CYCLOPES

CYBERCRIME LAW ENFORCEMENT PRACTITIONERS NETWORK

HANDBOOK FOR PARTICIPANTS attending the PRACTITIONER WORKSHOP Internet of Things (IoT) Devices

This project has received funding from the European Union's Horizon 2020 - the Framework Programme for Coordination and Support Action (2014-2020) under grant agreement No. 10102166

CONTENTS

INTERNET OF THINGS DEVICES

This document provides important information for invited participants attending the CYCLOPES Workshop on 'IoT Devices'.

1. Horizon 2020

Horizon 2020 is the European Union's research programme that covers a range of topics including secure societies, which has a budget of €1.7bn over the period of the programme up to 2020. The EU Commission recognise the value of impact in research and are now emphasising the need to involve end users in research programmes. This will enable the delivery of science and technology that makes a difference, rather than focussing on academic excellence alone. The programme covers a range of security topics including fighting crime and terrorism, borders and external security, digital security and critical infrastructure protection. For further information about the programme please go to: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

2. The CYCLOPES Project

The CYCLOPES project is funded by the European Union's Horizon 2020 Programme (H2020), under the heading of, ***"Pan European network of practitioners and other actors in the field of security".*** The lead agency coordinator for this project is the Polish Platform for Homeland Security, with consortium members being made up of 21 partners from 14 countries. These are as follows:

- Netherlands Organisation for Applied Scientific Research (TNO)
- Sheffield Hallam University (CENTRIC)
- IANUS Consulting Ltd (IANUS)
- Cybercrime Research Institute Gmbh (CRI)
- Austrian Standards International (ASI)
- Central Office for Information Technology in the Security Sector (ZITIS)
- Laurea University of Applied Sciences (LAUREA)

- University College Dublin, National University Of Ireland (UCD CCI)
- Home Office (HO)
- Provincial Police Headquarters in Gdansk (KWPG)
- Ministry of Interior of the Republic of Croatia (MUP)
- General Directorate for Combatting Organized Crime (GDCOC)
- Swedish Police Authority (SPA)
- Ministerio Del Interior (GUCI)
- Belgian Federal Police (BFP)
- State Police of Latvia (SPL)
- College of Policing (CPB)
- The National Police of the Netherlands (NPN)
- Malta Police Force (MPF)

CYCLOPES aim is to establish a network of different stakeholders across Europe, with a wide range of experience in the field of fighting cybercrime in order to:

- Build and maintain an innovation-driven network of LEAs combating cybercrime - accelerating the EU's ability to counteract growing pressures of cyber threats
- Create synergies between LEAs from MS and connect industry and academia by stimulating and sustaining dialogue on pressing security matters threatening the stability of Europe and Citizen safety
- Dedicated teams will scour markets, identifying solutions and research activities to highlight actions and innovative products to assist LEAs tackle the complexity of cybercrime
- The project will support the continued development of LEAs, working closely with practitioners to define current capacities and elicit capability gaps and requirements in crucial areas: procedures, training, legal and standardisation
- Identify priorities for standardisation; recommendations for innovation uptake and implementation; social, ethical and legal reports providing guidance and training suggestions for cybercrime investigators; dissemination of results through workshops, conferences, webinars, publications, policy papers and media.
- Create an ongoing dialogue with industries and academia who are delivering products and conducting research on solutions that fight cybercrime

- Synchronise with other activities and projects also working in the field of cybercrime. The CYCLOPES network will cooperate by exploiting the results of previous networks and initiatives, such as the European Network of Law Enforcement Technology Services (ENLETS), Europol Innovation Lab, ECTEG, EACTDA, iLEAD, iLEAnet, iProcureNet and EU-HYBNET.

The focus of the project is on technical aspects rather than social research and representatives will be invited to become part of a community network which will be made up of a set of three CYCLOPES Practitioner Groups (PG's). Each of the PG's will be managed by consortium members from: Poland, Germany and Sweden with each group comprising of three subject specific topics. Please see table below for the PG's and their related subject specific topics.

	Cybercrime: Affecting People Directly **(PG1)** Sweden	**Cybercrimes: Affecting Systems** **(PG2)** Poland	**Digital Forensics** **(PG3)** Germany
Year 1	'Social Engineering to enable Cybercrime' 30-31 March 2022 Stockholm	'Cybercrime related to Remote Desktop Protocols and similar technologies' 10-11 February 2022 Gdańsk	'Mobile devices & wearable technologies' 15 December 2021 Held online
Year 2	Cryptocurrency 7-8 December 2022 Riga	Investigations involving cloud services 21-22 February 2023 Vienna	Automotive digital forensics 20-21 September 2022 Munich
Year 3	*TBC*	*TBC*	*IoT Devices* *27-28 September 2023* *Sofia*
Year 4	*TBC*	*TBC*	*TBC*
Year 5	*TBC*	*TBC*	*TBC*

During the 5-year lifetime of the CYCLOPES project, each of the 15 topics will be the subject of a Practitioner Workshop, which will be held in various countries across the EU.
The purpose of the workshops is to:

- Bring together practitioners and technical specialists from Law Enforcement Agencies (LEA's) across all member states
- Provide a unique forum in which constructive dialogue on common issues will be encouraged
- Harvest innovative and unified ideas and technological solutions, and direct future research.

3. IoT Devices

Digital forensics of IoT devices is an increasingly important topic in today's connected world and is becoming more relevant in crime investigations. With the growing number of IoT devices used in our everyday lives, it is vital that law enforcement agencies are able to include these devices in the recovery and evaluation process. Digital forensics plays an important role in extracting and analysing potentially relevant data from IoT devices.

The term IoT refers to physical objects or "things" and the networking of these physical objects and devices with other devices or systems over the Internet. IoT devices are hardware devices, such as smartphones, smart home devices, wearables, connected cars or smart cities for example. While performing various tasks in our everyday lives, these devices collect, exchange and process a variety of data, including personal information, location data, and communication data. This type data has the potential to be misused for criminal activities, such as identity theft, fraud, or espionage.

To conduct a forensic investigation of IoT devices, specialised tools and techniques must be available to law enforcement agencies. These tools allow forensic investigators to extract, analyse and interpret data from the devices. In doing so, they must ensure that the integrity of the data is maintained and that no changes are made to the digital evidence extracted from these IoT devices.

A major challenge for law enforcement agencies is the variety of different IoT devices and their operating systems, as well as the constant and fast evolution and innovations in the field. Each device could have a different operating systems and software versions, making forensic investigation more complex. Forensic experts must therefore build and constantly expand their in-depth knowledge and experience of these different devices and systems.

Overall, digital forensics of IoT devices is a complex and important area that requires thorough investigation and analysis. It is critical that forensic scientists or practitioners have the necessary expertise and tools to conduct an effective forensic investigation. This is the only way to detect crimes and identify criminals. It is important for law enforcement agencies to continuously stay up-to-date and remain familiar with ever-evolving technologies.

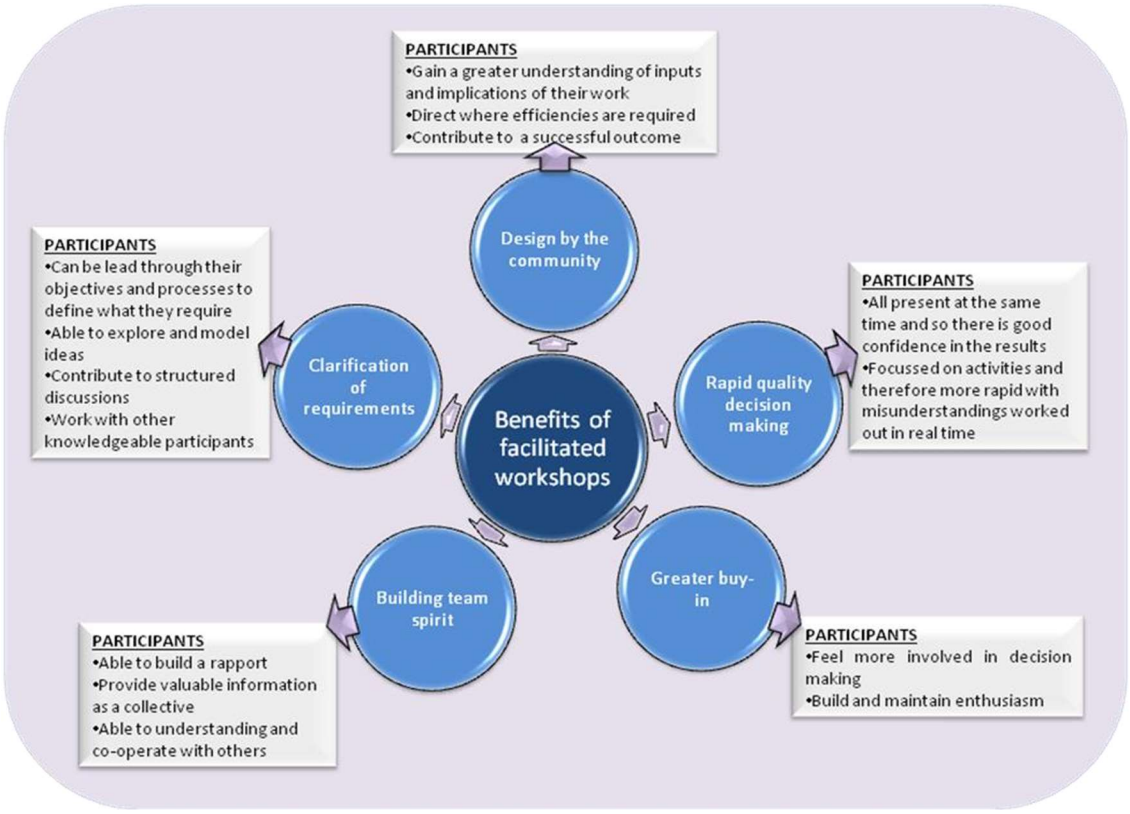
The CYCLOPES practitioner workshop "**Smart Home: Discovery, detection, collection, examination and analysis of IoT devices**" provides an opportunity and platform to discuss and evaluate how we as law enforcement agencies (LEAs) access and utilise data from IoT devices to aid investigations. We will explore the state of play from different participating LEAs, what problems investigators face regarding the acquisition and decoding of data, and the needs of LEAs concerning technology, legislation and standardisation.

The objectives of this workshop are to:

1. List the most common IoT devices analysed and which might be relevant in the future
2. List the key technologies and techniques used by LEAs in investigations involving IoT devices
3. Identify limits and concerns with the technologies and methods currently used for IoT investigations
4. Identify key legislative challenges surrounding investigations involving IoT devices
5. Develop common areas for innovation and requirements for standardisation in the field of investigations involving IoT devices

4. Practitioners Workshop

The success of the CYCLOPES project will be, to a greater part, down to the productive engagement with end-users. Therefore, the facilitated Practitioner Workshops have been designed to, not only benefit the project, but also be a useful and positive experience for the participant. The benefits to participants are shown the diagram below:



The workshops have been created to draw out specific and relevant information, and comprise of a number of structured activities which have a set of required themes and outcomes. However, these activities incorporate 'flexibility' so that participants can provide the steer and direction of the discussions, share information in real time and engage effectively with each other.

The objective of the CYCLOPES IoT Workshop is to bring together Law Enforcement Practitioners (LEP's) from across the EU who are presently working in the police officer end-user environment in order to:

- Think and act as a community

- Translate and define the priorities into real solutions
- Reduce fragmentation of the discipline across the EU

Another important facet to the workshop is the facilitator, who will ensure that every participant will be given the opportunity to talk about their experiences, issues and problems concerning IoT Devices within their own LEA. Then via the "multi-way" dialogue activities, practitioners will be able to identify where commonalties and synergies lay with colleagues from other LEA's. Furthermore, participants, as a collective, can then determine what the end-user priorities are for the future.

5. Workshop Participants

CYCLOPES is looking to have representation from between 10 – 12 EU Member States for the workshop; therefore, spaces will be limited. As the workshops are practitioner lead, invitations will be offered to individuals who are able to; actively contribute to the discussions and activities, provide an end-user perspective and provide directive to the future development of solutions for IoT Devices for LEA's across the EU.

Therefore, with this in mind we are seeking participants who:

"……have the appropriate operational background, a thorough understanding of the discipline and relevant knowledge and experience"

The discussion points and activities that will be covered within the workshop are as follows:

- **The current situation with regards to technology, processes and methodologies**
- **The capability gaps**
- **End user requirements and priorities**
- **Potential solutions to the priorities**
- **Possible areas for standardisation and procurement**

Please note that this Workshop is only being delivered on a face-to-face basis, with no option for remote participation.

6. Pre-Workshop Requirements for Participants

Survey

Prior to the workshop on IoT Devices, participants will be asked to complete a short survey. This survey is built around a number of the main objectives of the CYCLOPES project and explores areas such as: current technologies, current technology challenges, current and future needs, and opportunities for innovation in line with the workshops theme. The pre-workshop data will be collated from all participants, and the survey process repeated at a later stage in the project. The overall data will be used to identify, measure and evidence changes that have occurred within the cybercrime community and all results will be disseminated to the EU Commission and those working in relation to cybercrime. Completion of the survey will be required 2 weeks prior to the commencement of the workshop and all results will be held securely within the EU Survey platform.

PowerPoint Slides

As part of the workshop registration process, participants will be asked to prepare 3 PowerPoint slides (including introduction slide) using the CYCLOPES workshop PowerPoint Presentation template. Participants will be required to deliver a 10-15-minute presentation to other attendees of the CYCLOPES Practitioner Workshop. The slides will contribute to building a rich picture of the activities within this arena across the participating EU countries and used as part of the data gathering process.

The content of the presentation should include the following details:

- List the key technologies and techniques used by your LEA in investigations involving IoT Devices
- Describe the limits and issues of the currently used technology in the field of IoT Devices investigations
- Describe the legislative challenges you face surrounding investigations involving IoT Devices
- Explain what technologies you would like to see being developed to improve the way your LEA conducts investigations involving IoT Devices

The slides should be sent to Claudia Telfer at claudia.telfer@homeoffice.gov.uk and meera.barnett@homeoffice.gov.uk by **4th September 2023.**

Please note: The information to be included within the slides should not be of a sensitive nature nor should it breach participants LEA security and/or copyright protocols.

7. Post Workshop Activity

The data deriving from the workshop interaction and communication will be utilised CYCLOPES on practitioner's behalf, to drive and direct innovation and research and development in order to achieve 'fit for purpose' solutions where required.

Participants will receive the results of the workshops and be consulted on the following:

- Technology, research and innovation watch
- Standardisation information
- Procurement

Participants will also receive news and information on:

- Community networks
- Industry days
- CYCLOPES Permanent Information Sharing Platform
- Expert Register

8. Letter of Consent

Any data collection undertaken by any project consortium member will be carried out to a high ethical standard, and the following set of principles will be adhered to:

- The rights of the participants will be respected at all times
- Participants will be duly informed about the purpose, methods and results of the workshops

- High standards of integrity, quality and transparency with respect to any research undertaken will be maintained throughout the lifetime of the project

With this in mind we would like to draw your attention to the "Letter of Consent" at the end of this document which is a copy that should be retained for your records. The stand-alone copy should be completed by all workshop participants and sent via email to claudia.telfer@homeoffice.gov.uk and meera.barnett@homeoffice.gov.uk

9. Contacts

If you require further details of any of the information provided within this document please do not hesitate to contact Claudia Telfer at: claudia.telfer@homeoffice.gov.uk and meera.barnett@homeoffice.gov.uk

10. Acknowledgements

Thanks to Stephanie Kastner, Christopher Lenk and Andreas Sommer at ZITiS for helping to develop the scope of the workshop.

11. Further Information

You can keep up to date with the CYCLOPES Project using the following link:
https://cyclopes-project.eu/