



CC-DRIVER

Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour.

CC-DRIVER LEA Working Group

Human and societal aspects of cybersecurity

WP 7 — Dissemination, Exploitation and Communications

Abstract

The CC-DRIVER LEA Working Group is a discussion group of Law Enforcement Agencies that aims for an exchange of experiences and best practices with a specific focus on cybercrime. These meetings are a safe space to discuss human, social and societal aspects of security problems and their remedies.

The LEA Working Groups are one hour-long conference calls organised by Valencia Local Police on a quarterly basis, being open to any LEA external to CC-DRIVER.

If you are a LEA and would like to participate, please [contact Valencia Local Police](#).

Key words: CC-DRIVER, cybercrime, cybersecurity, grooming, awareness, hacktivism, young, human, police

Contributors

Lead

Valencia Local Police – Rubén Fernández

Other

- José Olivares, PLV
- Jesús Calvo, PLV





Contents

Introduction	4
Background and Objectives	4
Structure of the Report	6
The CC-DRIVER LEA Working Group and its Composition	6
Meeting Procedures	6
Summary of LEA Working Group Meetings	7
Conclusion	8

Introduction

The CC-DRIVER project is aimed at examining the drivers of cybercriminality in Europe, with a special focus on the factors that lead young people to cybercrime, as well as cybercrime-as-a-service. Multiple key research activities on the project focus on the challenges faced by LEAs, their needs, and requirements and in order to obtain valuable LEA feedback, a key activity promised in the CC-DRIVER's Grant Agreement Part B, aimed at creating a LEA Working Group.

The CC-DRIVER consortium partner Valencia Local Police has established the CC-DRIVER LEA Working Group, whose objective is to exchange experiences and knowledge among European LEAs on cybercrime-related topics with a special focus on juvenile cyber delinquency and to share information on relevant tools, resources, best practices and challenges.

Background and Objectives

This document supplements the findings in WP2 and WP5 in particular. While other project tasks assembled data from young people (WP3), policymakers (WP5) and CSOs (WP6), the LEA WG provides the project an input from the perspective of LEAs, especially on cyber juvenile delinquency. The findings of the LEA Working Group will be reflected in the project's recommendations (T6.5), but also at the project's final conference.

By setting a wide approach the LEA WG has helped participants discuss cybercrime issues not only from traditional LEA perspectives, such as intervention and conviction, but also from a human and societal perspective where prevention, awareness and innovative intervention strategies are core activities. In fact, from the experience of previous LEA Working Group meetings, the content and topics of discussion that have led to more engagement have been those related to the latter, namely, the human and societal perspective on prevention, etc. The Working Group has also had participating LEAs suggest topics: the discussion topic for the third meeting (awareness-raising) was brought up by an LEA participant external to the CC-DRIVER consortium who had a special interest in discussing this topic with other LEAs. A summary of the different gatherings is provided below.





Methodology

Conference calls following a structured agenda between LEA partners, SB members and any external LEA interested in participating. As cybercriminality is evolving rapidly, LEAs need to be able to share information and good practices. CC-DRIVER uses these conference calls between its LEA participants as the mechanism to do so.

Activities or results

Exchange of experiences and best practices among LEAs. An anonymised report featuring the key points shared by participants is published in the form of a blog post (uploaded to the CC-DRIVER website) after every edition.

The LEA WG has provided a safe space for LEAs to share:

- Cybercrime related experiences (including, as mentioned above, prevention, awareness and innovative intervention strategies)
- Best practices and initiatives on the addressed topic
- Public reports and databases, resources and tools
- Challenges and recommendations

Structure of the report

After testing different meeting agenda structures, the structure that has promoted more interactions and thus generated more valuable outcomes is to start with the general trend of the addressed topic in each participating country in order to contrast this data. Then, specific questions addressing the topic of discussion are launched, usually three to four questions are shared with the participants in this section. Later, a more open-ended discussion where participants share their challenges and best practices in that regard takes place. This part might be composed of different initiatives, tools and resources that participants have found particularly challenging, or those that have been used for enhancing their response or knowledge of the discussed issue. Finally, participants are encouraged to share their views on possible recommendations for further actions that would improve the LEAs response.

The CC-DRIVER LEA Working Group and its Composition

The CC-DRIVER LEA Working Group was initially composed of the LEA members of the CC-DRIVER project plus the LEA members of the Stakeholder Board, but after the first WG meeting it was clear that other European LEAs may be potentially interested in participating in these conference calls. Therefore, it has been open to any European LEA. Thanks to this measure, LEA personnel from eight countries/sovereign states (Finland, Germany, Greece, Portugal, Slovenia, Spain, Switzerland and the United Kingdom) have participated in at least one WG meeting. The coordinator of our sister project





RAYUELA particularly asked whether participation from his LEAs would be possible (to which we said yes, of course).

Meeting Procedures

The LEA Working Group meets by means of one-hour-long conference calls organised by Valencia Local Police on a quarterly basis.

These meetings provide a confidential space for LEAs to discuss the human, social and societal aspects of security problems and their remedies. The meetings have structured agendas aimed at better understanding the drivers of cybercrime, especially among the young, best practices among LEAs, where more precisely they should allocate scarce resources, etc. These conference calls provide an opportunity to discuss the CC-DRIVER research and innovations and their practicality.

The topics for discussion are open to proposals from LEA participants, thus increasing the engagement as well as focusing on cybercrime-related issues that are of special interest for LEAs.

Summary of LEA Working Group Meetings

LEA Working Group Edition 1

In its first meeting, where LEAs discussed hacktivism and civil disobedience on the Internet, Polícia Judiciária shared with the participants an intervention program using infiltrated agents to steer hacktivists to non-criminal, more socially constructive ways of cyber usage as an alternative to conviction in specific cases. LEAs discussed research studies showing that hackers usually suffer from dysfunctional home or domestic conditions and have mental health issues, which points to the necessity and utility of a multi-actor approach on this issue. This requires joint, coordinated efforts among LEAs, psychologists and social workers, among others.

LEA Working Group Edition 2

Regarding online grooming, which was addressed in the second edition of the LEA Working Group, LEAs discussed research showing how Internet usage has soared due to the COVID-19 pandemic and the effects on online child abuse. In addition, one participating LEA shared an innovative intervention method called the [Sweetie chatbot](#), developed by the NGO Terre des Hommes, which has proven to be helpful in fighting online grooming and child sexual exploitation.

LEA Working Group Edition 3

The third Working Group meeting addressed awareness-raising from an LEA perspective. LEAs agreed that they have a crucial role in preventing cybercrime by means of awareness-raising and, for this purpose, social media are a great way of putting LEAs in close touch with citizens, especially young people. The Spanish National Police's Twitter account ([@policia](#)) was shared as an example of a well-





managed LEA social media account. It has contributed to building trusted relationships with citizens, helped by dynamic two-way communication. This case contrasts with a challenge frequently pointed out in the Working Group: LEA Community Managers (CMs) might lack expertise in the field, as the best CMs are usually in the private sector, which offers higher earnings. Therefore, there is space for improvement in cybersecurity awareness-raising campaigns conducted by LEAs. LEAs noted that the [European Cyber Security Month \(ECSM\) 2020 Deployment Report](#) showed a three-fold increase in engagement in 2020 compared to 2019. The Working Group noted several best practices that helped to achieve this increase: the coordinated, simultaneous actions by means of a joint effort in the same topics (cyber scams and digital skills) and hashtags (primarily [#ThinkB4UClick](#)) seem to have helped in achieving these good results. The wide availability of material (easily downloadable and printable, translated into the participating members' 24 languages) as well as the use of different mass media have also played a crucial role. Europol campaigns "[Say No!](#)" and "[Cybercrime vs Cybersecurity: what will you choose?](#)" were also mentioned as examples of well-regarded campaigns.

[LEA Working Group Edition 4](#)

The last meeting in 2021 the LEA Working Group discussed online hate speech. Participants agreed that law enforcement agencies usually are not effective in preventing and mitigating online hate speech due to the possible reluctance of at-risk individuals to contact and communicate with police forces. Instead, the Working Group agreed that a multi-actor approach where civil society organisations, non-government organisations and charities are direct communicators with the at-risk individuals (coordinating efforts with LEAs) is advised, given the positive results LEAs (for instance, the Police Service of Northern Ireland, which participated in the meeting) have achieved with this approach. The key role of the [No Hate Speech Movement](#) was also mentioned. This youth campaign led by the Council of Europe's Youth Department seeks to mobilise young people to combat hate speech and promote human rights online. On its website, it provides information about the campaign and the resources developed to counter hate speech by promoting competing narratives.

[LEA Working Group Edition 5](#)

The last meeting to date has been held on 27th January 2022 from 11-12h (CET). 14 LEA participants from 6 different countries have attended the meeting, and the agenda was composed of the following points:

- Introduction
(focus of the meeting: meeting – sexting, online sexual coercion/extortion and revenge porn)
- Trend of the addressed topic in each participating country
- Specific questions:
 - Victim/perpetrator profiling (special focus on gender)
 - Modus operandi
 - Preferred SM platforms by perpetrators
- Challenges (legislative, technical tools, etc.)
- Best practices
- Recommendation for further action





The meeting report is currently being written and it is expected to be publicly available in mid-February.

Conclusion

As a final note, in order to cope with the evolving challenges that ICT have brought to our society, LEA WG participants have articulated numerous times that LEAs should go beyond their comfort zone where conservative strategies once worked and embrace innovative, multidisciplinary approaches that take into account human and societal aspects of cybercrime from related fields such as psychology, criminology and anthropology. As the average citizen is unaware of the many security risks on the Internet, law enforcement agencies (and stakeholders) need to enhance their cybersecurity education and awareness for a better prepared, resilient society. The LEA Working Group will keep seeking and promoting this approach within the framework of the CC-DRIVER research project.

The information, documentation and figures available in this deliverable were produced by the CC-DRIVER consortium under EC grant agreement No. 883543. The views expressed in this document should in no way be taken to reflect the views of the European Commission, nor can the European Commission be liable for any use made of the information contained herein. The commercial use of any information contained in this document may require a licence from the proprietor of that information. Neither the CC-DRIVER consortium as a whole nor any partner in the CC-DRIVER consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, nor do they accept any liability for loss or damage suffered from using this information

© 2019 - 2022 CC-DRIVER Consortium

