CYBER-TRUST

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

Grant Agreement: 786698

D9.5 Disseminations activities report (3rd 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: 31/10/2019

Document Submission Date: 31/10/2019

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

Document Information

Deliverable number:	D9.5
Deliverable title:	Dissemination activities report (3rd Report)
Deliverable version:	1.0
Work Package number:	WP9
Work Package title:	Dissemination and exploitation of results
Due Date of delivery:	31/10/2019
Actual date of delivery:	31/10/2019
Dissemination level:	PU
Editor(s):	Keltoum Bendiab (CSCAN), Stavros Shiaeles
Contributor(s):	Stavros Shiaeles, Keltoum Bendiab (CSCAN) Nicholas Kolokotronis, Sotirios Brotsis (UOP), Gohar Sargsyan (CGI), Clément Pavué (SCORECHAIN), Liza Charalambous, Micheal A. Skitsas (ADITESS), Dimitris Kavallieros (KEMEA), Olga Gkotsopoulou, Paul Quinn (VUB)
Reviewer(s):	Dimitris Kavallieros (KEMEA) 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	01/08/2019	CSCAN	Initial Draft
0.2	03/10/2019	CSCAN	Incorporated partners' dissemination activities
0.3	17/10/2019	All	Partners review their act
0.6	28/10/2019	KEMEA, VUB	Review
0.9	29/10/2019	CSCAN	Final editing and review
1.0	31/10/2019	KEMEA	Final version and submission to the EC

Acronyms

ACRONYM	EXPLANATION
AI	Artificial Intelligence
APIs	Application Programming Interface
ASGARD	Analysis System for Gathered Raw Data
BT	Boosted Tree
CIDN	Collaborative Intrusion Detection Network
CIDNs	Collaborative Intrusion Detection Networks
CPDP	Computers, Privacy and Data Protection
CSIRT-CY	Computer Security *Incident Response* Team
CSRIoT	Cyber Security and Resilience in the Internet of Things
CTI	Cyber threat intelligence
DIGILENCE	Digital Transformation, Cyber Security and Resilience
DPbD	Data Protection by Design
DT	Decision Tree
EU	European Union
EUNWA	European Neighbourhood Watch Association
GCSM	Graphical cyber security models
HSD	Hague Security Delta
IDS	Intrusion Detection System
IDS	Intrusion Detection Systems
iIRS	intelligent intrusion response systems
IoT	Internet of Things
JISA	Journal of Information Security and Applications
KPI	Key Performance Indicator
LEA	Law Enforcement Agency Application Programming Interface
LNCS	Lecture Notes in Computer Science
LR	Logistic Regression
ML	Machine Learning
MSE	Mediterranean Security Event
NetSoft	Network Softwarization
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NN	Neural Network
NYC	New York City
OAG	Open Access Government
OS	Operating System
OSINT	Open Source Intelligence
QoE	Quality of Experience
QoS	Quality of Service
RF	Random Forest
SDI	Software-Defined Infrastructures

SDN/NFV	Software-Defined Networking/Network Function Virtualization
SOINN	Self-Organizing Incremental Neural Network
SVM	Support Vector Machine

Contents

List of figures

List of tables

EXECUTIVE SUMMARY

This deliverable is the third of the reports that will overview the dissemination, communication, and exploitation activities of the Cyber-trust project partners, following the strategy outlined in D9.2 (Disseminations and use plan). This report covers the dissemination activities that been held from M13 (May 2019) until M18 (October 2019). From the many general communication activities undertaken in this period, we want to highlight the frequent update of the website, the activity in social networks and the publication of research undertaken in the project.

During this last period, the Cyber-Trust project had several peer-reviewed conference publications and journal articles accepted whereas other publications are under submission. Since the project started, it had seventeen accepted publications in total. All publications are available on the project website. Furthermore, Cyber-trust partners participated in several scientific and industry events, and conferences, where they had the chance to present the results of the project. Also, several meetings were conducted where the Cyber-trust project and ideas were presented and discussed with potentially interested parties.

Finally, we like to point out that efforts were made by the consortium members to promote the project and its findings to potential customers and stakeholders, including governmental organisations, universities, and commercial companies.

1. Introduction

This section will provide the purpose of the third dissemination activities report from the first of May (Month 13) until the end of October 2019 (Month 18).

The deliverable is organised as follows: After this introduction, next section presents the various dissemination and communication activities conducted by the Cyber-Trust partners in this period of the project life. It is divided into eight sections that correspond to the various communication channels. Firstly, section 2.1 discusses the Cyber-Trust website and the social media channels (Facebook, Twitter) statistics including visiting audience, users flow, Twitter engagement, posts on Facebook, etc. Then, section 2.2 provides information about all research papers that have been published or presented in scientific events. After that, section 2.4 gives information about the research papers that are accepted and published in journals. Information about publications in other communication channels such as the Open Access Government Magazine is given in section 2.5. Next, section 2.6 overviews the dissemination events arranged by the Cyber-Trust consortium members in this period. Then, section 2.7 reports the Cyber-trust partner's participation in events including meetings, workshops, conferences, etc. Finally, section 2.8 overviews Cyber-trust member's contributions to events organised by other consortiums in the Cybersecurity field.

Section 3 evaluates dissemination 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.

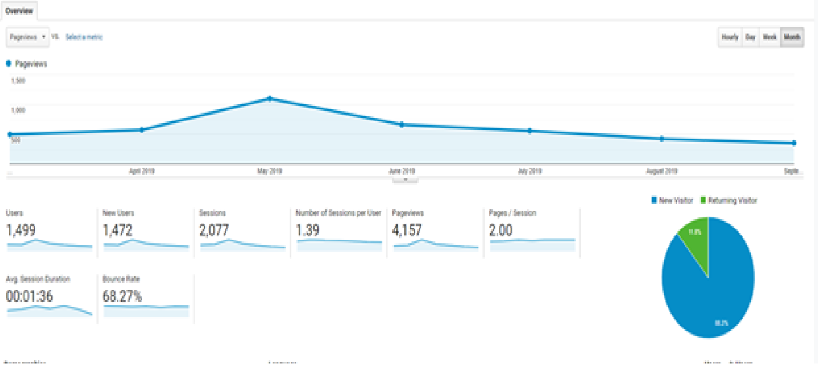
2. Dissemination activities across different channels

This section includes details of dissemination activities from all Cyber-Trust partners in the reporting period (Month 13- Month 18). The following subsections will provide more details on activities carried out from partners group based on the KPIs provided in Deliverable 9.2.

2.1 Websites and Blogs

The website hosts blog 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. The Cyber-Trust website has been officially released since the end of August 2018, meaning that it has been online for three months.

The following table gives a summary of the web site statistics in the reporting period including visiting audience, users flow and distribution of traffic sources.

Date	October 15, 2019				
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	Elisavet Charalambous				
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 (88.2% of users are new visitors while 11.8% are returning visitors). In total 1500, users have visited the Cyber-Trust website with a total of 4157page views.  Overview Pageviews ▾ VS. Select a metric Hourly Day Week Month ● Pageviews 1,500 1,000 500 April 2019 May 2019 June 2019 July 2019 August 2019 Septe... ■ New Visitor ■ Returning Visitor Users 1,499 New Users 1,472 Sessions 2,077 Number of Sessions per User 1.39 Pageviews 4,157 Pages / Session 2.00 Avg. Session Duration 00:01:36 Bounce Rate 68.27% 11.8% 88.2% Figure 2-1: Audience Overview Additionally, on an average visit, the user visits approximately 2 pages with a visit of 1 minutes and 36 seconds. 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 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 page with the list of deliverables, the consortium page, the page on the project objective and finally the page of news and events.

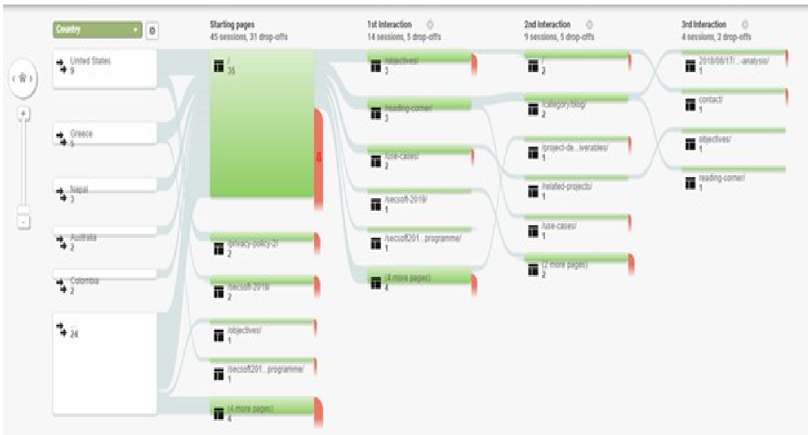


Figure 2-2: User flow

So far, the project website has gathered most visitation from Europe with most traffic occurring midday onwards between Wednesdays and Fridays (Figure 2-3)

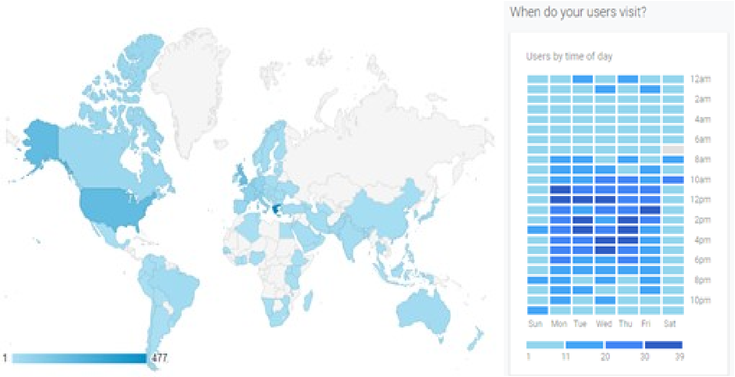
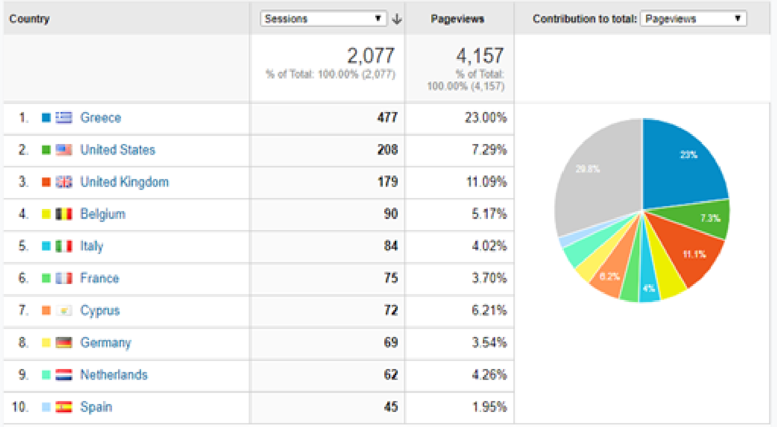


Figure 2-3: Visitation per continent and Distribution of visitation with respect to time of the day

Also important is the demographics on the country of origin of visiting users (*see* Figure 2-4). The top three countries are Greece (45%), Cyprus (39%) and UK (14%) and occupy 98% of visitation.



Country	Sessions	Pageviews	Contribution to total: Pageviews
	2,077 % of Total: 100.00% (2,077)	4,157 % of Total: 100.00% (4,157)	
1. 🟦 Greece	477	23.00%	
2. 🟩 United States	208	7.29%	
3. 🟥 United Kingdom	179	11.09%	
4. 🟨 Belgium	90	5.17%	
5. 🟦 Italy	84	4.02%	
6. 🟩 France	75	3.70%	
7. 🟧 Cyprus	72	6.21%	
8. 🟨 Germany	69	3.54%	
9. 🟩 Netherlands	62	4.26%	
10. 🟦 Spain	45	1.95%	

Figure 2-4: Country of Origin of Visiting Users

Most traffic on the Cyber-Trust website is acquired directly with the users typing the URL in the address bar on their internet browsers, the second source is through organic searching (i.e. through search engines) and finally through social media. As time progresses, it is expected that the traffic attained through social media channels will increase; result of their establishment (Figure 2-5).

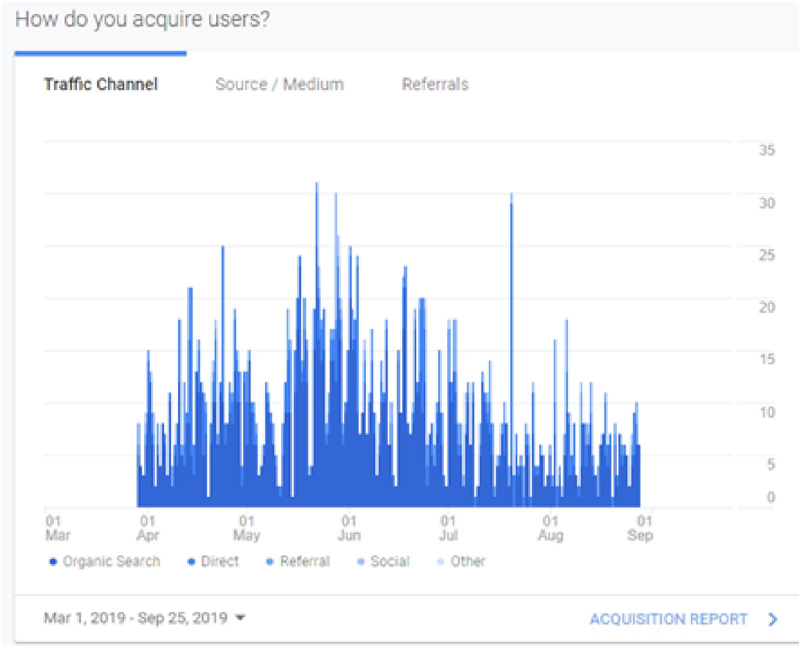


Figure 2-5: Distribution of traffic sources

Annotated photos	N/A

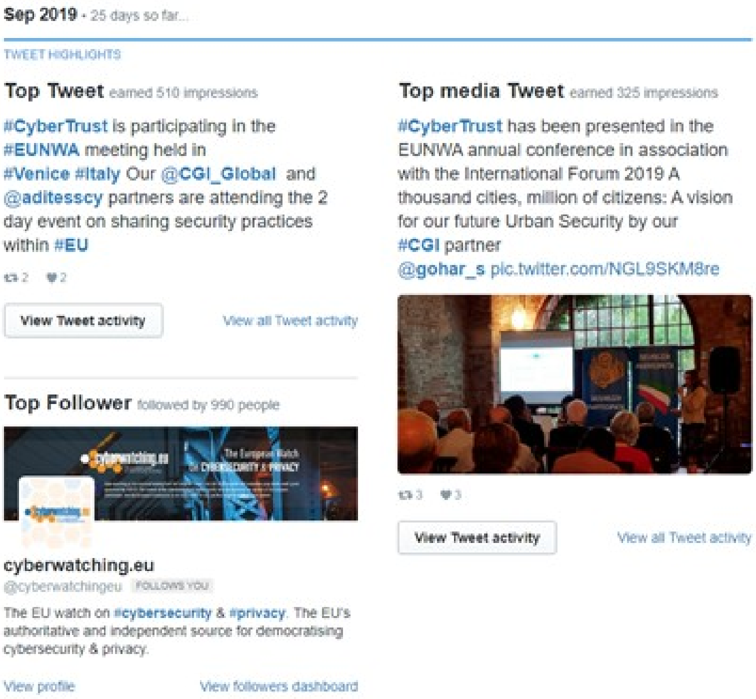
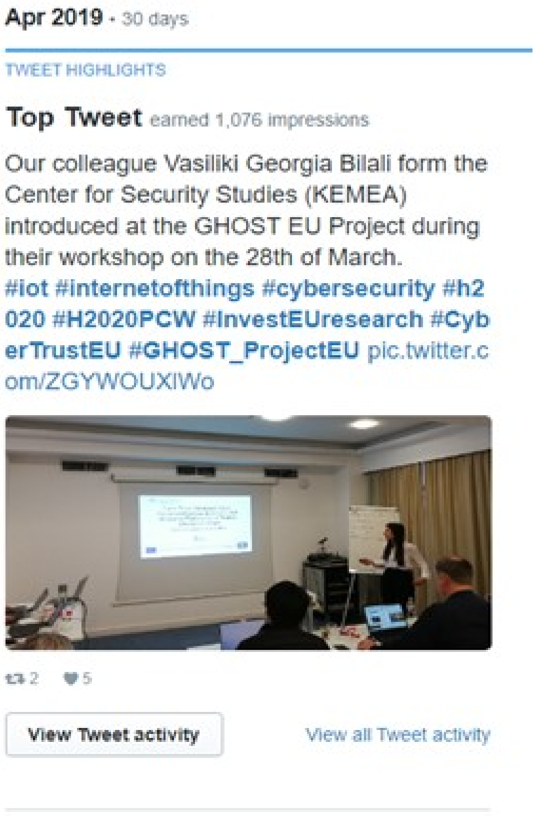
2.2 Social media analysis

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 Twitter

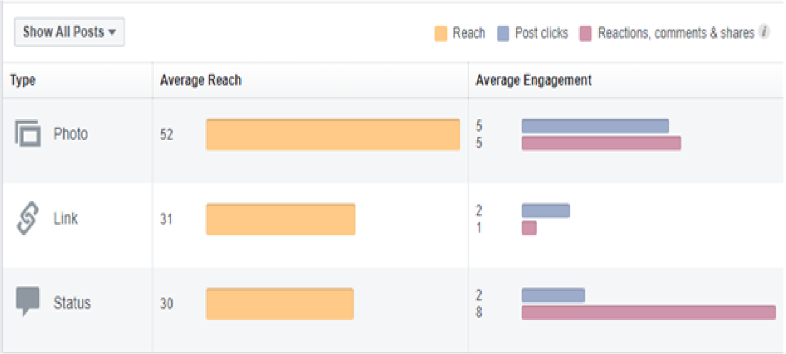
More information about communication of Cyber-Trust activities and outcomes performed through Twitter account is given in the table below.

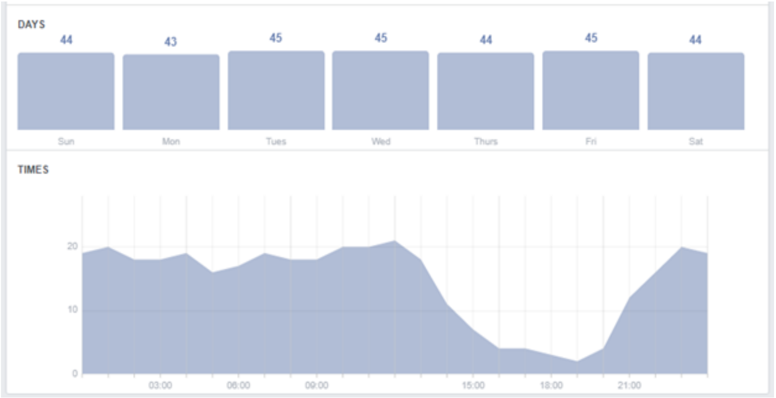
<table>
<tr><td>Date</td><td colspan="5">September 26, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Cyber-Trust Social Media</td></tr>
<tr><td>Communication type</td><td colspan="5">Twitter</td></tr>
<tr><td>Target audience</td><td>Partners
X</td><td>General
X</td><td>Academic
X</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">Elisavet Charalambous</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">The twitter profile has gathered approximately 5K impression over the so far spanned period with the months of May and September gaining most interest (Table 2-1). Over these two months, the consortium had been very busy with dissemination activities.
Table 2-1: Overall Twitter Engagement
<table>
<tr><th>Month</th><th>Tweet Impressions</th><th>Profile Visits</th></tr>
<tr><td><b>Sept 2019</b></td><td>2498</td><td>50</td></tr>
<tr><td><b>Aug 2019</b></td><td>1500</td><td>23</td></tr>
<tr><td><b>July 2019</b></td><td>1378</td><td>24</td></tr>
<tr><td><b>June 2019</b></td><td>1210</td><td>10</td></tr>
<tr><td><b>May 2019</b></td><td>1691</td><td>27</td></tr>
<tr><td><b>April 2019</b></td><td>2735</td><td>43</td></tr>
<tr><td><b>March 2019</b></td><td>1537</td><td>17</td></tr>
</table>
Figure 2-6 and Figure 2-7, shown below; illustrate highlights on Twitter and content that has gathered high interest in terms of engagement.</td></tr>
</table>

	 Sep 2019 · 25 days so far... TWEET HIGHLIGHTS **Top Tweet** earned 510 impressions #CyberTrust is participating in the #EUNWA meeting held in #Venice #Italy Our @CGI_Global and @aditesscy partners are attending the 2 day event on sharing security practices within #EU 2 2 View Tweet activity View all Tweet activity **Top Follower** followed by 990 people cyberwatching.eu @cyberwatchingeu FOLLOWS YOU The EU watch on #cybersecurity & #privacy. The EU's authoritative and independent source for democratising cybersecurity & privacy. View profile View followers dashboard **Top media Tweet** earned 325 impressions #CyberTrust has been presented in the EUNWA annual conference in association with the International Forum 2019 A thousand cities, million of citizens: A vision for our future Urban Security by our #CGI partner @gohar_s pic.twitter.com/NGL9SKM8re 3 3 View Tweet activity View all Tweet activity Figure 2-6: Highlights of September 2019  Apr 2019 · 30 days TWEET HIGHLIGHTS **Top Tweet** earned 1,076 impressions Our colleague Vasiliki Georgia Bilali form the Center for Security Studies (KEMEA) introduced at the GHOST EU Project during their workshop on the 28th of March. #iot #internetofthings #cybersecurity #h2020 #H2020PCW #InvestEUresearch #CyberTrustEU #GHOST_ProjectEU pic.twitter.com/ZGYWOUXIWo 2 5 View Tweet activity View all Tweet activity Figure 2-7: Highlights of April 2019
Annotated photos	N/A

2.2.2 Facebook

More information about communication of Cyber-Trust activities and outcomes performed through the Facebook page is given in the table below.

Date	September 26, 2019				
Communication activity	Cyber-Trust Social Media				
Communication type	Facebook				
Target audience	Partners X	General X	Academic X	Government X	Industry X
Partner(s) involved	ADITESS				
People involved	Elisavet Charalambous				
Description of the activity, relevance to the Project and Impact	The overall activity of the Cyber-Trust Facebook page has reached more than 1050+ users and gained engagement from 225+ users, the Facebook page gathered more than 90% of its interest organically. Cyber-Trust Posts appeared in the feed of almost 4000 Facebook users. The project Facebook page has so far concentrated 50 followers with 14 activity items. Facebook will be used as the channel of preference for the promotion of events in which consortium members will be participating. Facebook page insights also indicate that posting pictures results in higher reach, posting of links and status updates follow, see Figure 2-8. However, it is also revealed that in terms of engagements, status updates result in higher reaction rates while photos result in higher post click rates. Figure 2-9 shows that Facebook users are more likely to view content on the page midday onwards with a rise on Sundays.  Show All Posts ▾ Reach Post clicks Reactions, comments & shares Type Average Reach Average Engagement Photo 52 5 5 Link 31 2 1 Status 30 2 8 Figure 2-8: Engagement over post types				

	 Figure 2-9: Insights on times followers are active
Annotated photos	N/A

2.3 Research Conference presentations and publications

During this last period, the research undertaken in the project has already led to seven research publications that all accepted and presented in international conferences and are all available on publishers' websites. More details of these research publications are given in the tables below:

Date	June 24 - 26, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 120 people				
Partner(s) involved	CSCAN, UOP				
People involved	Bogdan Ghita, Stavros Shiaeles and Nicholas Kolokotronis				
Description of the activity, relevance to the Project and Impact	This paper examined the feasibility of using incremental machine learning to overcome the limitations that the signature- and rule-based industrial NIDS/NIPS suffer from, especially the low detection rates, the high false positives and the inability to detect unknown attacks. The paper introduced a novel Network Intrusion Prevention System that utilises a modified version of the Self-Organizing Incremental Neural Network (SOINN) for on-line clustering, coupled with a Support Vector Machine (SVM) to perform classification. This work was presented in the **10th IFIP International Conference on New Technologies, Mobility and Security (NTMS'2019)** that was held from 24 to 26 June 2019 in Canary Island – Spain (http://www.ntms-conf.org/ntms2019/). The paper is available at the publisher's website (https://ieeexplore.ieee.org/).				

	C. Constantinides, S. Shiaeles, B. Ghita and N. Kolokotronis, "A Novel Online Incremental Learning Intrusion Prevention System," ***2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)****, CANARY ISLANDS, Spain, 2019, pp. 1-6. DOI: 10.1109/NTMS .2019.8763842.* URL on the IEEE explore : :http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8763842&isnumber=8763770 This paper is directly related with the work carried out in the work-package WP6.
Annotated photos	N/A

Date	August 26 - 28, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 200 people				
Partner(s) involved	CSCAN, UOP				
People involved	Keltoum Bendiab, Stavros Shiaeles, Bogdan Ghita, Nicholas Kolokotronis				
Description of the activity, relevance to the Project and Impact	This paper examined limitations of traditional signature-based methods to protect IoT devices against the emerging security threats, by introducing a novel IoT malware traffic analysis approach using neural network and binary visualisation. This approach aims to fast analysis of real-time traffic data to detect and analyse unknown zero-day malware. The paper will be presented in the 19th International Conference on Next Generation Wired/Wireless Advanced Networks and Systems (NEW2AN/ruSMART 2019), LNCS, Springer, 2019, (http://www.new2an.org/#/). The conference was held on August 26 - 28, 2019 in St. Petersburg, Russia. The proceedings will be published in Springer LNCS (approved) and indexed in relevant databases including Scopus. *Shire, R., Shiaeles, S., Bendiab, K., Ghita, B., and Kolokotronis, N., (2019) Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation, 19th Int'l Conf. Next Generation Wired/Wireless Networking and 12th*				

	Conf. on Internet of Things and Smart Spaces (NEW2AN/ ruSMART 2019), LNC, Springer, 2019. DOI: https://doi.org/10.1007/978-3-030-30859-9_6 This work was developed based on the recommendations in deliverable D6.1 on the approaches and methods that are well suited for the Cyber-Trust platform, and it is directly related with the work carried out in the work-package WP6.
Annotated photos	N/A

Date	August 26 - 28, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 200 people				
Partner(s) involved	CSCAN				
People involved	Keltoum Bendiab, Stavros Shiaeles, Bogdan Ghita				
Description of the activity, relevance to the Project and Impact	This article studied the feasibility of using variations in overall Facebook user psychology to predict insider threats or prevent insider attacks and malicious activities. To this end, the paper introduced a new method to understand and evaluate user psychology Facebook user psychology through Open Source Intelligence (OSINT) and machine learning techniques. The paper will be presented in the **19th International Conference on Next Generation Wired/ Wireless Advanced Networks and Systems (NEW2AN/ ruSMART 2019), LNC, Springer, 2019.** Link to the conference: **(**http://www.new2an.org/#/**).** The conference was held on August 26 - 28, 2019 in St. Petersburg, Russia. The proceedings will be published in Springer LNCS (approved) and indexed in relevant databases **including Scopus.** *Panagiotou, A., Ghita, B., Shiaeles, S., and Bendiab, K., (2019), FaceWallGrap: Machine Learning in Detecting user's suspicious behaviour through Facebook wall, 19th Int'l Conf. Next Generation Wired/Wireless Networking and 12th Conf. on Internet of Things and Smart Spaces (NEW2AN/ruSMART 2019), LNC, Springer, 2019*. DOI: https://doi.org/10.1007/978-3-030-30859-9_11.				

	This work is directly related with the work carried out in the work-packages WP5 and WP6. The report is available at the Springer LNCS publisher's website.
Annotated photos	N/A

Date	July 8-13, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 120 people				
Partner(s) involved	CSCAN, UOP, MATHEMA				
People involved	Stavros Shiaeles, Nicholas Kolokotronis, Emanuele Bellini				
Description of the activity, relevance to the Project and Impact	This work focused on the inherent vulnerabilities of IoT devices and their inability to protect against outside attacks, due to the poor support for patching/updating and the poor on-board computational power. It mainly investigated the possibility of extracting valuable results regarding attacks' trends and predicting them, to have better protection against them, by crawling Deep/Dark and Surface web. The results of this work show that is possible to find the trend and be able to act proactively to protect the IoT ecosystem. The paper was presented in the **IEEE SERVICES 2019: 1st IEEE Services Workshop on Cyber Security and Resilience in the Internet of Things.** The workshop was held from 8 to 13 July 2019 in Milan – Italy (https://conferences.computer.org/services/2019/workshops/cybersecurity_workshop.html). The paper is now available at the IEEE publisher's website (https://ieeexplore.ieee.org/). *Shiaeles, S.***,** *Kolokotronis, N., Bellini, E., IoT Vulnerability Data Crawling and Analysis, IEEE SERVICES 2019: 1st IEEE Services Workshop on Cyber Security and Resilience in the Internet of Things, Milan, Italy, IEEE, 2019. DOI: 10.1109/SERVICES.2019.00028* This work is directly related with the work carried out in the work-packages WP5 and WP6				

Annotated photos	IoT Vulnerability Data Crawling and Analysis Stavros Shiaeles, Nicholas Kolokotronis, Emmanouil Bellini

<table>
<tr><td>Date</td><td colspan="5">July 8-13, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Scientific conference presentation and publication</td></tr>
<tr><td>Communication type</td><td colspan="5">Conference article</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General</td><td>Academic
X</td><td>Government</td><td>Industry
X</td></tr>
<tr><td>Number of participants</td><td colspan="5">Around 120 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">UOP, CSCAN</td></tr>
<tr><td>People involved</td><td colspan="5">Nicholas Kolokotronis, Sotirios Brotsis, Costas Vassilakis, Stavros Shiaeles</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">This paper examined the trust challenges raised by the Collaborative Intrusion Detection Networks (CIDNs). As a solution to these problems, it proposed the use of a trust-based blockchain in CIDNs to protect the integrity of the information shared among the CIDN peers, enhance their accountability, and secure their collaboration by thwarting insider attacks. A consensus protocol is proposed for CIDNs, which is a combination of a proof-of-stake and proof-of-work protocols, to enable collaborative Intrusion Detection System (IDS) nodes to maintain a reliable and tampered-resistant trust-chain. The paper was presented in the <b>IEEE SERVICES 2019: 1st IEEE Services Workshop on Cyber Security and Resilience in the Internet of Things.</b>
The workshop was held from 8 to 13 July 2019 in Milan – Italy (https://conferences.computer.org/services/2019/workshops/cybersecurity_workshop.html). The paper is now available at the IEEE publisher’s website (https://ieeexplore.ieee.org/).</td></tr>
</table>

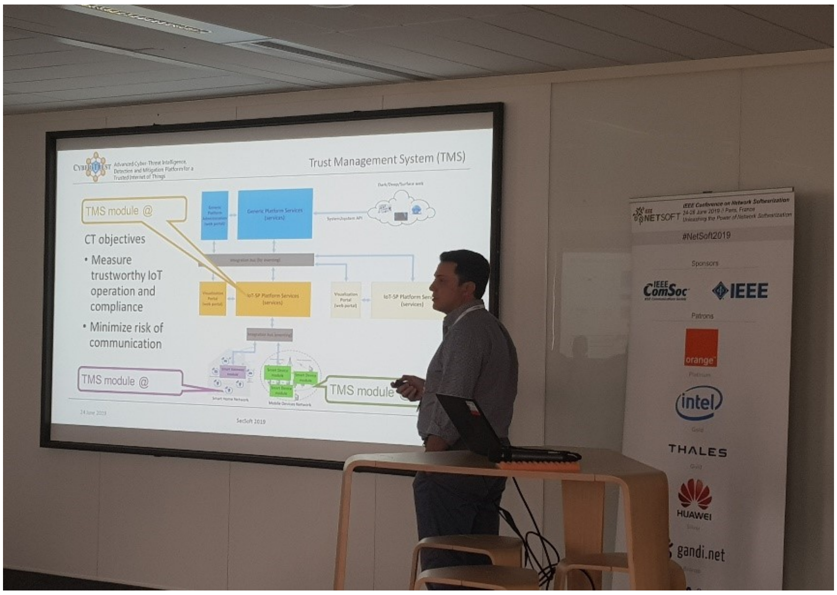
	Kolokotronis, N., Brotsis, S., Germanos, G., Vassilakis, C., and ***Shiaeles, S.,*** *(2019), On Blockchain Architectures for Trust-based Collaborative Intrusion Detection, IEEE SERVICES 2019: 1st IEEE Services Workshop on Cyber Security and Resiience in the Internet of Things, Milan, Italy, IEEE, 2019.* DOI: 10.1109/SERVICES.2019.00019. This work is directly related with the work carried out in the work-packages WP5 and WP6.
Annotated photos	

Date	July 8-13, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 120 people				
Partner(s) involved	UOP				
People involved	Paris Koloveas, Thanasis Chantzios, Christos Tryfonopoulos, Spiros Skiadopoulos				
Description of the activity, relevance to the Project and Impact	In this work, we focus on the information-gathering task of valuable cyber-security information that ---given the proper tools and methods ---may be identified, crawled and leveraged to actionable cyber-threat intelligence. We present a novel crawling architecture for transparently harvesting data from security websites in the clear web, security forums in the social web, and hacker forums/marketplaces in the dark web. The proposed architecture adopts a two-phase approach to data harvesting. Initially a machine learning-based crawler is used to				

	direct the harvesting towards websites of interest, while in the second phase state-of-the-art statistical language modelling techniques are used to represent the harvested information in a latent low-dimensional feature space and rank it based on its potential relevance to the task at hand. The proposed architecture is realised using exclusively open-source tools, and a preliminary evaluation with crowdsourced results demonstrates its effectiveness. The paper was presented in the **IEEE SERVICES 2019: 1st IEEE Services Workshop on Cyber Security and Resilience in the Internet of Things.** The workshop was held from 8 to 13 July 2019 in Milan – Italy (https://conferences.computer.org/services/2019/workshops/cybersecurity_workshop.html). The paper is now available at the IEEE publisher's website (https://ieeexplore.ieee.org/). *P. Koloveas, T. Chantzios, C. Tryfonopoulos, and S. Skiadopoulos, "A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence," accepted for publication in 1st IEEE Services Workshop on Cyber Security and Resilience in the Internet of Things (CSRIoT), 2019.* DOI: 10.1109/SERVICES.2019.00016. This work is directly related with the work carried out in the work-package WP5.
Annotated photos	

<table>
<tr><td>Date</td><td colspan="5">July 26-28, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Scientific conference presentation and publication</td></tr>
<tr><td>Communication type</td><td colspan="5">Conference article</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General</td><td>Academic
X</td><td>Government</td><td>Industry</td></tr>
<tr><td>Number of participants</td><td colspan="5">Around 120 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">UOP, KEMEA</td></tr>
<tr><td>People involved</td><td colspan="5">Thanasis Chantzios, Paris Koloveas, Spiros Skiadopoulos, Nicholas Kolokotronis, Christos Tryfonopoulos, Vassiliki-Georgia Bilali, Dimitris Kavallieros</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">In the recent years, due to the major increase of cyber-threats, CTI sharing is becoming increasingly important both as a subject of research and as a concept of providing additional security to organizations. However, selecting the proper tools and platforms for CTI sharing, is a challenging task, that pertains to a variety of aspects. In this paper, we start by overviewing the CTI procedure (threat types, categories, sources and the general CTI life-cycle). Then, we present a set of seven high-level CTI platform recommendations that can be used to evaluate a platform and subsequently we survey six state-of-the-art cyber-threat intelligence platforms. Finally, we compare and evaluate the six aforementioned platforms by means of the earlier proposed recommendations. The paper was presented in the <b>DATA 2019: 8th International Conference on Data Science, Technology and Applications</b>
The workshop was held from 26 to 28 July 2019 in Prague – Czech Republic (http://www.dataconference.org/?y=2019). The paper is now available at the publisher’s website (https://www.scitepress.org/ProceedingsDetails.aspx?ID=ntgme06zBBY=&t=1).
<i>T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V.-G. Bilali and D. Kavallieros, “The quest for the appropriate cyber-threat intelligence sharing platform,” in 8th Int’l Conference on Data Science, Technology and Applications (DATA), accepted for publication, 2019.</i>
This work is directly related with the work carried out in the work-packages WP5 and WP6.</td></tr>
<tr><td>Annotated photos</td><td colspan="5">N/A</td></tr>
</table>

Date	June 24-28, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 120 people				
Partner(s) involved	UOP, CSCAN, KEMEA, MATHEMA, Scorechain				
People involved	Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, Clement Pavue.				
Description of the activity, relevance to the Project and Impact	The technological evolution brought by the Internet of things (IoT) comes with new forms of cyber-attacks exploiting the complexity and heterogeneity of IoT networks, as well as, the existence of many vulnerabilities in IoT devices. The detection of compromised devices, as well as the collection and preservation of evidence regarding alleged malicious behaviour in IoT networks, emerge as areas of high priority. This paper presents a blockchain-based solution, which is designed for the smart home domain, dealing with the collection and preservation of digital forensic evidence. The system utilizes a private forensic evidence database, where the captured evidence is stored, along with a permissioned blockchain that allows providing security services like integrity, authentication, and non-repudiation, so that the evidence can be used in a court of law. The blockchain stores evidences' metadata, which are critical for providing the aforementioned services, and interacts via smart contracts with the different entities involved in an investigation process, including Internet service providers, law enforcement agencies and prosecutors. A high-level architecture of the blockchain based solution is presented that allows tackling the unique challenges posed by the need for digitally handling forensic evidence collected from IoT networks. The paper was presented in the **2019 IEEE Conference on Network Softwarization (NetSoft).** The workshop was held from 24-28 June 2019 in Paris, France, (https://netsoft2019.ieee-netsoft.org). The paper is now available at the publisher's website (https://ieeexplore.ieee.org/document/8806675). *S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros, E. Bellini, C. Pavué. "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments," 2019 IEEE*				

	Conference on Network Softwarization (NetSoft), Paris, France, 2019, pp. 110-114. [arXiv:1903.10770v1](https://arxiv.org/abs/1903.10770v1). This work is directly related with the work carried out in the work-packages WP5, WP6 and WP7
Annotated photos	 Trust Management System (TMS) TMS module @ CT objectives • Measure trustworthy IoT operation and compliance • Minimize risk of communication TMS module @ TMS module NETSOFT #NetSoft2019 ComSoc IEEE orange intel THALES HUAWEI gandi.net

Date	June 24-28, 2019				
Communication activity	Scientific conference presentation and publication				
Communication type	Conference article				
Target audience	Partners X	General	Academic X	Government	Industry X
Number of participants	Around 120 people				
Partner(s) involved	VUB, ADITESS, UOP, KEMEA, CGI, CSCAN,				
People involved	Olga Gkotsopoulou, Elisavet Charalambous, Konstantinos Limniotis, Paul Quinn, Dimitris Kavallieros, Gohar Sargsyan, Stavros Shiaeles, Nicholas Kolokotronis				
Description of the activity, relevance to the Project and Impact	The present paper deals with the elucidation and implementation of the Data Protection by Design (DPbD) principle as recently introduced in the European Union data protection law, specifically with regards to cybersecurity systems in a Smart Home environment, both from a legal and a technical perspective. Starting point constitutes the research conducted in the Cyber-Trust project, which endeavours the development of an innovative and customisable cybersecurity platform for cyber-threat intelligence gathering, detection and mitigation within the Internet of Things ecosystem. During the course of the paper, the requirements of DPbD with regards to the conceptualisation, design and actual development of the				

	system are introduced as prescribed in law. These requirements are then translated into technical solutions, as envisaged in the Cyber-Trust system. For trade-offs are not foreign to the DPbD context, technical limitations and legal challenges are also discussed in this interdisciplinary dialogue. The paper was presented in the **2019 IEEE Conference on Network Softwarization (NetSoft)** by KEMEA, the project coordinator. The workshop was held from 24-28 June 2019 in Paris, France, (https://netsoft2019.ieee-netsoft.org). The paper is now available at the publisher's website (https://ieeexplore.ieee.org/document/8806694) *O. Gkotsopoulou, E. Charalambous, K. Limniotis, P. Quinn, D. Kavallieros, G. Sargsyan, S. Shiaeles, N. Kolokotronis. "Data Protection by Design for cybersecurity systems in a Smart Home environment" 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 2019, pp. 101-109.* arXiv:1903.10778 This work is directly related with the work carried out mainly in the WP3, as well as WP5, WP6 and WP7.
Annotated photos	N/A

<table>
<tr><td>Date</td><td colspan="5">July 8-13, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Scientific conference presentation and publication</td></tr>
<tr><td>Communication type</td><td colspan="5">Conference article</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General</td><td>Academic
X</td><td>Government</td><td>Industry</td></tr>
<tr><td>Number of participants</td><td colspan="5">Around 120 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CGI</td></tr>
<tr><td>People involved</td><td colspan="5">Gohar Sargsyan, Nicolas Castellon, Raymond Binnendijk, Peter Cozijnsen</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">With the recent advances of IoT (Internet of Things) new and more robust security frameworks are needed to detect and mitigate new forms of cyber-attacks, which exploit complex and heterogeneity IoT networks, as well as, the existence of many vulnerabilities in IoT devices. The present paper introduces a high-level guide for the senior officials and decision makers in the organisations and technology managers for blockchain security framework by design principle for trust and adoption in IoT environments. The paper discusses Cyber-Trust project's blockchain technology development as a representative case study for offered security framework. Security and privacy by</td></tr>
</table>

	design approach is introduced as an important consideration in setting up the framework. The paper was presented in the "**IEEE World Congress on Services *(*IEEE SERVICES 2019**), that was held from 08-13 July 2019 at the Universita' degli Studi di Milano in Milan, Italy, (https://conferences.computer.org/services/2019/). The paper is now available at the publisher's website (https://ieeexplore.ieee.org/document/8817162). *SARGSYAN, Gohar, CASTELLON, Nicolas, BINNENDIJK, Raymond, et al. Blockchain Security by Design Framework for Trust and Adoption in IoT Environment. In: 2019 IEEE World Congress on Services (SERVICES). IEEE, 2019. p. 15-20.* ***DOI:*** *10.1109/SERVICES.2019.00018.* This work is directly related with the work carried out mainly in the WP3, as well as WP5, WP6 and WP7.
Annotated photos	ACKNOWLEDGMENT This paper is supported by the project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 786698. This work reflects authors' view and Agency is not responsible for any use that may be made of the information it contains.

2.4 Research Journal Publications

During this last period, Members of the consortium have published a research paper in the Elsevier Journal of Information Security and Applications (JISA) that focuses on original research and practice-driven applications with relevance to information security and applications. The journal has **1.537** Impact Factor and indexed the "**Emerging Sources Citation**" Index (ESCI). More information about the research publication is given in the following table.

Date	August, 2019				
Communication activity	Scientific publications				
Communication type	Journal article				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Over 400,000				
Partner(s) involved	CSCAN				
People involved	Muhammad Ali, Stavros Shiaeles				
Description of the activity, relevance to the Project and Impact	This journal paper investigated the behaviour of malware upon various Windows operating system versions to determine and correlate the relationship between malicious software and OS artefacts. This will enable an investigator to be more efficient in identifying the presence of new malware and provide a starting point for further investigation. The study analysed several versions of the Windows operating systems (Windows 7, 8.1 and 10) to identify how various forms of malware interact with key areas of the Registry. Using this knowledge, the study introduced an approach to predict the presence and type of malware present through an analysis of the Registry. To this end, different classifiers such as Neural Network (NN), Random Forest (RF), Decision Tree (DT), Boosted Tree (BT) and Logistic Regression (LR) were tested. This work has been published in the Journal of Information Security and Applications Volume 47, August 2019, Pages 139-155. The paper now available at the publisher's website (https://www.sciencedirect.com/science/article/pii/ S2214212618306367). *ALI, Muhammad, SHIAELES, Stavros, CLARKE, Nathan, et al. A proactive malicious software identification approach for digital forensic examiners. Journal of Information Security and Applications, 2019, vol. 47, p. 139-155. DOI: https://doi.org/10.1016/j.jisa.2019.04.013*. This scientific publication is directly related with the work carried out in the work-packages WP5, WP6, especially the Cyber defence service.				
Annotated photos	N/A				

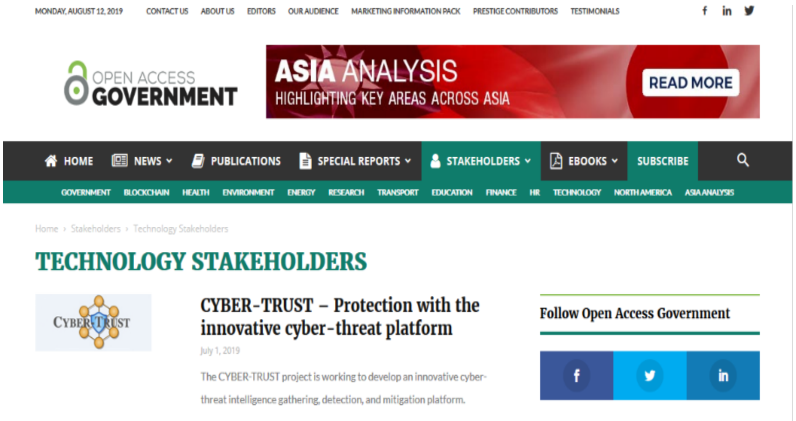
2.5 Other publications

In this last period of the Cyber-Trust project life, partners from CSCAN and UOP have been published several articles that promote the Cyber-Trust project, in the renowned magazine “**Open Access Government**”. This magazine is a Google News Approved website that has a wide audience across the public and private sectors, including the Research / Innovation and the local and central government sector. More details are given in the following tables.

<table>
<tr><td>Date</td><td colspan="5">July 1, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Publication in the Open Access Government Magazine</td></tr>
<tr><td>Communication type</td><td colspan="5">Press Releases</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 400,000 participants form the public and private sectors</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CSCAN</td></tr>
<tr><td>People involved</td><td colspan="5">Keltoum Bendiab, Stavros Shiaeles</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">

An advertisement of the Cyber-Trust project entitled “**CYBER-TRUST – Protection with the innovative cyber-threat platform**” (*see* Figure 2-10), which promote the Cyber-Trust project, has been published in the “**Technology Stakeholders**” rubric (*see* Figure 2-11*)*, in the renowned magazine “[Open Access Government](#)”. The article gives an overview of the Cyber-Trust project, the involved partners and the scientific publication in Conferences and Journals done in the first year of the project life.

Link to the full article: https://www.openaccessgovernment .org/cyber-trust/ 67800/).



TECHNOLOGY STAKEHOLDERS

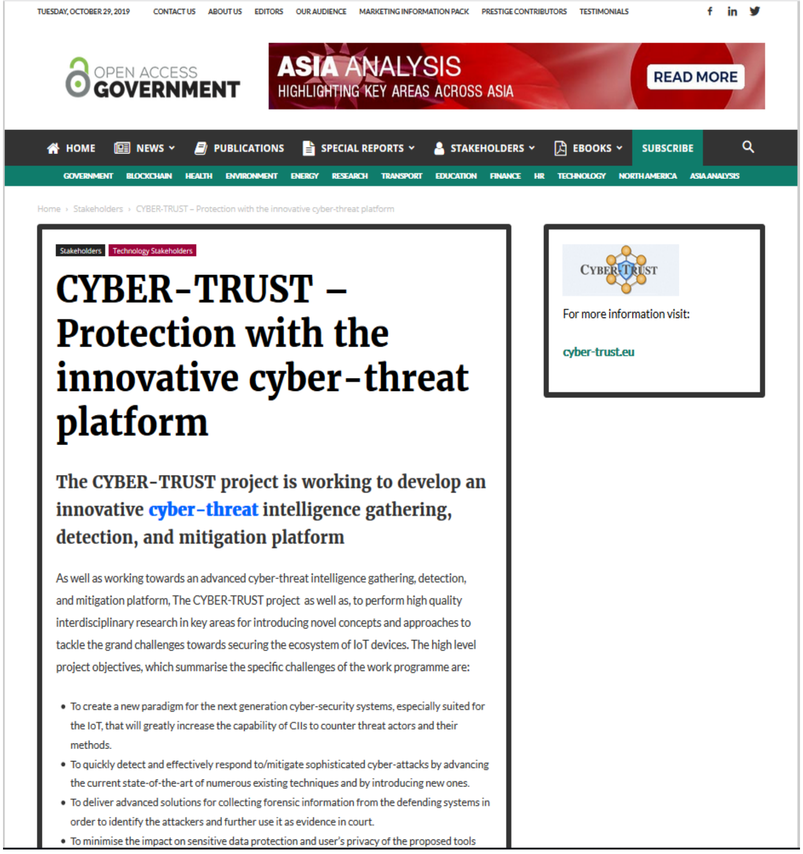
CYBER-TRUST – Protection with the innovative cyber-threat platform

July 1, 2019

The CYBER-TRUST project is working to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform.

Figure 2-10: Cyber-Trust project in the “Technology Stakeholders” rubric in “Open Access Government” magazine.

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



CYBER-TRUST – Protection with the innovative cyber-threat platform

The CYBER-TRUST project is working to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform

As well as working towards an advanced cyber-threat intelligence gathering, detection, and mitigation platform, The CYBER-TRUST project as well as, to perform high quality interdisciplinary research in key areas for introducing novel concepts and approaches to tackle the grand challenges towards securing the ecosystem of IoT devices. The high level project objectives, which summarise the specific challenges of the work programme are:

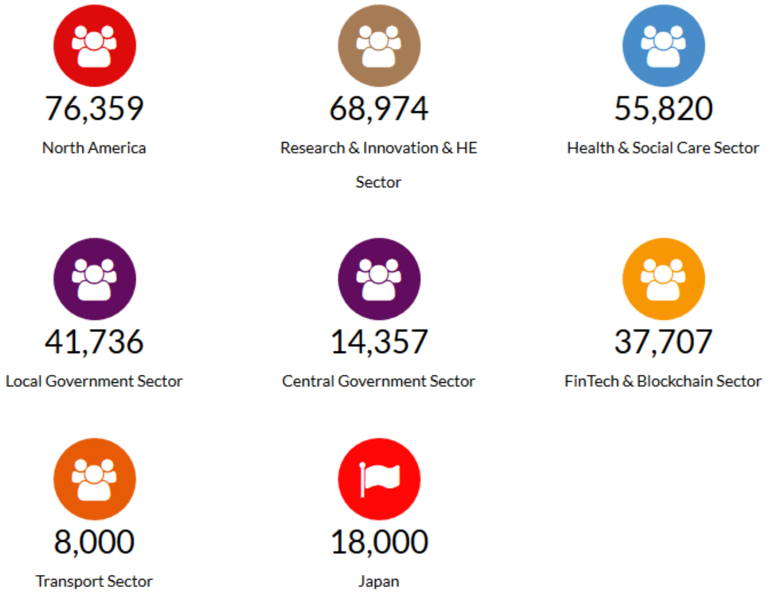
- To create a new paradigm for the next generation cyber-security systems, especially suited for the IoT, that will greatly increase the capability of CIIs to counter threat actors and their methods.
- To quickly detect and effectively respond to/mitigate sophisticated cyber-attacks by advancing the current state-of-the-art of numerous existing techniques and by introducing new ones.
- To deliver advanced solutions for collecting forensic information from the defending systems in order to identify the attackers and further use it as evidence in court.
- To minimise the impact on sensitive data protection and user's privacy of the proposed tools

Figure 2-11: Cyber-Trust project article in "Open Access Government" Magazine (Technology stakeholders)

The Open Access Government magazine has a wide audience across the public and private sectors, including the Research / Innovation and the local and central government sector more than **400, 000** participants from different public and private sectors, with more than **70,000** participants from the Research/Innovation sector. Open Access Government main publication gets distributed quarterly to over **100 000** key individuals, such as MEPs, EU commissioners, Government, Academic and Business leaders. Also, the website receives an average of 25 000 visits weekly.

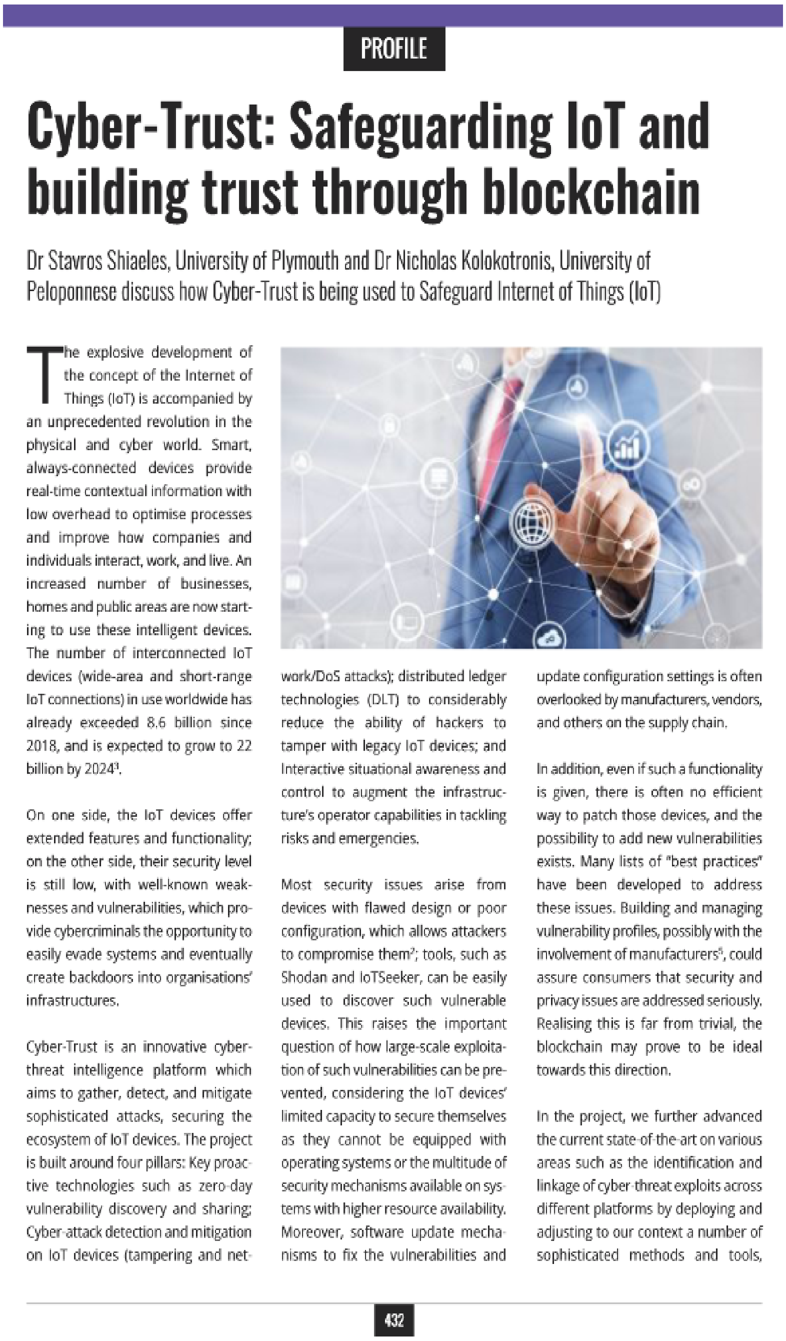
The distribution campaign from January achieved 27% open rate, and as you know the industry average is between 2-4%. This can only prove that OAG main document is in fact a trusted source of information to those key individuals.

Open Access Government is a Google News Approved website, so any news published really rank well in Google search results, with relative search terms.

Annotated photos	 Figure 2-12: Open Access Government audience

Date	July 1, 2019				
Communication activity	Publication in the Open Access Government Magazine				
Communication type	Press Releases				
Target audience	Partners	General X	Academic X	Government X	Industry X
Number of participants	More than **400,000** participants from the public and private sectors				
Partner(s) involved	CSCAN, UOP				
People involved	Stavros Shiaeles, Nikolaos Kolokotronis				
Description of the activity, relevance to the Project and Impact	Cyber-Trust partners from CSCAN and UOP have been published an article **entitled "Cyber-Trust: Safeguarding IoT and building trust through blockchain"** in the Open Access Government Magazine issue of July 2019 (Pages 432-433). The article presents an overview of the current security issues and vulnerabilities raised form IoT devices with flawed design or poor configuration. In order to overcome these drawbacks, the blockchain is presented as a pertinent technology to help stakeholders to better protect their assets against large-scale advanced cyber-attacks. The article is now available on the publisher web site (Pages 432-433). As mentioned before, this magazine has a wide audience across the public and private sectors, including the Research / Innovation and the local and central government sector (Figure 2-13).				

Link to the article: http://edition.pagesuite-professional .co.uk /html5/reader/production/default.aspx?pubname= &edid= d07278c7-9189-4e05-907f-4f904e1d68 5c, (Figure 2-13, Figure 2-14).



PROFILE

Cyber-Trust: Safeguarding IoT and building trust through blockchain

Dr Stavros Shiaeles, University of Plymouth and Dr Nicholas Kolokotronis, University of Peloponnese discuss how Cyber-Trust is being used to Safeguard Internet of Things (IoT)

The explosive development of the concept of the Internet of Things (IoT) is accompanied by an unprecedented revolution in the physical and cyber world. Smart, always-connected devices provide real-time contextual information with low overhead to optimise processes and improve how companies and individuals interact, work, and live. An increased number of businesses, homes and public areas are now starting to use these intelligent devices. The number of interconnected IoT devices (wide-area and short-range IoT connections) in use worldwide has already exceeded 8.6 billion since 2018, and is expected to grow to 22 billion by 2024[1].

On one side, the IoT devices offer extended features and functionality; on the other side, their security level is still low, with well-known weaknesses and vulnerabilities, which provide cybercriminals the opportunity to easily evade systems and eventually create backdoors into organisations' infrastructures.

Cyber-Trust is an innovative cyber-threat intelligence platform which aims to gather, detect, and mitigate sophisticated attacks, securing the ecosystem of IoT devices. The project is built around four pillars: Key proactive technologies such as zero-day vulnerability discovery and sharing; Cyber-attack detection and mitigation on IoT devices (tampering and network/DoS attacks); distributed ledger technologies (DLT) to considerably reduce the ability of hackers to tamper with legacy IoT devices; and Interactive situational awareness and control to augment the infrastructure's operator capabilities in tackling risks and emergencies.

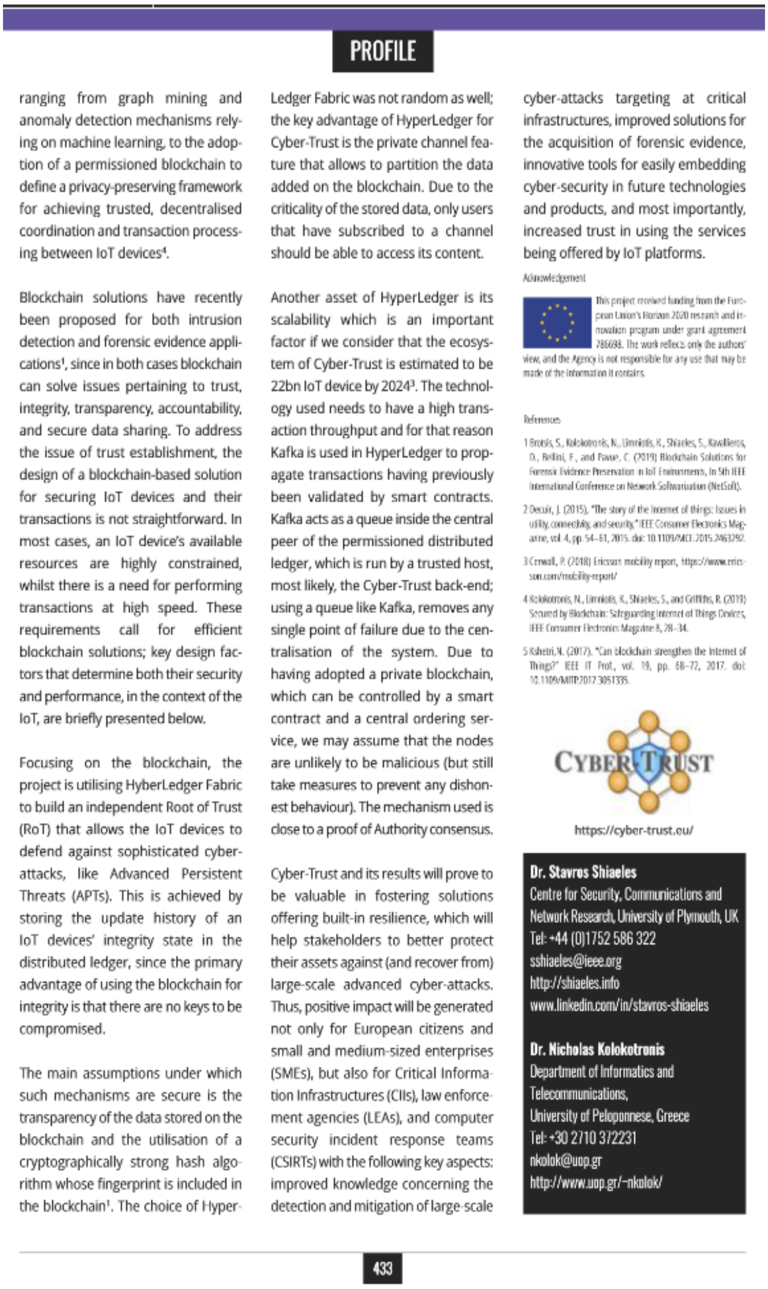
Most security issues arise from devices with flawed design or poor configuration, which allows attackers to compromise them[2]; tools, such as Shodan and IoTSeeker, can be easily used to discover such vulnerable devices. This raises the important question of how large-scale exploitation of such vulnerabilities can be prevented, considering the IoT devices' limited capacity to secure themselves as they cannot be equipped with operating systems or the multitude of security mechanisms available on systems with higher resource availability. Moreover, software update mechanisms to fix the vulnerabilities and update configuration settings is often overlooked by manufacturers, vendors, and others on the supply chain.

In addition, even if such a functionality is given, there is often no efficient way to patch those devices, and the possibility to add new vulnerabilities exists. Many lists of "best practices" have been developed to address these issues. Building and managing vulnerability profiles, possibly with the involvement of manufacturers[3], could assure consumers that security and privacy issues are addressed seriously. Realising this is far from trivial, the blockchain may prove to be ideal towards this direction.

In the project, we further advanced the current state-of-the-art on various areas such as the identification and linkage of cyber-threat exploits across different platforms by deploying and adjusting to our context a number of sophisticated methods and tools,

432

Figure 2-13:" Cyber-Trust: Safeguarding IoT and building trust through a blockchain" article published in the Open Access Government Magazine issue of July 2019 (Page 432).



PROFILE

ranging from graph mining and anomaly detection mechanisms relying on machine learning, to the adoption of a permissioned blockchain to define a privacy-preserving framework for achieving trusted, decentralised coordination and transaction processing between IoT devices[4].

Blockchain solutions have recently been proposed for both intrusion detection and forensic evidence applications[1], since in both cases blockchain can solve issues pertaining to trust, integrity, transparency, accountability, and secure data sharing. To address the issue of trust establishment, the design of a blockchain-based solution for securing IoT devices and their transactions is not straightforward. In most cases, an IoT device's available resources are highly constrained, whilst there is a need for performing transactions at high speed. These requirements call for efficient blockchain solutions; key design factors that determine both their security and performance, in the context of the IoT, are briefly presented below.

Focusing on the blockchain, the project is utilising HyberLedger Fabric to build an independent Root of Trust (RoT) that allows the IoT devices to defend against sophisticated cyber-attacks, like Advanced Persistent Threats (APTs). This is achieved by storing the update history of an IoT devices' integrity state in the distributed ledger, since the primary advantage of using the blockchain for integrity is that there are no keys to be compromised.

The main assumptions under which such mechanisms are secure is the transparency of the data stored on the blockchain and the utilisation of a cryptographically strong hash algorithm whose fingerprint is included in the blockchain[1]. The choice of HyperLedger Fabric was not random as well; the key advantage of HyperLedger for Cyber-Trust is the private channel feature that allows to partition the data added on the blockchain. Due to the criticality of the stored data, only users that have subscribed to a channel should be able to access its content.

Another asset of HyperLedger is its scalability which is an important factor if we consider that the ecosystem of Cyber-Trust is estimated to be 22bn IoT device by 2024[3]. The technology used needs to have a high transaction throughput and for that reason Kafka is used in HyperLedger to propagate transactions having previously been validated by smart contracts. Kafka acts as a queue inside the central peer of the permissioned distributed ledger, which is run by a trusted host, most likely, the Cyber-Trust back-end; using a queue like Kafka, removes any single point of failure due to the centralisation of the system. Due to having adopted a private blockchain, which can be controlled by a smart contract and a central ordering service, we may assume that the nodes are unlikely to be malicious (but still take measures to prevent any dishonest behaviour). The mechanism used is close to a proof of Authority consensus.

Cyber-Trust and its results will prove to be valuable in fostering solutions offering built-in resilience, which will help stakeholders to better protect their assets against (and recover from) large-scale advanced cyber-attacks. Thus, positive impact will be generated not only for European citizens and small and medium-sized enterprises (SMEs), but also for Critical Information Infrastructures (CIIs), law enforcement agencies (LEAs), and computer security incident response teams (CSIRTs) with the following key aspects: improved knowledge concerning the detection and mitigation of large-scale cyber-attacks targeting at critical infrastructures, improved solutions for the acquisition of forensic evidence, innovative tools for easily embedding cyber-security in future technologies and products, and most importantly, increased trust in using the services being offered by IoT platforms.

Acknowledgement

This project received funding from the European Union's Horizon 2020 research and innovation program under grant agreement 786698. The work reflects only the authors' view, and the Agency is not responsible for any use that may be made of the information it contains.

References

1 Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., and Pavue, C. (2019) Blockchain Solutions for Forensic Evidence Preservation in IoT Environments, In 5th IEEE International Conference on Network Softwarization (NetSoft).

2 Decuir, J. (2015). "The story of the Internet of things: Issues in utility, connectivity, and security," IEEE Consumer Electronics Magazine, vol. 4, pp. 54–61, 2015. doi: 10.1109/MCE.2015.2463292.

3 Cerwall, P. (2018) Ericsson mobility report, https://www.ericsson.com/mobility-report/

4 Kolokotronis, N., Limniotis, K., Shiaeles, S., and Griffiths, R. (2019) Secured by Blockchain: Safeguarding Internet of Things Devices, IEEE Consumer Electronics Magazine 8, 28–34.

5 Kshetri, N. (2017). "Can blockchain strengthen the Internet of Things?" IEEE IT Prof., vol. 19, pp. 68–72, 2017. doi: 10.1109/MITP.2017.3051335.

https://cyber-trust.eu/

Dr. Stavros Shiaeles
Centre for Security, Communications and Network Research, University of Plymouth, UK
Tel: +44 (0)1752 586 322
sshiaeles@ieee.org
http://shiaeles.info
www.linkedin.com/in/stavros-shiaeles

Dr. Nicholas Kolokotronis
Department of Informatics and Telecommunications,
University of Peloponnese, Greece
Tel: +30 2710 372231
nkolok@uop.gr
http://www.uop.gr/~nkolok/

433

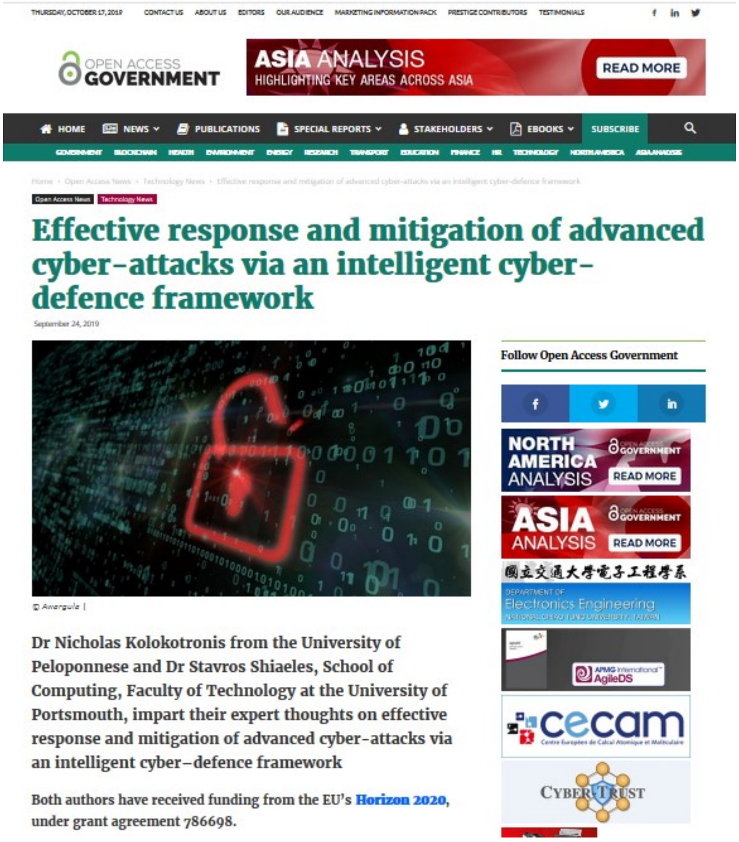
Figure 2-14:" Cyber-Trust: Safeguarding IoT and building trust through a blockchain" article published in the Open Access Government Magazine issue of July 2019 (Page 433).

Link to the Open Access Government Magazine issue of July 2019: https://www.openaccessgovernment.org/category/publications/,

Open Access Government is a Google News Approved website, so any news published really rank well in Google search results, with relative search terms.

Annotated photos	 OPEN ACCESS GOVERNMENT ISSN 2516-3817 • July 2019 Packets made from seaweed sturdy enough to contain liquids © Ooho 302 BUILDING A SUSTAINABLE FUTURE FROM OUR OCEANS TO ADDRESS MODERN-DAY SUSTAINABILITY CHALLENGES, THE EMBRC-ERIC WAS ESTABLISHED TO BRIDGE THE GAP BETWEEN MARINE BIOLOGICAL RESEARCH AND INNOVATION IN THIS ISSUE 18 **Paola Testori Coggi** speaks to Open Access Government about her work on defending investments in public health and the White Paper on food safety 188 **Jim Siegrist**, Associate Director at the U.S. Department of Energy details how the organisation is building for discovery, using the excellent example of their High Energy Physics program 192 **John Halligan TD**, Minister of State for Training, Skills, Innovation, Research and Development charts the research and innovation landscape in Ireland today Featured eBook KIT Featured eBook The Balgrist Featured eBook PLACEmaking Supported by University of Cambridge, UC Davis Veterinary Medicine Figure 2-15: Open Access Government Magazine issue of July 2019.

Date	September 24, 2019				
Communication activity	Publication in the Open Access Government Magazine				
Communication type	Press Releases				
Target audience	Partners	General X	Academic X	Government X	Industry X
Number of participants	More than **400,000** participants form the public and private sectors				
Partner(s) involved	CSCAN, UOP				
People involved	Stavros Shiaeles, Nikolaos Kolokotronis				
Description of the activity, relevance to the Project and Impact	Cyber-Trust partners from CSCAN and UOP have been published an article entitled **“Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework”** in the Open Access Government website (*see* Figure 2-16). The article presents an overview of the current security issues and vulnerabilities raised form IoT				

	devices and the importance of intelligent intrusion response systems (iIRS) in enhancing the capability of intrusion detection systems to respond to advanced cyber-attacks. The article highlights the benefit of combining ML-based intrusion detection systems (IDS) and GCSMs (Graphical cyber security models) for iIRS. Link to the article: https://www.openaccessgovernment.org/advanced-cyber-attacks/73967/ This work is directly related with the work carried out in the work-packages WP5 and WP6 of the Cyber-Trust project
Annotated photos	 THURSDAY, OCTOBER 17, 2019 CONTACT US ABOUT US EDITORS OUR AUDIENCE MARKETING INFORMATION PACK PRESTIGE CONTRIBUTORS TESTIMONIALS OPEN ACCESS GOVERNMENT ASIA ANALYSIS HIGHLIGHTING KEY AREAS ACROSS ASIA READ MORE HOME NEWS PUBLICATIONS SPECIAL REPORTS STAKEHOLDERS EBOOKS SUBSCRIBE GOVERNMENT BLOCKCHAIN HEALTH ENVIRONMENT ENERGY RESEARCH TRANSPORT EDUCATION FINANCE HR TECHNOLOGY NORTH AMERICA ASIA ANALYSIS Home › Open Access News › Technology News › Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework Open Access News Technology News Follow Open Access Government NORTH AMERICA ANALYSIS READ MORE ASIA ANALYSIS READ MORE 國立交通大學電子工程學系 DEPARTMENT OF Electronics Engineering APMG International AgileDS cecam Centre Européen de Calcul Atomique et Moléculaire CYBER-TRUST © Avergula | Effective response and mitigation of advanced cyber–attacks via an intelligent cyber–defence framework September 24, 2019 Dr Nicholas Kolokotronis from the University of Peloponnese and Dr Stavros Shiaeles, School of Computing, Faculty of Technology at the University of Portsmouth, impart their expert thoughts on effective response and mitigation of advanced cyber–attacks via an intelligent cyber–defence framework Both authors have received funding from the EU's **Horizon 2020**, under grant agreement 786698. Figure 2-16: Article "Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework" on the Open Access Government website.

2.6 Organised dissemination events

This section presents the disseminations events arranged or planned to be organised by Cyber-Trust partners during the reporting period, with the aim to promote Cyber-Trust conducted activities. The following tables give more information about these events.

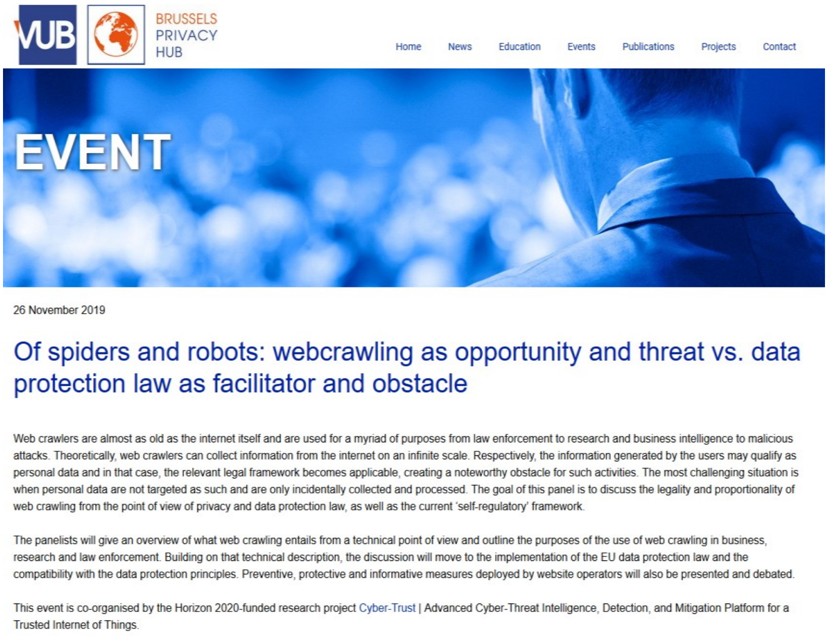
<table>
<tr><td>Date</td><td colspan="5">July 8-13, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Organization of IEEE SERVICES CSR-IoT workshop</td></tr>
<tr><td>Communication type</td><td colspan="5">All workshop’s organisational aspects</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General</td><td>Academic
X</td><td>Government</td><td>Industry
X</td></tr>
<tr><td>Number of participants</td><td colspan="5">Around 120 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">MATHEMA, CSCAN, UOP</td></tr>
<tr><td>People involved</td><td colspan="5">Emanuele Bellini, Stavros Shiaeles, Nicholas Kolokotronis</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">The workshop focuses on both the theoretical & practical aspects of the security, privacy, trust and resilience of IoT networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks.
TOPICS OF INTEREST
Topics of interest included but were not limited to:
▪ Blockchain applications in IoT
▪ Cyber-threat intelligence
▪ Game-theoretic security for IoT
▪ Identity management and access control for IoT
▪ IoT and cloud forensics
▪ Lightweight cryptography for IoT
▪ Malware detection and mitigation
▪ Network intrusion detection/mitigation
▪ Privacy and data protection in IoT
▪ Security in mobile applications
▪ System and data integrity
▪ Trust management for IOT
▪ Operation recovery and continuity in IOT
▪ Cyber-attack resiliency IoT architecture
▪ Cyber Threat adaptive capacity in IOT</td></tr>
<tr><td>Annotated photos</td><td colspan="5">
THE 1ST IEEE SERVICES WORKSHOP ON CYBER SECURITY AND RESILIENCE IN THE INTERNET OF THINGS
Figure 2-17: The workshop website</td></tr>
</table>

<table>
<tr><td>Date</td><td colspan="5">June, 2019 – October, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Preparation towards the organisation of a panel at CPDP 2020 (January 2020)</td></tr>
<tr><td>Communication type</td><td colspan="5">Exchange of emails; contact with speakers; taking care of organisational aspects</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>Number of participants</td><td colspan="5">1000+</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">VUB, KEMEA</td></tr>
<tr><td>People involved</td><td colspan="5">Olga Gkotsopoulou, Paul Quinn, Dimitris Kavallieros, Vasiliki Georgia Bilali</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">22-24 January 2020, Computers, Privacy and Data Protection (CPDP) 2020 – Data Protection and Artificial Intelligence CPDP is a non-profit platform originally founded in 2007 by research groups from the Vrije Universiteit Brussel, the University de Namur and Tilburg University. The platform holds every year a conference in Brussels (Belgium) which attracts more than 1000 attendees from academia, industry, government, EU institutions, tech and law enforcement.
Cyber-Trust will be represented, as research project, with a full panel on “<b>AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection?</b>”
More information on the conference can be found here: https://www.cpdpconferences.org/</td></tr>
<tr><td>Annotated photos</td><td colspan="5">
13th INTERNATIONAL CONFERENCE 22 - 24 JAN 2020 BRUSSELS, BELGIUM
CPDP 2020 DATA PROTECTION AND ARTIFICIAL INTELLIGENCE

ABOUT
CONTRIBUTE
SPONSORS &amp; PARTNERS
ATTEND
CONTACT

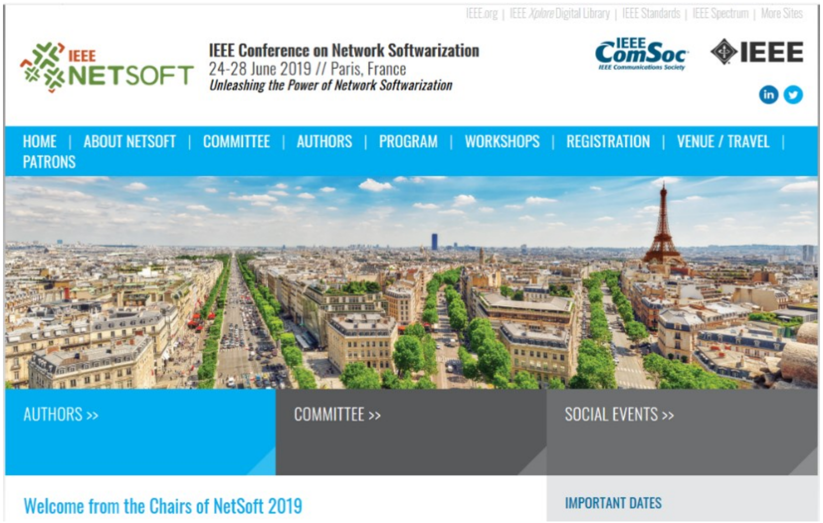
CPDP2020
REGISTER NOW!
Early bird fees available till November 30, 2019
Figure 2-18: CPDP 2020 conference website</td></tr>
</table>

<table>
<tr><td>Date</td><td colspan="5">June, 2019 – October, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Preparation towards the organisation of a panel in cooperation with Brussels Privacy Hub (November 2019)</td></tr>
<tr><td>Communication type</td><td colspan="5">Exchange of emails; contact with speakers; taking care of organisational aspects</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>Number of participants</td><td colspan="5">30-40</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">VUB (Lead), KEMEA, CGI</td></tr>
<tr><td>People involved</td><td colspan="5">Olga Gkotsopoulou, Paul Quinn, Dimitris Kavallieros, Vasiliki Georgia Bilali, Dimitra Papadaki, Georgia Melenikou, Gohar Sarsgyan</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">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.
The panelists will give an overview of what web crawling entails from a technical point of view and outline the purposes of the use of web crawling in business, research and law enforcement. Building on that technical description, the discussion will move 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 will also be presented and debated.
This event is co-organised by the Horizon 2020-funded research project Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things.
The panel is directly related to research conducted in WP3 and WP5.
Link to the event:
https://www.brusselsprivacyhub.eu/events/26112019.html</td></tr>
</table>

<table>
<tr><td>Annotated photos</td><td>
BRUSSELS PRIVACY HUB
Home News Education 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.
The panelists will give an overview of what web crawling entails from a technical point of view and outline the purposes of the use of web crawling in business, research and law enforcement. Building on that technical description, the discussion will move 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 will also be presented and debated.
This event is co-organised by the Horizon 2020-funded research project Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things.
Figure 2-19: Brussels Privacy Hub and Cyber-Trust event on 26 November 2019</td></tr>
</table>

<table>
<tr><td>Date</td><td colspan="5">June 24 – 28, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Organization of NetSoft 2019 workshop</td></tr>
<tr><td>Communication type</td><td colspan="5">Exchange of emails; contact with speakers; taking care of organisational aspects</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">200+</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">UOP, KEMEA, CSCAN</td></tr>
<tr><td>People involved</td><td colspan="5">N. Kolokotronis, S. Shiaeles, D. Kavallieros</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">The 5th IEEE International Conference on Network Softwarization (NetSoft 2019) will be held on June 24-28, 2019 in Paris, France. IEEE NetSoft has been created as a flagship conference aiming at addressing “Softwarization” of networks and systemic trends concerning the convergence of Cloud Computing, Software-Defined Networking (SDN), and Network Functions Virtualization (NFV).
IEEE NetSoft invites proposals for full-day or half-day workshops. The purpose of the workshops is to complement the conference program with in-depth or integration forums that are dedicated to related and emerging topics ((i.e. self-organizing smart networks, Big-Data-based management and control, management of tactile internet, edge software networks etc.) and/or other specific topics of NetSoft 2019.</td></tr>
</table>

	Proposals from industry and academia are welcome. Accepted and presented workshop papers will be published in the conference proceedings and will be submitted to IEEE Xplore. For reference, NetSoft 2019 will highlight the theme "*Unleashing the power of network softwarization*", covering topics that include the following: • Programmable SDN and NFV: languages, architectures, environments • Softwarized cloud, fog, and edge infrastructures • Cognitive and autonomic networking • Network slicing and slice management • Mobility management in software networks • Policy-based and Intent-Based Networking • Centralized vs Distributed control, management & orchestration • Abstractions and virtualization of resources, services, and functions • Service Function Chaining • Container/micro service-based network functions • Efficient network/service monitoring in SDN/NFV • AI techniques to support network automation • Analytics and big data approaches for managing softwarized networks • QoS and QoE in softwarized infrastructures • Resilience, reliability, and robustness of softwarized networks • Cooperative multi-party, multi-domain, multi-tenant SDN/NFV environments • Security, Safety, Trust and Privacy support in virtualized environments • SDN switch/router architecture and design • Dynamic resource discovery mechanisms and service parameter/resource negotiation schemes • APIs, protocols, and languages for programmable networks • Lifecycle management of network software • DevOps methodologies for network softwarization • Debugging and introspection of software-defined virtualized systems

	- Service fulfilment assurance systems in SDN/NFV environments - Softwarized platforms for Internet of Things (IoT) - Energy efficient and green software-defined infrastructures (SDI) - Transition strategies from existing networks to SDN/NFV - New service models and paradigms enabled by softwarization - New value chains and business models - Socio-economic impact and regulatory implications for softwarization
Annotated photos	 IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites IEEE NETSOFT IEEE Conference on Network Softwarization 24-28 June 2019 // Paris, France Unleashing the Power of Network Softwarization IEEE ComSoc IEEE Communications Society IEEE HOME | ABOUT NETSOFT | COMMITTEE | AUTHORS | PROGRAM | WORKSHOPS | REGISTRATION | VENUE / TRAVEL | PATRONS AUTHORS >> COMMITTEE >> SOCIAL EVENTS >> Welcome from the Chairs of NetSoft 2019 IMPORTANT DATES Figure 2-20: IEEE NetSoft website

Date	October 29-31, 2019				
Communication activity	Organization of the Mediterranean Security Event (MSE 2019)				
Communication type	All organisational aspects				
Target audience	Partners X	General X	Academic X	Government X	Industry X
Number of participants	Around 200 people				
Partner(s) involved	ADITESS, KEMEA				
People involved	Dimitris Kavallieros, Vasiliki Georgia Bilali				
Description of the activity, relevance to the Project and Impact	The Mediterranean Security event focuses on multiple security-oriented research areas that have been identified as of high priority by EU. MSE2019 embraces the need for a trust-based, multilateral and cross-sectoral cooperation among the community of Security R&D stakeholders in the European Union. MSE2019 is not only an event but an active inter-				

	national community integrating the experience and transferring the knowledge of experts and professionals. It is co-organized by Cyber-Trust partners with the community of Security R&D stakeholders in the European Union and takes place in in Fodele (Heraclion), Crete (Greece) on 29-31 October 2019. Link to the event: https://mse2019.kemea-research.gr/ Between the **29th and the 31st of October 2019**, **more than 250 attendees** are expected to join the event and have the opportunity to attend keynote speeches and projects presentations organized in thematic sessions, participate in plenary and parallel sessions, be informed on security research findings, join round tables, focused workshops and live demos of security solution MAIN THEMATIC SUBJECTS ▪ Protection of Critical Infrastructure and Public Spaces. ▪ European Initiatives on Security and Networks of Practitioners. ▪ Border and External Security ▪ Disaster management and Resilience ▪ Fight Against Crime and Terrorism ▪ Cyber and Digital Security Cyber-Trust is one of the 36 EU co-organising projects of the event. The project will have a dedicated booth during the three days in order to demonstrate the tools. Furthermore, at the last day of the event, which is dedicated at DS and FCT projects, Cyber-Trust will be presented to the audience.
Annotated photos	 Figure 2-21: Logo of the Mediterranean Security event

2.7 Event Participation

During the last period, CGI partner from the Cyber-Trust project have participated in Cybersecurity events in October that were organised by the Hague Security Delta (HSD) in conjunction with the European Cyber-security month. In these events, partners 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 police, government, academia, and industry. More details are provided in the following tables.

<table>
<tr><td>Date</td><td colspan="5">October, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Show case CyberTrust in European Cybersecurity months at HSD, The Hague, The Netherlands</td></tr>
<tr><td>Communication type</td><td colspan="5">Exhibition, and show case</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>Number of participants</td><td colspan="5">4600</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CGI</td></tr>
<tr><td>People involved</td><td colspan="5">Gohar Sargsyan (CGI)</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">Each year The Hague Security Delta (HSD), in cooperation with partners, organise and host Cybersecurity events in October. This year, in conjunction with the European Cyber-security month, HSD supported entire month of the events instead of one week like previous years. October was announced as cybersecurity month with series of events also in The Netherlands by HSD. CGI, as a member of HSD, each year contributes to the event and participates with showcases. Among other cybersecurity solutions, CGI show-cased Cyber-Trust project within this event in different occasions (workshops, innovation room, and show case sessions</td></tr>
<tr><td>Annotated photos</td><td colspan="5">

Thank you for your interest in the European Cybersecurity Month
This is an advocacy campaign taking place in October benefiting the citizens. It is supported by *ENISA* and *EC DG CONNECT* with the participation of many partners.

Staying secure online
October is CyberSecMonth

Figure 2-22: European Cybersecurity Month website</td></tr>
</table>

2.8 Presentations

In the last period, Cyber-Trust project has been presented in several events to spread the new knowledge generated by the partners and for enhancing its visibility to the academic community and the industry. More details are given in the following tables.

Date	May & September, 2019				
Communication activity	Presentation of the Cyber-Trust project to National CSIRT-CY				
Communication type	Presentation of the Cyber-Trust project to National CSIRT-CY				
Target audience	Partners	General	Academic	Government x	Industry
Number of participants	Around 15 people				
Partner(s) involved	ADITESS				
People involved	Elisavet Charalambous, Michael Skitsas, George Boulougaris, Nikolaos Koutras				
Description of the activity, relevance to the Project and Impact	National CSIRT-CY (https://csirt.cy/) envisions the increase of the security posture of The Republic of Cyprus by enhancing cyber protection of its National Critical Information Infrastructures (CII), banks and ISPs. National CSIRT-CY shall coordinate and assist CII owners/administrators, banks and ISPs to ensure the existence of (at least) a minimum level of security, by implementing proactive and reactive security services to reduce the risks of network information and cyber security incidents, as well as respond to such incidents as and when they occur. National CSIRT-CY shall also undertake awareness actions in order to educate the local population and National stakeholders about the adverse effects of cyber threats and cybercrime. In an earnest effort to enhance the security posture of the nation, the National CSIRT-CY shall provide timely advisories to all its constituents and make necessary efforts to introduce advanced security services such as security testing, vulnerability scanning, and active network monitoring. ADITESS had the chance to present the Cyber-Trust project and the two sides agreed in keeping a continuous communication link as regards the updates on project's results. Furthermore, in the near future and future meetings ways of exploitation of the Cyber-Trust project's outputs will be discussed more thoroughly.				
Annotated photos	N/A				

Date	May, 2019				
Communication activity	Presentation of the project during the ASGARD project Hackathons in Lisbon				
Communication type					
Target audience	Partners	General	Academic x	Government x	Industry x
Number of participants	Around 60 people				
Partner(s) involved	ADITESS				

People involved	Elisavet Charalambous
Description of the activity, relevance to the Project and Impact	The ASGARD hackathon is a bi-annually arranged event within the 42-month ASGARD (EU Restricted H2020) project with a rather large consortium and great attention from security stakeholders. During this event, project partners may present interesting technologies and the project relevant to ASGARD's interest.
Annotated photos	N/A

<table>
<tr><td>Date</td><td colspan="5">September 2-3, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Presentation of CyberTrust at Urban Security International Mayors' Forum and EUNWA Annual conference, Venice, Italy</td></tr>
<tr><td>Communication type</td><td colspan="5">Conference, workshop, presentation, focused groups meetings</td></tr>
<tr><td>Target audience</td><td>Partners
x</td><td>General</td><td>Academic
x</td><td>Government
x</td><td>Industry
x</td></tr>
<tr><td>Number of participants</td><td colspan="5">Around 172 participants</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CGI (lead), ADITESS (involved)</td></tr>
<tr><td>People involved</td><td colspan="5">Gohar Sargsyan (CGI), Elisavet Charalambous (ADITESS)</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">A Thousands Cities, Millions of Citizens: A Vision for our Future Urban Security International Mayors 'forum took place in Venice, Italy between Sept 2-3, 2019 in coloration with EUNWA annual conference. The event was opened by the Mayor of Venice. Some 50 city mayors were present and 14 of which were speakers which included, Antwerp, NYC, Prague, Moscow, Lisbon among others. The event was about sharing the safety and security of each country/city citizens and learning from each other how best to contribute to each other business. EUNWA was one of the partners of the event and also organised its annual conference linked to this mayor event. Among other safety cybersecurity was one of the key topics on today's life for vulnerable citizens. After a welcome note during the urban security event, CGI's Gohar Sargsyan presented Cyber-Trust to the mayors, LEA representatives and EUNWA members. The project was received with high interest and will be followed up with interested parties. Elisavet Charalambous from ADITESS as a support technology partner of EUNWA was also involved and supported further clarifications and questions on Cyber-Trust.
Link to the event: https://www.miict.eu/2019/09/26/miict-project-in-eunwa-conference-in-venice-2-3-september-2019/.</td></tr>
</table>

Annotated photos	

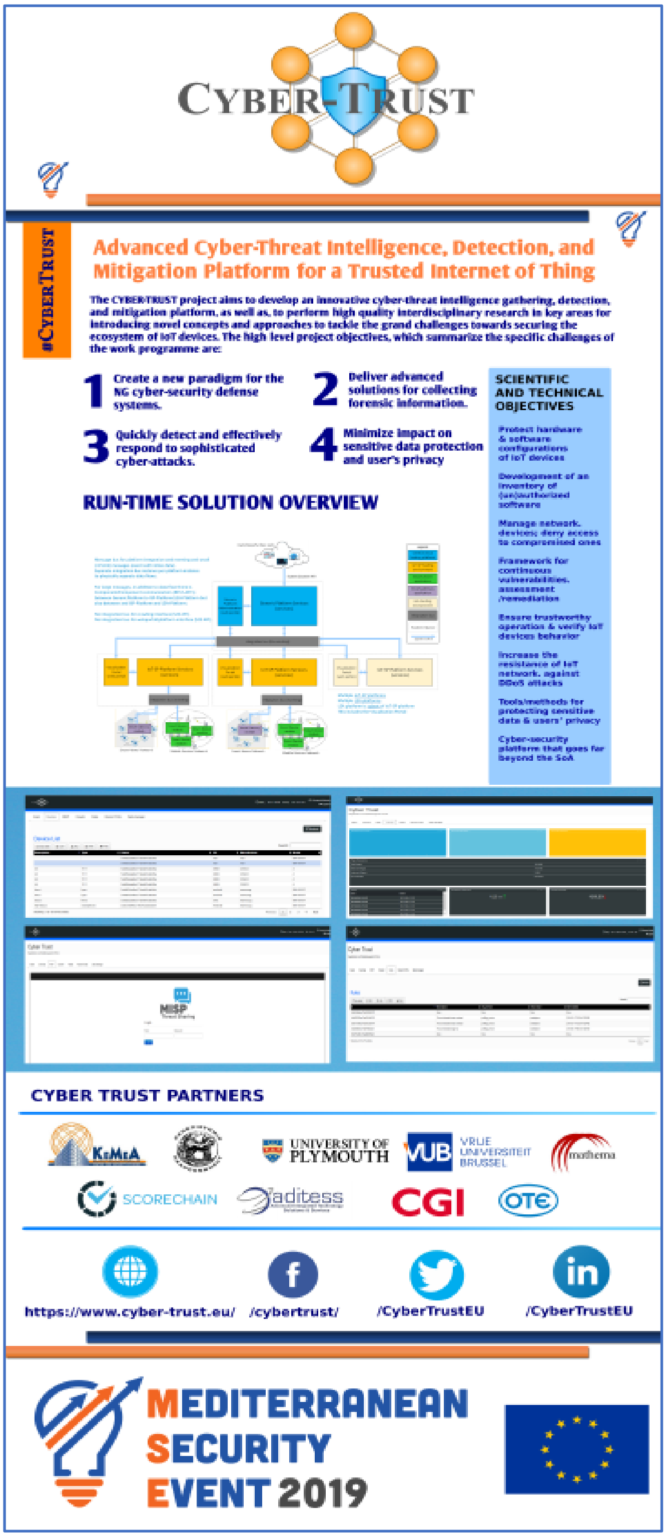
<table>
<tr><td>Date</td><td colspan="5">October 2, 2019</td></tr>
<tr><td>Communication activity</td><td colspan="5">Show case Cyber-Trust at the DIGILINCE 2019 event</td></tr>
<tr><td>Communication type</td><td colspan="5">Conference presentation</td></tr>
<tr><td>Target audience</td><td>Partners
X</td><td>General
X</td><td>Academic
x</td><td>Government
X</td><td>Industry
x</td></tr>
<tr><td>Number of participants</td><td colspan="5">212</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CGI</td></tr>
<tr><td>People involved</td><td colspan="5">Gohar Sargsyan (CGI), Mary Jo de Leeuw (Advisory board member)</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">During the event DIGILENCE 2019 (Digital Transformation, Cyber Security and Resilience) Cyber-Trust project was introduced among Cybersecurity solutions for IoT environments. The project's advisory board member Mary Jo de Leeuw was a speaker in the event and Gohar Sargsyan from CGI was a support partner
Link to the event: https://digilience.org/</td></tr>
<tr><td>Annotated photos</td><td colspan="5">

DIGILIENCE 2019
Sofia, Bulgaria
2-4 October 2019
NORTH AMERICA
SOUTH AMERICA
AFRICA
ASIA
Indian Ocean

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

2.9 Brochures and Leaflet

A conference banner was produced to be used in the **Mediterranean Security Event 2019** (MSE2019), which is organised by the community of Security R&D stakeholders in the European Union and takes place in Crete (Greece).



#CYBERTRUST

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

The CYBER-TRUST project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, to perform high quality interdisciplinary research in key areas for introducing novel concepts and approaches to tackle the grand challenges towards securing the ecosystem of IoT devices. The high level project objectives, which summarize the specific challenges of the work programme are:

1 Create a new paradigm for the NG cyber-security defense systems.

2 Deliver advanced solutions for collecting forensic information.

3 Quickly detect and effectively respond to sophisticated cyber-attacks.

4 Minimize impact on sensitive data protection and user's privacy

SCIENTIFIC AND TECHNICAL OBJECTIVES

Protect hardware & software configurations of IoT devices

Development of an inventory of (un)authorized software

Manage network. devices; deny access to compromised ones

Framework for continuous vulnerabilities. assessment /remediation

Ensure trustworthy operation & verify IoT devices behavior

Increase the resistance of IoT network. against DDoS attacks

Tools/methods for protecting sensitive data & users' privacy

Cyber-security platform that goes far beyond the SoA

RUN-TIME SOLUTION OVERVIEW

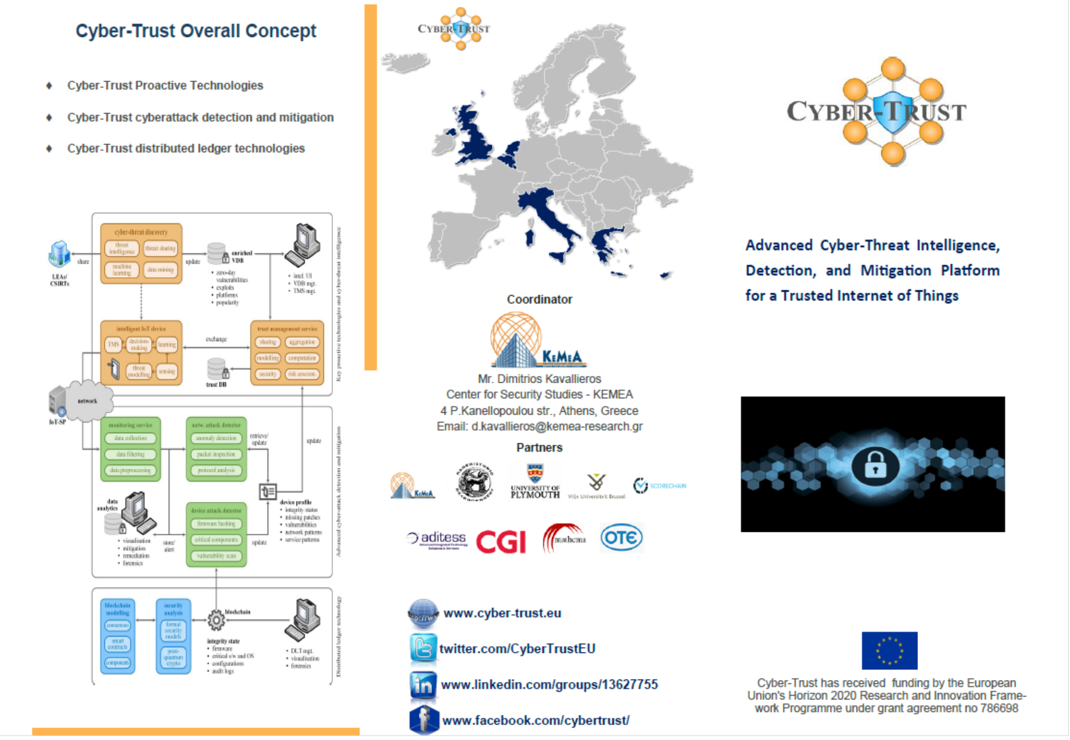
CYBER TRUST PARTNERS

https://www.cyber-trust.eu/ /cybertrust/ /CyberTrustEU /CyberTrustEU

MEDITERRANEAN SECURITY EVENT 2019

Figure 2-23: MSE Banner

A new leaflet (triptych) was designed in order to present the overall objectives, components and approach of the project.



Cyber-Trust Overall Concept

- Cyber-Trust Proactive Technologies
- Cyber-Trust cyberattack detection and mitigation
- Cyber-Trust distributed ledger technologies

cyber-threat discovery
threat intelligence
threat sharing
machine learning
data mining
share
LEAs/ CSIRTs
update
enriched VDB
• zero-day vulnerabilities
• exploits
• platforms
• popularity
• intel. UI
• VDB mgt.
• TMS mgt.
intelligent IoT device
TMS
decision-making
learning
threat modelling
sensing
exchange
trust management service
sharing
aggregation
modelling
computation
security
risk assessm.
trust DB
network
IoT-SP
monitoring service
data collection
data filtering
data preprocessing
netw. attack detector
anomaly detection
packet inspection
protocol analysis
retrieve/ update
update
device profile
• integrity status
• missing patches
• vulnerabilities
• network patterns
• service patterns
data analytics
• visualisation
• mitigation
• remediation
• forensics
store/ alert
device attack detector
firmware hashing
critical components
vulnerability scan
update
blockchain modelling
consensus
smart contracts
components
security analysis
formal security models
post-quantum crypto
blockchain
integrity state
• firmware
• critical s/w and OS
• configurations
• audit logs
• DLT mgt.
• visualisation
• forensics
Key proactive technologies and cyber-threat intelligence
Advanced cyber-attack detection and mitigation
Distributed ledger technology

CYBER-TRUST

Coordinator

KEMEA

Mr. Dimitrios Kavallieros
Center for Security Studies - KEMEA
4 P.Kanellopoulou str., Athens, Greece
Email: d.kavallieros@kemea-research.gr

Partners

KEMEA UNIVERSITY OF PLYMOUTH Vrije Universiteit Brussel SCORECHAIN aditess CGI mathema OTE

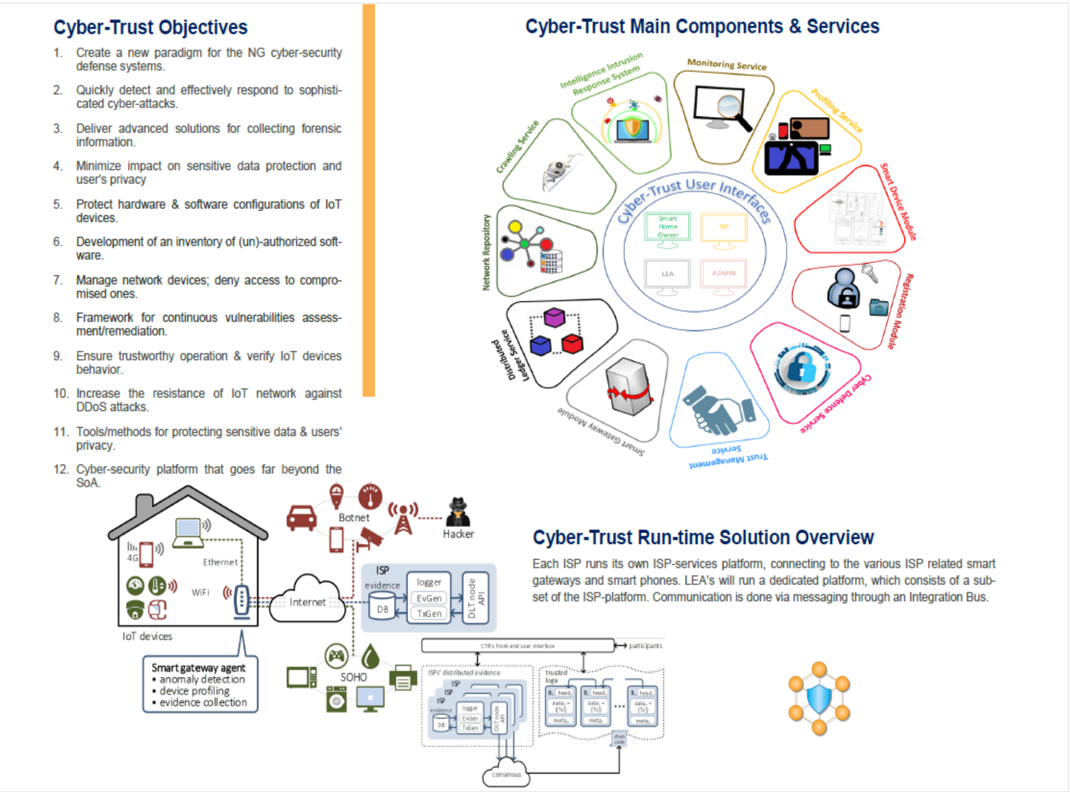
www.cyber-trust.eu
twitter.com/CyberTrustEU
www.linkedin.com/groups/13627755
www.facebook.com/cybertrust/

CYBER-TRUST

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

Cyber-Trust has received funding by the European Union's Horizon 2020 Research and Innovation Framework Programme under grant agreement no 786698

Figure 2-24: Leaflet for the Cyber-Trust project



Cyber-Trust Objectives

1. Create a new paradigm for the NG cyber-security defense systems.
2. Quickly detect and effectively respond to sophisticated cyber-attacks.
3. Deliver advanced solutions for collecting forensic information.
4. Minimize impact on sensitive data protection and user's privacy
5. Protect hardware & software configurations of IoT devices.
6. Development of an inventory of (un)-authorized software.
7. Manage network devices; deny access to compromised ones.
8. Framework for continuous vulnerabilities assessment/remediation.
9. Ensure trustworthy operation & verify IoT devices behavior.
10. Increase the resistance of IoT network against DDoS attacks.
11. Tools/methods for protecting sensitive data & users' privacy.
12. Cyber-security platform that goes far beyond the SoA.

Cyber-Trust Main Components & Services

Smart gateway agent
- anomaly detection
- device profiling
- evidence collection

Cyber-Trust Run-time Solution Overview

Each ISP runs its own ISP-services platform, connecting to the various ISP related smart gateways and smart phones. LEA's will run a dedicated platform, which consists of a sub-set of the ISP-platform. Communication is done via messaging through an Integration Bus.

Figure 2-25: Leaflet for the Cyber-Trust project

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 (M13 -M18) of the project life. The number of website visits reached more than 4157 visits, with a growth of approximately 70% compared to the previous period (M7-M12). In addition, social media channels garnered over 80% of its interest during this period. In terms of research publications and dissemination events, Cyber-Trust partners have published more than 18 research projects since the beginning of the project, exceeding the number of targeted publications.

Table 3-1: Summary of dissemination activities

Dissemination Type	Actual	Target (project life)
Website Visits	4157	10800
Brochure	3	3
Scientific Publications	18	15
Press Releases	3	8
Blogs	1	10 in total
Newsletter	0	5 in total
Workshops	10	At least 5
Presentations	20	30
Social Media	131	/
Direct Contact	3	/

In summary, according to the statistics in Table 3-1 and as self-assessment, Cyber-Trust partners think that they will reach and exceeds the KPIs introduced in D9.2 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 third period of the project life (May 2018–October 2019). 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.