CYCLOPES

GAPS AND NEEDS OF LEA PRACTITIONERS IN THE AREA OF

# INVESTIGATING CYBERCRIME RELATED SERVICES

PUBLIC VERSION

FOR CYCLOPES BY:
HOME OFFICE UK

Funded by
the European Union

JUNE 2024

# Introduction

CYCLOPES | Investigating
Cybercrime Related Services

This practitioner workshop focused on the investigation of Cybercrime affecting systems and networks, which are committed through the use of online devices, such as a computer, computer networks or other forms of information communications technology (ICT). These online devices are both the tool for committing the crime, and the target of the crime; for example, generating and spreading malware for financial gain and hacking to compromise data, computer networks or activity.

Cyber-attacks are challenging to investigate and often consist of multiple steps, with multiple threat actors, working on different parts of the 'crime-as-a-service' process. Law Enforcement Agencies (LEA) need to work with individuals, public and private sector organisations to secure and recover evidence to support judicial proceedings, however this can often be challenging due to the complex nature of cyber-attacks and the skills and experience of IT professionals and LEA specialist practitioners.

LEA investigations need to understand and exhibit the following:

- How a computer system and/or network has been compromised to gain unauthorised access, e.g., vulnerability exploited.
- What malicious program or code has been installed on the asset and what is it doing, e.g., rootkit, fake antivirus, or spyware.
- How the attacker(s) are communicating with the compromised devices, e.g., identity of the Command & Control centre.

The CYCLOPES practitioner workshop on Investigating Cybercrime Related Services provided an opportunity and platform for LEAs to discuss how to respond to these incidents, how they cooperate with public and private sector organisations and what evidence can be gathered from the compromised computer system and network server logs.

# Priorities of Law Enforcement in the field of Investigating Cybercrime Related Services

Businesses can often be reluctant to report an attack. Educating business' on how to keep themselves safe, the reasons why attacks should be reported, what to do when an attack occurs was flagged as a priority.

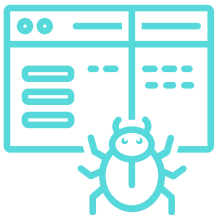
Practitioners agreed that it could also be challenging to obtain data needed from companies such as ISPs, social media platforms and Cloud servers. Better processes for obtaining the data, standardised data requests and improved collaboration with these organisations is needed.

In addition, data retention times varied significantly amongst the different European countries – from 7 days to 2 years. Practitioners agreed that it would be beneficial for European countries to adopt a more uniform approach in respect of these retention times.

# Opportunities for development within Investigations involving Cybercrime Relates Services

## 1. High Volume of Data

Typically, during an investigation of this type, large volumes of data is collected and this can present a number of challenges. More solutions are needed to analyse and triage this data and to automate some of the burdensome manual tasks.



## 2. Dark Web Crawler at a European level

Currently, dark web crawlers are typically maintained by individual LEAs. It was agreed that it could be beneficial for there to be just one European dark web crawler that was maintained by one central European agency.

## 3. A User Education Platform

It can require a lot of time to train a cyber investigator and the turnover of staff is high as they develop a valuable skillset. A user-education platform which could assist with training would be of benefit to LEAs.

# Opportunities for development within Investigations involving Cybercrime Relates Services

## 4. A Standard Data Model to be used by all Law Enforcement Agencies

In addition to the provision of more open-source software (see above), it would assist investigations if a standard data model was used throughout Europe.

## 5. More Open-Source Alternatives to Commercial Software

Many of the licences for commercial software are expensive. As cybercrime is a crime that often transcends borders it is beneficial to everyone for all countries to have access to the software that is needed to combat these crime types.

## 6. Better Sharing of Technical Knowledge

The expertise/knowledge of cyber criminals is ever evolving. For LEAs to keep up to date. It is imperative that intelligence and technical knowledge is better shared between LEAs. Tools and channels that would enable seamless international collaboration are needed.

CYCLOPES

## JOIN THE CYCLOPES NETWORK

## FOLLOW US

project-cyclopes

ProjectCyclopes

## WEBSITE

https://cyclopes-project.eu

## CONTACT

contact@cyclopes-project.eu

Funded by
the European Union