Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

Grant Agreement: 786698

D9.6 Disseminations activities report (4th report)

Work Package 9: Dissemination and exploitation

Document Dissemination Level

P	Public	☒
CO	Confidential, only for members of the Consortium (including the Commission Services)	□

Document Due Date: 30/04/2020

Document Submission Date: 29/04/2020

Co-funded by the Horizon 2020 Framework Programme of the European Union

Document Information

Deliverable number:	D9.6
Deliverable title:	Dissemination activities report (4th Report)
Deliverable version:	1.0
Work Package number:	WP9
Work Package title:	Dissemination and exploitation of results
Due Date of delivery:	29/04/2020
Actual date of delivery:	30/04/2020
Dissemination level:	PU
Editor(s):	Stavros Shiaeles, Gueltoum Bendiab (UOPHEC)
Contributor(s):	Gueltoum Bendiab, Stavros Shiaeles (UOPHEC) Olga Gkotsopoulou, Paul Quinn (VUB) Nicholas Kolokotronis, Konstantinos Limniotis, Brotsis Sotirios (UOP) Evangelos Sfakianakis (OTE) Gohar Sargsyan (CGI) Micheal A. Skitsas, Romaios Bratskas, Asimoula Kasioni (ADITESS) Dimitris Kavallieros (KEMEA), Vasiliki-Georgia Bilali (KEMEA)
Reviewer(s):	Evangelos Sfakianakis (OTE) Olga Gkotsopoulou (VUB)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	01/05/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Version History

Version	Date	Beneficiary	Description
0.1	06/03/2019	UOPHEC	Initial Draft
0.2	10/03/2020	UOPHEC	Second version
0.3	15/03/2020	UOPHEC	Partners' contribution
0.7	18/03/2020	All, UOPHEC	Partners review their act
0.8	23/03/2020	UOPHEC	Deliverable submitted for review
0.9	27/03/2020	VUB, OTE	Review comments received
1.0	28/03/2020	UOPHEC	Final version ready for submission

Acronyms

ACRONYM	EXPLANATION
ACARM	Alert Correlation, Assessment and Reaction Module
AI	Artificial Intelligence
AIDE	Advanced Intrusion Detection Environment
API	Application Programming Interface
CCIS	Communications in Computer and Information Science
CERT-EU	Computer Emergency Response Team for the EU Institutions
CIDN	Collaborative Intrusion Detection Network
CPU	Central Processing Unit
DLT	Distributed Ledger Technology
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUROPOL	European Police Office
GPS	Global Positioning System
HIDS	host-based intrusion detection system
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IMIS	Institute for the Management of Information Systems
IoT	Internet of Things
ISP	Internet Service Provider
IT	Information Technology
KPIs	Key Performance Indicators
LEA	Law Enforcement Agency
NIDS	Network Intrusion Detection System
NN	Neural Network
OSSEC	Open Source SECurity
PCAP	Packet Capture
ResNet	Residual Neural Network
SG	Smart Grids
SOINN	Self-Organizing Incremental Neural Network
TTL	Time-To-Live
URL	Uniform Resource Locator
VM	Virtual Machine
WP	Work Package

Contents

List of figures

List of tables

EXECUTIVE SUMMARY

This deliverable is the fourth of the reports that will overview the dissemination, communication, and exploitation activities of the Cyber-Trust project partners and their outcomes", following the strategy outlined in deliverable D9.2 (Disseminations and use plan). It presents the different dissemination activities that been held from M19 (November 2019) until M24 (April 2020) including the frequent update of the website, the activity in social networks, the publication of research undertaken in the project in conferences/journals, and participation of the Cyber-Trust partners in scientific and industry events, presentations of the project at other conference and workshops and other. This document also provides an evaluation of the dissemination activities progress against the initial expectations set out in the Cyber-Trust Consortium and KPIs identified in deliverable D9.2 (Disseminations and use plan). This evaluation gives a detailed insight into the promotion made around the project and will also provide clear guidance of the directions in which the Cyber-Trust project could seek further dissemination opportunities.

During this period of the project life, all partners have engaged in various dissemination activities including publications, conferences, workshops, website tasks and blogs, social media, presentations, newsletter, posters and other. Partners have also introduced and presented the project at fellow project events ranging from small workshops to bigger conferences. Finally, it is worth noting that due to force majeure and emergency lockdown measures for the containment of COVID-19, several events where Cyber-Trust partners are involved have been postponed and rescheduled.

1. Introduction

Deliverable D9.6 “Dissemination activities report: fourth Report” is the fourth biannual project dissemination reports, which overview the dissemination activities that have been made by the Cyber-Trust project partners in the period from M19 (November 2019) until M24 (April 2020). The aim of these deliverables is the documentation of all the dissemination activities that having been carried out by all partners in order to enhance the project visibility to both academic and industry community. List of the activities conducted in this period include Cyber-Trust website statistics, activities in the social media channels Facebook, Twitter and LinkedIn, presentations of the Cyber-trust project at other conferences and workshops, the publication of knowledge generated in the context of the project in conferences/journals, promotion via the project web site and social media Facebook, tweeter and LinkedIn, and other.

This deliverable is divided into four main sections, including the current introduction (Section 0) and conclusion (Section 0), where the various communications channels are presented. More precisely, the rest of the document is structured as follows:

- Second Section (Section 2) presents the dissemination and communication tools of the Cyber-Trust project. It is divided into seven subsections where the various communications channels are presented including the Cyber-Trust project web site traffic statistics and blogs (Section 2.1), communication of Cyber-Trust activities and outcomes to social media Facebook and tweeter (Section 2.2), publication of the research undertaken by the Cyber-trust partners in international conferences (Section 2.3), dissemination events arranged by the Cyber-Trust consortium members (Section 2.4), presentation and promotion of the Cyber-Trust project in well-known events ranging from small workshops to bigger conferences (Section 2.5), Cyber-trust partner’s participation in events including meetings, workshops, conferences, etc. (Section 2.7) and finally, presentation of the first issue of project Newsletter which provides the most recent news about the status of the project (Section 2.7).
- Third Section (Section 3) progress against the initial expectations set out in deliverable D9.2 (Disseminations and use plan), as well as the progress made towards the achievement of the objectives in the contractual arrangement under the EU.

2. Dissemination activities across different channels

This section will list all dissemination activities conducted by Cyber-Trust partners in this period (M19-M24) in order to raise awareness about the project and improve dissemination to specialists and potential users of the security technologies. All these activities aim to communicate the project outcomes to multiple audiences including the media and the public based on the dissemination and communication strategy defined in D9.2.The following subsections will provide more details on activities carried out from partners group based on the KPIs provided in Deliverable 9.2 (Disseminations and use plan).

2.1 Cyber-Trust Website and Blogs

The project's website was created to inform the stakeholders on the latest developments in Cyber-Trust project, its progress and generate interest of all the related communities with the exciting news in the research progress of the project. The website has been officially released since the end of August 2018, meaning that it has been online for 18 months. It hosts blogs and news pages where the consortium can share ideas and report technological achievements as they arise in the project; it is open to individual entities to allow active participation. The monitoring of website usage and traffic is accomplished with the free Google Analytics service.

Link to the website: https://cyber-trust.eu/.

The table below provides a summary of the web traffic statistics.

Date	21 April, 2020				
Communication activity	Cyber-Trust website				
Communication type	Website				
Target audience	Partners X	General X	Academic X	Government X	Industry X
Partner(s) involved	ADITESS				
People involved	Micheal A. Skitsas				
Description of the activity, relevance to the Project and Impact	The following figure (Figure 2.1) shows the overview of the visiting audience as a figure of new and returned visitors overall (89.2% of users are new visitors while 10.8% are returning visitors) for the period Oct 2019 to Apr 2020. In total 1800, users have visited the Cyber-Trust website with a total of 4710 page views.				

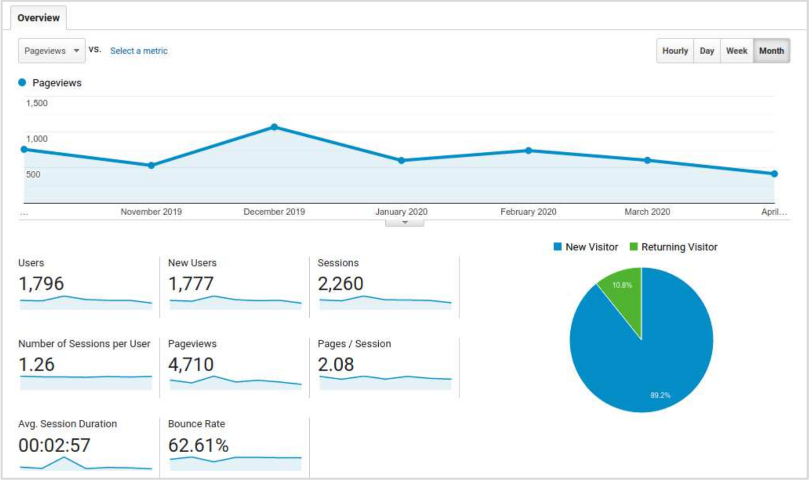


Figure 2.1: Audience Overview

Additionally, on an average visit, the user visits approximately two pages with a visit of 3 minutes. These metrics indicate that the average user finds interesting the content of the website as the lifetime per session is quite high. The navigation flow of users in the website is shown in the next Figure 2.2. with most users visiting the website homepage as their landing page as the project progresses and project outcomes see the light this figure will most probably change. The most commonly visited pages after the homepage are the consortium page, the page with objectives and news and events.

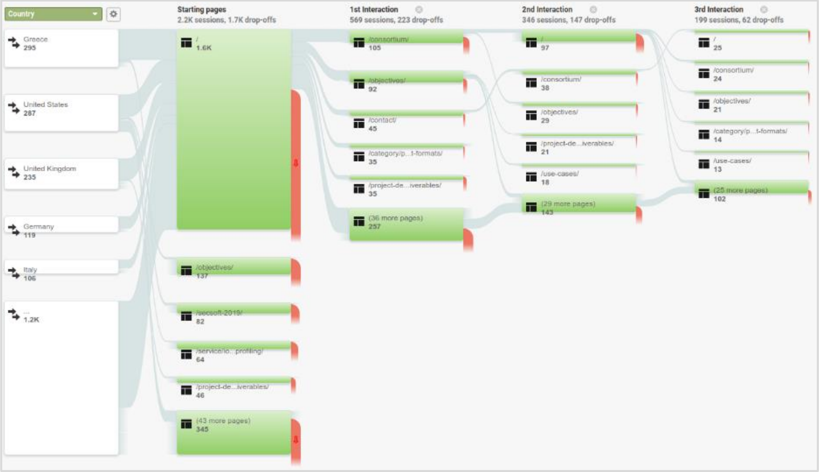


Figure 2.2: User flow

So far, the project website has gathered most visits from Europe while the United States are the top ranked as individual country (Figure 2.3).

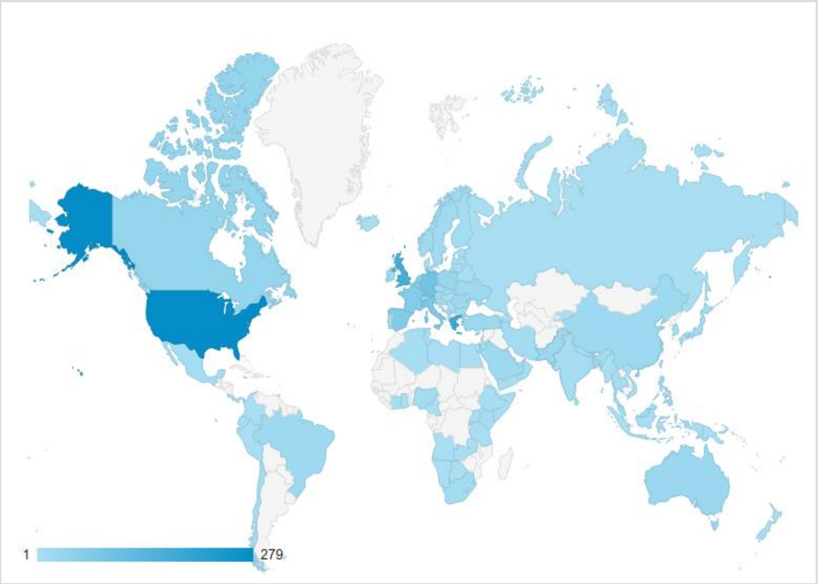
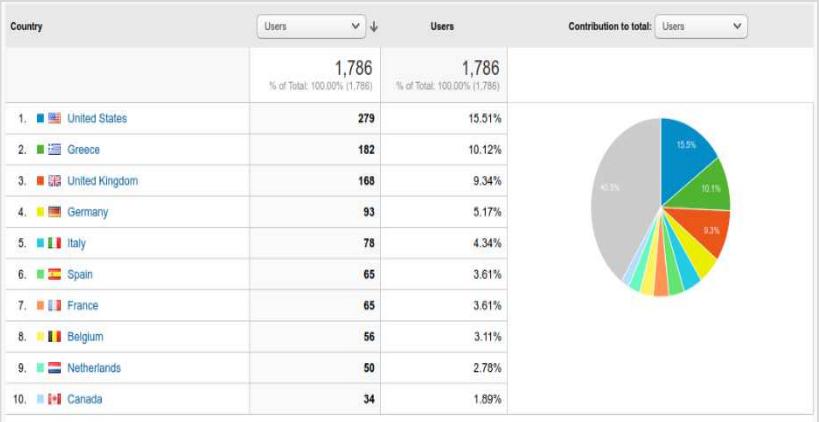


Figure 2.3: Visitation per continent

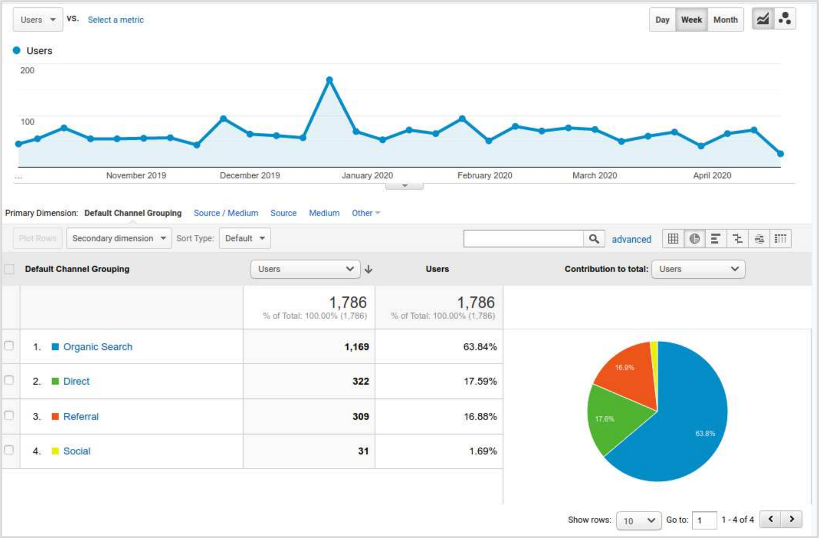
As illustrated in Figure 2.4, after the United States (15.51%) the top three countries per users are Greece (10.12%), UK (9.34%) and Germany (5.17%).



Country	Users	Users	Contribution to total: Users
	1,786 % of Total: 100.00% (1,786)	1,786 % of Total: 100.00% (1,786)	
1. United States	279	15.51%	
2. Greece	182	10.12%	
3. United Kingdom	168	9.34%	
4. Germany	93	5.17%	
5. Italy	78	4.34%	
6. Spain	65	3.61%	
7. France	65	3.61%	
8. Belgium	56	3.11%	
9. Netherlands	50	2.78%	
10. Canada	34	1.89%	

Figure 2.4: Country of Origin of Users

Most traffic on the Cyber-Trust website is acquired through organic searching (i.e. through search engines) while the direct access with the users typing the URL in the address bar on their internet browsers is the second source. The last two channels are through referral and social media (Figure 2.5).

<table>
<tr><td></td><td>


Primary Dimension: Default Channel Grouping Source / Medium Source Medium Other

Plot Rows Secondary dimension Sort Type: Default advanced

<table>
<tr><th>Default Channel Grouping</th><th>Users</th><th>Users</th><th>Contribution to total: Users</th></tr>
<tr><td></td><td>1,786
% of Total: 100.00% (1,786)</td><td>1,786
% of Total: 100.00% (1,786)</td><td></td></tr>
<tr><td>1. Organic Search</td><td>1,169</td><td>63.84%</td><td></td></tr>
<tr><td>2. Direct</td><td>322</td><td>17.59%</td><td></td></tr>
<tr><td>3. Referral</td><td>309</td><td>16.88%</td><td></td></tr>
<tr><td>4. Social</td><td>31</td><td>1.69%</td><td></td></tr>
</table>

Show rows: 10 Go to: 1 1 - 4 of 4

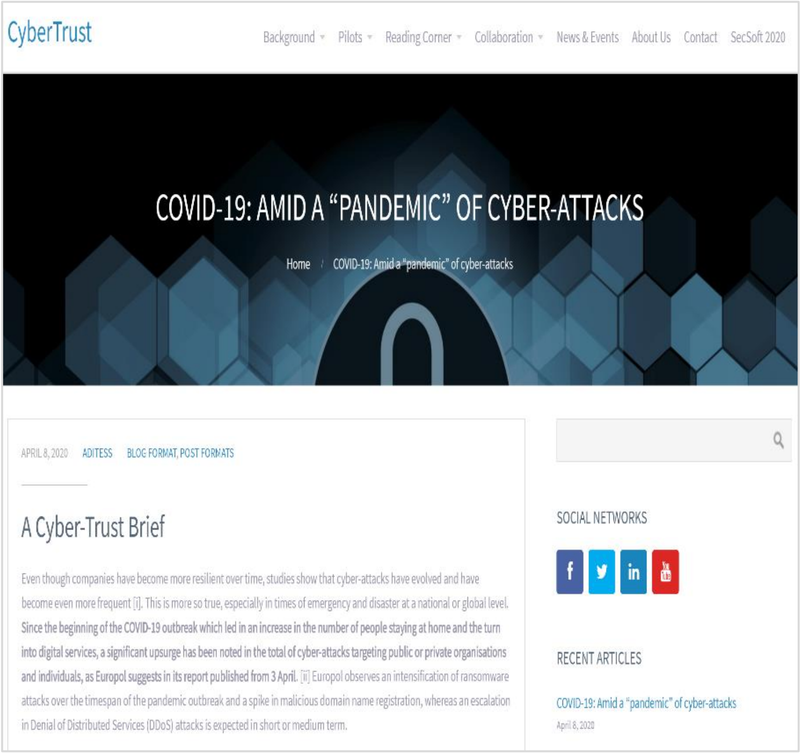
Figure 2.5: Distribution of traffic sources
</td></tr>
<tr><td>Annotated photos</td><td>N/A</td></tr>
</table>

2.1.1 Blogpost on Cyber-Trust website

Under the epidemic situation of COVID-19, the number of cyber-attacks has been multiplied highlighting once again the importance for data and security resilience as well as for the respective research and innovation to provide security solutions, including prevention and mitigation tools. In this context, a blog post entitled “C**OVID-19: AMID A “PANDEMIC” OF CYBER-ATTACKS"** has been added on our website. The blogpost presents an overview of the recommendations and guidelines, at EU level and at national level with reference to the countries where the Cyber-Trust partners are based. This blog is directly relating to policy work conducted in WP3 and in-parallel research in the areas of cyber-security and data protection.

The table below provides more details about the blog post.

Date	8 April, 2020				
Communication activity	Blogpost on Cyber-Trust website				
Communication type	Blog post				
Target audience	Partners X	General X	Academic	Government	Industry
Partner(s) involved	VUB (lead), KEMEA, ADITESS, UOPHEC				
People involved	Olga Gkotsopoulou, Dimitris Kavallieros, Michael Skitsas, Stavros Shiaeles				
Description of the activity, relevance to the Project and Impact	During the COVID-19 pandemic, the number of cyber-attacks has been multiplied highlighting once again the importance for data and security resilience as well as for the respective research and innovation to provide security solutions, including prevention and mitigation tools. With more and more people staying at home and an urging demand for digital services in order to fulfil their daily tasks and satisfy their needs for work, healthcare, education, entertainment and social contact, more and more organisations and				

	individuals are left exposed to vulnerability and security threats. From hospitals to national Ministries, and from teleconferencing platforms to scam and emails, threat is apparent and the risk for personal data breaches high. This has led many EU (European Union) institutions, Agencies and bodies, (European Commission, ENISA, EUROPOL, CERT-EU) as well as many state authorities, data protection authorities and law enforcement agencies to issue guidelines and recommendations on how to stay cyber-safe. The blogpost (Figure 2.6) presents an overview of those guidelines and recommendations at EU level and at national level with reference to the countries where the Cyber-Trust partners are based. It is relating to policy work conducted in WP3 and in-parallel research in the areas of cyber-security and data protection. Link to the blog: https://cyber-trust.eu/2020/04/08/amid-a-pandemic-of-cyber-attacks-a-cyber-trust-brief/.
Annotated photos	 CyberTrust Background Pilots Reading Corner Collaboration News & Events About Us Contact SecSoft 2020 Home / COVID-19: Amid a "pandemic" of cyber-attacks SOCIAL NETWORKS RECENT ARTICLESCOVID-19: AMID A "PANDEMIC" OF CYBER-ATTACKS APRIL 8, 2020 ADITESS BLOG FORMAT, POST FORMATS A Cyber-Trust Brief Even though companies have become more resilient over time, studies show that cyber-attacks have evolved and have become even more frequent [i]. This is more so true, especially in times of emergency and disaster at a national or global level. **Since the beginning of the COVID-19 outbreak which led in an increase in the number of people staying at home and the turn into digital services, a significant upsurge has been noted in the total of cyber-attacks targeting public or private organisations and individuals, as Europol suggests in its report published from 3 April.** [ii] Europol observes an intensification of ransomware attacks over the timespan of the pandemic outbreak and a spike in malicious domain name registration, whereas an escalation in Denial of Distributed Services (DDoS) attacks is expected in short or medium term. COVID-19: Amid a "pandemic" of cyber-attacks April 8, 2020 Figure 2.6: View of the blog on the Cyber-trust website

2.2 Social media analysis

Communication of Cyber-Trust activities and outcomes to the social media are performed through its Facebook Page and Twitter account and LinkedIn. Social media accounts have been set up with the aim to communicate a simplified presentation of the core activities of Cyber-Trust to general public. Overall, project social media accounts have a following of 28 members on LinkedIn, 53 followers on Twitter and 50 followers on Facebook.

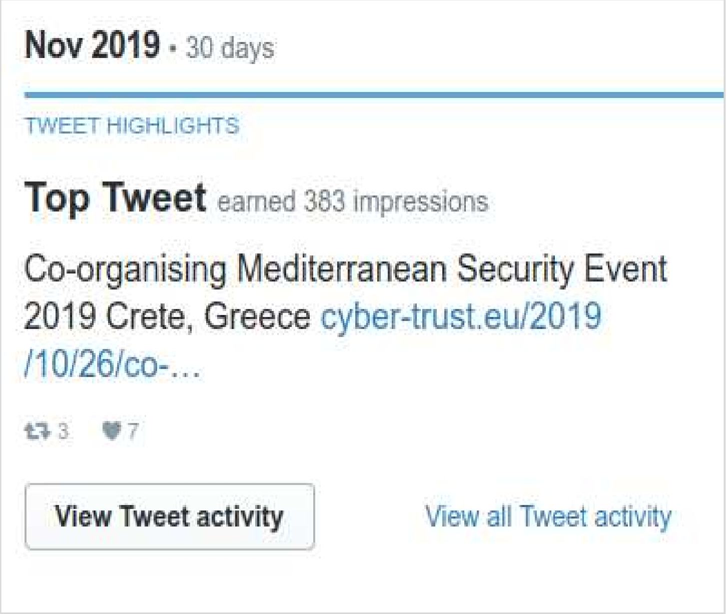
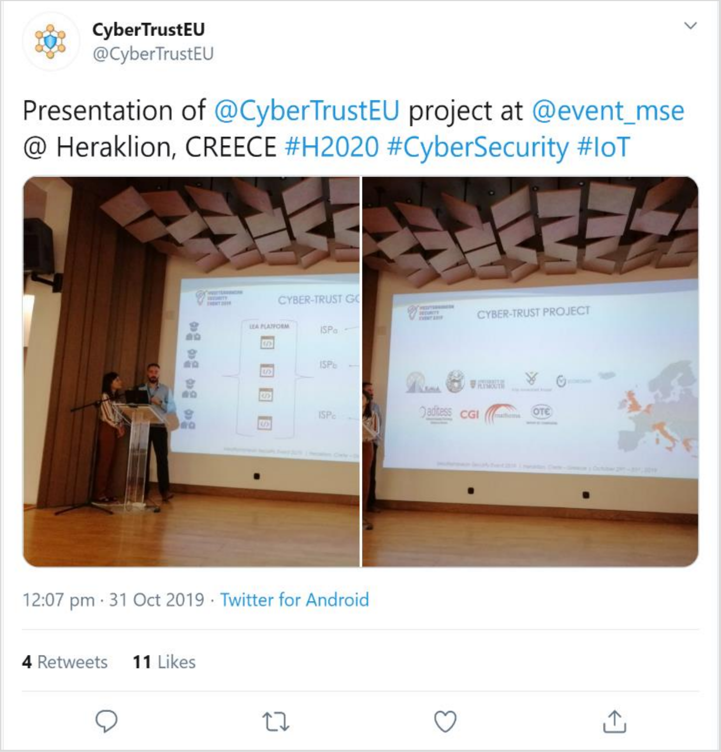
2.2.1 Tweeter

The twitter profile has gathered approximately 10K impression over the so far spanned period with the months of November 2019 and April 2020 gaining most interest. More information about communication of Cyber-Trust activities and outcomes performed through Twitter account is given in the table below.

Link to the twitter account: https://twitter.com/CyberTrustEU

<table>
<tr><td>Date</td><td colspan="5">20 April, 2020</td></tr>
<tr><td>Communication activity</td><td colspan="5">Cyber-Trust Social Media</td></tr>
<tr><td>Communication type</td><td colspan="5">Twitter</td></tr>
<tr><td>Target audience</td><td>Partners
X</td><td>General
X</td><td>Academic
X</td><td>Government
X</td><td>Industry
X</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">ADITESS</td></tr>
<tr><td>People involved</td><td colspan="5">Micheal A. Skitsas</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">In this period, the twitter profile has gathered approximately 10K impressions over the so far spanned period with the months of October and November most interesting (Table 2-1). Over these two months, the consortium had been very busy with dissemination activities where the co-organization of Mediterranean Security Event (MSE) 2019 took place.
Table 2-1: Overall Twitter Engagement
<table>
<tr><th>Month</th><th>Tweet Impressions</th><th>Profile Visits</th><th>New Followers</th></tr>
<tr><td><b>Apr 2020</b></td><td><b>491</b></td><td><b>10</b></td><td><b>1</b></td></tr>
<tr><td><b>Mar 2020</b></td><td>926</td><td>22</td><td>6</td></tr>
<tr><td><b>Feb 2020</b></td><td>1127</td><td>29</td><td>7</td></tr>
<tr><td><b>Jan 2020</b></td><td>1135</td><td>13</td><td>7</td></tr>
<tr><td><b>Dec 2019</b></td><td>1104</td><td>0</td><td>3</td></tr>
<tr><td><b>Nov 2019</b></td><td>3209</td><td>39</td><td>8</td></tr>
<tr><td><b>Oct 2019</b></td><td>2390</td><td>15</td><td>9</td></tr>
</table>

Figure 2.7 and Figure 2.8 shown below; illustrate highlights on Twitter and content that has gathered high interest in terms of engagement for the months October and November 2019.</td></tr>
</table>

	 Nov 2019 · 30 days TWEET HIGHLIGHTS Top Tweet earned 383 impressions Co-organising Mediterranean Security Event 2019 Crete, Greece cyber-trust.eu/2019/10/26/co-… 3 7 View Tweet activity View all Tweet activity Figure 2.7: Top tweet for November 2019  CyberTrustEU @CyberTrustEU Presentation of @CyberTrustEU project at @event_mse @ Heraklion, CREECE #H2020 #CyberSecurity #IoT 12:07 pm · 31 Oct 2019 · Twitter for Android 4 Retweets 11 Likes Figure 2.8: Top tweet for October 2019
Annotated photos	N/A

2.2.2 Facebook

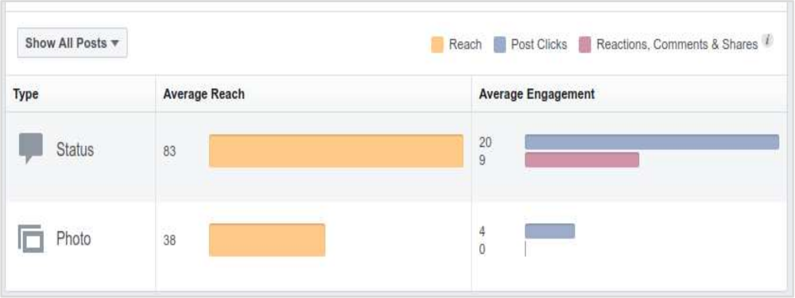
Facebook is used as the channel of preference for the promotion of events in which consortium members will be participating. In this period, the project Facebook page has so far concentrated 55 followers with 19 activity items. More information about communication of Cyber-Trust activities and outcomes performed through the Facebook page is given in the table below.

Link to the Cyber-Trust Facebook page: https://www.facebook.com/cybertrust/

<table>
<tr><td>Date</td><td colspan="5">20 April, 2020</td></tr>
<tr><td>Communication activity</td><td colspan="5">Cyber-Trust Social Media</td></tr>
<tr><td>Communication type</td><td colspan="5">Facebook</td></tr>
<tr><td rowspan="2">Target audience</td><td>Partners</td><td>General</td><td>Academic</td><td>Government</td><td>Industry</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">ADITESS</td></tr>
<tr><td>People involved</td><td colspan="5">Micheal A. Skitsas</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">

The overall activity of the Cyber-Trust Facebook page has reached more than 1280+ users and gained engagement from 200+ users, the Facebook page gathered almost the total of its interest organically. Cyber-Trust Posts appeared in the feed of almost 4000 Facebook users.

The project Facebook page has so far concentrated 55 followers with 19 activity items. Facebook will be used as the channel of preference for the promotion of events in which consortium members will be participating.



Type | Average Reach | Average Engagement
Status | 83 | 20 9
Photo | 38 | 4 0

Figure 2.9: Engagement over post types

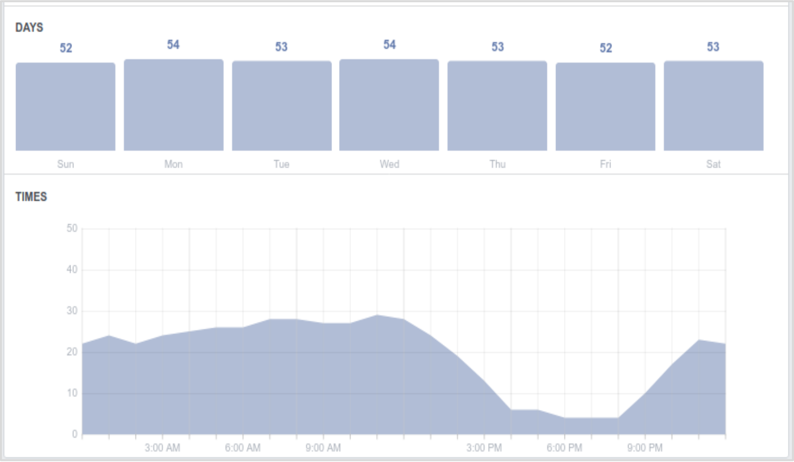


Figure 2.10: Insights on times followers are active

</td></tr>
<tr><td>Annotated photos</td><td colspan="5">N/A</td></tr>
</table>

2.3 Research Conference presentations and publications

In this period, the research undertaken in the Cyber-Trust project has led to 04 new research publications that were accepted and will be presented in peer-reviewed international conferences. The research work papers are developed to help advance the knowledge base that underpins the formulation and implementation of relevant policies in Europe, and to engage with relevant communities, stakeholders and practitioners in the research, again with the aim of supporting relevant policies and providing a clear view of the project results. All research papers are available on publishers' websites and most of them have an e-print copy that is available as open access in the "**arXiv**" repository.

The tables below provide more details about the six new research work papers.

Date	6 April, 2020				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry
Number of participants	Around 150 people				
Partner(s) involved	UOPHEC, UoP				
People involved	Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis				
Description of the activity, relevance to the Project and Impact	This paper focuses on enhancing intrusion detection systems (e.g. Suricata and snort) with machine learning by proposing a novel IoT malware traffic analysis approach using deep learning and visual representation for faster detection and classification of new malware (zero-day malware). This work is an extension of our previous works proposed in the context of Cyber-Trust project by using the learning algorithm Residual Neural Network with more samples of malware and legitimate PCAP files for the training and testing phases. The dataset used to evaluate this approach consists of 1000 PCAP files of normal and malware traffic that were collected from different network traffic sources. Comparative results of Resnet 34-layers (ResNet 34) and 50-layers (ResNet 50) with the Self-Organizing Incremental Neural Network (SOINN) and MobileNet NN shows that the Residual Neural Network (ResNet50) algorithm has the best overall performance, with higher accuracy (94.50%) and precision (95.78%). It is also observed that Resnet performs better with more layers (Resnet50). The paper was accepted and will be presented in the 2nd Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft), co-located with IEEE NetSoft 2020 that will be held in 3ed of July 2020, Ghent, Belgium. The paper will also be published in the conference proceedings and IEEE Xplore. *Gueltoum, Bendiab, Stavros Shiaeles, Abdulrahman Alruban, Nicholas Kolokotronis. " **IoT Malware Network Traffic Classification using Visual Representation and Deep Learning**."*				

	2020 IEEE Conference on Network Softwarization (NetSoft). IEEE, 2020. The work presented in this paper is directly related with the work carried out in the work-package 6 (WP6).
Annotated photos	N/A

Date	6 April, 2020				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry
Number of participants	Around 150 people				
Partner(s) involved	UOPHEC				
People involved	Vasileios Koutsouvelis, Stavros Shiaeles, Bogdan Ghita, Gueltoum Bendiab.				
Description of the activity, relevance to the Project and Impact	This paper investigated solutions that have been proposed to identify and alleviate the potential impact of Insider threat, which is one of the most damaging risk factors for the IT systems and infrastructure of a company or an organization. In this context, the paper studied the efficiency of Artificial Intelligence to detect malicious insider by proposing a new approach to discriminate between legitimate and malicious behaviour. For each category of users, the approach creates an image that depicted his/her activity and behaviour, as emerged from their interaction with various information systems. While the resulting images may appear visually different, they were processed through a machine learning algorithm in order to automatically recognize which subset of the users appear to exhibit malicious behaviour (and therefore posing a threat for the respective information systems) and which are legitimate/ benign ones. This approach is composed of three main steps: (a) collecting, processing, and classifying the data of the users tested; (b) visualizing the extracted data; (c) categorize the behaviour as malicious or normal. The paper was accepted and will be presented in the 2nd Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft), co-located with IEEE NetSoft 2020 that will be held in 3ed of July 2020, Ghent, Belgium. The paper will also be published in the conference proceedings and IEEE Xplore. Link to the Workshop: https://cyber-trust.eu/secsoft-2020/ *Vasileios Koutsouvelis, Stavros Shiaeles, Bogdan Ghita, Gueltoum Bendiab. "* ***Detection of Insider Threats using Artificial***				

	***Intelligence and Visualisation**." 2020 IEEE Conference on Network Softwarization (NetSoft). IEEE, 2020.* The work presented in this paper is directly related with the work carried out in the work-packages 6 and 7 (WP6, WP7).
Annotated photos	N/A

Date	12-13 December, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry
Number of participants	Around 100 people				
Partner(s) involved	UOP, UOPHEC				
People involved	Stylianos Monogios, Konstantinos Limniotis, Nicholas Kolokotronis, Stavros Shiaeles				
Description of the activity, relevance to the Project and Impact	The Android unrestricted application market, being of open source nature, has made it a popular platform for third-party applications reaching millions of smart devices in the world. This tremendous increase in applications with an extensive API that includes access to phone hardware, settings, and user data raises concerns regarding user's privacy, as the information collected from the apps could be used for profiling purposes. In this respect, this paper focuses on the geolocation data and analyses five GPS applications to identify the privacy risks if no appropriate safeguards are present. Our results show that GPS navigation apps have access to several types of device data, while they may allow for personal data leakage towards third parties such as library providers or tracking services without providing adequate or precise information to the users. Moreover, as they are using third-party libraries, they suffer from the intra-library collusion issue, that could be exploited from advertising and analytics companies through apps and gather large amount of personal information without the explicit consent of the user.				

	The paper was presented in the “8th occasion of the International Conference on e-Democracy" that was held in Athens, the cradle of democracy, on 12-13 December 2019. The paper is published in the Springer’s Communications in Computer and Information Science (CCIS) series, Online ISBN 978-3-030-37545-4. The conference paper is available via the Springer digital library: Link: https://link.springer.com/book/10.1007%2F978-3-030-37545-4 *Monogios, Stylianos, et al. "**A Case Study of Intra-library Privacy Issues on Android GPS Navigation Apps**." In the International Conference on e-Democracy. Springer, Cham, 2019. DOI: https://doi.org/10.1007/978-3-030-37545-4_3* This work is directly related with the work carried out in the work-package
Annotated photos	N/A

Date	18-21 December, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry
Number of participants	Around 220 people				
Partner(s) involved	UOPHEC, CSCAN, UoP				
People involved	Gueltoum Bendiab, Stavros Shiaeles, and Nicholas Kolokotronis				
Description of the activity, relevance to the Project and Impact	This paper focuses on examining the existing Open source IDSs, in order to find the most appropriate solution for smart homes in terms of resources consumption. To this end, several open-source network-based intrusion detection systems (NIDS) are available such as ACARM-ng, AIDE, Bro IDS, Snort, Suricata, OSSEC HIDS, Prelud Hybrid IDS, Samhain, Fail2Ban, Security Onion, etc. This study helps in identifying the best IDS that can protect smart devices used in home environments with a minimum of resources consumption, which is very important for the Cyber-trust project, especially work package 6. The paper presents the results of the experimental comparison between the widely used open-source NIDSs namely Snort, Suricata and Bro IDS to find the most appropriate one for smart homes in term of resources consumption including CPU and memory utilization. The chosen IDSs are deployed inside different Linux containers known as Dockers, instead of running them IDSs directly on a VM base operating system. Each container has its resources that are separated from other containers. Experimental Results				

	show that Suricata and Bro are the best performing NIDS for smart homes compared to snort. The paper was presented in the seventh Symposium on Security in Computing and Communications (SSCC'19), co-affiliated with the International Conference on Applied Soft computing and Communication Networks (ACN'19), co-located with the third International Conference on Computing and Network Communications (CoCoNet'19) that was held in Trivandrum, Kerala, India on December 18-21, 2019. Link: http://www.acn-conference.org/sscc2019/ The conference paper is available in the conference proceedings via the SpringerLink digital library. It is also available in the Communications in Computer and Information Science Series(CCIS),ISSN: 1865:0929, published by Springer. CCIS is indexed in DBLP, Google Scholar, EI-Compendex, Mathematical Reviews, SCImago and Scopus (https://www.springer.com/gp/book/9789811548246). *Faisal Alsakran, Gueltoum, Bendiab, Stavros Shiaeles, Nicholas Kolokotronis. "* ***Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study****." Seventh Symposium on Security in Computing and Communications (SSCC'19). Springer, 2019.* The experimental comparison study presented in this paper is directly related with the work carried out in the work-package 6 (WP6).
Annotated photos	N/A

2.4 Organised dissemination events

Cyber-Trust partners organised and participated in several scientific and industry events, conferences, and meetings, where they had the chance to present and discuss the results of the project with potentially interested parties.

The tables below present the organised events in this period of the project life.

Date	11 February 2020				
Communication activity	Business Workshop				
Communication type	Business workshop with thought leaders				
Target audience	Partners	General	Academic	Government	Industry X
Number of participants	Around 20 people				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				

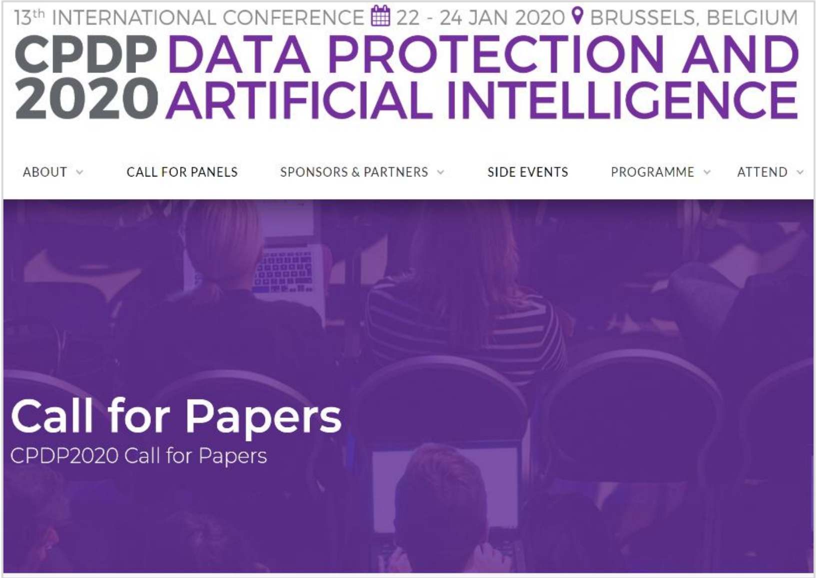
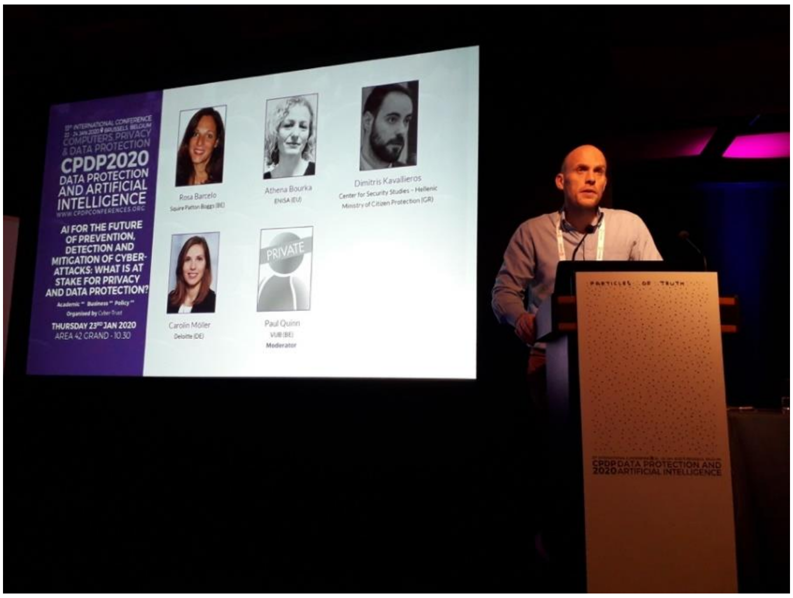
Description of the activity, relevance to the Project and Impact	On February 11, 2020, a business workshop within experts / thought leaders was organised to discuss the ongoing initiatives and way ahead for new partnership opportunities. Gohar Sargsyan presented Cyber-Trust for dissemination purposes. Following to discussions the thought leaders provided highly positive recommendations to start working on a follow-up opportunity. Besides the participants expressed high interest in following the development of the project especially on potential market uptake if the research results will bring.
Annotated photos	

Date	4 February, 2020				
Communication activity	Science and Business event				
Communication type	Science and Business annual event				
Target audience	Partners	General	Academic X	Government X	Industry X
Number of participants	More than 350 people				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	Science|Business is a forum convening public and private sector leaders for networking, intelligence and debates on research and innovation. organises a range of events from full conferences to private briefings. Some are open to the public, some for members of our Network only. We run our own events, and we also organise bespoke events for clients. But whatever the format, every Science|Business event shares the same unique imprint: it combines expert knowledge with bringing together the people who really matter in industry, research and policy – both as speakers and as audience. This year's annual membership event took place on the 4th of February in Brussels. CGI is a member of the network and was present in the event. The event was closed event to members only and some 100 members were present to discuss the agenda of the next year. During breakout sessions, the members had the opportunity to show case innovation, show case or any project they find suitable to the setting. Cyber-Trust was presented by Gohar Sargsyan from CGI in the breakout session and it was received very well by the participants. The session attended about 40 members.				

Annotated photos	 Figure 2.11: Picture from Science and Business annual event

Date	23 January, 2020				
Communication activity	Standalone panel and presentations				
Communication type	Debate, communication and dissemination				
Target audience	Partners x	General x	Academic x	Government x	Industry x
Number of participants	More than 1000 people				
Partner(s) involved	VUB (lead), KEMEA				
People involved	Olga Gkotsopoulou, Paul Quinn, Dimitris Kavallieros				
Description of the activity, relevance to the Project and Impact	The following panel intitled “**AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection?** was organised by VUB, on behalf of Cyber-Trust, at the CPDP 2020 - Artificial Intelligence and Data Protection, one of the biggest annual conferences in the field. The conference took place in Brussels (Belgium) on 22-24 January 2020. Cyber-Trust also received visibility as event partner. The Internet of Things (IoT) aims to establish an ecosystem of heterogeneous connected devices that communicate to deliver environments making our living, cities, transport, energy, and many other areas more intelligent. This amplifies concerns about the security of networked applications and services, based on known and unknown vulnerabilities and backdoors. More and more cybersecurity systems develop and deploy AI tools for the prevention, detection and mitigation of cyber-attacks, in particular in the field of cyber-threat intelligence and device profiling, aiming to simplify the threat identification process and improve the rate of remediation response. The panel aims to reflect upon what is at stake for data protection and privacy by the use of such automated tools, provided inter alia the requirements set in the recently adopted Cybersecurity Act at EU level for enhancing cybersecurity in products and services.				

	Since AI appears to become increasingly integrated in cybersecurity solutions, what applications are currently deployed, what is being developed by academia, business and the LEAs, how are models trained and what is aspired for in the short- and long-term future in the security sector? What are the advantages and challenges of using AI in the cybersecurity context with respect to data protection and privacy? In which ways can security research reconcile privacy, data protection and cybersecurity, creating compliant designs by advancing the principles of data protection and privacy by design and by default as well as integrating the learnings of the Data Protection Impact Assessments? Best practices and lessons learnt through hands-on experience. The panel is directly related to the work of WP3. **Relevant links and promotion:** • https://www.youtube.com/watch?v=zXkXxmLL-fI&list=PL8z0l8CAoah7nocn6fjCbeE9U-l_wNKer&index=6&t=0s • https://www.cpdpconferences.org/cpdp-panels/ai-for-the-future-of-prevention-detection-and-mitigation-of-cyberattacks-what-is-at-stake-for-privacy-and-data-protection • https://twitter.com/olga_gkot/status/1220285991673614336?s=20 • https://twitter.com/PaulQuinnBxl/status/1220359024513814530 Link to the event: • https://www.cpdpconferences.org/call-for-papers

Annotated photos	 13th INTERNATIONAL CONFERENCE 22 - 24 JAN 2020 BRUSSELS, BELGIUM CPDP 2020 DATA PROTECTION AND ARTIFICIAL INTELLIGENCE ABOUT · CALL FOR PANELS · SPONSORS & PARTNERS · SIDE EVENTS · PROGRAMME · ATTEND Call for Papers CPDP2020 Call for Papers Figure 2.12: CPDP 2020 event website  13th INTERNATIONAL CONFERENCE 22 - 24 JAN 2020 BRUSSELS, BELGIUM COMPUTERS, PRIVACY & DATA PROTECTION CPDP2020 DATA PROTECTION AND ARTIFICIAL INTELLIGENCE WWW.CPDPCONFERENCES.ORG AI FOR THE FUTURE OF PREVENTION, DETECTION AND MITIGATION OF CYBER-ATTACKS: WHAT IS AT STAKE FOR PRIVACY AND DATA PROTECTION? Academic ** Business ** Policy ** Organised by Cyber-Trust THURSDAY 23RD JAN 2020 AREA 42 GRAND - 10.30 Rosa Barcelo Squire Patton Boggs (BE) Athena Bourka ENISA (EU) Dimitris Kavallieros Center for Security Studies - Hellenic Ministry of Citizen Protection (GR) Carolin Möller Deloitte (DE) PRIVATE Paul Quinn VUB (BE) Moderator PARTICLES OF TRUTH CPDP DATA PROTECTION AND ARTIFICIAL INTELLIGENCE

	 AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection? **Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things** **Paul Quinn**, Vrije Universiteit Brussel **Rosa Barcelo**, Squire Patton Boggs **Athena Bourka**, ENISA - European Union Agency for Cybersecurity **Dimitris Kavallieros**, Center for Security Studies - Hellenic Ministry of Citizen Protection **Carolin Möller**, Deloitte #CPDP2020 PARTICLES OF TRUTH CPDP 2020 DATA PROTECTION AND ARTIFICIAL INTELLIGENCE Figure 2.13: Pictures from the CPDP 2020 event

Date	13-17 January, 2020				
Communication activity	Business side event				
Communication type	CGI leadership conference				
Target audience	Partners	General	Academic	Government	Industry X
Number of participants	More than 350 people				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	CGI Leadership business event gathered 350 leaders from around the world including senior executives of the company between 13 and 17 of January 2020 in Montreal, Canada. The event is a regular event for the level of Directors and higher. During this leadership conference a side event was organised dedicated to Cyber-Trust by Gohar Sargsyan. Business Innovation show was organised together with local Montreal innovation team. A brief presentation on the screen of the event, was shown and during exhibition session. As the session was walked in in a lobby of the large event, all participants had the opportunity to walk-in and have impressions on Cyber-Trust alongside with others who stopped by for longer time to discuss.				
Annotated photos	 Figure 2.14: Picture from the CGI leadership conference				

Date	26 November, 2019				
Communication activity	Business conference presentation and publication				
Communication type	Conference presentation				
Target audience	Partners	General X	Academic X	Government X	Industry X
Number of participants	Around 60-80 participants				
Partner(s) involved	OTE, KEMEA				
People involved	Ioannis Chochliouros, Evangelos Sfakianakis, Dimitris Kavallieros				
Description of the activity, relevance to the Project and Impact	The following Workshop was organised by OTE, by focusing upon 5G Security issues, as a side-event within the 21st Infocom World Conference & Exhibition, one of the biggest annual events for Industry in ICT, in Greece. The Conference took place in Athens (Greece) on November 26, 2019. The Cyber-Trust project also received visibility as presenter. The event was within a Parallel Session with 3 sub-sessions in room "MACEDONIA" under the title "Scientific Meeting: Perspectives and Challenges for the Development of Innovative 5G Applications and Services, through Modern Research Activities". The activity took place in the scope of Session C ("Modern Innovative Technologies and Broader 5G-related Aspects for Development and Growth with Emphasis set to Vertical Industries"). Two Cyber-Trust dedicated presentations took place, as follows: • Presentation 1 - Title: "***Meeting the Needs of Information among LEAs and ISPs from the LEA side".*** • Presentation 2 - Title: ***"Meeting the Needs of Information among LEAs and ISPs from the ISP side".*** Venue: Divani Caravel Athens Hotel, Athens, Greece • *https://divanicaravelhotel.com/* Relevant links and promotions: • https://www.infocomworld.gr/21o-infocom-world-2019/ • https://www.infocomworld.gr/21o-infocom-world-2019/5g-epistimoniki-synantisi-aithoysa-makedonia/ • https://www.infocomworld.gr/presentations/2019/ote/C20a_Kavallieros.pdf • https://www.infocomworld.gr/presentations/2019/ote/C20b_Sfakianakis.pdf This event is directly related to the work undertaken in WP2, WP4, WP6 and WP8.				

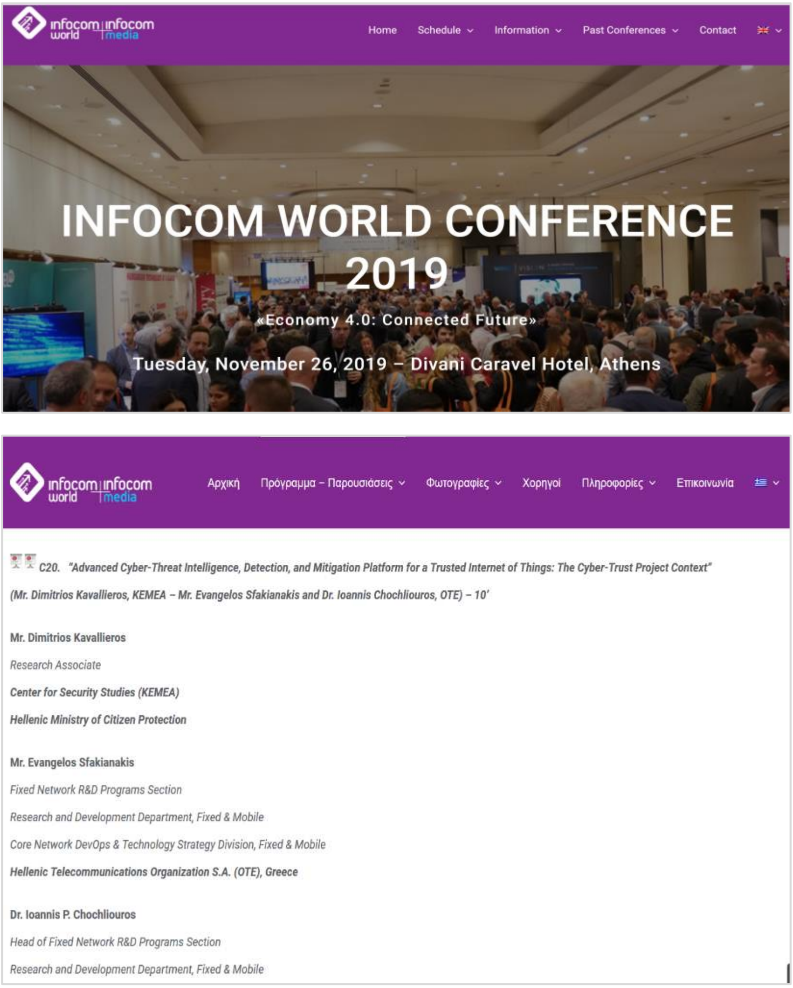
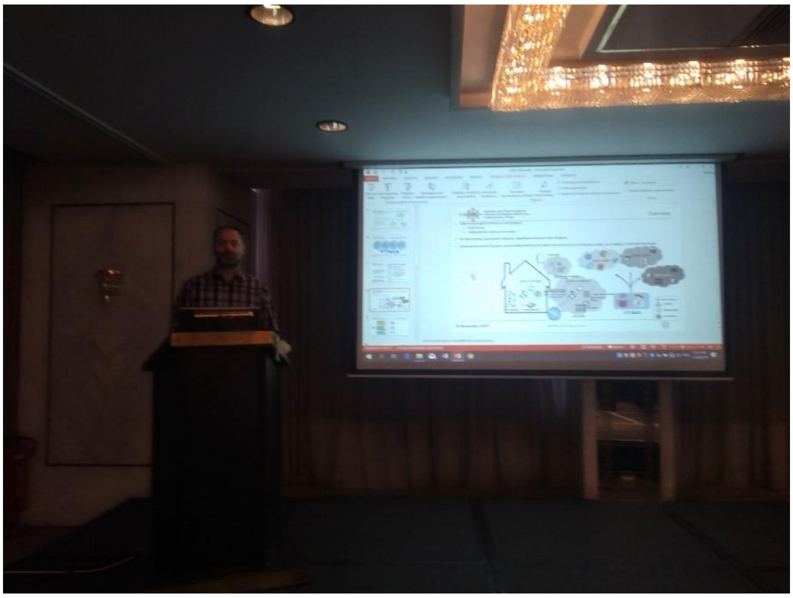
Annotated photos	 infocom world | infocom media Home Schedule Information Past Conferences Contact INFOCOM WORLD CONFERENCE 2019 «Economy 4.0: Connected Future» Tuesday, November 26, 2019 – Divani Caravel Hotel, Athens infocom world | infocom media Αρχική Πρόγραμμα – Παρουσιάσεις Φωτογραφίες Χορηγοί Πληροφορίες Επικοινωνία *C20. "Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things: The Cyber-Trust Project Context"* *(Mr. Dimitrios Kavallieros, KEMEA – Mr. Evangelos Sfakianakis and Dr. Ioannis Chochliouros, OTE) – 10'* **Mr. Dimitrios Kavallieros** *Research Associate* ***Center for Security Studies (KEMEA)*** ***Hellenic Ministry of Citizen Protection*** **Mr. Evangelos Sfakianakis** *Fixed Network R&D Programs Section* *Research and Development Department, Fixed & Mobile* *Core Network DevOps & Technology Strategy Division, Fixed & Mobile* ***Hellenic Telecommunications Organization S.A. (OTE), Greece*** **Dr. Ioannis P. Chochliouros** *Head of Fixed Network R&D Programs Section* *Research and Development Department, Fixed & Mobile* Figure 2.15: INFOCOM website 

	 Figure 2.16: Pictures from the INFOCOM event

Date	November 26, 2019				
Communication activity	Standalone panel and talks				
Communication type	Communication and dissemination of research results				
Target audience	Partners	General X	Academic X	Government	Industry
Number of participants	30 to 40 people				
Partner(s) involved	VUB (lead), KEMEA, CGI				
People involved	Olga Gkotsopoulou, Paul Quinn, Dimitris Kavallieros, Georgia Melenikou, Dimitra Papadaki, Gohar Sarsgyan				
Description of the activity, relevance to the Project and Impact	***Of spiders and robots: web crawling as opportunity and threat vs. data protection law as facilitator and obstacle*** Web crawlers are almost as old as the internet itself and are used for a myriad of purposes from law enforcement to research and business intelligence to malicious attacks. Theoretically, web crawlers can collect information from the internet on an infinite scale. Respectively, the information generated by the users may qualify as personal data and, in that case, the relevant legal framework becomes applicable, creating a noteworthy obstacle for such activities. The most challenging situation is when personal data are not targeted as such and are only incidentally collected and processed. The goal of this panel was to discuss the legality and proportionality of web crawling from the point of view of privacy and data protection law, as well as the current 'self-regulatory' framework. The panellists gave an overview of what web crawling entails from a technical point of view and outlined the purposes of the use of web crawling in business, research, and law enforcement. Building on that technical description, the discussion moved to the implementation of the EU data protection law and				

	the compatibility with the data protection principles. Preventive, protective and informative measures deployed by website operators were presented and debated. **This event is co-organised by the Brussels Privacy Hub and the Horizon 2020-funded research project Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things.** **Panelists**: **Constantinos Patsakis**, Assistant Professor at the Department of Informatics, University of Piraeus and Adjunct researcher at the Institute for the Management of Information Systems (IMIS) of Athena Research and Innovation Centre. **Gohar Sargsyan**, ICT Innovation Lead EU, Director Consulting Information Driven Operations and Digital Transformation, CGI Netherlands. **Georgia Melenikou**, Lawyer and Research Associate, Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection. **Dimitra Papadaki**, Lawyer and Research Associate, Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection. **Venue:** U-Residence, Vrije Universiteit Brussel, Pleinlaan 2, 1050, Brussel (Access also via Generaal Jacqueslaan 271, 1050 Brussels) **Relevant links and promotion:** • https://www.brusselsprivacyhub.eu/events/26112019.html • https://lsts.research.vub.be/en/lunchtime-panel-on-web-crawling-and-data-protection-26-november-2019-vub/ • https://lsts.research.vub.be/en/of-spiders-and-robots-webcrawling-as-opportunity-and-threat-vs-data-protection-law-as-facilitator/ • https://twitter.com/privacyhub_bru/status/1199297752204808192 This event is directly related to the work undertaken in WP3 and WP5.

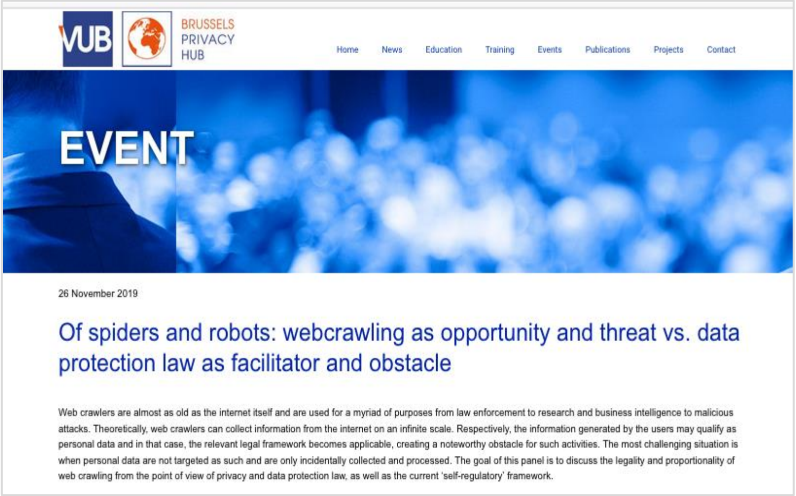
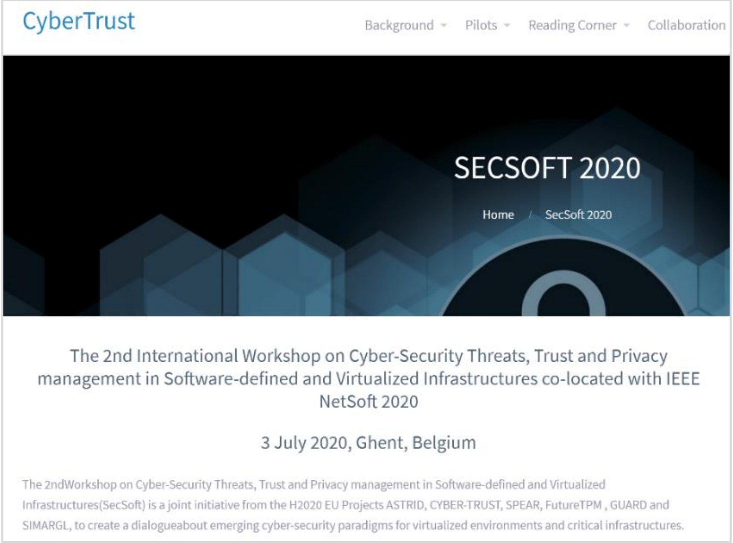
Annotated photos	 BRUSSELS PRIVACY HUB Home News Education Training Events Publications Projects Contact EVENT 26 November 2019 Of spiders and robots: webcrawling as opportunity and threat vs. data protection law as facilitator and obstacle Web crawlers are almost as old as the internet itself and are used for a myriad of purposes from law enforcement to research and business intelligence to malicious attacks. Theoretically, web crawlers can collect information from the internet on an infinite scale. Respectively, the information generated by the users may qualify as personal data and in that case, the relevant legal framework becomes applicable, creating a noteworthy obstacle for such activities. The most challenging situation is when personal data are not targeted as such and are only incidentally collected and processed. The goal of this panel is to discuss the legality and proportionality of web crawling from the point of view of privacy and data protection law, as well as the current 'self-regulatory' framework. Figure 2.17: View of the event on the VUB website CYBER-TRUST IoTCrawler is an advanced search and discovery mechanism of IoT and smart objects in the Internet that will support the security and privacy restrictions that user and owners of IoT devices will provide related to how to disclose the data that the IoT can publish IoTCrawler deals with the challenge of crawling the internet of IoT and bi opportunity will be open to provide advanced services and application t Constantinos PATSAKIS Gohar SARGSYAN Georgia MELENIKOU Dimitra PAPADAKI BRUSSELS Of spiders and robots Webcrawling as opportunity & threat vs data protection law as facilitator & obstacle Olga GKOTSOPOULOU Paul QUINN Constantinos PATSAKIS BRUSSELS PRIVACY HUB

	 Figure 2.18: Pictures from the panel

<table>
<tr><td>Date</td><td colspan="5">29 June – 3 July, 2020</td></tr>
<tr><td>Communication activity</td><td colspan="5">Organization of a workshop</td></tr>
<tr><td>Communication type</td><td colspan="5">SecSoft 2020 workshop</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General
X</td><td>Academic
X</td><td>Government
X</td><td>Industry
X</td></tr>
<tr><td>Number of participants</td><td colspan="5">More than 250 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">UOPHEC</td></tr>
<tr><td>People involved</td><td colspan="5">Stavros Shiaeles</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">The Second International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft 2020) is a joint initiative from EU Cyber-Security and 5G projects: ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD and 5GENESIS. The organisation of this workshop (https://www.astrid-project.eu/secsoft/) co-hosted at 6th IEEE International Conference on Network Softwarization (NetSoft 2020) that was planned to be held in Ghent, Belgium on 29 June- 3 July, 2020. However, Based on the current situation of the coronavirus COVID-19 pandemic sanitary crisis, the 6th IEEE International Conference on Network Softwarization (IEEE NetSoft 2020) will run as a virtual conference On June 29 – 3 July, 2020. IEEE NetSoft 2020 aims at bringing together students, researchers and security experts on areas under consideration by Cyber-Trust. Indicative topics of interest included:
• Cyber-security platforms and architectures for digital services.
• Security, trust and privacy for industrial systems and the IoT (including smart grids (SGs)).</td></tr>
</table>

	• Monitoring and advanced data collection and analytics. • Virtual and software-based cyber-security functions. • Orchestration of security functions. • Novel algorithms for attack detection and threat identification. • Intelligent attack mitigation and remediation. • Machine learning, big data, network analytics. • Secure runtime environments, including trustworthy systems and user devices. • Formal methods for security and trust. • Novel threat and attack models. • Authentication, Authorization and Access control. • Honeypots, forensics and legal investigation tools. • Threat intelligence and information sharing Link to the workshop: https://cyber-trust.eu/secsoft-2020/ or https://www.astrid-project.eu/secsoft/ Topics in this workshop are directly related with work carried out in work-packages WP5, WP6, and WP7. The special session's proceedings will be made available at the publisher's website (https://ieeexplore.ieee.org/). It is also expected that the accepted and presented workshop papers will be published in the workshop proceedings before the end of 2020 and will made available at the publisher's website, (https://ieeexplore. ieee.org/).
Annotated photos	 CyberTrust Background Pilots Reading Corner Collaboration Home / SecSoft 2020 SECSOFT 2020 The 2nd International Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures co-located with IEEE NetSoft 2020 3 July 2020, Ghent, Belgium The 2ndWorkshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures(SecSoft) is a joint initiative from the H2020 EU Projects ASTRID, CYBER-TRUST, SPEAR, FutureTPM , GUARD and SIMARGL, to create a dialogueabout emerging cyber-security paradigms for virtualized environments and critical infrastructures. Figure 2.19: SecSoft 2020 CFP on the Cyber-Trust Website

2.5 Event Participation

During the last period, ADITESS partner from the Cyber-Trust project have participated in the Science and Business annual event "Nicosia Risk Forum 2019" that was held in the European University Cyprus in Nicosia, Cyprus. In this event, ADITESS partner had the chance to raise awareness of the Cyber-Trust project and to gauge the level of interest and impact of the project on the wider community of stakeholders, including academia, and industry. More details are provided in the following table.

Date	14 November, 2019				
Communication activity	Science and Business annual event /conference presentation				
Communication type	Conference presentation				
Target audience	Partners	General	Academic	Government	Industry
		X	X	X	X
Number of participants	Around 150 people				
Partner(s) involved	ADITESS LTD				
People involved	Michael Skitsas, Romaios Bratskas, Nikolaos Koutras, Asimoula Ksioni				
Description of the activity, relevance to the Project and Impact	The Nicosia Risk Forum 2019 event took place at European University Cyprus in Nicosia, Cyprus, November 21, 2019. "The Nicosia Risk Forum 2019 provides the platform for an array of stakeholders –hailing from government, academia and the private sector– to exchange views and experiences, making it a truly multi-disciplinary event that produces a high level of discourse at a timely juncture. An exciting line of speakers and presentations were planned. Among others, on Nicosia Risk Forum 2019 important presentations were made by: EU Commissioner for Humanitarian Aid and Crisis Management, Dr Christos Stylianides HE the Minister of Foreign Affairs of the Republic of Cyprus, Dr Nikos Christodoulides The Deputy Government Spokeswoman, Ms Klelia Vasileiou Secretary General for Civil Protection of the Hellenic Republic, Mr Nikos Hardalias Head of NEMA, State of Israel, Mr Zeev Tsuk-Ram, VOVA Commissioner of Cyprus Civil Defense Force of the Republic of Cyprus, Mr Andreas Frantzis During the sessions of the Nicosia Risk Forum 2019 the Cyber-Trust project (https://cyber-trust.eu/) was presented by ADITESS LTD (www.aditess.com) . Relevant links and promotions: • https://cerides.euc.ac.cy/nicosia-risk-forum/ • https://aditess.com/main/2019/11/22/cybertrust-project-at-nicosia-risk-forum-2019/				

Annotated photos	 2nd Annual Symposium Center of Excellence in Risk & Decision Sciences (CERIDES) Nicosia Risk Forum 2019 Thursday, 21 November 2019 Cultural Center, European University Cyprus OBJECTIVES CYBER-TRUST PROJECT Figure 2.20: Pictures form Nicosia Risk Forum 2019

2.6 Synergies with other Projects

To ensure cohesion with the wider research efforts undertaken by related concurrent EU projects, members of the consortium established contact and communication, in order to build up collaborations on aspects of mutual interest with other H2020 projects. More details about collaboration activities are given below:

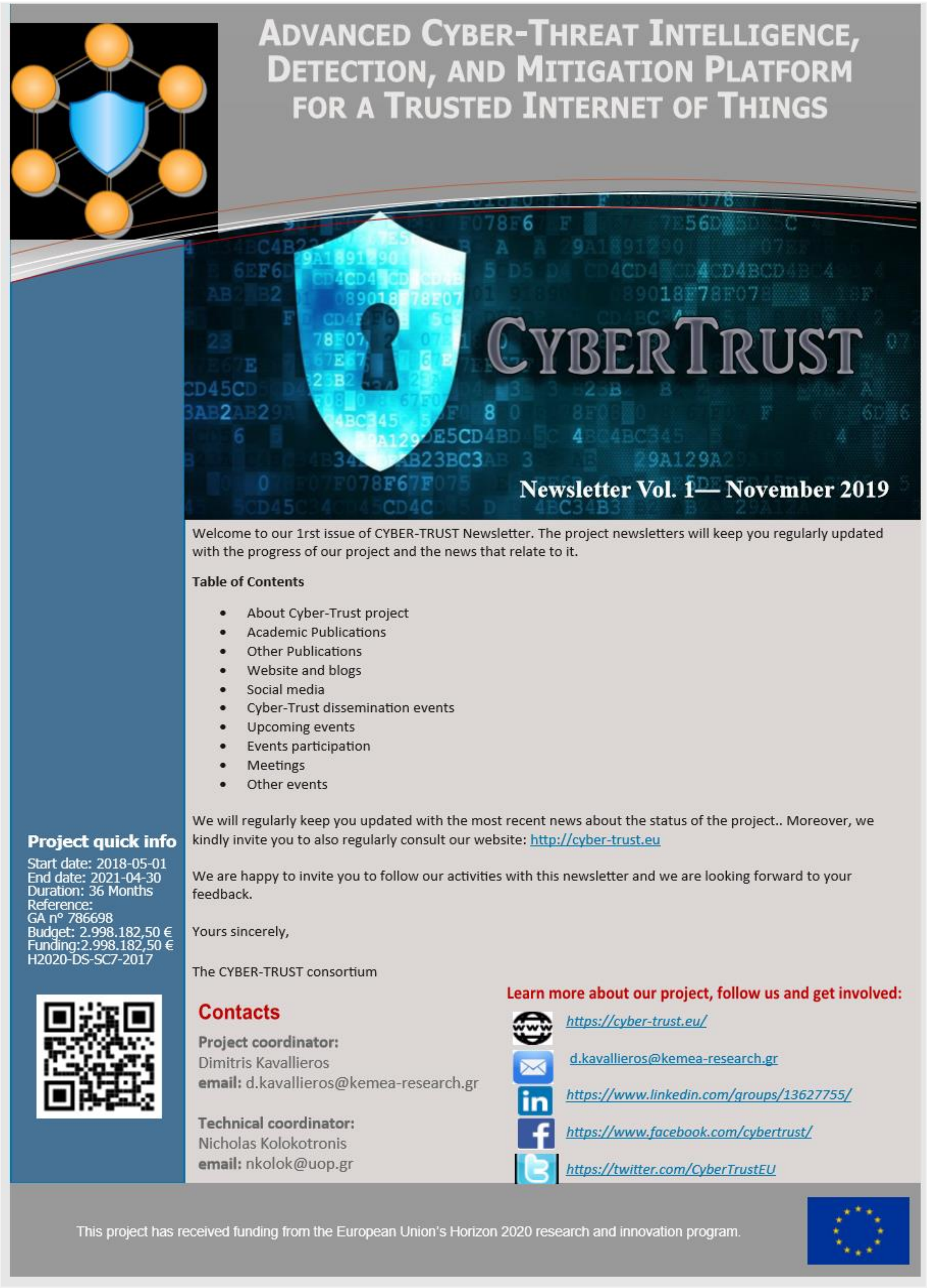
Date	January-March 2020				
Communication activity	Synergy establishment for the organisation of a standalone panel and talks				
Communication type	Debate, communication and dissemination				
Target audience	Partners	General	Academic	Government	Industry
	X	X	x	x	x
Number of participants	around 30-40 people				
Partner(s) involved	VUB (lead), SCORECHAIN, KEMEA				
People involved	Olga Gkotsopoulou, Paul Quinn, Clement Pavue, Dimitris Kavallieros				
Description of the activity, relevance to the Project and Impact	***Due to force majeure (emergency lockdown measures for the containment of COVID-19), the below event has been postponed and will be rescheduled.*** On 29 April 2020, the Brussels Privacy Hub in synergy with the Horizon 2020-funded research projects **LOCARD**, **Cyber-Trust** and **FASTER** will present the panel 'The Promise of "Blockchain": DLT-based applications re-shape data storage and sharing, but can they be compliant with the EU data protection law?' In recent times, much discussion has taken place among policy makers, academia and the private sector. Distributed Ledger Technologies (DLT) for data storage and sharing offer high potential and benefits in various contexts. Albeit, their use may give birth to implications with respect to data protection law. Design choices - giving preference to more centralised or decentralised solutions, opting for a permissioned or permissionless type of DLT, or resorting to an on-chain/off-chainscheme - create complications for researchers, DLT experts and businesses, as they can lead to different legal considerations, provided the characteristics specific to each application as well as the inherent limitations of each technology. Design choices can render compliance with the data protection and privacy framework easier or impossible and thus, can have a significant impact on the success of a project or product. The panel will address issues relating to DLT-based applications beyond Blockchain, understanding which questions have to be asked during the conceptualization and design of a solution as well as during its actual implementation. The panelists, focusing on three innovative use cases of DLT (cyber-security, law enforcement and emergency response), will further address more general concerns and other issues, including the basic technical characteristics of DLTs and the current state-of-the-art. The backend legal research supporting those design choices will be extensively discussed.				

	All in all, Blockchain-enthusiasts or sceptics, attendees will have the opportunity to hear about novel technical solutions which aim to render DLT-based applications compliant with data protection law and ensure the enforcement of data subjects' rights, such as the notion of Private Data, the adoption of different access levels and the Time-To-Live (TTL) feature. This activity is directly related to the work carried out in WP3 and WP7.
Annotated photos	N/A

2.7 Newsletter

First issue of Cyber-Trust Newsletter (November 2019) has been published in order to keep regular updates with the progress of the project and the news that relate to it. This first issue gives information about the main achievements of the project in its first year. The main topic presented in Newsletter include information about the Cyber-Trust academic and other project publications, Cyber-Trust Website and blogs, Social media, Organised events by the Cyber-trust consortium as well as upcoming events, attended events and meetings with the full spectrum of stakeholders, including police, government, academia, and industry.

This issue of the Newsletter is available on the Cyber-Trust project website (https://cyber-trust.eu/newsletters/) as well as the project social media including Facebook, Tweeter and LinkedIn.



ADVANCED CYBER-THREAT INTELLIGENCE, DETECTION, AND MITIGATION PLATFORM FOR A TRUSTED INTERNET OF THINGS

CYBERTRUST

Newsletter Vol. 1— November 2019

Welcome to our 1rst issue of CYBER-TRUST Newsletter. The project newsletters will keep you regularly updated with the progress of our project and the news that relate to it.

Table of Contents

We will regularly keep you updated with the most recent news about the status of the project.. Moreover, we kindly invite you to also regularly consult our website: http://cyber-trust.eu

We are happy to invite you to follow our activities with this newsletter and we are looking forward to your feedback.

Yours sincerely,

The CYBER-TRUST consortium

Project quick info

Start date: 2018-05-01
End date: 2021-04-30
Duration: 36 Months
Reference:
GA n° 786698
Budget: 2.998.182,50 €
Funding:2.998.182,50 €
H2020-DS-SC7-2017

Contacts

Project coordinator:
Dimitris Kavallieros
email: d.kavallieros@kemea-research.gr

Technical coordinator:
Nicholas Kolokotronis
email: nkolok@uop.gr

Learn more about our project, follow us and get involved:

https://cyber-trust.eu/
d.kavallieros@kemea-research.gr
https://www.linkedin.com/groups/13627755/
https://www.facebook.com/cybertrust/
https://twitter.com/CyberTrustEU

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Figure 2.21: First issues of Cyber-Trust Newsletter

3. Progress Monitoring

This section provides an evaluation of the dissemination activities progress against the KPIs of deliverable 9.2 in order to have close monitoring and corrective action to be taken if necessary. As shown in Table 3-1, Cyber-Trust partners disseminated the project effectively during the third period (M19 -M24) of the project life. All the partners have contributed to the dissemination activities to relevant stakeholders and engaged in various activities.

Table 3-1 : Summary of dissemination activities

Dissemination Type	Actual	Target (project life)
Website Visits	5957	10800
Brochure	3	3
Scientific Publications	23	25
Press Releases	3	8
Blogs	2	10 in total
Newsletter	1	5 in total
Workshops	11	At least 5
Presentations	22	30
Social Media	227 followers	/
Direct Contact	4	/

As shown in Table 3-1, there are numerous outcomes of the dissemination activities listed above. For instance, the research undertaken in the Cyber-Trust project has already led to 23 research publications, of which 20 were accepted and presented in peer-reviewed international conferences and three in peer-reviewed journals. This shows that the Cyber-Trust partners are very close to the target number identified in D9.2, which is 25 publications. In addition, during this period of the project life, many of the KPIs introduced in D9.2 have been achieved like the number of designed brochures for promoting the Cyber-Trust project. One poster was designed and distributed during the MEDIA4SEC - Innovative Market Solutions Workshop. One other banner and two Leaflets were designed and distributed in the Mediterranean Security Event (MSE 2019). Also, the project's website statistics show that the website is currently attracting a significant number of visitors and in total 1800 users have visited the Cyber-Trust website with a total of 5957 page-views, with a growth of approximately 89.2% compared to the previous period (M13-M18). In addition, social media channels garnered over 76% of its interest during this period.

This overview proves that Cyber-Trust partners have done a great promotion of the project during the aforementioned period. In fact, statistics in Table 3-1 provide a good insight into communication done and opens up opportunities for further promotion of the project and their results. Further, Cyber-Trust partners believe that they will reach and exceeds all the KPIs introduced in D9.2 (Disseminations and use plan) as well as the exploitation objectives introduced in D9.9 by the end of the project.

4. Conclusion

This deliverable provided the dissemination and communication activities undertaken by consortium partners of Cyber-Trust during the fourth period of the project life (November 2019– April 2020). It detailed the dissemination activities, which have been undertaken in this period, together with the potential future events. The detailed description of the dissemination activities involved during this period leads to the conclusion that the partners have been involved in many important activities to disseminate the project and raise its presence, noting that due to force majeure and emergency lockdown measures for the containment of COVID-19, several events where Cyber-Trust partners are involved have been postponed and rescheduled.