Ref. Ares(2018)5611289 - 01/11/2018

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

Grant Agreement: 786698

D9.3 Disseminations activities report (1st 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: 31/10/2018

Document Submission Date: 01/11/2018

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

Document Information

Deliverable number:	D9.3
Deliverable title:	Dissemination activities report (1st Report)
Deliverable version:	1.0
Work Package number:	WP9
Work Package title:	Dissemination and exploitation of results
Due Date of delivery:	31/10/2018
Actual date of delivery:	01/11/2018
Dissemination level:	PU
Editor(s):	Stavros Shiaeles (CSCAN)
Contributor(s):	Bogdan Ghita, Stavros Shiaeles (CSCAN) Christos Tryfonopoulos, Costas Vassilakis, Nicholas Kolokotronis, Paris Koloveas (UOP) Emanuele Bellini (MATH) Gohar Sargsyan, Raymond Binnendijk (CGI) Dimitrios Kavallieros, George Kokkinis (KEMEA) Liza Charalambous, Romeos Bratska (ADITESS)
Reviewer(s):	Giovana Bilali (KEMEA) Xenia Pouli (MTN)
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	1/10/2018	CSCAN	Initial Draft
0.1	18/10/2018	CSCAN	Incorporated partners' dissemination activities
0.5	24/10/2018	ALL	Partners review their act
0.8	27/10/2018	KEMEA, MTN	Review
0.9	31/10/2018	CSCAN	Final editing and review
1.0	01/10/2018	KEMEA	Final version and submission to the EC

Acronyms

ACRONYM	EXPLANATION
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
KPI	Key Performance Indicator
LEA	Law Enforcement Agency Application Programming Interface
NFV	Network Functions Virtualization
SDN	Software Defined Networking

Contents

EXECUTIVE SUMMARY 5

1. Introduction 6

2. Dissemination activities across different channels 7

2.1 Websites and Blogs 7

2.2 Research Conference presentations and publications 16

2.3 Research Journal Publications 21

2.4 Organised dissemination events 22

2.5 Event Participation 25

2.6 Presentations 27

2.7 Synergies with other Projects 32

2.8 Brochures and Poster 33

3. Progress Monitoring 35

4. Conclusion 36

List of figures

Figure 2.1: Audience Overview 8
Figure 2.2: User flow 8
Figure 2.3: Visits per continent and Distribution of visitation with respect to time of the day 9
Figure 2.4: Country of Origin for Visiting Users 9
Figure 2.5: Distribution of traffic sources 10
Figure 2.6: Highlights of October 2018 11
Figure 2.7: Highlights of September 2018 12
Figure 2.8: Highlights of May 2018 12
Figure 2.9: Activity summary for a 28-day duration 13
Figure 2.10: Posts on Facebook Page 14
Figure 2.11: Engagement over post types 15
Figure 2.12: Insights on times followers are active 15
Figure 2.13: Dr Stavros Shiaeles explaining Cyber-Trust and the work been conducted 19
Figure 2.14: Dr Stavros Shiaeles explaining simulated environment for LDDoS attacks 19
Figure 2.15: Mr Muhhamad Ali presenting paper on malware detection using dynamic analysis and agentless sandboxes as part of his PhD studies 21
Figure 2.16: Proposed special session in GIIS 2018 conference 24
Figure 2.17: Mr Kavallieros presenting Cyber-Trust in the 6th Exposec 27
Figure 2.18: Mr Kavallieros presenting Cyber-Trust in EuCNC 2018 28
Figure 2.19: Ms Elisavet Charalambous presenting Cyber-Trust 30
Figure 2.20: Workshop attendees 30
Figure 2.21: Cyber-Trust Flyer 33
Figure 2.22: Cyber-Trust Poster 34

List of tables

Table 2.1: Overall Twitter Engagement 10
Table 3.1: Summary of dissemination activities 35

EXECUTIVE SUMMARY

This dissemination report is the first of the reports that will encircle the disseminations of activities of Cyber-Trust project partners. The activities that will be reported in this document are covering the activities been held from May 2018 until October 2018 M1-M6.

1. Introduction

This section will provide the purpose of the first Dissemination Report from the start of Cyber-Trust project until end of October 2018.

The deliverable is organized as follows: Section 2 presents the dissemination and communication tools of the Cyber-Trust project. It is divided into seven subsections where the various communications channels are presented. These are the Cyber-Trust website, the social media channels (Facebook, Twitter, LinkedIn, Youtube), the scientific publication in Conferences and Journals, presentations in various events, dissemination material (Brochures, roll top banner and Newsletters) and Synergies with other projects. Finally, Section 3 – Progress Monitoring presents Cyber-Trust performance information with respect to the KPIs introduced in D9.2 – "Dissemination and Exploitation plan".

2. Dissemination activities across different channels

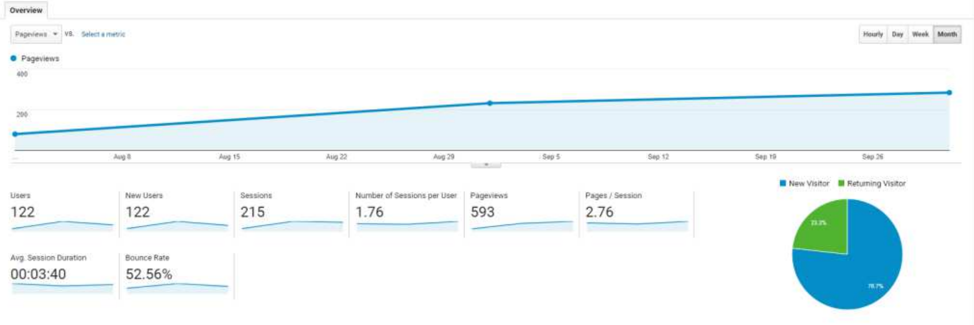
This section will list all Cyber-Trust partners activities from month 1 to month 6. Cyber-Trust partners as can be concluded from the subsection followed, disseminate the project drastically during the last six months. The subsection followed will provide details on activities carried out from partners group based on the KPIs provided in Deliverable 9.2.

2.1 Websites and Blogs

The website hosts a 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 website is used as a first line of dissemination, providing up to date information on activities as soon as they happen. The website usage is monitored using the free Google Analytics service to determine the level of engagement from the research and commercial community, items that generate more interest, and any queries raised by visitors. The Cyber-Trust website has been officially released since the end of August 2018. The tables below provide a summary of the web traffic statistics.

In addition to the web presence, the project also has dedicated Twitter and Facebook feeds, included in the analysis below.

Date	29 October 2018				
Communication activity	Cyber-Trust website				
Communication type	Website				
Target audience	Partners	General	Academic	Government	Industry
	X	X	X	X	X
Partner(s) involved	ADITESS				
People involved	Elisavet Charalambous				
Description of the activity, relevance to the Project and Impact	The following figure (see Figure 2.1) shows the overview of the visiting audience as a figure of new and returned visitors overall (76.7% of users are new visitors while 23.3% are returning visitors). In total 122 users have visited the Cyber-Trust website with a total of 593 page views.				



Users 122

New Users 122

Sessions 215

Number of Sessions per User 1.76

Pageviews 593

Pages / Session 2.76

Avg. Session Duration 00:03:40

Bounce Rate 52.56%

Figure 2.1: Audience Overview

Additionally, on average, the user visited approximately 3 pages with a visit duration of 3 minutes and 40 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 2.2Figure 2.2: User flow, 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.

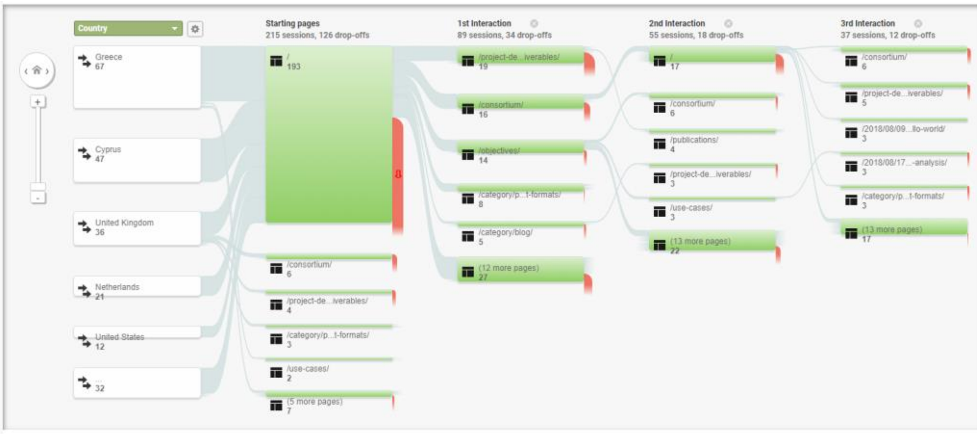


Figure 2.2: User flow

So far, the project website received most visits from Europe, with most traffic occurring midday onwards between Wednesdays and Fridays (see Figure 2.3).

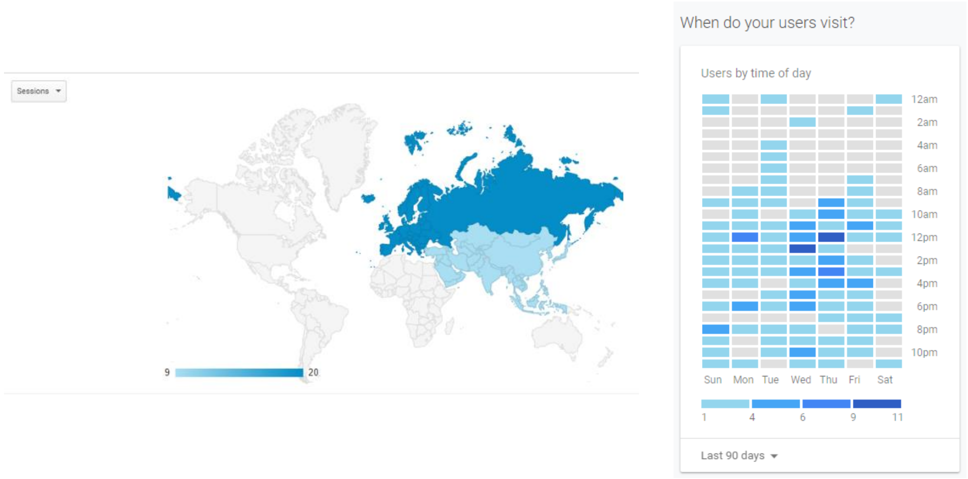
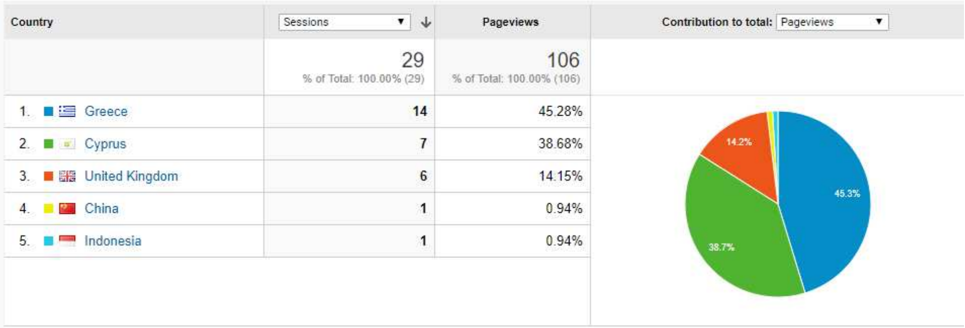


Figure 2.3: Visits per continent and Distribution of visitation with respect to time of the day

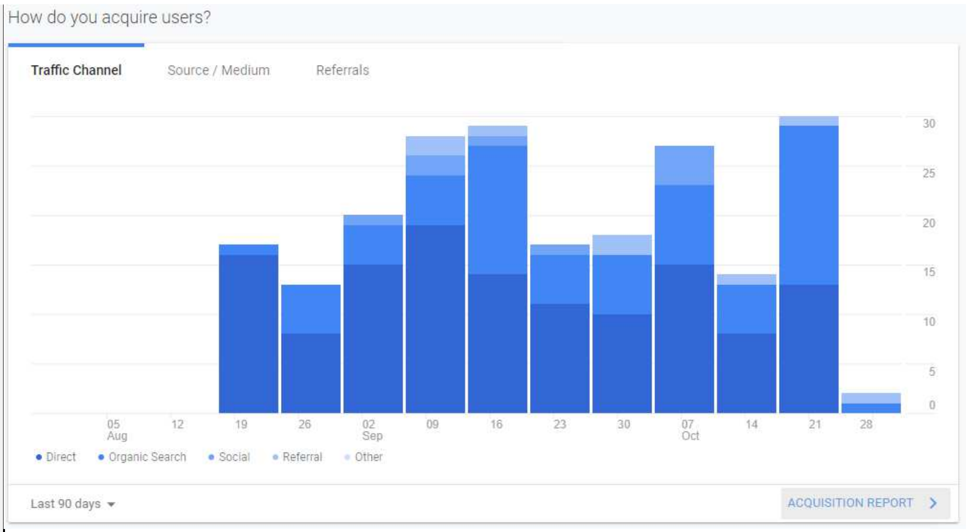
Also important is the demographics on the country of origin of visiting users (see **Error! Reference source not found.**). The top three countries are Greece (45%), Cyprus (39%) and UK (14%) and occupy 98% of visitation.



Country	Sessions	Pageviews	Contribution to total: Pageviews
	29 % of Total: 100.00% (29)	106 % of Total: 100.00% (106)	
1. 🟦 Greece	14	45.28%	
2. 🟩 Cyprus	7	38.68%	
3. 🟥 United Kingdom	6	14.15%	
4. 🟨 China	1	0.94%	
5. 🟦 Indonesia	1	0.94%	

Figure 2.4: Country of Origin for Visiting Users

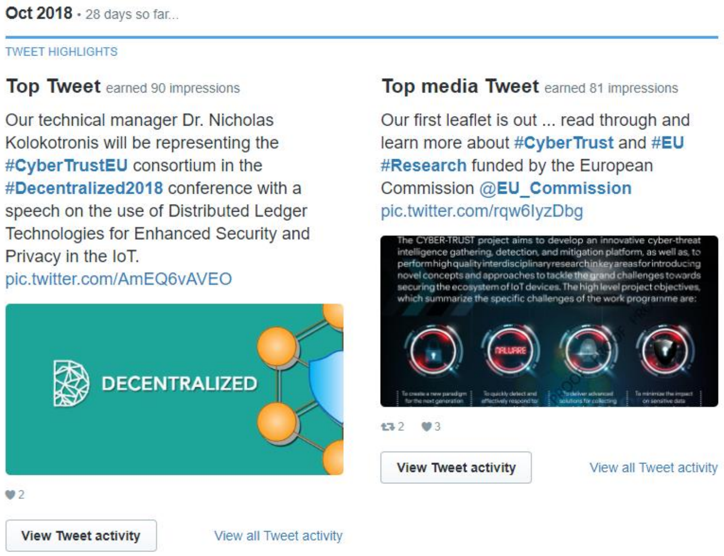
Most visits on the Cyber-Trust website are generated by the visitors typing the URL in the address bar on their Internet browsers, the second source is through organic searching (i.e. through search engines) and finally through social media. As time progresses, it is expected that the traffic attained through social media channels will increase, as a result of the project increased visibility.

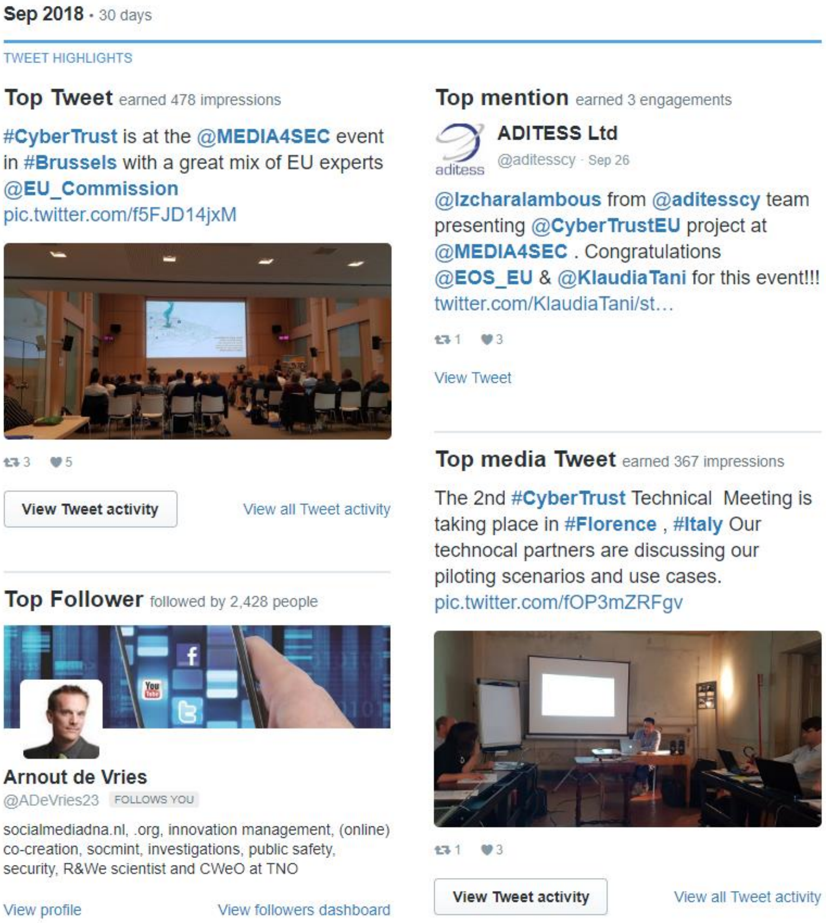
	 Figure 2.5: Distribution of traffic sources
Annotated photos	N/A

Date	29 October 2018				
Communication activity	Social Media				
Communication type	Twitter				
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 twitter profile has gathered approximately 5K impression over the so far spanned period with the months of May and September gaining most interest (see Table 2.1). Over these two months the consortium had been very busy with dissemination activities.				

Table 2.1: Overall Twitter Engagement

Month	Tweet Impressions	Profile Visits
Oct 2018	516	24
Sept 2018	1305	13
Aug 2018	215	5
July 2018	96	6
June 2018	504	1
May 2018	2301	43

	Figure 2.6, Figure 2.7, Figure 2.8 shown below, illustrate highlights on Twitter and content that has gathered high interest in terms of engagement.  **Oct 2018** · 28 days so far... TWEET HIGHLIGHTS **Top Tweet** earned 90 impressions Our technical manager Dr. Nicholas Kolokotronis will be representing the **#CyberTrustEU** consortium in the **#Decentralized2018** conference with a speech on the use of Distributed Ledger Technologies for Enhanced Security and Privacy in the IoT. pic.twitter.com/AmEQ6vAVEO ♥ 2 View Tweet activity View all Tweet activity **Top media Tweet** earned 81 impressions Our first leaflet is out ... read through and learn more about **#CyberTrust** and **#EU** **#Research** funded by the European Commission **@EU_Commission** pic.twitter.com/rqw6lyzDbg 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: MALWARE To create a new paradigm for the next generation To quickly detect and effectively respond to To deliver advanced solutions for collecting To minimize the impact on sensitive data ⇄ 2 ♥ 3 View Tweet activity View all Tweet activity Figure 2.6: Highlights of October 2018



Sep 2018 · 30 days

TWEET HIGHLIGHTS

Top Tweet earned 478 impressions

#CyberTrust is at the @MEDIA4SEC event in #Brussels with a great mix of EU experts @EU_Commission pic.twitter.com/f5FJD14jxM

⇄ 3 ♥ 5

View Tweet activity View all Tweet activity

Top Follower followed by 2,428 people

Arnout de Vries
@ADeVries23 FOLLOWS YOU

socialmediadna.nl, .org, innovation management, (online) co-creation, socmint, investigations, public safety, security, R&We scientist and CWeO at TNO

View profile View followers dashboard

Top mention earned 3 engagements

ADITESS Ltd
@aditesscy · Sep 26

@lzcharalambous from @aditesscy team presenting @CyberTrustEU project at @MEDIA4SEC . Congratulations @EOS_EU & @KlaudiaTani for this event!!! twitter.com/KlaudiaTani/st…

⇄ 1 ♥ 3

View Tweet

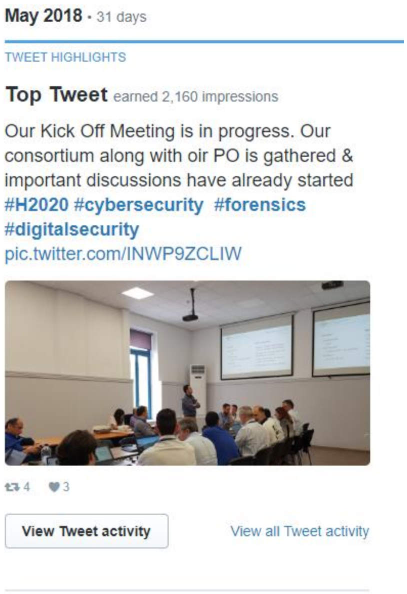
Top media Tweet earned 367 impressions

The 2nd #CyberTrust Technical Meeting is taking place in #Florence , #Italy Our technocal partners are discussing our piloting scenarios and use cases. pic.twitter.com/fOP3mZRFgv

⇄ 1 ♥ 3

View Tweet activity View all Tweet activity

Figure 2.7: Highlights of September 2018



May 2018 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 2,160 impressions

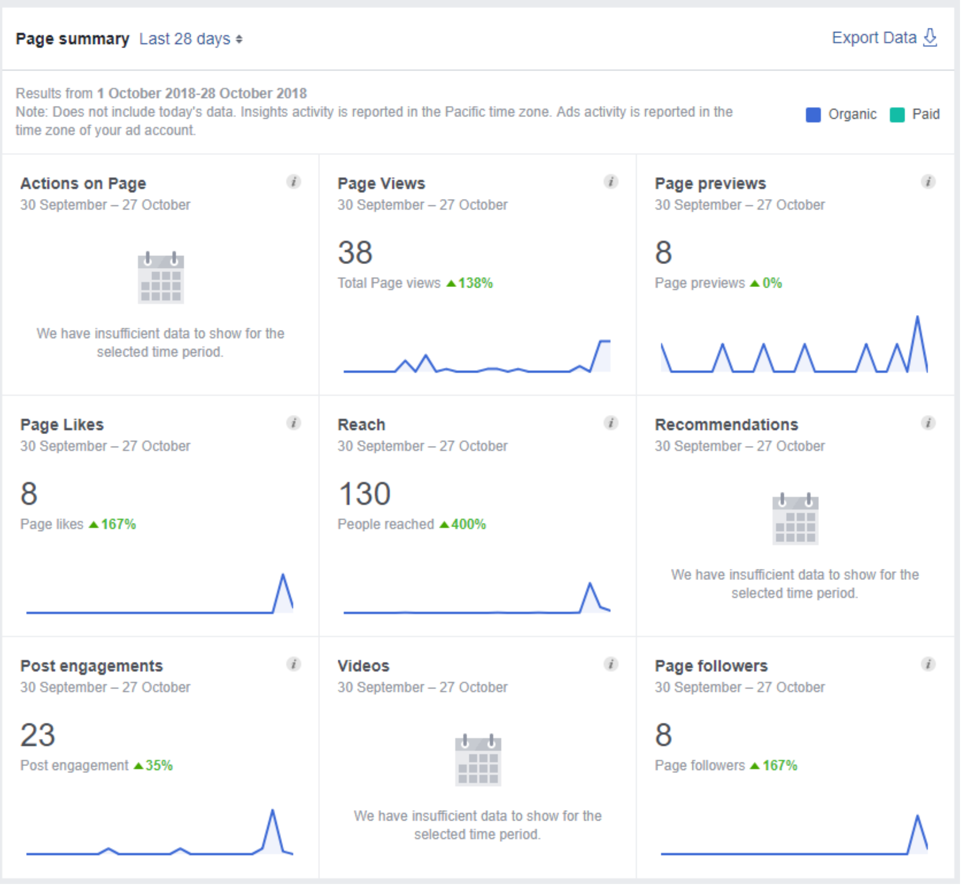
Our Kick Off Meeting is in progress. Our consortium along with oir PO is gathered & important discussions have already started #H2020 #cybersecurity #forensics #digitalsecurity pic.twitter.com/INWP9ZCLIW

⇄ 4 ♥ 3

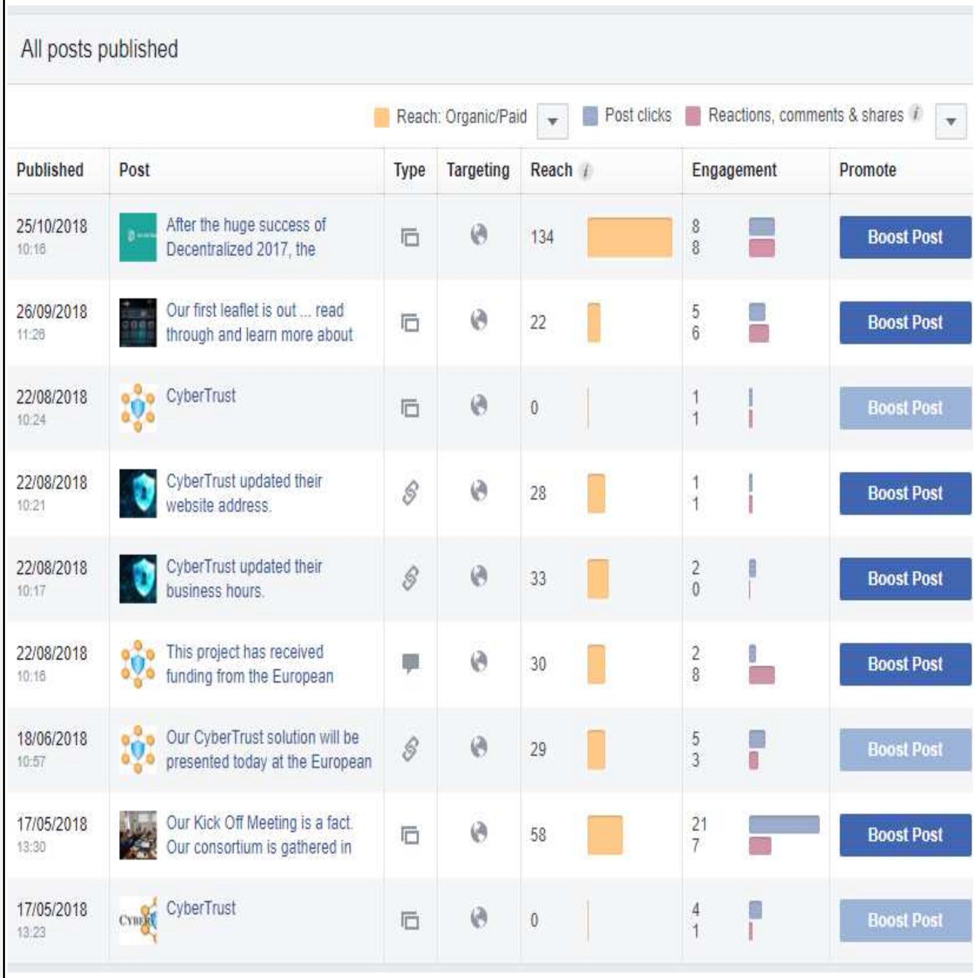
View Tweet activity View all Tweet activity

Figure 2.8: Highlights of May 2018

Annotated photos	N/A

Date	29 October 2018				
Communication activity	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 on the Cyber-Trust Facebook page is summarized in Figure 2.9**Error! Reference source not found.**, indicating that the page has gathered 38 page views, reached 130 Facebook users and managed 23 post engagements.  **Page summary** Last 28 days ⬍ Export Data Results from **1 October 2018-28 October 2018** Note: Does not include today's data. Insights activity is reported in the Pacific time zone. Ads activity is reported in the time zone of your ad account. 🟦 Organic 🟩 Paid **Actions on Page** 30 September – 27 October: We have insufficient data to show for the selected time period. **Page Views** 30 September – 27 October: 38 Total Page views ▲138% **Page previews** 30 September – 27 October: 8 Page previews ▲0% **Page Likes** 30 September – 27 October: 8 Page likes ▲167% **Reach** 30 September – 27 October: 130 People reached ▲400% **Recommendations** 30 September – 27 October: We have insufficient data to show for the selected time period. **Post engagements** 30 September – 27 October: 23 Post engagement ▲35% **Videos** 30 September – 27 October: We have insufficient data to show for the selected time period. **Page followers** 30 September – 27 October: 8 Page followers ▲167% Figure 2.9: Activity summary for a 28-day duration The project Facebook page has so far concentrated 38 followers with 9 activity items, shown in Figure 2.10. Facebook will be used as the channel				

of preference for the promotion of events in which consortium members will be participating. Two events that have been so far promoted is the Project Kick-off meeting and our participation in the Decentralised 2018 summit.



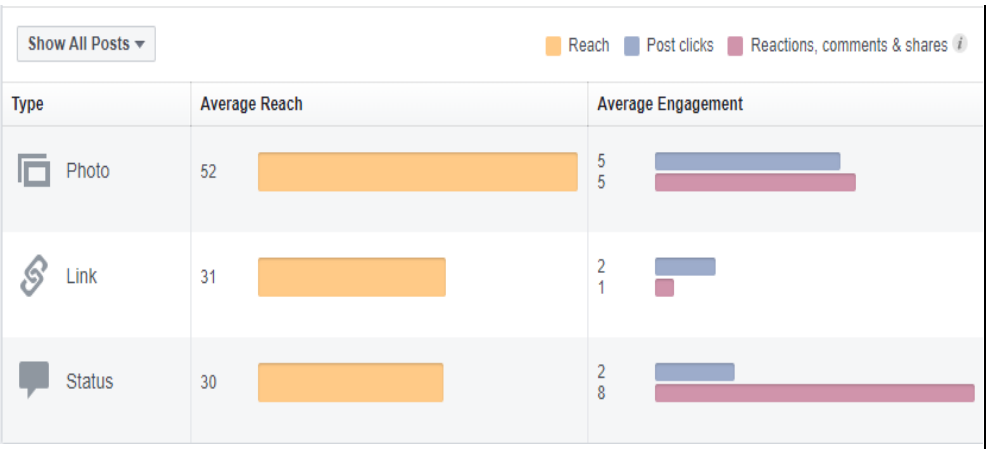
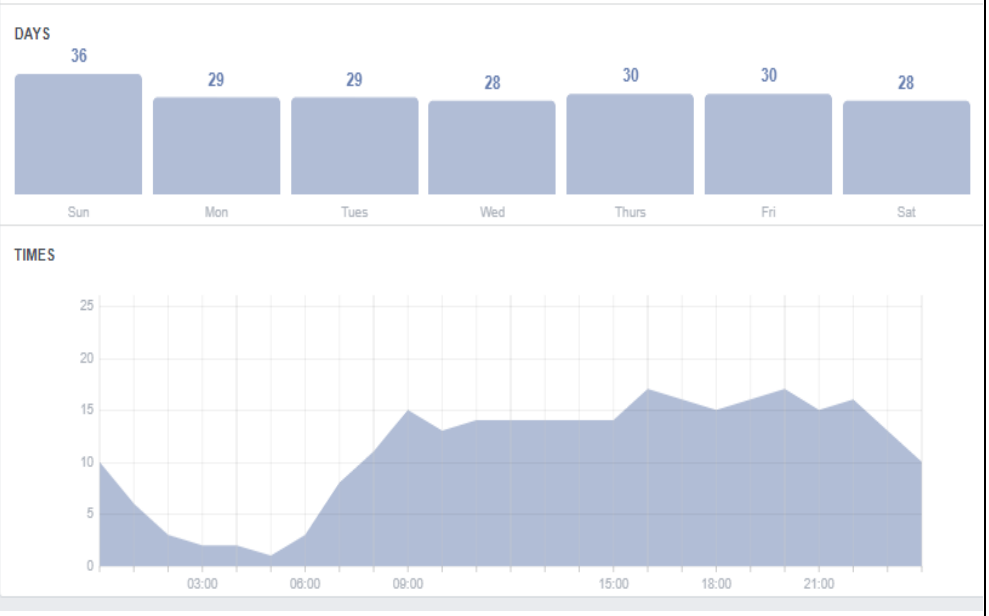
All posts published

🟧 Reach: Organic/Paid ▾ 🟦 Post clicks 🟥 Reactions, comments & shares ▾

Published	Post	Type	Targeting	Reach	Engagement	Promote
25/10/2018 10:16	After the huge success of Decentralized 2017, the	⧉	🌐	134	8 8	Boost Post
26/09/2018 11:26	Our first leaflet is out ... read through and learn more about	⧉	🌐	22	5 6	Boost Post
22/08/2018 10:24	CyberTrust	⧉	🌐	0	1 1	Boost Post
22/08/2018 10:21	CyberTrust updated their website address.	🔗	🌐	28	1 1	Boost Post
22/08/2018 10:17	CyberTrust updated their business hours.	🔗	🌐	33	2 0	Boost Post
22/08/2018 10:16	This project has received funding from the European	💬	🌐	30	2 8	Boost Post
18/06/2018 10:57	Our CyberTrust solution will be presented today at the European	🔗	🌐	29	5 3	Boost Post
17/05/2018 13:30	Our Kick Off Meeting is a fact. Our consortium is gathered in	⧉	🌐	58	21 7	Boost Post
17/05/2018 13:23	CyberTrust	⧉	🌐	0	4 1	Boost Post

Figure 2.10: Posts on Facebook Page

Facebook page insights also indicate that posting pictures results in higher reach, posting of links and status updates follow, see Figure 2.11. 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 2.12 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 2.11: Engagement over post types  Figure 2.12: Insights on times followers are active
Annotated photos	N/A

Date	12–15 August 2018				
Communication activity	Website				
Communication type	Blog post				
Target audience	Partners X	General X	Academic X	Government X	Industry X
Number of participants	Around 100 people				
Partner(s) involved	ADITESS				
People involved	Elisavet Charalambous				
Description of the activity, relevance to the Project and Impact	A blog post have been added on our website that can be found in link https://www.cyber-trust.eu/2018/08/17/threat-sharing-methods-comparative-analysis/ where the importance of				

	Threat Intelligence is been explaining which is related to Deliverable D2.1. This is also the preamble of the work that will follow in WP5.
Annotated photos	N/A

2.2 Research Conference presentations and publications

The research undertaken in the project has already led to five research publications, of which four were accepted for publication in peer-reviewed international conferences and one in a peer-reviewed journal. It is an excellent result, given the research is in a rather incipient, early phase, with the core of the investigation yet to begin. Beyond the references that the papers are likely to gather, a more immediate dissemination impact was the level of interest received during the conference events, all very well attended by fellow researchers.

Date	12–15 August 2018				
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 and CSCAN				
People involved	Nicholas Kolokotronis and Stavros Shiaeles				
Description of the activity, relevance to the Project and Impact	This paper investigates solutions for solving challenges related to the management of (users', devices', etc.) identities in large groups and ecosystems, like those envisioned in Cyber-Trust. In a typical such ecosystem, decentralized and dynamic management of trust is vital for ensuring safe, secure, and transparent use of sensitive data. The article presents a novel solution on how trust could be established without the need for a centralized authority (such as an identity provider) by relying on the blockchain. The paper was presented in 16th IEEE DASC (http://cyber-science.org/2018/dasc/) conference that was held in Athens, Greece, 12–15 Aug. 2018. K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "A novel blockchain–based trust model for cloud identity management," in *16th IEEE International Conference on Dependable, Autonomic and Secure Computing — DASC, 2018*, pp. 724–729. It is directly related with the work carried out in the work-packages WP5 and WP7. It is expected that the report will soon be available at the publisher's website (https://ieeexplore.ieee.org/).				

	The audience was very keen in making questions with regards to the use of blockchain for trust.
Annotated photos	N/A

Date	12–15 August 2018				
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 and CSCAN				
People involved	Konstantinos-Panagiotis Grammatikakis, Stavros Shiaeles, and Nicholas Kolokotronis				
Description of the activity, relevance to the Project and Impact	This paper considers the case of malware that targets at mobile devices running the Android OS and infects them by means of cracked applications carrying malicious payloads. In order to provide further insight into Cyber-Trust's host-based intrusion detection system design, a number of indicators (permissions, CPU and RAM usage, as well as, open TCP and HTTP ports) were studied and compared for a sample of (official and cracked) applications. The paper was presented in 16th IEEE DASC (http://cyber-science.org/2018/dasc/) conference that was held in Athens, Greece, 12–15 Aug. 2018. K.-P. Grammatikakis, A. Ioannou, S. Shiaeles, and N. Kolokotronis, "Are cracked applications really free? An empirical analysis on Android devices," in *16th IEEE International Conference on Dependable, Autonomic and Secure Computing — DASC, 2018*, pp. 730–735. It is directly related with the work carried out in the work-package WP6. It is expected that the report will soon be available at the publisher's website (https://ieeexplore.ieee.org/). The audience was very keen in making questions with regards to the malware behaviour characteristic on Android OS.				
Annotated photos	N/A				

Date	23–25 October 2018				
Communication activity	Scientific conference presentation and publication				
Communication type	Organization of conference special session				
Target audience	Partners	General	Academic	Government	Industry

			X		X
Number of participants	Around 100 people				
Partner(s) involved	CSCAN				
People involved	Stavros Shiaeles and Bogdan Ghita				
Description of the activity, relevance to the Project and Impact	In this research work a methodology for detection of LDDoS attacks, based on characteristics of malicious TCP flows, is proposed and research is conducted using combinations of two datasets: one generated from a simulated network and the other from the publicly available CIC DoS dataset. Both datasets contained the attacks slowread, slowheaders and slowbody, alongside legitimate web browsing. TCP flow features are extracted from all connections. Experimentation was carried out using six supervised AI algorithms to categorise attack from legitimate flows. Decision trees and k-NN accurately classified up to 99.99% of flows, with exceptionally low false positive and false negative rates, demonstrating the potential of AI in LDDoS detection. M. Siracusano, S. Shiaeles and B. Ghita, Detection of LDDoS *"Attacks Based on TCP Connection Parameters"* in Global Information Infrastructure and Networking Symposium (GIIS 2018), Thessaloniki, Greece It is directly related with the work carried out in the work-package WP6 and It is expected that the paper will soon be available at the publisher's website (https://ieeexplore.ieee.org/). The presentation received many questions regarding the LDDOS detection features used as well as the testbed setup. Also, participants show great interest for the dataset produced. Cyber-Trust was also presented as this research work is part of WP6 and that led exchanging ideas between Dr Stavros Shiaeles and the coordinator of SPEAR project Dr Panagiotis Sarigiannidis who was present in the session been organised. Emails where also for common dissemination activities and further collaboration between the two researchers.				

Annotated photos	 • Detect application layer LDDoS attacks through TCP flow metadata analysis, from a distributed attack • The specific application layer attacks that will attempt to be categorised will be those that exploit the slow read and slow post weaknesses of HTTP: slowread, slowheaders and slowpost. These have been chosen due to the difficulty in ascertaining the maliciousness of this traffic using static signatures within Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) because of their similarity to legitimate web traffic. Figure 2.13: Dr Stavros Shiaeles explaining Cyber-Trust and the work been conducted Figure 2.14: Dr Stavros Shiaeles explaining simulated environment for LDDoS attacks

Date	23–25 October 2018
Communication activity	Scientific conference presentation and publication

<table>
<tr><td>Communication type</td><td colspan="5">Organization of conference special session</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 100 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CSCAN</td></tr>
<tr><td>People involved</td><td colspan="5">Stavros Shiaeles, Bogdan Ghita and Maria Papadaki</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">Malicious software is detected and classified by either static analysis or dynamic analysis. In static analysis, malware samples are reverse engineered and analyzed so that signatures of malware can be constructed. These techniques can be easily thwarted through polymorphic, metamorphic malware, obfuscation and packing techniques, whereas in dynamic analysis malware samples are executed in a controlled environment using the sandboxing technique, in order to model the behavior of malware. In this paper, we have analyzed Petya, Spyeye, VolatileCedar, PAFISH etc. through Agent-based and Agentless dynamic sandbox systems in order to investigate and benchmark their efficiency in advanced malware detection.

M. Ali, S. Shiaeles, B. Ghita and M. Papadaki, <i>“Agent-based Vs Agent-less Sandbox for Dynamic Behavioral Analysis”</i> in Global Information Infrastructure and Networking Symposium (GIIS 2018), Thessaloniki, Greece

It is directly related with the work carried out in the work-packages WP5 and WP6 and it is expected that the paper will soon be available at the publisher’s website (https://ieeexplore.ieee.org/). The conference had more than 100 attendees and the presentation intrigued the interest of attendees.

The audience was very keen in making questions with regards to the agentless dynamic malware analysis proposed method and many interesting ideas were exchanged with regards to further improvements of the system.</td></tr>
</table>

Annotated photos	Figure 2.15: Mr Muhhamad Ali presenting paper on malware detection using dynamic analysis and agentless sandboxes as part of his PhD studies

2.3 Research Journal Publications

This section is focus on original research publication accepted in journals. Members of the consortium have already published a paper in IEEE Consumer Electronics Magazine with Impact Factor 1.434 and Article Influence Score 0.283. The journal publications are available through Digital Libraries reaching researchers and people interested in specific topics around the world.

Date	23 August 2018				
Communication activity	Scientific publications				
Communication type	Journal article				
Target audience	Partners	General X	Academic X	Government	Industry X
Partner(s) involved	UOP, CSCAN, and SCORECHAIN				
People involved	Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles and Romain Griffiths				
Description of the activity, relevance to the Project and Impact	This paper investigates whether (and how) the blockchain and distributed ledger technologies could enhance the security of IoT-enabled consumer electronics (CE) devices in a cryptographically verifiable manner. The article presents main ideas of the project, at a high level that is also suitable for the readers coming from the industry and the general public. The paper has been accepted for publication in				

	N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, “Blockchain technologies for enhanced security and privacy in the Internet of things,” *IEEE Consumer Electronics Magazine*, 2018, accepted, Special issue: blockchain technologies for consumer electronics. It is directly related with the work carried out in the work-packages WP5, WP6, and WP7. It is expected that the special issue will be published by the end of 2018 and will then be made available at the publisher’s website (https://ieeexplore.ieee.org/). Research papers have create impact in research community, industry and generally our society as they help the knowledge to elevate as well as new ideas to growth.
Annotated photos	N/A

2.4 Organised dissemination events

Members of the consortium have already organised two workshop events and a dedicated session within a research conference. The approach aimed to ensure breadth of dissemination channels, including both the academic/research community (as part of the research conference) as well as the Industrial community, through the two workshops.

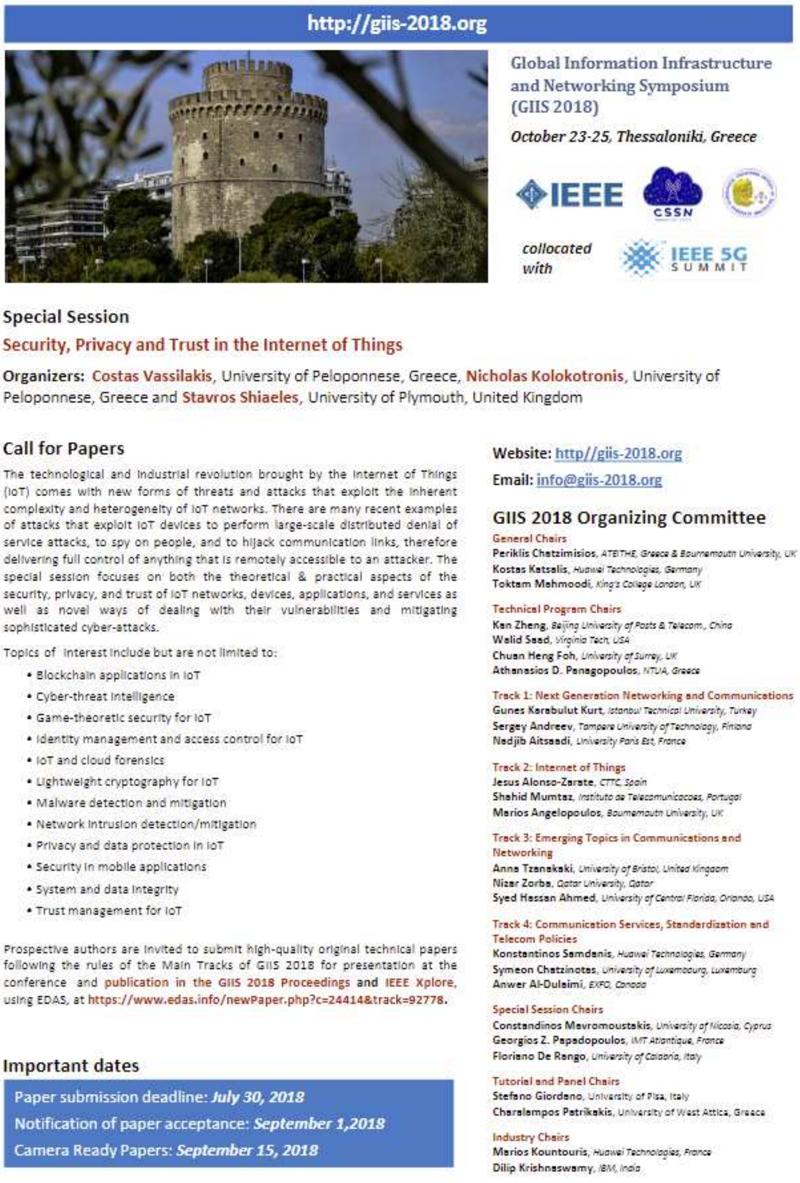
Date	25 May 2018				
Communication activity	Participation to a workshop				
Communication type	Innovation Workshop - border security at FRONTEX				
Target audience	Partners	General	Academic	Government X	Industry X
Number of participants	50 Participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	Among other services and solutions Gohar Sargsyan pitched about Cyber-TRUST at the Innovation workshop on border security at FRONTEX				
Annotated photos	N/A				

Date	28 May 2018				
Communication activity	Organisation of a workshop				
Communication type	FRONTEX / CGI SPARK session				
Target audience	Partners	General	Academic	Government	Industry X
Number of participants	13 Participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				

Description of the activity, relevance to the Project and Impact	Hosting FRONTEX at CGI SPARK innovation centre - security and safety solutions and services presented. among others, Cyber-TRUST was presented. Gohar Sargsyan on behalf of project consortium presented the Cyber-Trust project among other security and safety projects where CGI participates in Rotterdam, The Netherlands.
Annotated photos	N/A

<table>
<tr><td>Date</td><td colspan="5">01 August 2018</td></tr>
<tr><td>Communication activity</td><td colspan="5">Organisation of a workshop</td></tr>
<tr><td>Communication type</td><td colspan="5">Workshop with CyberSecurity global experts</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General</td><td>Academic</td><td>Government</td><td>Industry
X</td></tr>
<tr><td>Number of participants</td><td colspan="5">26 Participants</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">CGI</td></tr>
<tr><td>People involved</td><td colspan="5">Gohar Sargsyan</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">Meeting with Global CyberSecurity Experts in London August 1, 2018 an event organised by CGI Global.
Gohar Sargsyan on behalf of project consortium presented the Cyber-Trust project input received from the coordinator Dimitris Kavallieros to 26 participants.</td></tr>
<tr><td>Annotated photos</td><td colspan="5">N/A</td></tr>
</table>

<table>
<tr><td>Date</td><td colspan="5">23–25 October 2018</td></tr>
<tr><td>Communication activity</td><td colspan="5">Scientific conference special session</td></tr>
<tr><td>Communication type</td><td colspan="5">Organization of conference special session</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 20 people</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">UOP and CSCAN</td></tr>
<tr><td>People involved</td><td colspan="5">Costas Vassilakis, Nicholas Kolokotronis, and Stavros Shiaeles</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">The organization of this special session at the 2018 IEEE GIIS (http://giis-2018.org/) conference that will be held in Thessaloniki, Greece, 23–25 Oct. 2018, aims at bringing together students, researchers, security experts, and IT people from the industry on areas under consideration by Cyber-Trust. Indicative topics of interest included
▪ Blockchain applications in IoT
▪ Cyber-threat intelligence
▪ Game-theoretic security for IoT
▪ Identity management and access control for IoT
▪ IoT and cloud forensics</td></tr>
</table>

	▪ 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 It is directly related with the work carried out in the work-packages WP5, WP6, and WP7. It is expected that the special session’s proceedings will be published by the end of 2018 and will be made available at the publisher’s website (https://ieeexplore.ieee.org/).
Annotated photos	 http://giis-2018.org Global Information Infrastructure and Networking Symposium (GIIS 2018) *October 23-25, Thessaloniki, Greece* IEEE CSSN *collocated with* IEEE 5G SUMMIT **Special Session** **Security, Privacy and Trust in the Internet of Things** **Organizers: Costas Vassilakis**, University of Peloponnese, Greece, **Nicholas Kolokotronis**, University of Peloponnese, Greece and **Stavros Shiaeles**, University of Plymouth, United Kingdom **Call for Papers** The technological and industrial revolution brought by the Internet of Things (IoT) comes with new forms of threats and attacks that exploit the inherent complexity and heterogeneity of IoT networks. There are many recent examples of attacks that exploit IoT devices to perform large-scale distributed denial of service attacks, to spy on people, and to hijack communication links, therefore delivering full control of anything that is remotely accessible to an attacker. The special session focuses on both the theoretical & practical aspects of the security, privacy, and trust 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 include but are 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 Prospective authors are invited to submit high-quality original technical papers following the rules of the Main Tracks of GIIS 2018 for presentation at the conference and **publication in the GIIS 2018 Proceedings** and **IEEE Xplore**, using EDAS, at **https://www.edas.info/newPaper.php?c=24414&track=92778.** **Important dates** Paper submission deadline: ***July 30, 2018*** Notification of paper acceptance: ***September 1,2018*** Camera Ready Papers: ***September 15, 2018*** **Website:** http//giis-2018.org **Email:** info@giis-2018.org **GIIS 2018 Organizing Committee** General Chairs **Periklis Chatzimisios**, *ATEITHE, Greece & Bournemouth University, UK* **Kostas Katsalis**, *Huawei Technologies, Germany* **Toktam Mahmoodi**, *King's College London, UK* Technical Program Chairs **Ken Zheng**, *Beijing University of Posts & Telecom., China* **Walid Saad**, *Virginia Tech, USA* **Chuan Heng Foh**, *University of Surrey, UK* **Athanasios D. Panagopoulos**, *NTUA, Greece* Track 1: Next Generation Networking and Communications **Gunes Karabulut Kurt**, *Istanbul Technical University, Turkey* **Sergey Andreev**, *Tampere University of Technology, Finland* **Nadjib Aitsaadi**, *University Paris Est, France* Track 2: Internet of Things **Jesus Alonso-Zarate**, *CTTC, Spain* **Shahid Mumtaz**, *Instituto de Telecomunicacoes, Portugal* **Marios Angelopoulos**, *Bournemouth University, UK* Track 3: Emerging Topics in Communications and Networking **Anna Tzanakaki**, *University of Bristol, United Kingdom* **Nizar Zorba**, *Qatar University, Qatar* **Syed Hassan Ahmed**, *University of Central Florida, Orlando, USA* Track 4: Communication Services, Standardization and Telecom Policies **Konstantinos Samdanis**, *Huawei Technologies, Germany* **Symeon Chatzinotas**, *University of Luxembourg, Luxemburg* **Anwer Al-Dulaimi**, *EXFO, Canada* Special Session Chairs **Constandinos Mavromoustakis**, *University of Nicosia, Cyprus* **Georgios Z. Papadopoulos**, *IMT Atlantique, France* **Floriano De Rango**, *University of Calabria, Italy* Tutorial and Panel Chairs **Stefano Giordano**, University of Pisa, Italy **Charalampos Patrikakis**, University of West Attica, Greece Industry Chairs **Marios Kountouris**, *Huawei Technologies, France* **Dilip Krishnaswamy**, *IBM, India* Figure 2.16: Proposed special session in GIIS 2018 conference

2.5 Event Participation

Several meetings took place between CGI and the full spectrum of stakeholders, including police, government, academia, and industry. The main purpose of participating in the events was to raise awareness of the project and to gauge the level of interest and impact of the project on the wider community.

Date	21 June 2018				
Communication activity	Meeting				
Communication type	Advisory Board member /CGI meeting				
Target audience	Partners X	General	Academic	Government	Industry X
Number of participants	9 Participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	CGI met advisory board member Geleyn Meijer and ICT department / digital security Gohar Sargsyan presented the Cyber-Trust project and informed the status of the project in Amsterdam, The Netherlands				
Annotated photos	N/A				

Date	27 June 2018				
Communication activity	Meeting				
Communication type	Swedish police/CGI				
Target audience	Partners	General X	Academic	Government X	Industry X
Number of participants	30 Participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	Meeting CGI with Swedish police customer. Gohar Sargsyan on behalf of project consortium presented the Cyber-Trust project among other security and safety projects where CGI participates in Stockholm, Malmo and Rotterdam.				
Annotated photos	N/A				

Date	26 July 2018				
Communication activity	Meeting				
Communication type	Advisory Board member /CGI meeting				
Target audience	Partners	General	Academic	Government	Industry

	X				X
Number of participants	5 Participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	CGI met advisory board member Mary Jo-Leeuw and cybersecurity network Gohar Sargsyan presented the Cyber-Trust project and informed the status of the project in Amsterdam, The Netherlands				
Annotated photos	N/A				

Date	01-05 October 2018				
Communication activity	Conference participation				
Communication type	CGI alongside with HSD				
Target audience	Partners	General X	Academic X	Government X	Industry X
Number of participants	Around 2000 participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan with CGI other colleagues				
Description of the activity, relevance to the Project and Impact	Cybersecurity Week - The Hague Security Delta - The Hague, The Netherlands - Cyber-Trust project was introduced in innovation room. Oct 1-5, Cyber security Week at The Hague, The Netherlands. CGI together HSD (The Hague Security Delta) participated in the event in the innovation room introducing Cyber-Trust among other CGI security and safety solutions and services.				
Annotated photos	N/A				

Date	16 October 2018				
Communication activity	Participation to a workshop				
Communication type	Industry invitation - border security at FRONTEX				
Target audience	Partners	General	Academic	Government X	Industry X
Number of participants	36 Participants				
Partner(s) involved	CGI				
People involved	Gohar Sargsyan				
Description of the activity, relevance to the Project and Impact	Industry workshop by invitation only on border security with the focus on migration topic - relevant security and safety services introduced. Gohar Sargsyan pitched Cyber-TRUST among other projects.				
Annotated photos	N/A				

2.6 Presentations

Date	16 May 2018				
Communication activity	Conference				
Communication type	Presentation				
Target audience	Partners	General	Academic X	Government X	Industry X
Number of participants	Around 60 individuals				
Partner(s) involved	KEMEA				
People involved	Dimitrios Kavallieros				
Description of the activity, relevance to the Project and Impact	"Defending against cyber attacks" was presented at the 6th Exposec-DefenseWorld conference which took place at the Hellenic Armed Forces Officers' Club (LAED) on May 15, 2018, in Athens, in partnership with The American-Hellenic Chamber of Commerce." Website of the event: www.exposecdefenseworld.gr/				
Annotated photos	AMERICAN-HELLENIC CHAMBER OF COMMERCE EXPOSEC Conference 2018 DEFENSEWORLD Figure 2.17: Mr Kavallieros presenting Cyber-Trust in the 6th Exposec				

Date	18-21 June 2018				
Communication activity	Conference				
Communication type	Presentation				
Target audience	Partners	General X	Academic X	Government	Industry X
Number of participants	Around 50 individuals				
Partner(s) involved	KEMEA				
People involved	Dimitrios Kavallieros				
Description of the activity, relevance to the Project and Impact	Cyber-Trust: An innovative cybersecurity platform for IoT was presented at EuCNC 2018: European Conference on Networks and Communications.				

	EuCNC 2018 is the 27th edition of a successful series of a conference in the field of telecommunications, sponsored by the European Commission. The conference focuses on various aspects of 5G communications systems and networks, including cloud and virtualisation solutions, management technologies, and vertical application areas. It targets to bring together researchers from all over the world to present the latest research results, and it is one of the main venues for demonstrating the results of research projects, especially from successive European R&D programmes co-financed by the European Commission. Website of the event: https://www.eucnc.eu
Annotated photos	Cyber-Trust: An innovative cybersecurity platform for IoT Dimitrios Kavallieros Figure 2.18: Mr Kavallieros presenting Cyber-Trust in EuCNC 2018

<table>
<tr><td>Date</td><td colspan="5">18 September 2018</td></tr>
<tr><td>Communication activity</td><td colspan="5">Technical presentation at Telecom Italia – TLab (Torino)</td></tr>
<tr><td>Communication type</td><td colspan="5">Presentation</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 10 participants</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">MATH</td></tr>
<tr><td>People involved</td><td colspan="5">Emanuele Bellini</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">A meeting was held at the TLab of Telecom Italia, to present the project and to explore next opportunities of collaboration for application of Cyber Trust solutions mainly in IoT domain</td></tr>
<tr><td>Annotated photos</td><td colspan="5">N/A</td></tr>
</table>

Date	25 September 2018				
Communication activity	Presentation				
Communication type	Technical presentation in the context of an Erasmus+ visit				
Target audience	Partners	General	Academic X	Government	Industry
Number of participants	Around 20 participants				
Partner(s) involved	UOP				
People involved	Christos Tryfonopoulos				
Description of the activity, relevance to the Project and Impact	During the academic visit the presentation titled ”Democratising social interactions: the case of distributed social networks” was presented. The presentation involved an overview of technical issues and related solutions pertaining a wide range of distributed applications. The topics of the presentation included, among others, issues on privacy and trust in various distributed scenarios such as distributed social networks and IoT devices. In this context, highlights of the Cyber-Trust project were briefly presented. The presentation took place at Tomas Bata University in Zlin, Czech Republic and targeted postgraduate (MSc and PhD) students and faculty members, and is directly related with the work carried out in work-package WP5.				
Annotated photos	N/A				

Date	27 September 2018				
Communication activity	Workshop				
Communication type	Presentation				
Target audience	Partners	General	Academic	Government	Industry X
Number of participants	Around 100 participants				
Partner(s) involved	ADITESS				
People involved	Elisavet Charalambous				
Description of the activity, relevance to the Project and Impact	Cyber-Trust: An innovative cybersecurity platform for IoT was presented at MEDIA4SEC - Innovative Market Solutions Workshop. The attended workshop focused on the impact of social media platforms and information revealed by such platforms. Within the workshop a number of innovative solutions related to the investigation of cybercrime and cybersecurity were presented. Cyber-Trust gained a lot of interest from LEAs participating to the event. The audience was very keen in making questions with regards to the involvement of LEAs in the project, the preparation of the pilot setup as well as the use of blockchain for use by LEAs				

Annotated photos	The posters and flyers shown on section 2.7 where used during this event. Also, event photos can be found below: 26 September 2018 Innovative Market Solutions WORKSHOP TNO Figure 2.19: Ms Elisavet Charalambous presenting Cyber-Trust Figure 2.20: Workshop attendees

Date	3 October 2018				
Communication activity	Technical presentation at University of Florence – Center for Cyber Security (Florence)				
Communication type	Presentation				
Target audience	Partners	General	Academic X	Government	Industry
Number of participants	Around 10 participants				
Partner(s) involved	MATH				
People involved	Alessandro Bellini, Emanuele Bellini				
Description of the activity, relevance to the Project and Impact	A meeting was held at the University of Florence with the international research group of the Center for Cyber Security.				

	The goal of the meeting was to discuss the possible common research field for synergies in research and technology transfer
Annotated photos	N/A

<table>
<tr><td>Date</td><td colspan="5">11 October 2018</td></tr>
<tr><td>Communication activity</td><td colspan="5">Technical presentation at University of Milan – SESAR Lab (Milan)</td></tr>
<tr><td>Communication type</td><td colspan="5">Presentation</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 10 participants</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">MATH</td></tr>
<tr><td>People involved</td><td colspan="5">Emanuele Bellini</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">A meeting was held at the University of Milan, SEcure Service-oriented Architectures Research Lab.
The goal of the meeting was to present the project and to explore next opportunities of collaboration especially in the application of blockchain technology.</td></tr>
<tr><td>Annotated photos</td><td colspan="5">N/A</td></tr>
</table>

<table>
<tr><td>Date</td><td colspan="5">20 October 2018</td></tr>
<tr><td>Communication activity</td><td colspan="5">Technical presentation at THALES, Sesto Fiorentino (FI)</td></tr>
<tr><td>Communication type</td><td colspan="5">Presentation</td></tr>
<tr><td>Target audience</td><td>Partners</td><td>General</td><td>Academic</td><td>Government</td><td>Industry
X</td></tr>
<tr><td>Number of participants</td><td colspan="5">Around 10 participants</td></tr>
<tr><td>Partner(s) involved</td><td colspan="5">MATH</td></tr>
<tr><td>People involved</td><td colspan="5">Alessandro Bellini, Emanuele Bellini</td></tr>
<tr><td>Description of the activity, relevance to the Project and Impact</td><td colspan="5">A meeting was held at THALES, Sesto Fiorentino (FI) to present the overall project and the perspective of cyber security, particularly blockchain in the aero-industry.
The goal of the meeting was to raise awareness about the last advances in research and technology and to foster synergies with the project.</td></tr>
<tr><td>Annotated photos</td><td colspan="5">N/A</td></tr>
</table>

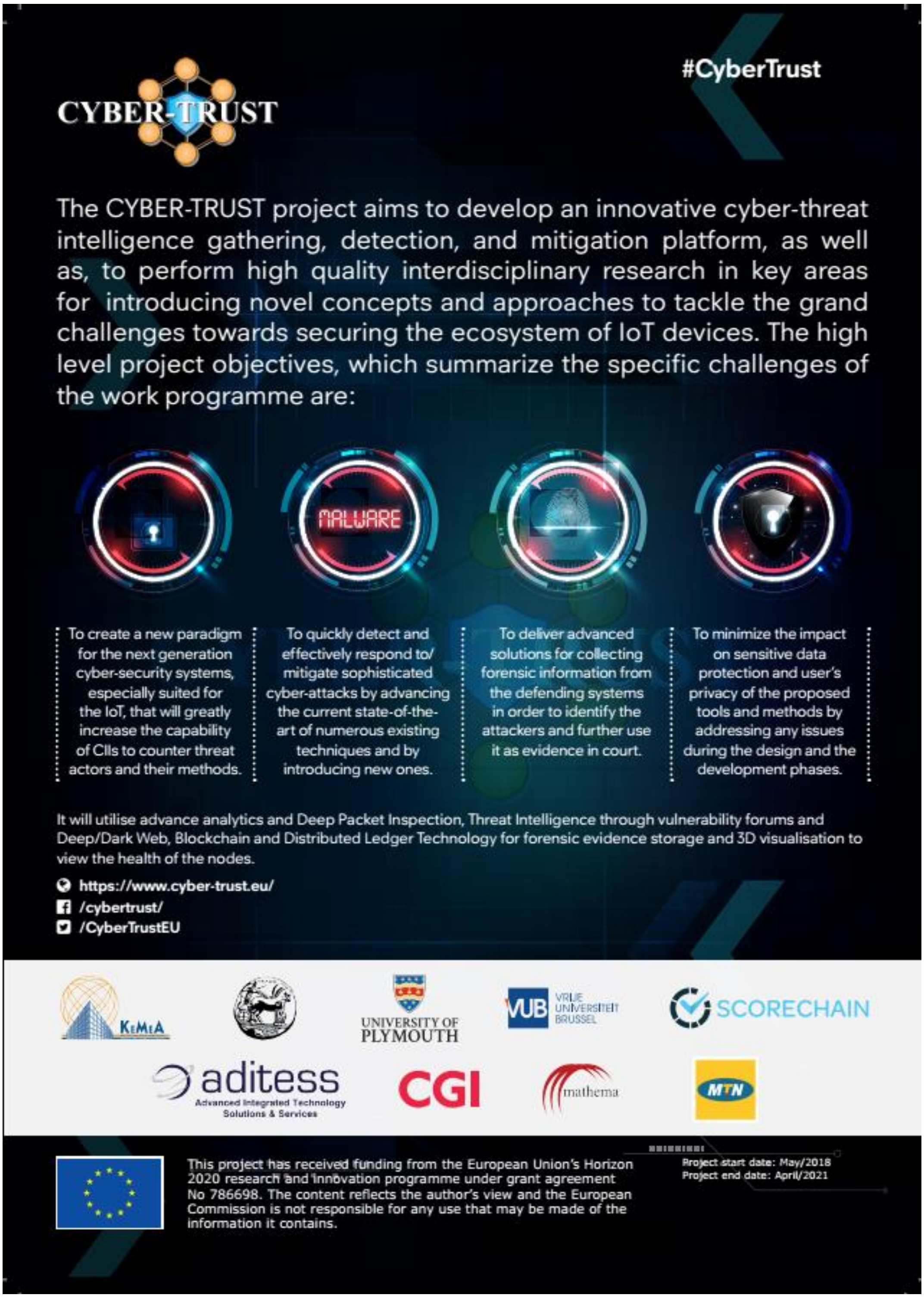
2.7 Synergies with other Projects

In order to ensure that the project integrates well with concurrent work in the area, the consortium established contact and communication, in order to build up the collaboration with ASTRID, an ongoing EU research project.

Date	16 October 2018				
Communication activity	Collaboration				
Communication type	Join workshop proposal, Email exchange				
Target audience	Partners	General	Academic X	Government	Industry X
Number of participants	Around 80 participants				
Partner(s) involved	ADITESS, KEMEA, CSCAN, UOP				
People involved	Romeo Bratska, Elisavet Charalambous, Stavros Shiaeles, Nikolaos Kolokotronis, Dimitris Kavallieros				
Description of the activity, relevance to the Project and Impact	Initiation of Collaboration with ASTRID project on an organizing a join workshop in the 5th IEEE International Conference on Network Softwarization (NetSoft 2019) will be held on June 24-28, 2019 in Paris, France. 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 of Cyber-Trust, ASTRID as well as other H2020 projects under the same DS7 call. 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).				
Annotated photos	N/A				

2.8 Brochures and Poster

The following flyer and poster were produced by University of Plymouth and were used/distributed during MEDIA4SEC - Innovative Market Solutions Workshop as well as other events partners attended and promoted Cyber-Trust.



#CyberTrust
CYBER-TRUST
MALWARE
KEMEA
UNIVERSITY OF PLYMOUTH
VUB VRIJE UNIVERSITEIT BRUSSEL
SCORECHAIN
aditess Advanced Integrated Technology Solutions & Services
CGI
mathema
MTN

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:

- 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 minimize the impact on sensitive data protection and user's privacy of the proposed tools and methods by addressing any issues during the design and the development phases.

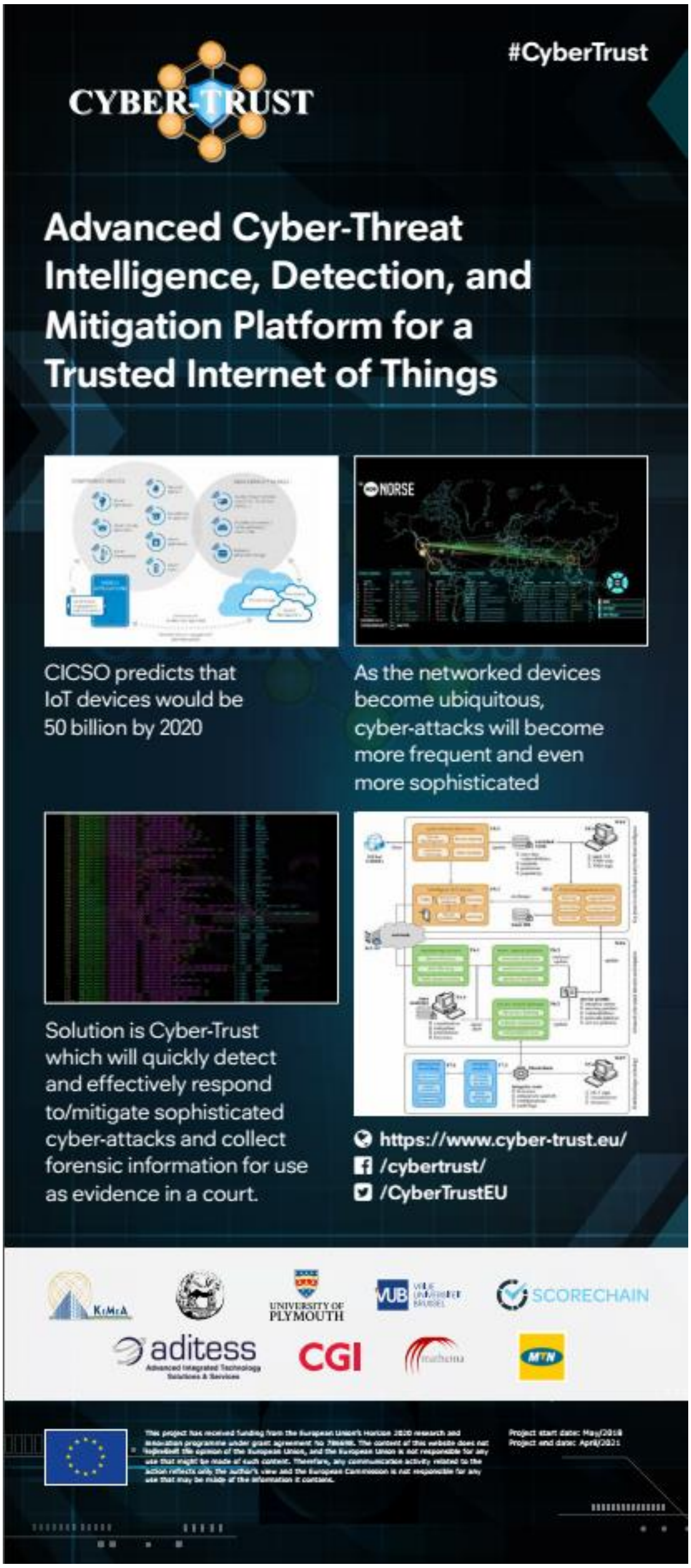
It will utilise advance analytics and Deep Packet Inspection, Threat Intelligence through vulnerability forums and Deep/Dark Web, Blockchain and Distributed Ledger Technology for forensic evidence storage and 3D visualisation to view the health of the nodes.

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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. The content reflects the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Project start date: May/2018
Project end date: April/2021

Figure 2.21: Cyber-Trust Flyer



#CyberTrust

CYBER-TRUST

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

CICSO predicts that IoT devices would be 50 billion by 2020

As the networked devices become ubiquitous, cyber-attacks will become more frequent and even more sophisticated

Solution is Cyber-Trust which will quickly detect and effectively respond to/mitigate sophisticated cyber-attacks and collect forensic information for use as evidence in a court.

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

NORSE
KEMEA
UNIVERSITY OF PLYMOUTH
VUB VRIJE UNIVERSITEIT BRUSSEL
SCORECHAIN
aditess Advanced Integrated Technology Solutions & Services
CGI
mathema
MTN

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. The content of this website does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content. Therefore, any communication activity related to the action reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Project start date: May/2018
Project end date: April/2021

Figure 2.22: Cyber-Trust Poster

3. Progress Monitoring

In this instance, all communication will be handled by CSCAN, in conjunction with the Project Coordinator, in order to fully assess the impact of our activities to the project and to ensure the continuity of the Consortium and the work conducted. In Table 3.1 is a summary of the key performance indicators identified across all partners during this first report and how they map to the KPIs of the deliverable 9.2.

Table 3.1: Summary of dissemination activities

Dissemination Type	Actual	Target (project life)
Website Visits	800	300 per month
Brochure	1	3
Scientific Publications	5	15
Press Releases	1	8
Blogs	1	10 in total
Newsletter	5	
Workshops	5	At least 5
Presentations	13	30
Social Media	84 followers	
Direct Contact	3	

As can be concluded from the summary Table 3.1 Cyber-Trust partners did well in disseminating the project even just six months since the project started and are working hard to meet the targets set in deliverable 9.2. This progress will be closely monitored from the Dissemination Manager and all partners.

4. Conclusion

This deliverable is the first of a series of deliverables providing the dissemination activities undertake by consortium partners of Cyber-Trust in order to monitor the KPIs introduced in D9.2. It can be concluded from table 3.1 that the partners even in the first six months of the project have been involved in many activities in order to advertise the project and create awareness. It worth mentioning that are notable results from conferences presentation as well as scientific publication been produced until now providing a clear view that project results would be prosperous. To this end the Cyber-Trust partners are confident that the KPIs introduced in D9.2 will be reached as well as the exploitation objectives that will be introduced in D9.9 soon. Overall this is a very ambitious project and the comments been received from various stakeholders are very positive looking for a system that could help them live in cyber-safer world.