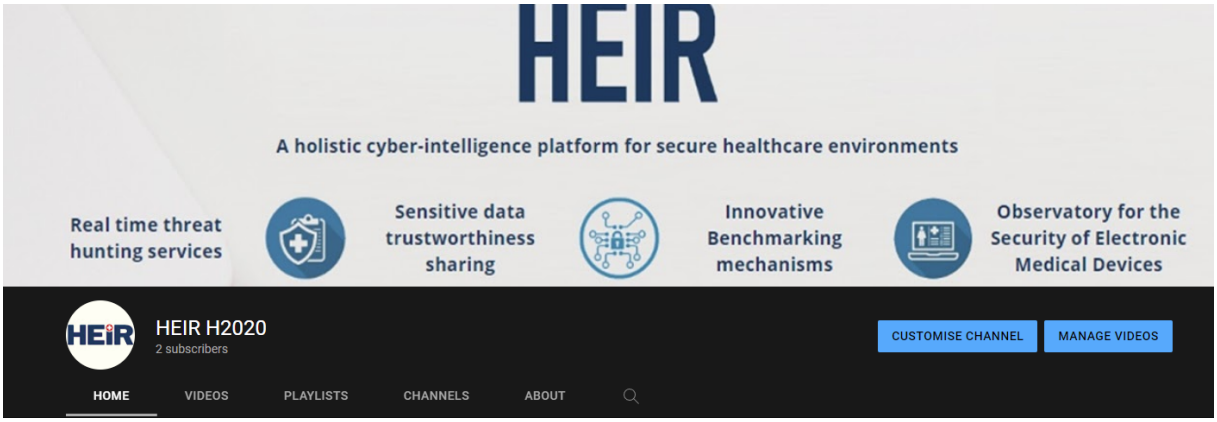

Figure 8 YouTube account

[4] https://www.youtube.com/channel/UC_boW9_lfvcZxNpbSlQ8acw

2.4 Dissemination strategy and material

2.4.1 Open access

One of the main goals of HEIR consortium is to share the knowledge on an open-access basis. The Consortium will fully address the European Commission requirements through the support of open access for published articles. All scientific publications of project's results will be granted open access. To fulfil this goal, HEIR will utilise the ZENODO open-access repository[5] and make its publications available under the Open Access Infrastructure for Research in Europe (OpenAIRE[6]) community. Lastly, we have also created the HEIR's ZENODO Community[7] (presented in Figure 9) to make it easier for interested parties to locate HEIR related material.

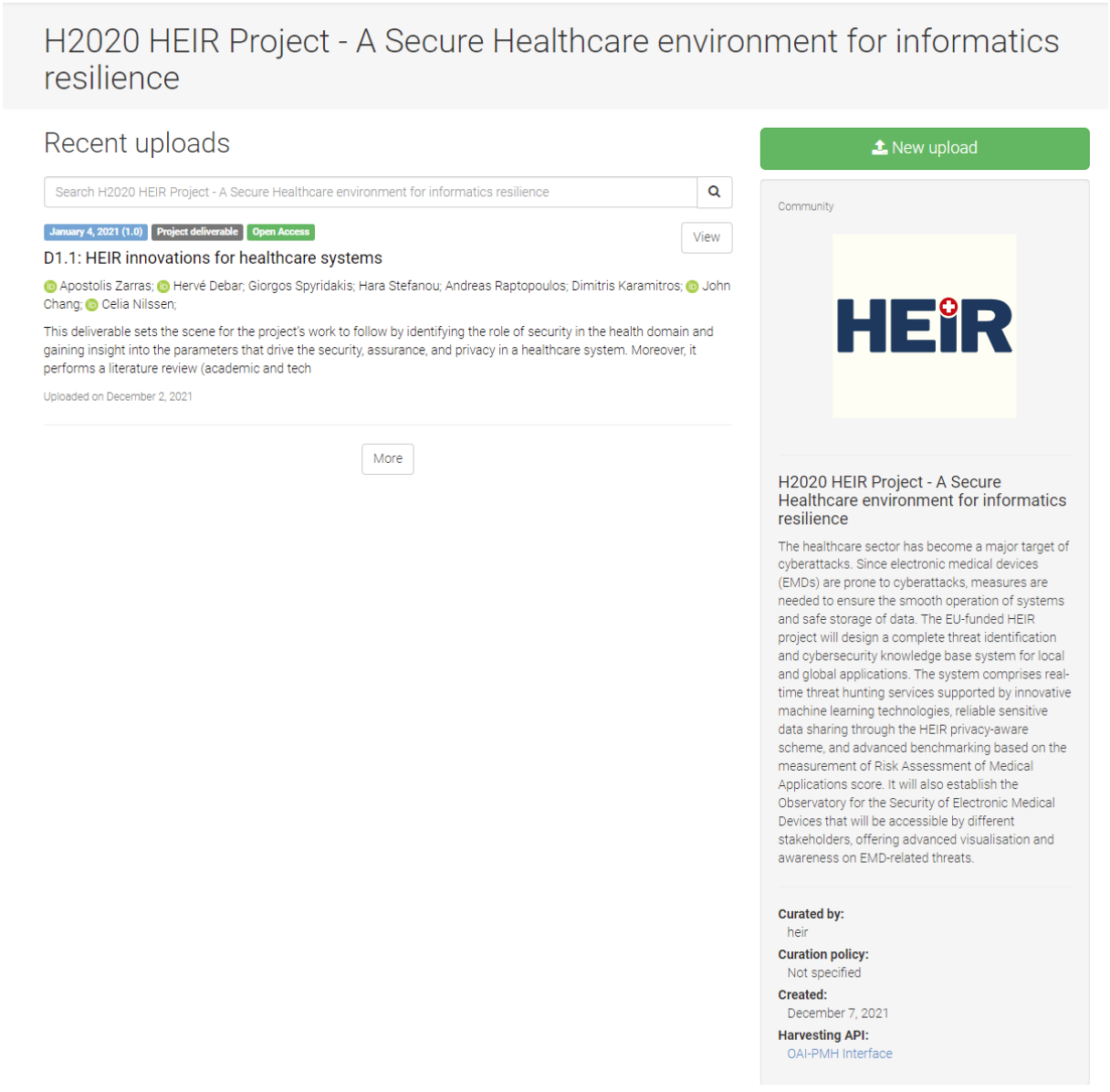

Figure 9 Zenodo Community

[5] https://zenodo.org/
[6] https://www.openaire.eu/
[7] https://zenodo.org/communities/heir_project/

2.4.2 Scientific dissemination

In terms of scientific dissemination, the HEIR project relies on publications by its members in scientific venues. We focus our contributions on cybersecurity and healthcare journals or conferences held in Europe, with preferably open-access proceedings. Preprint versions of our papers will be made available through open access media. The targeted groups of scientific communication are the scientific/research community, industrial companies, and SMEs.

In addition, the project will organize workshops in relevant cybersecurity conferences. The ongoing actions are presented in section 4.1.

2.4.3 Healthcare-oriented dissemination

Healthcare professionals are generally not IT professionals, and their level of understanding of cybersecurity issues is generally low. They focus on functionality, security in physical patient interaction and treatment, and trust between peers. As such, they are often vulnerable to social engineering attacks (in addition to attacks that target medical devices directly through software vulnerabilities). This particular state of mind requires specific communication strategies adapted to non-technical personnel.

Within HEIR, expertise on communication with the healthcare community is brought in by the healthcare partners, providing use cases. These partners develop specific material and addresses to their communities, sustaining the penetration and understanding of cybersecurity issues and proper remediation within the EU healthcare community.

Availability of health data for quality improvement, interoperability and research work is subject to national strategic efforts in several countries, and thus will be addressed especially by the use cases in the scope of cybersecurity communication. Dissemination activities in connection to the use cases will involve user representants and university/higher education institutions.

In addition, two of the External Advisory Board members are representatives of the healthcare community:

- Dr. Nada Y. Philip (Senior Member, IEEE) received the Ph.D. in mHealth, with the thesis title 'Medical Quality of Service for Optimized Ultrasound Streaming in Wireless Robotic Tele-ultrasonography System,' from Kingston University London, U.K., in 2008. She is currently an Associate Professor in the field of mobile health (mHealth) with Kingston University London. She is the Founder of the research group Digital Media for Health in 2012. Her research interests are mainly in the advancement and challenges of data and multimedia communication, networking and mobile computing for healthcare applications. The challenges include; privacy and security, interoperability and reliability. She is the PI and Co-PI of many national and international mHealth projects in the areas of personalized health for Diabetes, Cancer, Autism and COPD conditions, 5G health, cloud computing, IoT, Big data analytics for health, social robotics for health, End to End QoS, and QoE in medical video streaming. She is the author and co-author of more than 80 peer-reviewed papers. She is a member of the editorials and the review panels for many journals, including the IEEE-IoT and JSAC. She is the Editor of the IEEE e-health TC newsletter. She is a reviewer on both the MRC and the NIHR funding research bodies. She is currently leading on the privacy sub-group in the International IEEE standards of the Clinical IoT Device and Data Interoperability with TIPPSS (Trust, Identity, Privacy, Protection, Security and Safety). She is a fellow of the Higher Education Academy, and a Senior Member of the IEEE Communication Society and the IEEE Engineering in Medicine and Biology Society (EMBS).
- Saber Aloui, PhD, is the CIO of the Groupe Hospitalier Bretagne Sud in Lorient, France.He is responsible in his organization to manage staff and outsourced resources (70 engineers and technicians), define security and privacy requirements, and manages IT services deployment for the hospitals. His particular focus in cybersecurity is related to crisis management, and he has a

significant experience in deploying crisis exercices demonstrating how hospitals can handle a cybersecurity incident.

These two external experts will bring significant expertise reviewing the communication material of the project oriented towards the healthcare community.

An EAB hybrid meeting is planned in June 2022 to present the first prototype to the EAB.

2.4.4 Cybersecurity-oriented dissemination

From a cybersecurity perspective, the healthcare sector is a critical infrastructure; thus, it must receive the tools needed to comply with the relevant regulations. The HEIR project includes several major cybersecurity tools and services providers (Siemens, BitDefender, IBM, Aegis, ITML, Sphynx, Wellics) that have a direct interest in communicating the results of HEIR to prospective or existing customers.

In order to present the results of HEIR to the wider cybersecurity community, the project will participate in industry fora to present the results of the project. We are continuously monitoring event announcements to determine if there are occasions to participate and have a positive impact for the project. The ongoing actions are presented in section 4.1.

2.4.5 Brochure

A paper and electronic brochure in English, enriched with the scientific approach and activities of HEIR, will be developed, in order to serve as an essential tool for the dissemination at external events targeting academic and research institutes, industrial partners and clinical experts. The brochure will be updated regularly with HEIR's latest achievements and results. The printed brochure will be translated and distributed to the general public, in order to invite them to participate in the project. This leaflet will be distributed by all project partners at the public events, such as conferences but also local events raising awareness amongst potential users.

2.4.6 Newsletters

Starting from M4, HEIR creates quarterly newsletters including:

- reporting the news of project
- information about the next project events and how to participate
- presence on events
- publication in journals
- research advancement and results
- other relevant news

The newsletters are published in HEIR's social media channels and the website and is available for download.

3. Stakeholders' engagement and ecosystem building between CERTs and healthcare providers

This section presents the initial version of the report concerning the activities of Task 7.3, which focus on building a community and an ecosystem around the HEIR's results. This work includes networking and liaisons with technical and domain-specific communities by creating live operational liaisons with EU associations (i.e. EuroVR, BDVA), standardization bodies, organisation of stakeholders' workshops, linking with other H2020 projects and EU CERTs/CSIRTs. The establishment of these links will assist the achievement of two objectives. Firstly, it will provide useful insights on the efficacy and added value of the platform through the hands-on experience of the platform and the feedback received and secondly it will assist the adoption and longevity of HEIR's outcomes even after the project's end.

Specifically, in this deliverable, the initial report of all the activities under the Task 7.3 is provided, including the results from the first half of the project's duration and the plan for the successful establishment of active liaisons during the second half of the project's lifetime. The final version will be submitted in the next iteration of the deliverable at M36.

For the analysis of the said activities, next subsections provide more details about the ***methodology*** that was used to identify the liaisons and provides the first plan for the liaison activities; the ***liaison opportunities***, in which we identify the liaison activities that can be pursued throughout the lifespan of the project; the ***reported activities and outcomes*** so far. The annex of this document include the invitation letter and information sheet that was sent to the EU CERTs/CSIRTs in order to invite them to the liaison activities of HEIR.

3.1 Methodology

A simple methodology will be followed for the liaison activities of HEIR, Identify, Contact, Connect, Participate and Maintain.

1. **Identify** all the potential liaison links within the consortium. This is achieved through a shared file where each partner lists all liaison links that can be exploited by HEIR. This is a living document that is regularly updated by consortium partners. We target mainly EU CERTs/CSIRTs, ISACs, SMEs/Public Sector and other EU-Funded projects. This is a continuous process that is supported by the whole consortium.
2. **Contact**. After the collection and identification of all potential links, HEIR will initiate the contact with them either as a consortium via specific partners or through each individual partner. The goal of this stage is to provide initial information on HEIR's goals, achievements and offerings to the liaison contacts in order to connect and establish operational liaison links.
3. **Connect**. At this stage we will be receiving all the requested contact information and consents for establishing the communication links between our project and the external counterparts. These initial connection activities will allow us to present HEIR's visions and objectives in more details, set the joint objectives and plan ahead for activities that will produce useful results both for HEIR and the external partner.
4. **Participate**. This is the stage, where the planning of activities continues while most of the planning is materialized into specific events and activities. These events will be the backbone of the liaison activities providing to external contacts/participants access to the HEIR's framework internals, the architecture and access to the platform and its features for using it and providing feedback to the consortium
5. **Maintain**. This last stage refers to the maintenance of the liaison links through specific activities e.g. workshop, conferences, trainings and try to activate HEIR's exploitation plan, achieving bilateral agreements that will ensures HEIR's sustainability even after the project's end.

In this first stage of task 7.3 we focused on the first three (3) steps of the aforementioned methodology. So, we set the initial plan, the processes and files and managed to identify various

stakeholders for our liaison activities. Up to the time of this writing, we prepared and sent out invitation focusing firstly on the difficult task of creating links with the largest possible number of CERTs/CSIRTs. We have received acceptance letters by four CERTs/CSIRTs - ISACs, thus achieving steps one up to three from our proposed methodology. Moreover, we plan to participate in numerous activities promoting HEIR objectives and identifying potential liaison links, which is part of step 4 of our methodology.

3.2 Liaison opportunities with EU CERTs / CSIRTs – ISACs

In order to recognize all the existing links with EU CERTs/CSIRTs the CSIRTs list inventory by ENISA [1] was provided to the partners in order to find all the connection points that can be exploited for the purposes of Task 7.3. Moreover, extensive research has been conducted to find ISACs, specifically by the health sector, taking to account the ENISA report for ISACs in Europe [2]. Through that process fifteen (15) CERTs/ CSIRTs and one (1) ISAC were identified and are presented in Table 2, based on this list invitations were sent out.

Table 2: EU CERTs/CSIRTs -ISACs invited to participated in HEIR's Liaison activities

Full name	Constituency	Country	Contact point
GRNET-CERT	NREN, NIS appointed	Greece	FORTH
National Authority Against Electronic Attacks (NAAEA) – National CERT	Government	Greece	FORTH
Greek military Cert	Government	Greece	FORTH
CERT POLSKA	NREN, National	Poland	FORTH
CZ.NIC-CSIRT	Non-Commercial Organisation	Czech Republic	FORTH
CERT-EU	EU Institutions	European Union	FORTH
Computer Emergency Response Team Austria	National	Austria	FORTH
CSIRT Malta	National	Malta	FORTH
National CSIRT-CY	CIIP, Government, National	Cyprus	FORTH
National Cyber Security Centre (NCSC – NCKB in Czech)	Government, Private and Public Sectors	Czech Republic	FORTH
Computer Security Incident Response Team - Italia	Government, National	Italy	FORTH
Information Technologies Security Incident Response Institution (CERT.LV)	Government, National	Latvia	FORTH
Norwegian healthcare sector CERT	Government	Norway	FORTH

Full name	Constituency	Country	Contact point
The Norwegian National Cyber Security Centre	National	Norway	FORTH
Vysočina Region Regional Authority	Regional Authority	Czech Republic	FORTH
Empower European ISACs	EU	European Union	FORTH

3.3 Liaison opportunities with SMEs / Public Sector

Public sector and initiatives of public sector are also targeted in order to promote HEIR's outcomes and create operational links via the participation of individual partners or bilateral cooperation with HEIR consortium. At the moment we have not identified specific SMEs that will participate in the liaison activities but when the prototype and a mature version of HEIR are released we will reach out to the SME community through the PRAXI network [3]. The current identified stakeholders as well as the involved HEIR partner are depicted in Table 3.

Table 3: List of SME Associations, Public Bodies

External Stakeholder	Type	Involved Partner	Description
ENISA - European Union Agency for Cybersecurity	EU-Agency/Policy Maker	FORTH	Prof. Sotiris Ioannidis of FORTH is a member of ENISA Advisory Group (AG).
PRAXI Network	Technology Transfer Organization / SME association	FORTH	It is a distinct administrative unit operating within the Foundation for Research and Technology – Hellas (FORTH).
Big Data Value Association (BVDA) - SRIA	Public-Private Partnerships	IMT, FORTH, ITML	IMT, FORTH, ITML are members of the Big Data Value Association (BVDA) from the European Public Private Partnership on Big Data Value (PPP BDV). Thus, the project will be aligned with PPP activities like SRIA.
ECSO	Industry association	FORTH	FORTH is a core member of the ECSO-cPPP.
5G-PPP / SNS JU	Public-Private Partnerships	FORTH, IMT	FORTH and IMT are involved in the Security WG.
ECSO-PPP	Public-Private Partnerships	IMT	IMT is a member of ECSO-PPP elected at the partnership board and present in the research and education working groups.
ETSI, ETSI TC Cyber	Public-Private Partnerships	IMT	IMT is involved in ETSI, both from an IoT and cybersecurity standpoint. IMT was formerly the vice-chair of the Information Security Indicators (ISI) Industry Specification Group, whose activities are now maintained in ETSI TC Cyber.

External Stakeholder	Type	Involved Partner	Description
M2M, MPEG4 and 3GPP	Public-Private Partnerships	IMT	IMT is involved in M2M, MPEG4 and 3GPP standardization activities and in the AIOTI alliance.
I-MECH project under ECSEL JU	Public-Private Partnerships	ITML, WEL	ITML is dissemination/exploitation/communication manager in I-MECH project under ECSEL JU.
Orange Grove	Public-Private Partnerships	WEL	WEL is a member of the London ecosystem of wellness start-ups and of Orange Grove.
Israeli Public Committee for the Protection of Privacy» and «National Retail Federation (ARTS)»	Public-Private Partnerships	IBM	Partners from IBM are involved in protection/privacy reporting and guidance prevision to «Israeli Public Committee for the Protection of Privacy» and «National Retail Federation (ARTS) ».
LEAs	Public-Private Partnerships	BD	BD is actively supporting public entities (LEAs) in fighting against cybersecurity attacks, threats and risks.
Dark-Net criminal activities	Public-Private Partnerships	BD	BD is involved in tackling Dark-Net criminal activities, providing ransomware solutions or advising on imminent malware threats.
World Health Organization (WHO) Collaborating Centre for Telemedicine and eHealth	Public-Private Partnerships	NSE	NSE is now in its 18th year as a WHO Collaborating Centre within e-health and telemedicine.
NHS	Public-Private Partnerships	CUH	Croydon Health Care NHS Trust is part of the wider NHS structure within the UK. Any projects that could materially improve NHS function can be show cased at national and international meetings. Exploitation via Health Innervation Networks (HIN).
South London Clinical Research Network (SL CRN)	Public-Private Partnerships	CUH	Croydon Health Services NHS Trust is a member of the South London Clinical Research Network. Projects and developments could be disseminated in formal and informal meetings within the network.

3.3.1 Liaison opportunities with other EU Projects

HEIR envisions to create a number of active connections with other H2020 project that can cooperate and benefit from HEIR and vice versa. An initial list of projects was compiled based on the participation of HEIR partners to other funded projects and initiatives were created.

Moreover, through partners' link we plan to promote HEIR propositions, receiving feedback and create joint initiatives like webinars. Table 4 depicts the affiliated projects in which partners directly participate, as well as projects that are relevant to our objectives and scope. Throughout the project's duration we will try to establish operational links with them.

Table 4: Affiliated EU projects

Name	Type	Involved Partner	Description
Aegle	H2020 funded project	CUH	Aegle involves handling of Big data in 3 disease models: ITU setting, Type 2 diabetes, and genomic data for Chronic lymphatic leukaemia. The projects involve anonymisation of big data, transmitting it over the internet safely and securely for analysis to be performed on summated data.
Welcome	EU FY7 programme	CUH	Development of wearable devices for remote management of COPD
C4IIoT	H2020 funded project	FORTH, AEGIS, ITML, STS	C4IIoT aims to deploy a cybersecurity framework focusing on addressing challenges in manufacturing environments of the automotive industry
CONCORDIA	EU Cybersecurity Pilot Project	FORTH	Prof. Sotiris Ioannidis of FORTH is acting as deputy Coordinator of this Pilot Project.
SPARTA	EU Cybersecurity Pilot Project	IMT	IMT is coordinating one of the research programs of SPARTA and the task on professional education
SOCCRATES	European project on network security	IMT	It is a project that has proposed a model for threat detection and mitigation in critical infrastructures. The contribution of IMT concerned the development of the Return on Response Investment (RORI) indicator, that helped operators select the appropriate countermeasure when facing cyberattacks against critical infrastructure
Full Flow of Health Data Between Patients and Health Care Systems	The Research coucil of Norway	NSE	The project aim to a collective expertise on national level archetypes, the security of technologic communication for medical purposes and economic understanding of how mobile health tools can and should be integrated into a medical system will benefit not only patients but health actors too.

Name	Type	Involved Partner	Description
Diabetes Digital Guidelines	Northern Norway Regional Health authorities	NSE	Design and validation of instruments to assess efficacy, effectiveness and safety of apps and online resources aimed at Norwegians with diabetes.
The need for new evaluation methods for eHealth and mHealth services – study of a dynamic concept for efficient trials	Northern Norway Regional Health authorities' research fund	NSE	Project goals are to identify the factors that hinder or facilitate the successful completion of eHealth and mHealth intervention studies, and to increase our knowledge and ability to perform more efficient and effective studies in the future by addressing these factors.
PREVISION	H2020 funded project	UM	The mission of PREVISION is to empower the analysts and investigators of LEAs with tools and solutions not commercially available today, to handle and capitalize on the massive heterogeneous data streams that must be processed during complex crime investigations and threat risk assessments
MaTHiSiS	H2020 funded project	UM	This product-system consists of an integrated platform, along with a set of re-usable learning components, which will respond to the needs of a future educational framework, and provide capabilities for: i) adaptive learning, ii) automatic feedback, iii) automatic assessment of learner's progress and behavioral state, iv) affective learning and v) gamebased learning
RESIST	H2020 funded project	FORTH, STS	RESIST aims to develop a physical infrastructures safety and security monitoring framework. SPHYNX's focus is on security
AI4HEALTHSEC	H2020 funded project	AEGIS, STS, FORTH	AI4HEALTHSEC proposes a state of the art solution that improves the detection and analysis of cyber-attacks and threats on Health Care Information Infrastructures (HCIIs), and increases the knowledge on the current cyber security and privacy risks.
CyberSane	H2020 funded project	FORTH, STS	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures. Protecting critical information infrastructure from cybercriminals.

Name	Type	Involved Partner	Description
SMART-BEAR	H2020 funded project	FORTH, STS, IBM	The aim of the SMART BEAR platform is to integrate heterogeneous sensors, assistive medical and mobile devices to enable the continuous data collection from the everyday life of the elderly, which will be analysed to obtain the evidence needed in order to offer personalised interventions promoting their healthy and independent living.
ASCAPE	H2020 funded project	FORTH, STS	The main objective of ASCAPE is to take advantage of the recent ICT advances in Big Data, Artificial Intelligence and Machine Learning to support cancer patients' quality of life and health status.
PUZZLE	H2020 funded project	FORTH, AEGIS	PUZZLE will implement a highly usable cybersecurity, privacy and data protection management marketplace targeted at SMEs&MEs that enables them to monitor, forecast, assess and manage their cyber risks through targeted cybersecurity services, increase their cybersecurity awareness through the efficient heterogeneous information processing, the establishment of knowledge sharing with other SMEs&MEs and extract insights based on advanced analytics.
CYRENE	H2020 funded project	ITML, STS	CYRENE vision is to enhance the security, privacy, resilience, accountability and trustworthiness of Supply Chains (SCs) through the provision of a novel and dynamic Conformity Assessment Process (CAP) that evaluates the security and resilience of supply chain services, the interconnected IT infrastructures composing these services, and the individual devices that support the operations of the SCs.

4. Report on Activities, Outcomes and Future plans

In this subsection, we will report all the work done and the liaisons achieved in this first period of the task (M1-M18). In the following, we will describe what we have achieved so far in each of the categories of targeted liaisons.

4.1 Participation in venues

Given the covid pandemic and the difficulty in organizing events, we have little to report at this stage.

Concerning the cybersecurity community, we are currently planning activities at Security Research Event 2022, March 1-2 2022, in Paris, France, and at Forum International de la Cybersécurité, June 7-9 2022, in Lille, France. The later venue is a major industry-oriented event in France and constitutes a great opportunity for the industry partners to pitch the advances realized in HEIR.

We are also forecasting attendance at FIC 2023, end of January 2023 in Lille.

Concerning the research community, we are currently planning a workshop during the ARES 2022 conference.

We have taken the opportunity to present the project to our partners. The project has been presented to Accenture at the Télécom SudParis information forum on the ICT and healthcare track ("parcours santé"[8]). Accenture is a major provider of consulting services on IT related topics to healthcare organizations. Other seminars will present the project to the other partners of the track.

4.2 Report on EU CERTs / CSIRTs – ISACs Liaison Activities

As mentioned above (see Subsection 3.2), we identified fifteen CERTs/ CSIRTs established in EU, based on ENISA's Inventory [1] and one (1) ISAC based on ENISA report for ISACs in Europe [2]. We sent out sixteen (16) invitations describing HEIR proposition and our requesting their participation in HEIR's liaison activities. We received back five (5) responses four (4) of them were positive, one negative and up to the time of this writing we have not received responses from the rest. Table 5 presents the status of each invitation accompanied with some details on the dates of the communication and some brief explanation where needed. The Invitations that were sent are depicted in ANNEX I Invitation sent to EU CERTs/ CSIRTS - ISACs of this deliverable and the file with the initial presentation of HEIR that was shared is present in ANNEX II HEIR Information sent to EU CERTs/CSIRTs - ISACS.

Based on the results so far we are in discussion internally in order to send to the external contacts/participants a questionnaire about HEIR's architecture and exploitation activities in order to request their feedback to the consortium. Also, we plan to propose to the respective external parties to identify the number and dates of the hands-on workshops regarding the collaboration and knowledge exchange between HEIR and the CERTs/CSIRTs - ISACs community. All these activities will be reported in the second (final) iteration of this deliverable (M36).

[8] https://www.telecom-sudparis.eu/formation/ingenieur-generaliste-parcours-sante/

Table 5: EU CERTs/CSIRTs – ISACs liaison status

Full name	Country	Contacted on	Status(date)
GRNET-CERT	Greece	09/09/2021	Accepted (03/10/2021)
National Authority Against Electronic Attacks (NAAEA) – National CERT	Greece	09/09/2021	Response Pending
Greek military Cert	Greece	09/09/2021	Response Pending
CERT POLSKA	Poland	09/09/2021	Accepted (10/09/2021)
CZ.NIC-CSIRT	Czech Republic	09/09/2021	Response Pending
CERT-EU	European Union	09/09/2021	Response Pending
Computer Emergency Response Team Austria	Austria	09/09/2021	Response Pending
CSIRTMalta	Malta	09/09/2021	Response Pending
National CSIRT-CY	Cyprus	09/09/2021	Response Pending
National Cyber Security Centre (NCSC – NCKB in Czech)	Czech Republic	09/09/2021	Response Pending
Computer Security Incident Response Team - Italia	Italy	09/09/2021	Response Pending
Information Technologies Security Incident Response Institution (CERT.LV)	Latvia	09/09/2021	Declined (13/09/2021)
Norwegian healthcare sector CERT	Norway	09/09/2021	Response Pending
The Norwegian National Cyber Security Centre	Norway	09/09/2021	Response Pending
Vysočina Region Regional Authority	Czech Republic	09/09/2021	Accepted (01/11/2021)
Empower European ISACs	European Union	09/09/2021	Accepted (17/09/2021)

4.3 Report on SMEs / Public Sector Liaison Activities

We have identified a number of links that can be exploited throughout the lifespan of HEIR. All the so far identified connections are depicted in Table 3. For the liaison activities of the SMEs and Public Sector, we are currently relying on the individual activities of each involved partner. Once the Beta release of HEIR will be available, we will exploit these liaison links to further promote the technical advances and capabilities developed in HEIR to the SME community and Public sector.

4.4 Report on EU Projects

The initial list of identified projects is presented in Table 4. At the time of this writing, we have identified seventeen (17) related projects; most of them partners from HEIR's consortium are also full partners in the respective project creating a direct communication and collaboration link when possible.

5. Conclusion

Deliverable 7.3 reports on the HEIR dissemination strategy and provides elements related to the execution of this strategy during the first project period.

While several actions have taken place, it is clear that Covid19 has had an impact on the execution of the strategy, such as participation to events or organization of workshops. Most scientific conferences have gone fully virtual, and events such as FIC have been cancelled or moved in time during this first period of the project.

At the time of writing this deliverable, we have a strong plan in place, and significant dissemination activities, both industrial and scientific, planned in the coming 6 to 8 months.

6. References

[1] ENISA CSIRT Inventory – "CSIRTs by Country - Interactive Map", https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[2] ENISA - Information Sharing and Analysis Center (ISACs) - Cooperative models https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

[3] PRAXI Network, https://praxinetwork.gr/en/

ANNEX I Invitation sent to EU CERTs/CSIRTS – ISACs

Dear «Name»,

I am writing to invite you to participate in the creation of an operational link between your organization and "HEIR: a secure Healthcare Environment for Informatics Resilience"[1] EU-funded project. Through that link, we will be able to interact, cooperate and exchange valuable information for arising threats in electronic medical systems, new approaches of sensitive data trustworthiness sharing and risk assessment of medical applications, with the focus on preventing future incidents and raising security awareness in healthcare domain overall.

*Moreover, being part of the **HEIR** ecosystem will give you the chance to get updated with the major developments of **HEIR** framework, test and provide valuable feedback that will assist us in the creation of the final **HEIR platform**.*

Please respond to this letter, via email, stating that you are interested in collaborating with our project and we can contact you, or any other contact person that you will provide, in the future for discussions and common collaborative actions.

On behalf of HEIR Project,
Eftychia Lakka,
elakka@ics.forth.gr

HEIR Contact details:
Website: https://heir2020.eu/
Project Coordinator: **Prof. Hervé Debar**
e-mail: **herve.debar@telecom-sudparis.eu**

[1] https://heir2020.eu/

ANNEX II HEIR Information sent to EU CERTs/CSIRTs - ISACS

HEIR: a secure Healthcare Environment for Informatics Resilience

HEIR at a Glance

HEIR will design and deploy an **Electronic Medical Devices Cybersecurity Framework** that will facilitate intelligent threat identification and hunting services leading to the delivery of the envisioned **Risk Assessment of Medical Applications** (RAMA). The outcome of these analyses will be available to the IT personnel responsible for the medical devices. More to that, the RAMA client software will submit anonymized statistical data to a central server which will host the envisioned **Observatory for the Security of Electronic Medical Devices** (OSEMD). The Observatory will provide statistics for each threat identified in the EMD Risk Index Score through advanced visualization tools. Therefore, the medical IT Personnel and the hospital manager will be able to measure how well the specific hospital or medical center performs compared to average aggregated mean scores. The client will identify outlier values to medical IT personnel, highlight issues, which require actions and suggest possible solutions to improve the RAMA and minimize risks. This information will be available via the RAMA client to the IT medical personnel only. OSEMD will be a web-based platform accessible to stakeholders, scientists, researchers, hospital managers, medical IT personnel, public servants, law enforcement agents, legislators, **CERTs and CSIRTs**. It will comprise intelligent knowledge-base and interactive visualization tools and its focus will be on depicting the landscape of cyberthreats for electronic medical devices, detailed cybersecurity assurance statuses, and their evolution over time. It will provide insights about the sectors that require further attention and raise awareness to the health services ecosystem. Finally, it will regularly publish the best practices and recommendations based on the analysis of the collected data.

HEIR's Impact

The HEIR consortium has developed an Impact Maximisation strategy that is based on four fundamental pillars presented below:

- **Pillar 1 - Mission-oriented approach**: The project focuses on cracking specific challenges on ICT impact assessment addressing rising challenges that many European and non-European countries face nowadays.
- **Pillar 2 – Openness**: The project prioritises strengthening open science through open-access sharing of knowledge and cross-fertilisation with other EU funding programmes and policies.
- **Pillar 3 - Sustainability**: HEIR heavily invests in research and innovation in order to produce new knowledge and advance existing one, ensuring a sustainable growth for the technological advancements that will be delivered.
- **Pillar 4 - Public engagement**: HEIR aims to effectively engage citizens and secure their support to promote breakthrough innovation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275.

HEIR Architecture

HEIR system is based on a **multi-layered hierarchical architecture.** It comprises **HEIR clients,** operating at local level in a wired or wireless LAN in a healthcare facility, providing data for further analysis in the **HEIR aggregators.** The vision is to (i) provide a detailed analysis of the adoption of good technical practices and at the same time (ii) underline cybersecurity issues that are common in the healthcare sector and pinpoint interesting outlier values, which require further attention. The information will be presented in different levels (facilitating both general / high level and detailed / low level visualisations); daily snapshots will also be kept in order to generate time series of the developments in every aspect of healthcare cybersecurity. The HEIR System is also **modular;** it can be further extended to support new types of threats and provide additional recommendations. It can also be modified to support different and more complex healthcare environments. A deeper hierarchical architecture ensured with the provision of HEIR Aggregator. In large healthcare environments as a hospital with many departments, different types of medical devices and subnetworks, a single HEIR client may not be enough to support the IT administrators understanding all the necessary details for every department. The HEIR Aggregator will collect the data from all HEIR Clients, will make the necessary evaluations and assessments for each HEIR Client and finally will provide detailed feedback. Thus, the HEIR Aggregator will be acting as a ***"1st level HEIR Observatory"***, assisting the IT personnel to identify which departments in the hospital face critical cybersecurity issues. The HEIR Aggregator will also operate as a ***1st level cybersecurity and resilience benchmarking tool,*** comparing the cybersecurity status at an organizational level. The aggregated information is further transmitted to the global HEIR Observatory so as to extract the cybersecurity and resilience benchmark score of the whole organization in comparison with the global trends documented from other organizations.

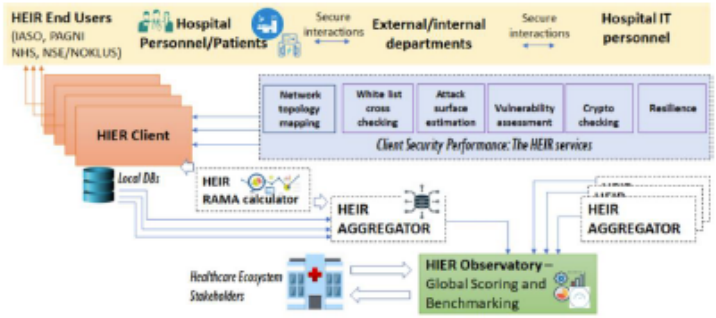

Figure 1. The HEIR high-level architecture.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275.