CC-DRIVER

Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour.
A Research – CC-DRIVER

D6.4 – Summary of interviews with CSOs

[WP6 – Ethics, data protection, socio-economic impact assessment]

Lead contributor	Caneppele Stefano, Christine Burkhardt and Amandine da Silva, University of Lausanne (UNIL)
	stefano.caneppele@unil.ch
Other contributors	Krzysztof Garstka and Richa Kumar, Trilateral Research (TRI)
	Meltini Christodoulaki and Nineta Polemi, Foundation for Research and Technology (FORTH)
	Bianca Becker-Eck, Sven-Eric Fikenscher and Andree Heikes, University of Applied Sciences for Public Service in Bavaria (BayHfoeD)
	Lavinia Dinca, Software Imagination & Vision (SIMAVI)
	Bruce Page, Information Security Forum (ISF)
	Djordje Djokic, Farhan Sahito and Kossay Talmoudi Privanova (PN)
	Lucia Lebre, Policia Judiciária (PJ)
Peer reviewers	Eirini Papadopoulou, Center for Security Studies, KEMEA
	Ruby Farr and Kirsty Phillips, University of East London (UEL)

Due date	31.07.2022
Delivery date	31.07.2022
Type	Report
Dissemination level	PU = Public

Keywords	Civil society organisation, cybercrime, prevention, victim support

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883543.

Abstract

This report presents the findings from 34 interviews conducted with civil society organisation representatives and other stakeholders about their views on cybercriminality in Europe. In addition, the study enquires about difficulties linked to the implementation and use of EU research projects results.

First, the report provides an overview of the interviews. Then we present the interviewees' perspective on the phenomenon of cybercrime, focusing on the most recurrent manifestations of cybercrime and the impact of cybercrime on victims. This is followed by a specific focus on civil society organisations, exploring the different roles they play, with a particular emphasis on victim support, the cooperation they engage in, and the challenges they face in their practice. From a global perspective, we then discuss the key elements that can improve the prevention of cybercrime. Finally, some considerations regarding EU research projects are provided.

The results illustrate various perspectives on cybercrime phenomena based on the practices of the interviewees. The rise in cybercrime, and the easy access to it, shows the importance of strengthening assistance to cybercrime victims – the main point being to recognise the status of a victim – but also highlights the importance of developing a network to support perpetrators since existing networks are often poor. Furthermore, the results show that awareness raising is essential. To do this, engaging and educational messages are recommended while adopting a holistic approach to both the stakeholders and the prevention tools. In this sense, new technology should be used to spread knowledge of cybercrime. Finally, European research projects need to be more widely disseminated and promoted so that society can benefit from them.

Revision Procedure

Version	Date	Description	Reason for Change	Author(s)
V0.1	30.06.2022	Table of Content	-	UNIL
V1.1	12.07.2022	First Draft	-	UNIL
V1.2	25.07.2022	Comments	Internal peer review	KEMEA, UEL
V2.1	27.07.2022	Draft	Application of feedback	UNIL
V2.2	29.07.2022	Comments	Peer review	SAB
V2.3	29.07.2022	Comments	Coordinator review	TRI
V3.1	31.07.2022	Final Version – currently awaiting approval by the EC, watermarked as draft until approval.	Application of feedback	UNIL

Contents

Authorship and acknowledgements

We would like to acknowledge the valuable contribution of each partner.

- UNIL, as task leader, coordinated, wrote and edited this deliverable. Furthermore, UNIL drafted the interview guidelines, contacted civil society organisations and the stakeholder board members, coordinated the interviews, and conducted and transcribed 4 interviews with civil society organisations and stakeholder board members.
- TRI contributed to this deliverable by providing contacts for the interviews. TRI conducted 11 interviews and transcribed 10 interviews with civil society organisations and stakeholder board members.
- FORTH contributed to this deliverable by providing contacts for the interviews. FORTH conducted and transcribed 11 interviews with civil society organisations.
- BayHfoeD contributed to this deliverable by providing contacts for the interviews. BayHfoeD conducted 7 interviews and transcribed 8 interviews with stakeholder board members.
- SIMAVI contributed to this deliverable by providing contacts for the interviews. SIMAVI conducted and transcribed 1 interview with a civil society organisation.
- ISF, PN and PJ contributed to this deliverable by providing contacts for the interviews.
- KEMEA contributed to this deliverable by providing contacts for the interviews and by carrying out the peer review process.
- UEL contributed to this deliverable by carrying out the peer review process.

This document is a deliverable of the CC-DRIVER project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 883543.

Executive summary

This deliverable is part of the larger CC-DRIVER project, which is a research and innovation project funded by the European Commission as part of the Horizon 2020 programme. The goal of the project is to understand the drivers of cybercriminality and develop new methods to prevent, investigate and mitigate cybercriminal behaviour.

This report was developed during the second year of the CC-DRIVER project within Task 6.4 entitled "Interview and analyse the views of civil society organisations on cybercriminality in the EU". While previous CC-DRIVER tasks have already addressed the views of many stakeholders such as academics, law enforcement agencies (LEAs), and even cyber offenders, Task 6.4 brings a complementary perspective from civil society organisations (CSOs), defined as a "non-profit, voluntary citizens' group which is organized on a local, national or international level"[1].

Objectives

This study has two objectives. The first one explores the perceptions of CSOs and CC-DRIVER stakeholders on cybercriminality in Europe and how they address vulnerabilities and social impact. To a lesser extent, the second objective identifies possible difficulties, particularly ethical ones, linked to the implementation and use of research project results. This deliverable focuses on four topic areas:

1) the profile of the CSO interviewed;
2) the CSO's perception of the cybercrime phenomenon;
3) the role of CSOs in preventing, reporting and monitoring cybercrime and cybersecurity issues; and
4) the dissemination of results from European Commission-funded research projects and related ethical issues.

Methodology

The partners conducted in-depth semi-structured interviews with CSO representatives and CC-DRIVER stakeholder board members. We used a non-probability sample approach (convenience and snowball sampling techniques) techniques to recruit participants. Due to the COVID-19 pandemic in 2021–2022, we conducted all interviews online. We recorded and transcribed all interviews. We then applied a continuous thematic approach to analyse the transcripts.

The thematic analyses of the interviews raised different themes that we grouped under five headings:

- profiles of interviewees,
- perceptions on the cybercrime phenomenon and its impacts on victims,
- CSOs and the fight against cybercrime,
- key elements to enhance cybercrime prevention, and

[1] Retrieved from https://www.un.org/en/get-involved/un-and-civil-society

- views on EU research projects.

Interviews overview

This study is based on 34 interviews, of which 21 were conducted with CSO representatives and 13 with stakeholders. Representatives were located in 17 different countries mainly in Europe, with only four participants located outside Europe (i.e., Australia, Canada and Singapore). Regarding the field of activity, the majority of CSOs interviewed are involved in assisting (potential) victims; only one focuses on assistance to (potential) offenders. In terms of the stakeholders, the CSOs are mainly working in LEAs and academic institutions.

Results

Perceptions on cybercrime and its impacts on victims. Most interviewees agreed that cybercrime is on the rise and that the global COVID-19 pandemic has been a precipitator in shifting human interactions to the Internet and exposing more people to the risks of the digital world.

In general, the interviewees highlighted the prevalence of cyber sexual violence, followed by attacks against property. However, while CSO representatives put more emphasis on cyber-enabled crimes (i.e., cyber sexual violence and attacks against property and theft), stakeholders were more sensitive to cyber-dependent crimes (i.e., attacks against data and systems).

Although several interviewees were aware of the concept of cybercrime-as-a-service (CaaS), few of them had encountered this phenomenon in their practice. Nevertheless, they raised concerns about the consequences that this easier access to crime could have, especially for young people, such as the depersonalisation and normalisation of crime.

The impact on the victims of cybercrime was also discussed. We observed a range of different reactions and impacts – social, physical, psychological, economic – which underlines the importance of an individualised approach to victim assistance. However, the social and psychological impacts of victimisation seem to be more relevant than the financial ones.

Civil society organisations and the fight against cybercrime. Almost all the CSOs interviewed are involved in victim assistance (focusing mainly on advisory support, awareness or education services and legal support). The value of CSOs in preventing cybercrime is widely recognised by both CSO representatives and stakeholders. In contrast, monitoring and investigation are less common in CSO activities.

In the context of victim support, the interviewees highlighted certain challenges and needs for improvement. The lack of recognition of the status of a cybercrime victim and the lack of trained specialists in victim support were raised. In addition, the interviewees also underlined the relative scarcity of prevention and support services for perpetrators.

In terms of cooperation with other stakeholders, all CSO representatives agreed on the importance of such cooperation to fight cybercrime. Many collaborations with the police, prosecutors, policymakers, psychologists, schools and universities, and other CSOs were outlined. However, experiences with collaboration vary widely among the interviewees in terms of their nature, systematic character and formalisation.

Key elements to enhance cybercrime prevention. Even if more awareness-raising campaigns and education programmes are being implemented, more work still needs to be done. Based on the views of the interviewees, we identified four dimensions in the implementation of prevention measures: knowledge, holistic approach, entertaining and educational prevention, and evaluation.

Knowledge can either prevent one from becoming a victim or give one the tools to react in the best way possible if one becomes a victim. From this perspective, more awareness should be raised about cybercrime manifestations, modi operandi, risks related to the Internet and connected devices, penal liabilities, protection tools and coping mechanisms.

Several interviewees highlighted the importance of adopting a holistic approach in the implementation of prevention measures. According to them, the responsibility to prevent cybercrime and educate populations lies with all of us, whether we are part of LEAs, educational systems, families, leisure facilities or service and product providers.

In addition, more effort has to be put towards finding the right channel and message to capture people's attention, especially young people and adults who are not sensitive to the risks of cybercrime victimisation. Prevention methods should adapt to the evolution of society and take advantage of new technologies, such as social media, to disseminate entertaining and educational prevention messages.

We mention the scarcity of evidence-based programmes for cybercrime prevention. Even if prevention measures seem to work, it is essential to carry out evaluations (intermediate or final) in order to check on and improve the effectiveness of such programmes.

Views on EU research projects. Very few interviewees had opinions on this subject due to their lack of experience in the field. Indeed, the people interviewed in the study are not involved in research much, and even less so at the European level. They have raised various considerations ranging from project planning to the implementation of results.

Implications for research

Further efforts should address the methodology of cybercrime to determine its socio-psychological impact and how to respond to it. Also, further research should focus on new prevention strategies in line with technological development and consumption habits and on how to prevent the normalisation of cybercrime. Lastly, more effort should be put towards enhancing the evaluation process for any related prevention programmes.

List of figures

List of tables

List of acronyms/abbreviations

Abbreviation	Explanation
CaaS	Cybercrime-as-a-service
COVID-19	Coronavirus disease 2019
CSO	Civil society organisation
EC	European commission
EU	European Union
GDPR	General Data Protection Regulation
ICCAM	I "see" (c)-Child Abuse Material
INTERPOL	International Criminal Police Organisation
IT	Information technology
LEA	Law enforcement agency
LGBTQIA+	Lesbian Gay Bisexual Transgender Queer Intersex Assexual +
NGO	Non-governmental organisation
SB	Stakeholder board of the CC-DRIVER project
UK	United Kingdom
UNIL	University of Lausanne
USA	United States of America
WP	Work package

Table 1 List of acronyms/abbreviations

Glossary of terms

Term	Explanation
Civil society organisation	"A civil society organisation is any non-profit, voluntary citizens' group which is organized on a local, national or international level".[2][retrieved from United Nations' website]
Cybercrime	For the purposes of the CC-DRIVER research project, the term 'cybercrime' refers to broad spectrum of behaviours encompassing all online behaviours that result in harm, including online harms, cyber deviance, cyber delinquency and crimes conducted in cyberspace or through the use of digital technology[3].

Table 2 Glossary of terms

[2] https://www.un.org/en/get-involved/un-and-civil-society

[3] See Phillips, Davidson, Farr, Burkhardt, Caneppele and Aiken, 2022. This is represented within the new framework presented in CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", p. 20. For a further discussion of cybercrime definitions, see Chapter 3 of CC-DRIVER deliverable 2.1 titled "Nature of and perspectives on cybercrime", pp. 15-29, and Chapter 1 of CC-DRIVER deliverable 3.1, pp.11-20.

1. Introduction

CC-DRIVER is a research and innovation project funded by the European Commission (EC) as part of the Horizon 2020 programme. The goal of the project is to understand the drivers of cybercriminality and develop new methods to prevent, investigate and mitigate cybercriminal behaviour. This research focuses on the factors leading young people to cybercrime, as well as on the understanding of cybercrime-as-a-service (CaaS). The project consortium consists of 13 stakeholders from across Europe, including law enforcement agencies (LEAs), academic institutions, non-governmental organisations (NGOs) and organisations in the industry.

In the following sections, we contextualise this report within the CC-DRIVER project; the objectives of this deliverable are described, as well as the way in which the different chapters of this report are articulated. Finally, we provide some clarifications on the scope and limitations of this contribution.

1.1 Background

This report was developed during the second year of the CC-DRIVER project and more precisely within the framework of work package (WP) 6 entitled "Ethics, data protection, socio-economic impact assessment". As stated in the title, this WP addresses multiple aspects including ethics, data protection, citizens' views on cybercriminality in the EU and its impacts.

This deliverable is the output of the activities carried out within Task 6.4 titled "Interview and analyse the views of civil society organisations on cybercriminality in the EU". While previous CC-DRIVER tasks have already addressed or will address the views of academics, LEAs[4], policymakers[5], experts from various domains, young people[6] and even cyber offenders, Task 6.4 brings a complementary perspective from civil society organisations (CSOs) that have not yet been involved.

1.2 Objectives

The primary objective is to explore – through interviews – the perceptions of CSOs and CC-DRIVER stakeholder board (SB) members on cybercriminality in Europe and how they address this phenomenon and its social impacts. To a lesser extent, the second objective is to identify possible difficulties, particularly ethical ones, linked to the implementation and use of EU research project results.

[4] See the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", CC.DRIVER deliverable 5.1 titled "Review of cybersecurity legislation in eight countries and gap analysis", and CC-DRIVER deliverable 5.2 titled "Toolkit for policymakers". Deliverable 5.2 will be released in spring 2023.
[5] CC-DRIVER deliverable 5.2, titled "Toolkit for policymakers", will be released in spring 2023.
[6] CC-DRIVER deliverable 3.2, titled "Youth self-assessment metric", will be released in spring 2023.

Since cybercrime is a multifaceted phenomenon, the contributors decided to cover four topic areas:

1) the profile of the CSO interviewed;
2) the CSO's perception on the cybercrime phenomenon;
3) the role of CSOs in preventing, reporting and monitoring cybercrime and cybersecurity issues; and
4) the dissemination of results from EC-funded research projects and related ethical issues.

1.3 Key deliverables relevant to the D6.4

This deliverable builds on several other already-submitted deliverables, notably D2.1 (Nature of and perspectives on cybercrime and crime as a service,) and D2.2 (Drivers, trends and technology evolution in cybercrime), both of which provide the cybercrime context for the interviews. Also pertinent is D3.1 (Report on drivers of cyber juvenile delinquency), which helped inform our questions of the CSOs. D6.1 (Ethics and data protection requirements) and D6.2 (Ethics and data protection protocol and guidance for partners) are also relevant to ensure that interviews and their summaries do not violate any ethical or data protection issues.

In terms of deliverables yet to come, D6.4 will provide a valuable input to D7.9, the project's exploitation plan, and D7.12 (Report of the final conference). As we prepare the agenda for the final conference, we will want to use that event to further disseminate our findings from D6.4, which we believe will be of interest to most, if not all conference participants.

We make references to other deliverables throughout the report, as an indicator of their importance to this report and, in turn, its influence on remaining deliverables.

1.4 Structure of the report

This report is structured into four chapters. Following this introductory chapter, the methodology for data collection and data analysis is described in Chapter 2. Then Chapter 3 presents a summary of the interviews, which are framed in five topic areas. Finally, we provide a concluding section along with recommendations for future research on cybercrime.

1.5 Scope and limitations

The scope of this report is to provide some insight into the views of CSOs on cybercrime and to determine how they are engaged in the fight against cybercrime and how their involvement might evolve. We took this opportunity to note their views on research, especially the scope for improvement in relation to research processes and the dissemination of results.

To meet the objectives stated in the Grant Agreement and to be consistent with the other activities of the CC-DRIVER project, the geographical scope is focused on Europe. However, given that cybercrime is a global phenomenon, the study interviewed four non-European experts. A larger number of interviews would have been necessary in order to cross-check the data collected with European and non-European organisations.

Another limitation that should be highlighted is that the CSOs interviewed mainly focus their activities on victim support. According to our knowledge, there are more victim support organisations than offender support organisations. Although organisations focusing on offender or industry support were contacted, they did not respond (positively) to our request. Most of the results in this report should, therefore, be read in light of this consideration.

2. Methodology

This chapter presents the methodology of the data collection process through semi-structured interviews and the analytical strategy adopted to investigate the data collected.

2.1 Data collection: Semi-structured interviews

In order to collect the data, we adopted a qualitative semi-structured in-depth interview approach. As required by the CC-DRIVER Grant Agreement, the qualitative interview approach is of great interest when participants are asked to share their knowledge and experience[7]. This process consists of several phases that need to be organised and defined before conducting the interviews. In the following sections, the study sample, the recruitment procedure, the interview design and the data management are described.

2.1.1 Study sample and inclusion/selection criteria

According to the CC-DRIVER Grant Agreement, the interviews must be conducted with CSOs and CC-DRIVER stakeholder board (SB) members.

Civil society organisations (CSOs)
With regard to CSOs, the Grant Agreement did not provide a definition for categorisation. Thus, to be considered a CSO for this study, the task contributors defined three criteria to guide recruitment.

a) The organisation should comply as closely as possible with the broad definition of a CSO retrieved from United Nations' website: "A civil society organisation is any non-profit, voluntary citizens' group which is organized on a local, national or international level"[8].
b) The organisation should deal directly or indirectly with the phenomenon of cybercrime (e.g., by publishing reports on cybercrime, organising events, managing hotline platforms, producing awareness materials or supporting cybercrime prevention campaigns).
c) The organisation is mainly active in Europe. Even though cybercriminality has no territorial boundaries, the contributors decided to include this criterion since the goal of the activity is to discuss cybercriminality in Europe. However, two out of the 25 CSOs are active in North America and Oceania.

The Grant Agreement stated that the number of CSOs to be interviewed was 30. As explained in the next section (2.1.2), it was not possible to achieve this objective.

CC-DRIVER stakeholder board (SB) members
The SB consists of 23 members from different fields (government, LEA, academia, companies) across Europe who share the CC-DRIVER consortium's interest in cybercrime on the one hand and in turning research into innovation on the other hand. The number of SB members to be interviewed was not mentioned in the Grant Agreement. Thus, the task contributors decided to conduct 10 interviews. Since this is already a very small group, no specific selection criteria

[7] Ramos, 2015, p. 45.
[8] https://www.un.org/en/civil-society/page/about-us

were defined. Nevertheless, our intention was to cover a variety of professional fields and geographical areas[9].

2.1.2 Participant recruitment

In the following paragraphs, we explain how we recruited the participants as well as the difficulties encountered during the recruitment procedure.

As the participants come from two different target groups, we used distinct recruitment methods:

- *Civil society organisations (CSOs)*: Convenience sampling (non-probability sampling) was used based on publicly available records on the Internet and our partners' suggestions to create the primary sample. When an email address was available, we sent an invitation email explaining the objectives of the project and the interview as well as the terms of participation and confidentiality. If an email address was not available, we sent the same information through the contact form on the organisation's website. In addition, a snowball sampling technique was used to expand the primary sample by asking the first interviewees if they had other contacts that we could invite for an interview.
- *CC-DRIVER Stakeholder Board (SB)*: Convenience sampling (non-probability sampling) was used based on the SB contact list provided by the project coordinator. An invitation email explaining the interview's goal, as well as the terms of participation and confidentiality, was sent to all SB members.

Nevertheless, the recruitment phase proved to be more complex than expected as accessing professionals working in this field was very difficult. Indeed, the participation rate was 20%. Without providing an in-depth explanation, we have formulated several hypotheses: (1) the lack of human resources due to the global COVID-19 pandemic (normally these types of organisations already have relatively small teams), (2) the nature of their work is confidential and (3) being a CSO in a very competitive environment, their representatives prefer to not disclose information on their activities.

To increase the level of participation, several measures were adopted:

a) The interview period was extended by six months.
b) Reminder emails were sent to the CSOs and the SB members who did not reply a few weeks after the initial contact, explaining that the window for the interview had been extended, detailing the anticipated interview length and emphasising that the interview required no preparation.
c) Further open-access searches were carried out repeatedly to identify other CSOs.
d) All SB members were invited to participate in the interview study without regard to their professional fields and geographical areas.
e) A short presentation was made during an SB meeting to explain the task and encourage SB member to participate in the interview study.
f) Various calls were made to task contributors and other CC-DRIVER partners to gather suggestions about CSOs that could be interviewed.

[9] However, as some members did not respond to our invitation, even after a reminder, we were obliged to renounce this approach and invite all SB members for interview.

In total, 34 interviews were conducted between August 2021 and April 2022, of which 25 interviews were with CSOs and 9 interviews were with SB members.

- *Civil society organisations (CSOs)*: Out of 126 organisations approached, only 54 of them replied. Out of those that replied, 21 declined to participate mainly because of limited resources. Meanwhile, 33 initially agreed to be part of our interview-based study. When scheduling the interviews, some organisations withdrew (n=3) or stopped replying to our emails (n=5).
- *CC-DRIVER stakeholder board (SB)*: Out of 22 invited members, 11 agreed to participate in the interviews. Nevertheless, one member withdrew and another one stopped responding.

However, after analysing the transcripts, it emerged that four interviews could not be labelled as CSOs. Two of the people interviewed were involved in a CSO as an ancillary activity and focused on their experiences with their main activities during the interview. And although the two other interviews were conducted with people working in the cybercrime field, the individuals did not belong to a CSO. Thus, we decided to include these four interviewees in the stakeholder group and to rename the stakeholder group as simply "Stakeholders" instead of SB members.

2.1.3 Interview design

In-depth semi-structured interviews based on the interview schedule detailed in the annex were carried out. Although the questions differed slightly between the interviews with CSOs (Annex 1) and those conducted with the stakeholders (Annex 2), they both covered the following four topic areas:

1) the profile of the CSO/person interviewed,
2) the CSO's/person's perception on the cybercrime phenomenon,
3) the role of CSOs in preventing, reporting and monitoring cybercrime and cybersecurity issues, and
4) the dissemination of the results from EC-funded research projects and related ethical issues.

Due to the COVID-19 pandemic situation in 2021–2022, all interviews were conducted online and directly recorded on Microsoft Teams.

The interviews lasted on average 1 hour for the CSO representatives and 30 minutes for the stakeholders. They were conducted largely in English. Indeed, only 4 interviews (out of 34) were conducted in another language since doing so was more comfortable for the interview participants. Two interviews were conducted in French, one in Greek, and one in Italian.

In order to facilitate the analysis of the interviews, full verbatim transcripts were requested. However, due to time constraints and high workloads, some contributors were not able to provide full verbatim transcripts and instead made minutes of the interviews[10].

[10] This occurred with 11 of the 34 interviews. However, the analyst listened to each of the interviews concerned once (except for one that was conducted in a language not understood by the analyst) in order to get a more general view of these interviews and understand the dynamics of these interactions.

2.1.4 Ethics and data management procedures

UNIL, as task leader, was responsible for sending the invitations to participate in this interview-based study to the CSOs and stakeholders (the interview participants). In case of a positive response, UNIL connected the interview participant with an interviewer (a CC-DRIVER contributor). Interviewee contact information, which was used to arrange the interview, was also collected, stored and used in adherence with data protection regulations (General Data Protection Regulation [GDPR] best practices). Identifying information (participant names and assigned participant IDs) is being kept in a separate file and stored on a computer encrypted and protected with a password. These files will be archived and destroyed when they are no longer needed or five years after the end of the project (whichever is sooner).

An information sheet and consent form were given to the interview participants before an interview (Annex 3). These documents provided participants with all the general information about the goal of the study, as well as details on the way data is collected, stored and used. A signed copy of the consent form had to be sent back in order to proceed with the analysis of the data collected. Signed consent forms will be held by the task leader (UNIL) until the end of CC-DRIVER project. The files are stored on a specific computer belonging to the UNIL team, and the computer is encrypted and protected with a password. Any other existing copies of the consent forms (e.g., those in emails) will be permanently deleted once the deliverable has been validated by the EC.

As previously mentioned, interviews were recorded directly on Microsoft Teams, which is a GDPR-compliant platform. Access to both audio files and transcripts is restricted to the UNIL (as task leader) research team and another CC-DRIVER partner's (as task contributor and interviewer) team.

Any identifying information (e.g., names and institutions) was removed from the transcripts and replaced with, for example, pseudonyms (e.g., CSO-1 and SB-1). The transcripts are being held on a specific computer belonging to the UNIL team, and the computer is encrypted and protected with a password. Once the deliverable has been validated by the EC, all recording files will be permanently deleted.

2.2 Analytical strategy: Continuous thematic approach

The second stage of producing this deliverable involved analysing the information collected through the in-depth interviews. For this purpose, a continuous thematic approach was applied. Thematic analysis is often used to explore qualitative data. In addition, thematic analysis may be favoured when the time available is short and the objective is to provide a descriptive analysis of the data collected[11]. On the one hand, thematic analysis consists of extracting themes from the content, in this case the interview transcripts, in relation to the object and objectives of the research[12]. On the other hand, the continuous approach consists of reading all the content to be analysed while systematically identifying the themes addressed and all themes relevant to the object of study[13].

[11] Paillé and Mucchielli, 2013, p.231.
[12] Paillé and Mucchielli, 2013, p. 323.
[13] Paillé and Mucchielli, 2013, p. 237.

Our analytical approach followed four steps, inspired by the methodology developed by Paillé and Mucchielli (2013):

- *Step 1 – Reading the corpus*: Several readings of the material, in this case the interview transcripts, were necessary to grasp the central elements and the whole corpus available[14].
- *Step 2 – Identifying themes*: For each transcript, themes were identified, named and annotated in the margins of the documents[15].
- *Step 3 – Identifying thematic areas*: The themes identified were systematically recorded on a separate document for each transcript, under headings corresponding to the interview guide[16]. Then, if necessary, the themes were merged, subdivided and prioritised[17] in order to identify thematic areas while preserving the meaning and context of the material[18].
- *Step 4 – Building a thematic map*: The themes and thematic areas were integrated into a thematic map along with raw data extracts (verbatim). This step facilitates the cross-sectional analysis of the interview transcripts[19] and the establishment of links between the different statements (opposition, convergence, complementarity, connection, etc.)[20].

2.3 Limitations and challenges

Although the methodology was thought through and validated by the CC-DRIVER task contributors, the researchers were not exempt from encountering difficulties. While conducting the interviews, some interviewers noted a few limitations and challenges. These concerns can be clustered into three main categories: issues related to the definition of certain concepts, issues related to the cybercrime field of study, and issues related to the interview methodology.

2.3.1 Definitional challenges

An understanding of key concepts had not always acquired before an interview, thus leading to the interviewer needing to provide some explanations. As a result, it was difficult to know whether an interviewer's explanation had influenced the answers given by an interviewee. Below we provide some examples of concepts that required clarification:

- *The concept of cybercrime*: As noted many times in the literature, there is a lack of consensus on the definition of cybercrime and cybersecurity, and legal provisions may differ across countries[21]. During the interviews, interviewees would sometimes ask for clarification on the meaning of cybercrime, and that is a challenge as there is no common vantage point from which to conduct the interview.

[14] Paillé and Mucchielli, 2013, pp. 240-241.
[15] Paillé and Mucchielli, 2013, p. 244.
[16] Paillé and Mucchielli, 2013, p. 271.
[17] Paillé and Mucchielli, 2013, p. 242.
[18] Ramos, 2015, p. 101.
[19] Paillé and Mucchielli, 2013, p. 257.
[20] Paillé and Mucchielli, 2013, p. 284.
[21] See Phillips, Davidson, Farr, Burkhardt, Caneppele and Aiken, (2022); CC-DRIVER deliverable 2.1 titled "Nature of and perspectives on cybercrime"; and CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency".

- *The concept of civil society organisations (CSOs)*: In the first interviews with stakeholders, it seems that the interviewees were not familiar with the term CSO and did not ask for clarification. Therefore, a definition was provided at the beginning of all subsequent interviews.
- *The concept of ethical issues related to the research project*: As the interviewees were rarely involved in the research field, it was difficult to have a discussion about the ethical aspects of the research.

2.3.2 Other challenges related to cybercrime

Two other challenges were addressed regarding cybercrime as a field of study.

- *Technical nature of cyber matters*: Cybercrime in its very nature is technical, and often descriptions of how cybercrime happens become difficult to understand as the technical explanations obfuscate the social and political aspects of the cybercrime.
- *Influence of current affairs on cybercrime*: During the interviews, it was common for a discussion to shift to current events. In the context of this study, the issue of the Pegasus Project coming to light in 2021 is an example of a topic that came up in several interviews. It was then difficult to keep the focus on the CC-DRIVER project and the interview guide, and not to spend too much time on these cases as one hour of interview time passes very quickly.

2.3.3 Methodological challenges

The last challenges identified relate mainly to the methodology used and the distribution of tasks among the contributors.

- *Adapting to different interview situations*: As cybercrime crosses legal and territorial jurisdictions, one of the challenges was adapting to the different interview situations and/or interviewee profiles. Respondents were spread across different countries and areas of work, and it was sometimes difficult to refine the questions to tailor them to an interviewee's profile.
- *Relevance of interviewing SB members*: The Grant Agreement stated that SB members were also to be interviewed as part of this task. However, as the interviews progressed, the relevance of such discussions in relation to CSOs was questioned as the interviewees had little or no experience with nor opinions on CSOs' activities. On the other hand, the input from stakeholders was valuable in terms of understanding the evolution of cybercrime.
- *Caution of interviewees*: Some interviewees were cautious when giving answers. Once we reassured them that there were no wrong answers, they were more open in their responses. The fact that some interviewees were not native English speakers may also have played a role in these interactions.
- *Analytical difficulties*: In an ideal situation, the interviews would have all been conducted and analysed by the same researcher. Such a set-up allows the researcher to have an overall view and understanding of the interviews and the material collected. However, due to the time allocated to each contributor, the tasks had to be divided, so the interviews were conducted by four different partners and the analysis was carried out by a fifth partner. This division of tasks made the analysis more complex, and some aspects may have been missed by the analyst (especially as some transcripts were summarised).

3. Results

This chapter presents the findings from the interviews conducted with CSO representatives and other stakeholders. The thematic analyses of the interviews raised different themes that were grouped under five headings:

- profiles of interviewees,
- perceptions on the cybercrime phenomenon and its impacts on victims,
- CSOs and the fight against cybercrime,
- key elements to enhance cybercrime prevention, and
- views on EU research projects.

Throughout this results chapter, direct quotes from CSO representatives will be labelled as CSO-1 and so forth and those from stakeholders as S-1 and so forth.

As will be shown in the first section, some CSOs, as well as stakeholders, specialise in specific types of cybercrime and support. Therefore, some of the contributions are mainly based on their professional experience or areas of research and the data they have collected in the scope of their activities.

3.1 Interviews overview

Of the 34 interviews conducted, 21 were conducted with CSO representatives and 13 with stakeholders. In total, 37 individuals participated in the interviews as some CSOs had several representatives present. In addition, there was an almost equal split between men and women as 18 women and 19 men participated in the interviews.

The CSOs included in this study were founded between 1990 and 2021. The median being in 2013 means that half of them were founded before 2013 and the other half after 2013.

The interviews in total comprise 1714 minutes (28,57 hours) of recorded discussion. While the interviews with CSOs lasted on average 55 minutes, the conversations with stakeholders were substantially shorter with an average duration of 30 minutes (as foreseen in the interview guide).

In the following subsections, we provide some general information about the interviews and the participants regarding their geographical locations, fields of activity, audiences targeted, and cybercrime areas targeted.

3.1.1 Geographical distribution

Interview participants were located in 17 different countries mainly in Europe (see Figures 1 and 2), which corresponds to the objective of the task, namely, discussing cybercrime in Europe. The most represented countries are Greece (5 interviews) and Switzerland (4 interviews)[22].

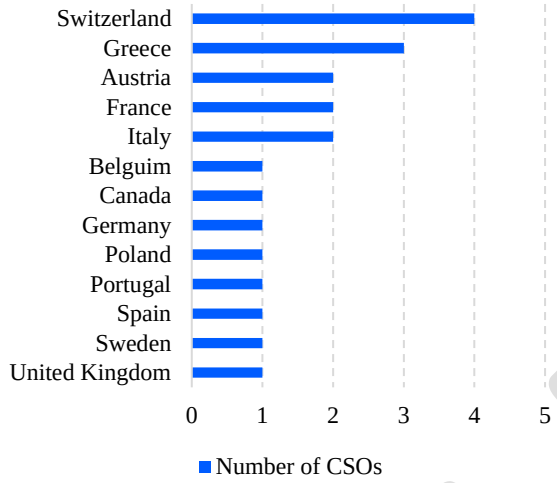

Figure 1 CSOs' geographical distribution (n=21)

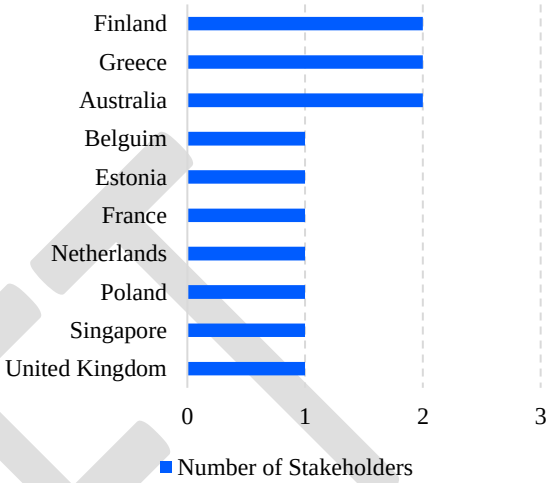

Figure 2 Stakeholder participants' geographical distribution (n=13)

However, we note four interviews with participants outside Europe, including Canada, Singapore, and Australia. These interviews concern one CSO and three stakeholders.

Although most organisations represented focus their activities at the national level, several organisations have an international scope.

3.1.2 Field of activity

As regards the fields of activity, the majority of CSOs interviewed are active in assisting victims or potential victims. Only one CSO focuses on providing assistance to offenders. The different roles will be described in Section 3.3.1 below.

[22] As far as it concerns CSOs, this is probably because two of the report contributors are from these countries.

In terms of the stakeholders, they are mainly from LEAs and the academic community (see Figure 3). And finally, one interviewee is active in the industry, one in a CSO and another in a government department.

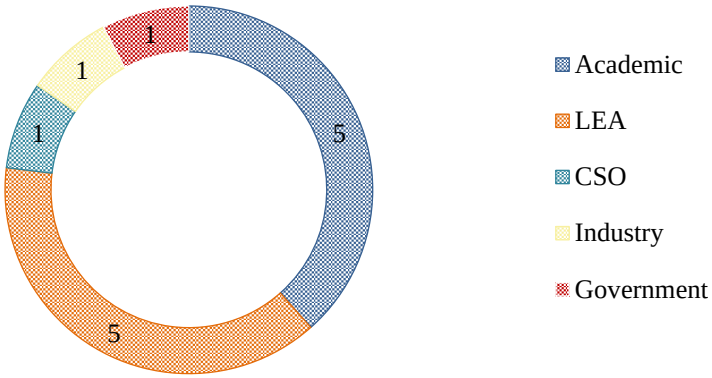

Figure 3 Stakeholder participants' fields of activity (n=13)

3.1.3 Civil society organisations' target groups

An organisation may offer its services to individuals (regardless of age and gender), or it may focus on a specific population. In this study, just over half of the CSOs interviewed have a focus on a specific population (see Figure 4). While nine organisations aim to actively support both children and adults, nine other organisations target a specific group of (potential) victims or (potential) perpetrators. Of these, the majority provides support to children and young people (n=6), and three are focused on the adult population (one specifically on female victims). In addition, four CSOs are also providing support to NGOs (but only one has this activity as its main focus).

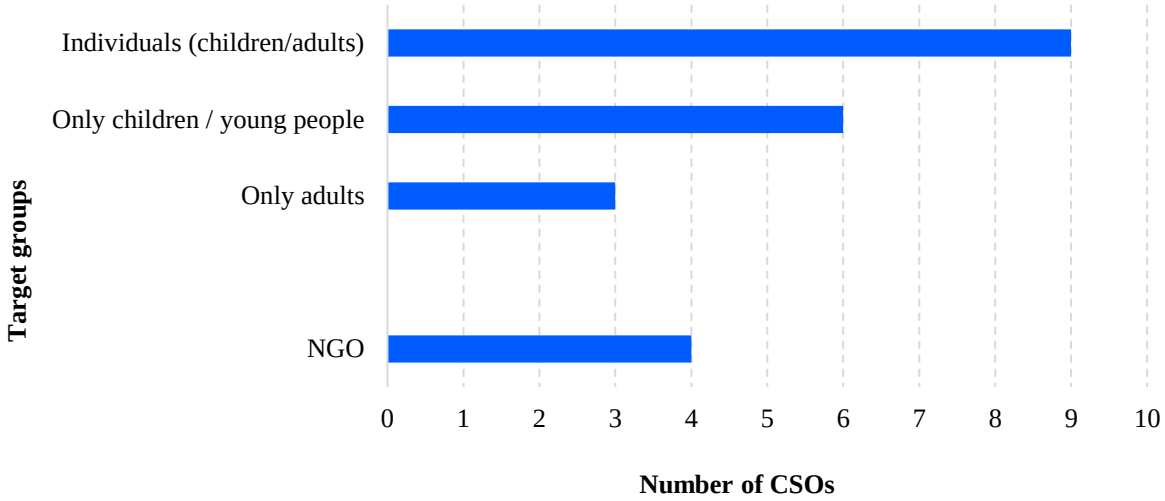

Figure 4 CSOs' target groups (based on 21 CSOs[23])

[23] The number of CSOs considered may have multiple target groups. Therefore, the overall counting is bigger than the number of CSOs.

3.1.4 Cybercriminal behaviours addressed by civil society organisations

The last characteristic analysed is the type of crime considered by the CSOs interviewed. Almost a quarter of the CSOs provide support to victims[24] of cybercrime, regardless of the exact nature of the crime. In contrast, as shown in Figure 5, other CSOs focus on specific types of crime. In this case, most organisations work in the field of cyber sexual violence, which includes sexual online offenses, sexual abuse material, sextortion and so forth. The second category is cyber interpersonal violence that refers mainly to cyberbullying. Four CSOs are also interested in cyber fraud and online trading. Then a more limited number of CSOs are involved in violence against groups such as hate speech (n=3), traditional crime online (i.e., money laundering, n=1) and attacks against data and systems (n=1).

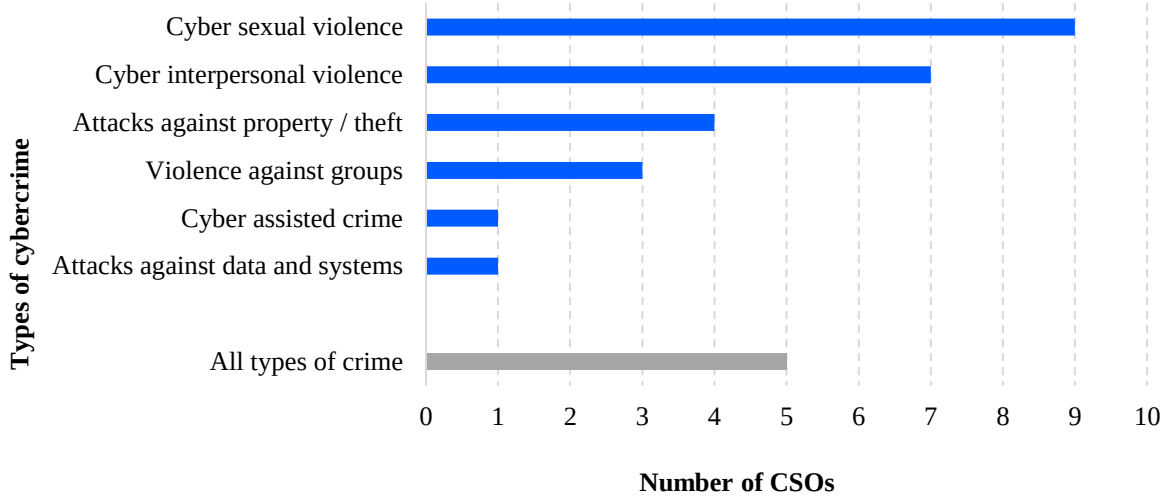

Figure 5 CSOs' types of cybercrime addressed (based on 21 CSOs[25])[26]

3.2 Perceptions on cybercrime and its impacts on victims

In this section, we describe the perceptions of the interviewees on the development of cybercrime as well as its most recurrent forms. After some considerations on the concept of CaaS, we discuss the various impacts that cybercrime may have on victims. Finally, we point out some challenges that make it difficult to have a global view of cybercrime.

3.2.1 Current cybercrime manifestations, characteristics and trends

Most of the interviewees – CSO representatives and stakeholders – expressed their perceptions on the evolution of cybercrime in recent years and identified, in their opinions, the most recurrent forms of cybercrime. Before presenting these results, it is important to stress again that these interviews were conducted between August 2021 and April 2022, that is, in the midst of the COVID-19 pandemic.

[24] The only organisation providing support to perpetrators limits its scope of activity to sexual child pornography.
[25] The number of CSOs considered may address multiple cybercrime behaviours. Therefore, the overall counting is bigger than the number of CSOs.
[26] The categories shown in Figure 5 are based on the cyberdeviance and cybercrime framework developed within the CC-DRIVER project. For more details on the complete framework, see the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", p. 20.

Using the cyberdeviance and cybercrime framework developed within the CC-DRIVER project (deliverable 3.1)[27], we present here the categories including the cybercrimes most frequently mentioned by the interviewees as recurrent manifestations of cybercrime.

In general, we note that interviewees highlighted the prevalence of cyber sexual violence, followed by attacks against property/theft (see Figure 6). While attacks on data and systems were raised by some interviewees, cyber interpersonal violence, violence against groups and other more traditional crimes were less frequently cited. An interesting point is that CSOs put more emphasis on cyber-enabled crimes (i.e., cyber sexual violence and attacks against property/theft), while stakeholders were more sensitive to cyber-dependent crimes (i.e., attacks against data and systems). An explanatory hypothesis is that the organisations interviewed are more active in assisting individual victims rather than companies, with the latter being more prone to data and system attacks.

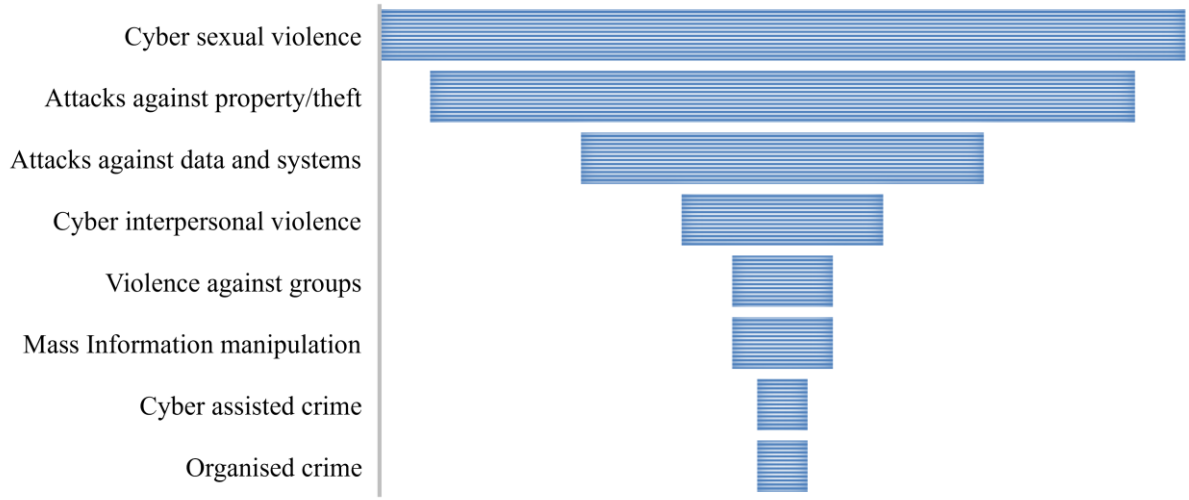

Figure 6 Most recurrent manifestations of cybercrime according to the interviewees

In the following paragraphs, we provide the views of interviewees on the characteristics of victims/perpetrators, modi operandi or trends when available.

a) Cyber sexual violence

When it comes to cyber sexual offences, interviewees reported **sextortion**, **non-consensual intimate image sharing** and **child sexual abuse material** as the most common offences. **Online grooming** and **online stalking** were also mentioned as recurrent manifestations. Most interviewees who reported these five types of offences agree that they have increased during the COVID-19 pandemic.

Concerning victims'/perpetrators' characteristics, most of the interviewees perceived *non-consensual image sharing* as a gender-based crime since victims are mainly women, although one interviewee pointed out that the number of male victims is increasing[28]. A

[27] For more details on the complete framework, see the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", p. 20.
[28] On the other hand, a CSO representative pointed out that labelling a crime as a "gender-based offence" risks forgetting some of the victims. Men are also victims of these crimes, although they are proportionately a smaller population.

particular concern identified young people aged between 12 and 15 years old and engaged in sexting as a vulnerable group.

Even for *stalking*, the gender-based dimension was perceived as relevant, while a technological divide in modi operandi can also be observed according to some of the interviewees: younger people are mainly victimised on social media or through email boxes, and older victims are more often targeted offline by telephone or through personal contact.

b) Attacks against property/theft

In this category, interviewees underlined **phishing**, **identify theft**, **identity theft by morphing** and **different types of online fraud** (e.g., card fraud, romance fraud[29], fake influencer partnerships, COVID-19-related fake shops and cryptocurrency investment fraud) as the most common offences. Based on the interviews, *identity theft* and *card fraud* are perceived as targeting middle-aged victims, while *cryptocurrency investment fraud* is targeted mainly at young people who are technologically savvy but rather inexperienced in investing. Another fraud scheme which targets young victims is the *fake influencer partnership* that often takes place on social media. While non-consensual intimate image sharing and online stalking are perceived as mainly gender-based against women, *love scams* have been depicted as a crime with predominantly men victims[30].

c) Attacks against data and systems

As far as attacks against data and systems are concerned, **ransomware** was mentioned as the most recurrent manifestation by the interviewees. Other types of **systems interference** (i.e., against schools or companies), **cryptocurrency account hacking** and **attacks against critical infrastructure** were also mentioned. During the interviews, different perceptions emerged regarding *attacks against a system*. One interviewee maintained that there is an ongoing shift in target from small companies to big companies which will be reversed again as soon as large companies have taken the necessary security measures. From another perspective, one interviewee shed light on CSOs such as human rights defenders and activist organisations, as well as those supporting LGBTQIA+ movements. In the interviewee's opinion, these types of CSOs could be considered vulnerable to ideologically motivated attacks. With regard to *cryptocurrency hacking*, some interviewees suggested that during the pandemic, people were not aware of how to secure their purchases, leading to an increase in victimisations.

d) Cyber interpersonal violence

In this category, only **cyberbullying** phenomena were mentioned. All the interviewees who spoke on this subject perceived an increase in cases of cyberbullying. And two of them added that they had observed an increase in cyberbullying victims with suicidal thoughts. Based on their experiences, vulnerable groups were children, young people, and

[29] Also known as love scams or dating fraud.

[30] The characteristics of the victims of romance fraud deserve to be explored further. Regarding the gender, Whitty (2018, p. 107) and, Buil-Gil and Zeng (2021, p. 9) note that more women are victims of love fraud. However, when comparing the November-December period of 2019 and 2020 – even though women are more victimised – Buil-Gil and Zeng (2021, p. 9) observe a more significant increase in male victimisations. In addition, the dating and romance fraud statistics provided by the Australian competition & consumer commission show a slight predominance of male victims in 2021 and in the first half of 2022 (Scamwatch, 2022). These contradictory findings suggest that more research is needed.

people suffering from mental disabilities or with migrant backgrounds. During the first months of the COVID-19 pandemic, one interviewee reported that people of Asian origin became the target of cyberbullying due to the virus spreading from Asia.

e) Violence against groups

Hate speech was mentioned by two interviewees as a recurrent cybercrime manifestation. While one interviewee talked about a shift from hate speech against politicians to hate speech between young people, another warned of an increase in hate speech against the LGBTQIA+ community.

f) Cyber-assisted crime

In this last category, **money laundering** and **money mulling** were cited as the most recurrent phenomena. Concerning vulnerable groups, some interviewees suggested that youths and people suffering from mental disabilities were at greater risk of being involved in *money mulling*.

Most interviewees recognised that cybercrime is on the rise and that the COVID-19 pandemic has been a precipitator in shifting human interactions to the internet and exposing more people to the risks of the digital world. As one interviewee pointed out, the COVID-19 pandemic "is going to have a global legacy of changing the way we deliver business and deliver services", leading to new ways and opportunities of committing a cybercrime (S-1). The interviewee also added that the evolution and expansion of the internet of things should not be ignored; these changes will also provide new opportunities for criminals. Indeed, cybercriminals have frequently demonstrated their great capacity to adapt to new situations and exploit new opportunities. As stated by a CSO representative:

> *"We see that needs are exploited so whenever there is a need for something, it's the COVID or the e-bikes, or it's the new iPhone, is it, you know it will be exploited, so this is always the new stuff coming […]." (CSO-2)*

Overall, interviewees agreed that crime is increasingly moving into cyberspace, suggesting a continuous rise in both cyber-enabled crimes and cyber-dependent crimes.

3.2.2 Cybercrime-as-a-service

Very few interviewees mentioned the structure and organisation of criminal groups, which can be seen as a business model[31]. Nevertheless, as CaaS is a matter of concern in political agendas, the interviewers introduced this topic with CSO representatives where possible. Out of 10 interviews where the concept of CaaS came up, 8 CSO representatives were aware of the concept. However, not all of them had encountered it in their activities. As for the stakeholders, 3 of them spontaneously mentioned CaaS and underlined the increasing trend.

Based on the interviews, CaaS does not seem to be suitable for all types of crime. For example, a representative of a CSO mentioned that emotionally based crimes – such as cyberstalking –

[31] For more details on the type of services offered covered by the concept of CaaS, see CC-DRIVER R-1 Landscape Study of Cybercrime-as-a-Service.

are not well suited to this type of service. Another interviewee concurred, adding that the perpetrator is more interested in establishing a relationship with the victim, so using a service does not seem compatible with the perpetrator's goal. This interviewee also noted that there is a moral panic around this phenomenon in relation to stalking. According to the interviewee, the perpetrator would rather turn to his relatives (family and friends) or social networks for technical support as it appears that the techniques used by stalkers are often not that sophisticated. Nevertheless, CaaS could be imagined in the context of stalkers with several victims at the same time.

Another example of the use of CaaS refers to divorce proceedings. It appears that there have been some cases in which people in divorce proceedings have used phishing or malware services in order to find compromising information about their partners.

Lastly, a few interviewees discussed the impact of CaaS. They first highlighted that with CaaS, crime is within the reach of more people due to the availability of such services. Furthermore, their concern was that CaaS may be accessible to children and young people with technical skills who are looking to get money easily. Finally, they perceived CaaS as a vector for more sophisticated threats in the future.

> *"[…] cybercrime as a service is going to be a big issue for us looking forward. It will mean that we will get a lot more threat actors [inaudible] and more sophisticated about using tools. There's a range of different business models around criminal activity, which is going to be difficult for us as a community. I'd say that things are going to get a lot worse before they get better, unfortunately." (S-1)*

Secondly, according to one of the interviewees, this easy access may lead to a depersonalisation of crime[32]. In this sense, some people allow themselves to behave on the internet in ways that they would not face-to-face. Some barriers may fall away when a person is facing a screen and not another person.

> *"How on earth, would you or I, in the past, find somebody to kill your partner? You'd have to go to some really dodgy area and put your personal safety at risk. Now what you do, you just type a few things, you depersonalise the whole process and off you go. Obviously, it's not that simple, but it's a lot easier to get crimes done by others now than it has ever been […]." (CSO-3)*

Thirdly, this depersonalisation, as well as the prevalence of these behaviours, risk drifting towards a normalisation of some criminal acts. According to one interviewee, this normalisation of crime is already perceived among young people in general, noting that older victims are often

[32] This echoes Suler's (2004) online disinhibition effect framework, which considers the following six factors that contribute to online disinhibition: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimization of authority. Based on Suler's framework, an "Online Disinhibition Scale" has been developed by Udris (2014). This scale has been used in the CC-DRIVER youth survey (Task 3.2) to measure online disinhibition.

more outraged when they are victimised than young people, who sometimes do not care[33]. Cybercrime as a business model could therefore accentuate this normalisation phenomenon.

Furthermore, the hidden implications of using this type of criminal service were also emphasised. While the service purchased may seem benign, the money earned by the criminal group may be used to fund far more serious criminal acts.

> *"[…] where does that money go, because maybe the criminal service that you access is relatively harmless, on a scale of things. But then the organisation offers that are actually there, are on trafficking human beings or on a criminal gang that murders people without a thought. So I think that's all a part of it, there's the impact, the availability and its impact on the individuals, of the use of that crime service, but then there is the financial support of the crime itself, and it encourages people to go into crime as well." (CSO-3)*

While CaaS is about offering and monetising services, one of the interviewees mentioned that, in his opinion, this phenomenon is not as widespread as assumed. Although he did not question the increasingly organised structure of some cybercriminal groups, he observed a growth of national and local cyber markets at the expense of cyber transnational markets. Thus, new concerns about community development at the local level are emerging.

> *"I mean, it's not the service, but it's the availability of all these products. I think it's opened up a lot of opportunities for a lot of people who used to be involved in small-scale local drug dealing or things like that. […] I think it's more relevant than cybercrime as a service, now it's the localisation of cybercrime. Because with these marketplaces, with these platforms, we are able to have small communities of cybercriminals at the local level that will survive because they manage to attract enough people among the members of street gangs, among the members of petty criminals, who previously would have been involved in drug trafficking." (CSO-24)*

3.2.3 Impacts on cybercrime victims

In the interviews with CSO representatives, we also discussed the impact of cybercrime on the people who are the victims of it. While one part of the population is rather resilient, another part of the population "will suffer more and to varying degrees" (CSO-3). This may depend on individual characteristics, the type of cybercrime experienced and the network of support[34]. For example, children will potentially experience victimisation differently than adults. Being born into the internet era, their social lives are likely to be more dependent on the internet and social networks.

Whether social, psychological or financial, the consequences of victimisation are often interconnected. Nevertheless, interviewees generally emphasised the importance of the social and psychological consequences of victimisation, rather than the financial ones. Indeed, a CSO representative mentioned that before and after assisting a victim, an impact survey is sent to the victim. It appears that financial impact is very often mentioned last even in the context of a

[33] A certain normalisation of harmful online behaviours among young people was also identified in interviews with experts under Task 3.1. For more details, see the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", p. 42.
[34] Associação Portuguesa de Apoio à Vítima APAV, 2021, p. 73.

victimisation for scams or cryptocurrency crime. However, this does not mean that there is no financial impact as this can be a direct or indirect consequence of the victimisation as we can see below. According to these impact surveys, loss of trust in technology, impact on daily and family life, and isolation were the most important impacts identified. In a society where relationships are becoming increasingly virtual, the loss of trust in technology can have serious consequences. Several interviewees noted that during the COVID-19 pandemic, these impacts became even more pronounced.

> *"Especially, during the pandemic period where many people did not have any other means of communication rather the online means, it was very serious if they felt that they would be hacked. There was not online trust, and they had the fear of a cyberattack." (CSO-9)*

Other emotions noted by interviewees included anxiety, anger, shame and worry. But victimisation can also lead to changes in behaviour or habits, such as dropping the use of social networks or the internet in general or, on the contrary, gaining a compulsive need to see what is being said on the networks (especially in cases of cyberbullying or hate speech). Thus, the impacts on mental health should not be forgotten.

Speaking more specifically about violent crimes such as cyberbullying, hate speech and sexual abuse, some interviewees emphasised consequences such as fear, insecurity at home, negative feelings about the body, isolation, sleep disorders, depression, phobia about going to school and loss of concentration (at school or at work). The loss of work can then indirectly lead to economic consequences for the victim.

Since the internet is so prominent in daily life, a victim may feel they have no escape. These traumas can lead to drug/alcohol use, self-harm and even the fatal outcome of suicide. Interviewees reported several cases of suicide or suicidal thoughts in cyberbullying situations.

With regard to the lack of trust, it is not just about new technologies and related services. Several interviewees stressed the impact of fake news and deepfakes[35]. These processes lead to a lack of trust in people as it becomes more difficult to determine the authenticity of a piece of information or a situation. Whereas before an image or video was more reliable than text, image manipulation now raises a sense of mistrust. This can lead to a lack of trust in everything, creating a threat to democratic processes.

> *"I think there's the potential for this to sort of sow mistrust, and we see things like fake news as a phenomenon, a deepfake as a result, that could lead us to a situation where we don't know if we can trust the authenticity, and it's impossible to tell the authenticity of video footage which could have wide-ranging implications that regulators and civil society would need to be mindful of. So it's probably going to be a growing problem." (S-5)*

From the same view, another interviewee highlighted the dangers of hate speech (especially racism and anti-Semitism) and bullying for democratic processes as they may lead to disinformation, fear and isolation.

[35] Deepfakes are "hyper-realistic digital falsification[s] of images, video, and audio" (see Chesney and Citron, 2019, p. 1757).

"[Hate speech] will help haters [to] create division into a population that will create an isolation for different groups. And because people will be more isolated and people will be afraid […],they will feel that they are not in capacities to act to defend themselves or to reach out to other communities. […] I feel like those kind of hate speech are very dangerous in the democratic system." (CSO-13)

However, the impact on businesses was barely discussed in the interviews as the majority of CSOs are active in assisting individual victims. Even when asked whether their CSOs had been victims of cybercrime, only one CSO answered affirmatively. On the other hand, several mentioned being aware of the risks and taking the necessary steps to regularly assess their information technology (IT) infrastructures, especially for those receiving sensitive data from victims.

In addition, one of the interviewees briefly commented on the impact of an attack on systems in the healthcare environment. According to him, such attacks bring additional stress to medical staff and a sense of powerlessness to those who have had their data stolen, for example. He also highlighted the psychological pressure on chief security officers.

"[…] the chief information security officers because it's like when you defend a castle, you need to be sure that nobody can enter and the attacker is this just need to find one single entry point, so is it kind of like a difference […] difference in position and obviously the stresses is additional stress, and most of the time when there's a successful cyberattack in a company, the first thing they do is they fire the CSO, and now because it's for the reputation of the company in front of shareholders, something has to be done and someone has to be blamed." (CSO-10)

Furthermore, some consequences or impacts can last for years or even a lifetime. For example, in the case of identity theft, it can take years to fully regain one's identity. Also, some crimes can leave traces or have repercussions many years later – for example, when intimate photos are published – since the material that was uploaded can never be permanently deleted.

"[…] this has an impact in the social life of the survivor they feel most of the time the survivors feel embarrassed in the working environment, they feel they are the victims all the time and they feel vulnerable they cannot trust other people." (CSO-26)

"[…] this is what [is] so difficult with some forms of cybercrime is that that could be a lifelong risk because of the inability to permanently remove the danger, so it may be related to identity theft and then you may stop the one criminal, but that data can still be out there, and be reused in five, ten, twenty years' time or the next day, so you have to learn to live with that threat, and then you have to come up with (and it helps to come up with) strategies on how to deal with it." (CSO-3)

We thus observe a range of different reactions and impacts – social, physical, psychological, economic – which underlines the importance of an individualised approach to victim assistance, while taking into account the victim's environment, which may also be very different from one

victim to another (socially, religiously, etc.). But the impact on individuals needs to be further investigated as existing studies are relatively sparse[36].

3.2.4 Challenges regarding perceptions on the cybercrime phenomenon

The interviewees repeatedly emphasised that it is very difficult to have a global view of the evolution of cybercrime. The three main challenges identified are (1) the confusion created by diverse cybercrime definitions, (2) the lack of data on cybercrime and (3) the dark figure of cybercrime linked to non-reporting.

a) Confusion created by the lack of consensus on some cybercrime definition

Some interviewees pointed out that some cybercrimes are not clearly defined. This problem can lead to confusion among the population when experts adopt different perspectives when talking about the same phenomenon or when the scope of legislation is too broad or too narrow. To illustrate this problem, two interviewees mentioned the confusion that can exist between revenge porn and non-consensual intimate image sharing. Revenge porn is the widely used term; however, it is one form of image-based abuse and is rather narrow in scope as it does not include acts of extortion and acts with a humiliating purpose. Another example given by an interviewee concerns the nature of stalking. Sometimes, victims of stalking do not consider themselves victims because the content of the persistent messages is rather kind or flattering. However, it is not so much the content of the messages that is important but rather the harassing behaviour.

> *"[…] we can get thousands of emails or thousands of messages saying that somebody loves us. It doesn't matter it's also stalking. [...] The most important is that this kind of message, there a lot of them, we don't want them and we informed about it, we informed our stalker about it that we don't want them, and this is a kind of persecution somehow, a besetment of our person. So no matter what's in the message, persistence is the most important." (CSO-4)*

A more specific definition would allow those affected to better identify that they are experiencing illegal behaviour and report it but also allow different stakeholders, such as CSOs, to better address the phenomena concerned.

b) Lack of data on cybercrime

The lack of global and reliable statistics was noted by several interviewees. As a result, most of the interviewees expressed themselves on the basis of cases encountered in their professional practice and the statistics that their organisations have recorded[37]. Apart from problems of reliability and comparison between countries, the available data are often included in rather broad categories. One example cited by an interviewee relates to fraud. Such cases are often represented by a single category, not allowing for distinctions between the various forms of fraud. Some interviewees also mentioned the need for information on the costs of cybercrime. All this information would provide an

[36] Associação Portuguesa de Apoio à Vítima APAV, 2021, p. 73.
[37] For more details on cybercrime measurement issues, see the CC-DRIVER deliverable 2.1 titled "Nature of and perspectives on cybercrime", pp. 38-42; Aebi, Caneppele and Molnar, 2022; da Silva, Burkhardt and Caneppele, 2022.

overview of the cybercrime evolution and would help us to better understand the phenomena, to set priorities and to take the right decisions.

c) Dark figure of cybercrime linked to non-reporting

In addition to the lack of statistics on cybercrime, the interviewees also pointed out the low rate of reporting by victims. Indeed, cybercrimes are presumed to be less reported to the police than traditional crimes[38]. Thus, even if reliable indicators were implemented, they would only give a partial overview of the situation.

3.3 Civil society organisations and the fight against cybercrime

In this section, we describe the main activities provided by the CSOs, as well as the perceptions of stakeholders. Some considerations on victim status are subsequently outlined. Then we discuss collaboration between CSOs and other stakeholders. Lastly, we present some challenges and needs for improvement identified by the interviewees.

3.3.1 Role and activities of civil society organisations

The role of CSOs was mainly explored in three dimensions: prevention, monitoring and investigation. The first observation is that the investigative dimension is not reflected in the activities of the CSOs interviewed. Both CSO representatives and stakeholders share the view that investigation is mainly the responsibility of law enforcement authorities or cybersecurity companies. Indeed, only one CSO carries out investigations, but these are more technical/IT security related. The CSOs interviewed noted that the cross-border nature of cybercrime, as well as collaboration with providers, hinders their ability to investigate and resolve cases. Also, one of the interviewees pointed out the ethical risks that can arise when civil parties engage in investigation, such as the risk of breaking the law without being aware of it.

> *"Sometimes they can do it [breaking the law] accidently, or sometimes they just see the issue differently than the law enforcement agencies, for example, if you think about aggressive paedophile hunting, so if you try to encourage somebody to commit a crime instead of like waiting for a paedophile to approach your fake profile, there is a difference […]." (S-2)*

The role of CSOs in monitoring cybercrime is more controversial. While some spoke about the independence of CSOs and the support they could provide to the police, others raised concerns about trustworthy and comparable data standards. Although some organisations interviewed collect data, this is not their main purpose. Rather, they use the data to guide and improve their prevention and support activities. However, it is important to note that the organisations that are members of the wider INHOPE (International Association of Internet Hotlines) network contribute to the ICCAM database on child sexual exploitation material, to which INTERPOL (the International Criminal Police Organization) also has access[39].

[38] Gercke, 2012, pp. 14-15; Reep-van den Bergh and Junger, 2018, pp. 1-2.
[39] For more details, see https://www.inhope.org/EN/articles/iccam-what-is-it-and-why-is-it-important.

On the other hand, with regard to prevention – be it primary, secondary or tertiary prevention – and assistance, the value of CSOs is widely recognised both by CSOs representatives and by stakeholders. Indeed, the CSOs interviewed are all active in prevention and assistance to (potential) victims (only one deals with [potential] perpetrators).

The assistance provided by the CSOs can appear in several forms. Based on the CSOs interviewed, eight types of support were identified:

1) advisory support, including counselling via helpline/hotline, chat box, email, publishing articles and prevention guides and organising prevention events (such as a national day);
2) advocacy work, including mainly policy work;
3) awareness and education support, including school prevention classes, conferences and webinars, and training for stakeholders such as LEAs;
4) investigative support;
5) legal support, including legal advice, legal counselling and funding of legal proceedings;
6) psychological support;
7) research work; and
8) technical support, including to find the nature of an attack, to assess a security system and to remove illegal content from an online platform.

The interviews show that CSOs sometimes pursue their prevention and assistance objectives through different channels, implementing several types of activity. As far as those we interviewed were concerned, they mainly focus on advisory support, awareness/education services and legal support. As shown in Figure 7, CSOs doing investigations, advocacy work and technical support are less represented in our sample. We can also note that only a quarter of these organisations have research engagement. Only one organisation is research based, with the others being more reliant on the allocation of funds and resources to conduct research.

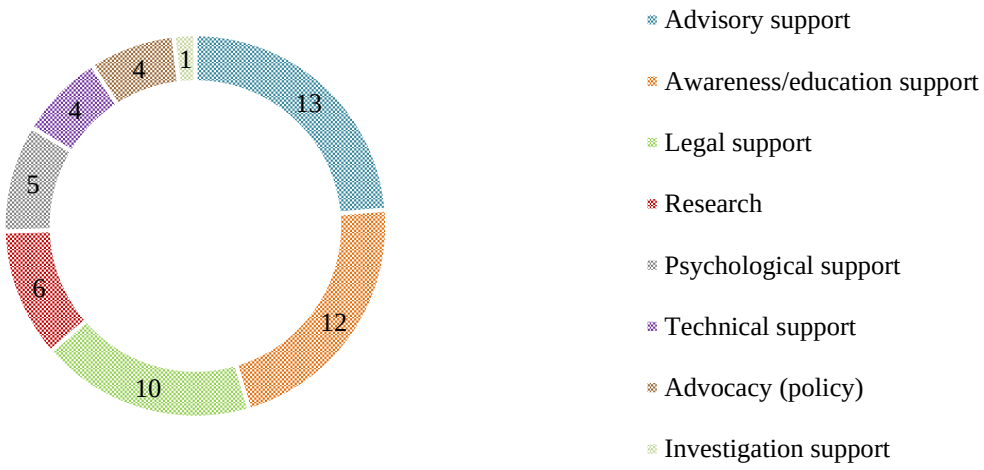

Figure 7 CSOs' types of activity (based on 21 CSOs[40])

From a stakeholder perspective, CSOs have a major role to play in preventing, educating, networking and informing debates. The latter was not emphasised much by the CSOs

[40] The number of CSOs considered may have multiple fields of activity. Therefore, the overall counting is bigger than the number of CSOs.

themselves in the interviews, but this does not mean that the CSOs do not do it at all. The independence that CSOs have is seen as a valuable asset for the dissemination of knowledge.

> *"Civil society can provide an independent view of the issues in policy and law making around cybersecurity and cyber laws and cybercrime and the responses to it […] So I think the roles of civil society is really important, and they should play an important role in building understanding around the harms of cyber." (S-5)*

3.3.2 Considerations on victim assistance

Victim assistance is a theme that came up several times during the interviews. This is due to the fact that almost all the CSOs interviewed are involved in the field of victim assistance. It therefore seemed important to us to dedicate a section to this theme by addressing the recognition of victimisation (direct and indirect) and the treatment of victims.

a) Recognition of the victim (direct victimisation)

Many interviewees raised the issue of the recognition of a victim status at different levels. On the one hand, some people do not see themselves as victims as cybercrime is sometimes perceived as less serious because it occurs in cyberspace and through technological devices. In these situations, victims do not share their experiences and do not report the crimes to the police.

> *"[…] people are kind of thinking it's only digital, so it's not severe enough that I need to get help and I need to find help of course because people are like from the surroundings of victims of digital head if they are not sensible when it comes to the topic they're saying yeah but then just like turn off the laptop or a turn off your phone or whatever, that we are recommending like to everyone please contact us but of course we have limits as well." (CSO-6)*

On the other hand, several interviewees mentioned that victim status is not always recognised by policies and the legal system[41]. In this sense, victims do not feel that they are taken seriously when they report a cybercrime because of the reluctance of some police officers to register the complaint. According to diverse testimonies, victims may sometimes be accused of being careless. Or police officers discourage victims from filing a complaint because of the time and resources that would need to be allocated to the investigation without much guarantee of a resolution.

[41] The recognition of victimisation is the most important need of victims of cybercrime according to a recent study. See Leukfeldt, Notté and Mash, 2020, p. 60.

> *"The other problem is the approach of law enforcement organisations, such as police, that discourage people or especially women, who come there and notify or send a notification to the prosecutor's office that something might have happened, and they've been victims of some kind of a crime, and they are discouraged they hear that generally they should withdraw their notification because it won't be successful, and it will be a long wait, they will not catch the offender – especially if it's cybercrime. And there really are a lot of money that has to be probably spent by the police or the prosecutor's office to investigate it, and the result will not be satisfactory for them, so they're not so willing to proceed this sort of cases, so this is the main problem." (CSO-4)*

b) Recognition of the other victims (indirect victimisation)

Some interviewees also noted the need to redefine the notion of a victim in the sense of broadening the definition. Indeed, others may be impacted by a cybercrime (or a traditional crime) beyond the direct victim[42]. These additional victims can range from the relatives of the direct victim to the police officers who are involved in the triage of child pornography images. According to these interviewees, more considerations and support should be provided to these indirect victims. Referring to the police, one interviewee added that if the people who are supposed to provide help are not supported themselves, they will not be able to help others.

> *"[…] we're developing this training on empathy and effective communication, and it was important point made, which is that it's difficult for police to have empathy with victims when people don't have empathy for their own suffering. So if you have a police service which doesn't look after its own, how can you expect them to look after the community, victims and others? So if you want to have really impactful solutions, you have to think about the human being, so if you're being targeted, and how they work, so I think that may be an important reflection within the cybercrime field as well." (CSO-3)*

c) Specialists in victim support

The last aspect relates to the support of victims and the need to have specialists trained in this area in order to improve the assistance provided. For example, it is important to familiarise the various stakeholders with the victim's perspective. Indeed, these specialists should be involved at every stage of the victim's support, whether in the legal system (i.e., as prosecutors) and with first responders (i.e., as police officers) or through associations.

> *"Because sometimes, from the objective point of view, it's hard to understand why they [the victims] are behaving in a way as they behave, or why they don't leave the offenders, so they are in a relationship still with them. So sometimes for the charges and for the prosecutors, it's totally non-understandable. So this is also our role, to make them familiar with these issues […]." (CSO-4)*

[42] As part of a project on victims of terrorism, a circles of impact schema was developed, identifying various victims: victims present at the attack, family and loved ones, first responders, the local community and the wider population. For more details, see EU Centre of Expertise for Victims of Terrorism, 2021.

The lack of empathy was also mentioned by some interviewees, especially with regard to police officers. In addition, interviewees remarked on the need to take a broader approach to victim support, which should include better assistance to victims in terms of being informed of their rights and being socially and/or psychologically assisted after the victimisation event[43].

Finally, in general, several interviewees agreed that the specialisation of stakeholders could improve the support available for victims, especially on the issues of filing a complaint, safeguarding evidence and following up on information about a case.

3.3.3 Cooperation between civil society organisations and other stakeholders

Cooperation between CSOs and stakeholders was discussed with the majority of interviewees. Although all agreed on the importance of such cooperation in the fight against cybercrime, very different mechanisms were noted. On the one hand, some CSOs have several more or less tight collaborations, including with the police, prosecutors, policymakers, psychologists, schools and universities, and other CSOs. However, on the other hand, some organisations face obstacles and collaborations are difficult to establish.

"Gender-based violence that are seen in platforms that use end-to-end encryption, and they are not allowing for example helpline to have a voice or to have the communication channel for us to alert them of what is happening in their platform and how that affects victims of those types of violence is something that for us, as a victim support organisation, it hinders our support because there are some situations where we cannot do anything in order to prevent that violence." (CSO-7)

Based on distinct testimonies from the interviews, we have identified three criteria:

- *Cross-country variation*: In some countries, CSOs are more recognised than in others, thus facilitating links with various stakeholders. For example, a representative of a CSO with offices in several countries reported that collaboration with the police may be very good in one country and non-existent in another, even though it is still the same CSO.
- *Size of the organisation and national/international network affiliation:* It seems to us that the larger associations, which are also part of a network (such as INHOPE or Safer Internet Children), mentioned more collaborations than the smaller associations. However, we cannot assert a causal link between these two parameters. Nevertheless, several organisations mentioned that being part of a network favours the exchange of information and good practices and increases the possibility of obtaining funding.
- *Type of crime:* Several organisations pointed out that the quality of cooperation can also depend on the type of crime being addressed. A lot of progress and cooperative efforts (e.g., with the police and service providers) were highlighted in relation to child sexual exploitation and terrorism. However, less attention has been paid to other types of behaviour such as cyberbullying.

[43] Referring specifically to children and young people, the importance of psychological and pathological support for direct victims of online crime and those who put themselves at risk on the Internet was also identified in the interviews with the experts under Task 3.1. For more details, see the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", p. 57.

3.3.4 Challenges and improvements

To conclude this section focusing on the activities of CSOs, we highlight some challenges that they encountered in their practice and some areas that could be improved to strengthen the prevention of cybercrime and provide better support for victims and perpetrators. Many of these challenges or improvements are interconnected in some way.

a) Evolution of cybercrime

One of the major challenges in cybercrime that is relevant to all stakeholders is its fast evolution. Cybercriminals adapt quickly to technological advances and new opportunities. One of the interviewees illustrated this problem by talking about fraud:

> *"The first challenge is to stay up to date. It's evolving so fast and then to be able to get the information out as quickly as the perpetrators do with their new type of fraud. It's really about being able to have up-to-date information to make people aware of what kind of scheme they're going to use, what kind of platform they're going to use to reach them and the mechanisms they're going to undertake to execute the fraud." (CSO-24)*

b) Cooperation and information sharing

Although the interviewees reported several collaborations, they are not necessarily formalised and systematic. Accordingly, some interviewees stressed the value of establishing memoranda of understanding. Collaboration with universities should also be favoured as they often share the same objectives. Lastly, some CSO representatives highlighted the non-cooperation of some service providers, which prevents them from offering adequate support in certain situations. On the other hand, some note that as CSOs it is more difficult to access official data. To orient and improve the services offered, it is essential for CSOs to be able to consult data on concrete cases, promoting greater transparency. Thus, the formalisation of certain collaborations would perhaps also facilitate access to data.

c) Cross-border component

Several CSOs mentioned that their scope of action is quickly restricted when the victim is abroad or when there is another international component. Organisations that are not familiar with the foreign legislation or even the culture of a country prefer to refer a victim to an organisation in the foreign country or simply to the police.

d) Legal framework

In terms of legal provisions, although a few interviewees felt that the current legal framework was sufficient, more interviewees indicated an urgent need to harmonise cybercrime laws, first at the European level and then overseas. As an interviewee stated, "it's very difficult to put doors on the sea" (CSO-11). Therefore, alignment on the Council of Europe's (2001) Convention on Cybercrime (also known as the Budapest Convention) would be seen as a first step[44].

[44] By July 2022, 66 States have become Parties to the Budapest Convention (including 21 non-members of the Council of Europe). Status as of July 5, 2022 (Council of Europe – Treaty Office, 2022).

Beyond a harmonisation of the provisions criminalising cybercrime, few comments were made on other aspects of the law. For example, one interviewee referred to data protection legislation. This puts in place measures to protect sensitive data which may nevertheless hinder victim support as CSOs are not recognised as essential services to the population (which is already the case in some countries). On the other hand, from the perspective of one interviewee, a European framework is needed with regard to cyberbullying as this behaviour sometimes lies in a grey area and is therefore not always criminalised.

The last point refers to the inclusion of assistance to victims and perpetrators in the law. Some interviewees noted that both prevention and assistance should be part of the legal framework. From this perspective, not only the direct victim but also people indirectly affected by a crime should be addressed in the law, mirroring the broadening of the definition of a victim as discussed above (Section 3.3.2).

e) Law implementation

Having a legal framework is one thing, but its implementation is another. Indeed, several interviewees noted that some laws or provisions were not always applied. Or even if perpetrators are convicted, they often benefit from a probationary period, having their sanctions suspended. These situations contribute to discouraging victims from filing a complaint because they do not benefit. In addition, in the area of juvenile delinquency, some interviewees encouraged the use of alternative sanctions such as mediation.

> *"So this is something that is a huge problem because a lot of victims are not willing to notify it even because they know somehow, from media and generally they've got knowledge, that even if they notify it and they will be a participant of these proceedings, in the end they will not be awarded because either the offender will not be punished or if he is punished he won't be punished sufficiently. So sometimes they're not so willing, eager to notify it to the police." (CSO-4)*

f) Prevention and support for perpetrators

As the sample in our study illustrates, organisations specialising in prevention and support for perpetrators are rather rare or at least significantly less in number than those for victims. Thus, several interviewees stressed the importance of developing initiatives and support networks for this population as well (as seen in Germany, the UK and the USA).

More specifically for young perpetrators, programmes to promote their skills in a positive way were encouraged. Several programmes have already been implemented in the UK, either targeting all young people (even before they engage in a criminal trajectory) or as a diversion programme (for those who have already committed a crime)[45].

[45] For more details and an example, see CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", pp. 158-159, 161-162.

g) Reaching the audience

The last challenge relates to the difficulty of reaching people to deliver prevention messages. Even if channels are well established, particularly for young people (through schools), the CSOs interviewed still face challenges in capturing the attention of young people on the one hand, as well as parents and non-victimised adults on the other. Indeed, the people who will be receptive are often those who are more sensitive due to previous victimisation. It is therefore important to find new ways to raise awareness in the whole community. For example, one CSO reported that, during a workshop, they asked participants to bring along someone who had never been confronted with the topic being discussed that day.

> *"That is to say, when we send out messages about prevention or the risks of cyber fraud, no one really wants to listen. Finally, the people who are attentive to these messages are already people that we don't need to reach because they will spontaneously look for this information. And the big challenge is to try to reach entire segments of the population with a message that is quite didactic or a message of protection." (CSO-24)*

3.4 Key elements to enhance cybercrime prevention

The prevention of cybercrime was widely discussed in the interviews with CSOs as all of them carry out some kind of prevention work (be it primary, secondary or tertiary prevention). Based on the views of the interviewees, we have identified four central dimensions in the implementation of prevention measures, with a particular focus on young people.

3.4.1 Raising awareness

Knowledge is the most important measure, as stated by a large number of interviewees. Even if more and more awareness-raising campaigns and education programmes are being implemented, more work still needs to be done. Indeed, knowledge is the central element that can either prevent one from becoming a victim or give one the tools to react in the best way possible if one becomes a victim. As a CSO representative mentioned:

> *"[…] to make an effective prevention programme is to raise the awareness and spread about these issues because knowledge gives you the power to deal with these cases." (CSO-26)*

Based on the interviews, such knowledge should cover at least the following three aspects.

a) Definition, manifestations and modi operandi

Interviewees stressed the importance of improving knowledge about the phenomena that constitute cybercrime as "cybercrime" is an umbrella term encompassing a variety of behaviours. Its various manifestations, as well as the differences, need to be explained. For example, it would be worthwhile to address the various types of fraud or the difference between revenge porn and non-consensual image sharing. Furthermore, it is important to inform people about the techniques used by criminals so that individuals are better able to recognise the red flags of a malicious virus, for example.

b) Dangers and penal liability

The second dimension relates to the consequences of cybercrime. As one of the interviewees below pointed out, when referring to a cyberattack, the invisible and intangible nature of cyberspace may prevent people from realising the dangers of the internet.

> *"[…] if you make a parallel with the physical world, when you have conflict, you are more aware of it as you can see movement of troops, you have damages, you have unfortunately people lose their life but in the cyber world is a bit hidden, is a bit intangible and that's a problem that people are not conscious of how dangerous cyberspace can be for themselves or for the beloved ones around them […]." (CSO-10)*

But this observation can also be applied to other forms of cybercrime. Some people, especially young people, are too innocent and do not realise the risks they run when using the internet or connected tools, for example, when joining a WhatsApp group without knowing the people who are located around the world. When we are children, we are often told not to talk to strangers in the street. Therefore, the same advice and prevention measures should be applied in the virtual world: "*you don't have to trust on someone who is just trying to be your friend*" (CSO-11).

Finally, besides the risk of becoming a victim of cybercrime, young people may not realise when they commit a crime themselves. They may perceive their behaviour as a challenge or a joke. The limits, the legal framework and applicable sanctions should therefore be explicitly explained to children and young people.[46]

> *"The problem is that they [young people] have to learn that there is a limit, what is real crime, that they can go to prison, it's not only a 'challenge'. And I think in schools they don't talk about this so much, the personality element, the online grooming […] So the difference between jokes and crime and I think that it's important for them to learn it from the beginning." (CSO-11)*

[46] The challenge and fun dimensions, as well as the lack of awareness of the legal framework, were also reflected in the interviews with experts under Task 3.1 and in the literature. For more details, see the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", pp. 43-46; Aiken, Davidson and Amann, 2016.

c) Coping mechanisms and protection tools

For this last aspect, the interviewees emphasised various points. First of all, it is important to raise awareness of accessible support environments so that victims know where to ask for help if needed. This could be a victim support organisation or a functionality on a platform to report an incident. Indeed, it appears that some young people do not know who to talk to or how to talk about a cybercrime. This leads us to the need to work on resilience and the mental self-defence that a few CSOs referred to. While self-defence courses are provided to protect against physical aggression, mental self-defence work should also be developed in relation to online victimisation[47,48].

The second element refers to technical knowledge and, more specifically, to cybersecurity. Thus, several interviewees discussed how prevention and training should not only focus on cybercrime or digital hygiene but also include cybersecurity concepts.

> *"They have to learn about technical; they need a good cybersecurity training course at school, including programming languages, hacking, what is dangerous from IT and technical standpoint. A training course. I think that it can be not only for the students but also for parents for example." (CSO-11)*

Lastly, several interviewees pointed out the lack of knowledge about evidence gathering. For example, in relation to stalking, one interviewee mentioned that the first reaction is often to block the stalker on the phone or platforms. However, if legal action is taken, only partial evidence will be available. Thus, there should be more communication on how to behave when faced with such a situation in order to avoid mistakes and to facilitate legal proceedings.

Generally, CSOs recommended developing an awareness strategy which should be based on a long-term learning awareness process. For example, one CSO interviewed suggested working on a joint project with students throughout the year. In this way, young people feel involved in the process and become active contributors to prevention.

3.4.2 Adopting a holistic approach

As we know, any of us can become a victim of cybercrime. And, to quote one of the stakeholders, "*I think everyone has a responsibility for cybercrime. I think we have to be a community in this*" (S-1). Indeed, several interviewees highlighted the importance of adopting a holistic approach in the implementation of prevention measures. According to them, the responsibility to prevent cybercrime and educate the population lies with all of us, whether we belong to LEAs, the educational system, families, leisure facilities or service and product providers. To ensure a comprehensive approach, it is therefore recommended to strengthen coordination between the stakeholders and to develop national prevention strategies.

As far as children and young people are concerned, a holistic approach is advised in order to include the whole environment of the child or young person and to strengthen preventive

[47] One of the interviewees went even further, mentioning that this resilience needs to be developed with children to help them overcome all sorts of life traumas, such as the loss of a grandparent.
[48] For example, one of the CSOs interviewed has organised fem-do-trainings which is a martial art that combines physical, verbal, mental and emotional defence techniques.

messages. Thus, according to the opinion of the interviewees, the responsibility does not lie only with teachers and educators but with all those who take care of children, such as parents, grandparents, administrative and supervisory staff in schools, youth leisure centres and so forth. But in order to educate children in the use of new technologies, these people also need to be trained in or at least aware of the technologies. However, according to several interviewees, there is sometimes a generation gap between children and adults, where the adults do not always know how to use new devices or how to properly advise children and may feel overwhelmed by technological advances. In line with this observation, some interviewees reported that they still have difficulty connecting with parents.

Lastly, as it happens for crime prevention in physical environment, it seems that many teenagers do not pay attention to prevention messages and the dangers associated with the internet and new technologies. Thus, several interviewees noted that prevention should start at an early age. Examples were mentioned where digital literacy education starts as early as kindergarten.

> *"[…] at the personal level, especially the younger generation, we were talking with many of them and for me, uh, they're more concerned about their reputation rather than privacy and security so they only say, 'Oh, I don't care but my reputation is everything to me' […] so the different profile on social networks so that […] they have a very shiny, well-rounded profile for their reputation and then they have more like and they don't really care of the security around it […]." (CSO-10)*

3.4.3 Making both entertaining and educational prevention

As mentioned above, it is sometimes difficult to reach out to people who are not sensitive to cybercrime issues. Therefore, more effort has to be put towards finding the right channel and the right message to capture people's attention.

Awareness schooling is an appropriate and easy way to reach children and young people. But doing prevention in schools does not ensure that the message is understood (or listened to) by the students. Thus, many interviewees emphasised that the interventions should be fun while sharing an educational message. For this reason, theoretical lessons with slide projections should be avoided – as they risk losing the attention of young people – in favour of more interactive means. In terms of cyberbullying, one of the interviewees suggests starting by asking children a series of questions to find out their social media habits, and this helps to create a link with the audience. For older children, using a real case or a newspaper article to create a common reflection on the phenomenon is also a method favoured by the interviewee.

> *"So they [the students] would try to put himself/herself in the victim's shoes, in the perpetrator's shoes. Or, for example, you could also ask, I don't know, a newspaper article made in this way, in your opinion was written, let's say 'correctly'? That is, in your opinion […] what message is getting through this newspaper article, for instance?" (CSO-25)*

Another way of getting young people's attention is through peer education. For example, the representatives of two CSOs highlighted the advantage of having young people or young adults (around 20–23 years old) involved in these interventions in order to establish a close

relationship with the students[49]. Involving a young moderator also helps the CSOs to be more aware of trends in the use of social media and new technologies while illustrating cybercrime with concrete and current examples.

For adults, awareness raising is mainly done through workshops (addressed to the public or for a specific occupational group) or information events for parents, for example. For older people, the interviewees suggested workshops or interventions in places of leisure, such as community centres or associations (e.g., a music association).

The approaches presented so far are methods that can be considered classical. This raises the question of whether prevention methods should not also adapt to the evolution of communication channels and the use of new technologies. Various organisations have set up websites to provide information on prevention and counselling, as well as spaces for discussion (e.g., forums or chat boxes). However, what is the place of internet platforms (such as social media, gaming and search engines) in the field of prevention? In this regard, one CSO representative raised the scope of audio-visual content consumption, mentioning, for example, YouTube channels that publish videos on cyber fraud prevention and are viewed millions of times. It is therefore legitimate to question the scope of such a video compared to more traditional awareness campaigns[50]. Reflecting on the possibilities offered by new communication channels to reinforce the prevention of cybercrime would be relevant.

"So what it brings to my mind is, can we turn the message [...] into entertainment and make it both a distraction and also a learning opportunity for people that it was better to protect them. Because if it's just learning, in my opinion, it won't be enough. In the same way that fraudsters use Instagram and TikTok to reach their target, I think we also need to think about how to make the messages much more attractive." (CSO-24c)

3.4.4 Conducting evaluations of prevention programmes

Finally, we emphasise the lack of evidence-based programmes on crime prevention, especially with regard to cybercrime[51]. Although this observation was only explicitly made by three interviewees (1 CSO and 2 stakeholders from academia), we feel it is important to mention it to conclude this section on crime prevention. In fact, none of the interviewees reported that they had carried out an evaluation of their prevention measures. However, even if initiatives seem to work, it is essential to conduct evaluations (intermediate or final) in order to check on the measures and improve their effectiveness if necessary.

[49] It also emerged from the expert interviews under Task 3.1 that peer mentoring programmes are beneficial for developing "responsible computer skills for legal purposes". For more details, see the CC-DRIVER deliverable 3.1 titled "Report on drivers of cyber juvenile delinquency", pp. 50-51.
[50] Within a Swiss study on the protection of minors from cyber sexual offences, the experts interviewed emphasised that prevention should be implemented where young people are, which means including social networks and online gaming platforms (Caneppele, Burkhardt, da Silva, Jaccoud, Muhly and Ribeiro, 2022).
[51] For more details, see Brewer, de Vel-Palumbo, Hutchings, Holt, Goldsmith and Maimon, 2019.

3.5 Views on EU research projects

This last section takes a rather different perspective by addressing the secondary objective of the activity. The aim was to collect the opinions of the interviewees on research funded by the EC, with a particular focus on possible ethical issues.

The first observation is that very few interviewees expressed themselves on the subject (3 CSOs and 4 stakeholders) due to a lack of experience in the field. Indeed, the people interviewed in the study are not involved in research much, and even less so at the European level. However, we have drawn some interesting considerations that could guide European research procedures and all research projects.

The issues identified by the interviewees are rather disparate and were often mentioned by only one person. These considerations have been grouped into six areas ranging from project planning to the implementation of the results.

- *Amount of management duties*: This observation concerns the allocation of time to project management. In the context of EU-funded projects, the management aspect should not absorb too much time. Nevertheless, one interviewee emphasised that management or communication – between internal and external partners – is an integral part of a project conducted on a European scale and should be taken into account in one way or another.

> *"[…] actually, realistically then don't call it project management but internal communications need a lot of time and is often not, you know, considered something […], but you need a lot of communication time I think." (CSO-2)*

- *Content of projects*: Two considerations were made in relation to the content of projects. While the former refers to the themes investigated, the latter deals with the geographical scope. From an overall perspective, one CSO representative noted that the perspectives of victims and victim support are not sufficiently reflected in the projects, which rather take a more police-oriented approach on how to improve LEAs' work. This observation is in line with several elements mentioned in this report stating that victim support needs to be strengthened in various respects. Also, this echoes the reflection shared by one stakeholder on the allocation of funds, questioning whether certain themes will be given more prominence by the funding institution.

> *"I suppose when funding is linked to a supranational entity like the European Union. I think a lot of the ethical issues, or the limitations if you like, might come from when the funding is allocated itself, is the EU going to fund research always in every case that is potentially critical of its standpoint or not, research that's going to say things that the EU wants to hear issues of that nature may arise at the sort of funding stage and afterwards I don't […]." (S-5)*

The second comment, from a stakeholder, relates specifically to projects on cybercrime, which should take a broader perspective than those at the European level.

> *"In total, half of internet users are based in Asia. The nature of much cybercrime is that it transcends traditional borders and jurisdictions, and so it's important to include perspectives that go beyond the global north in understanding the nature of these problems and in coordinating responses in a productive way." (S-5)*

- *Ethical issue*: According to the interviewees, in general, the Commission's requirements are sufficient to prevent ethical issues. However, this depends mainly on the topic being studied. From this perspective, based on current technological advances, one of the interviewees pointed out that ethical problems may arise in connection with projects using artificial intelligence procedures in the coming years. Secondly, another issue raised is the various consent forms that are required in some data collection procedures (e.g., interviews, questionnaires, etc.). While two interviewees mentioned the administrative burden of this process, suggesting that these forms are not necessary when no sensitive data is exchanged, another interviewee highlighted the problem of storing these documents with signatures and names. This raises questions not only about the protection of signatures but also about the strength of the anonymisation process.
- *Outcome of deliverables*: Another observation relates to the outcomes of the projects. One of the interviewees mentioned that sometimes the quality of some deliverables do not meet the expected standards. To address this issue, the interviewee suggested having "some assessment post-delivery on how viable is the output and if there's some lesson learnt and that can be true for other calls" (CSO-10).
- *Dissemination*: One stakeholder noted the difficulty in finding reports for some projects. Several projects have created dedicated websites to disseminate information on project progress and make various publications, including deliverables, available. However, it is acknowledged that deliverables are not immediately available pending Commission approval or for other relevant reasons.
- *Use of results*: The use of the results was also discussed by some interviewees in the sense that the knowledge produced is not exploited, the results are not implemented in practice. Indeed, it appears that it is sometimes difficult to see how scientific knowledge can be integrated into practice.

> *"They [the projects] go to the shelf, and everybody forgets what's done etc. because our projects are mainly too small in order to be effective in a society point of view. So we have like small projects everywhere, but what is the nice blue line to follow? That is a little bit unclear for the R&D point of view." (S-4)*

4. Conclusion

This contribution presented various perspectives of CSOs and other stakeholders on cybercrime in Europe. The focus was on the evolution and different manifestations of the phenomenon, as well as on the responses to it in terms of prevention and victim support.

The most recurrent consideration that emerged from CSOs and other stakeholders concerns the relevance of knowledge and awareness-raising against cybercrime. The pervasiveness of the internet and connected tools in our daily lives calls for making all citizens conscious of both the benefits and risks of cyberspace. Whether it is to avoid becoming a victim or perpetrator of cybercrime, or to know how to respond to or intervene in victimisation, knowledge is

considered the most valuable tool. Thus, more effort is needed to increase awareness and knowledge about the various forms of cybercrime to be able to recognise them, about coping strategies and about criminal consequences. The last consideration is very important, especially among young people, as the intangibility and "anonymity" of cyberspace can blur the boundaries between lawful and harmful online behaviours. As a result, concerns were raised over the risk of depersonalisation and trivialisation of cybercrime, particularly among young generations.

Moreover, it is essential to find the right channels and the right message to capture people's attention. In this sense, entertaining and educational messages should not only be disseminated through what might be considered to be the more traditional channels (e.g., through awareness campaigns and awareness schooling) but also benefit from utilising various internet platforms (such as social media, gaming and search engines).

The second point that was discussed in this report is support for cybercrime victims. While cybercrime is often associated with fraud and financial consequences, the social and psychological impacts on victims of cybercrime remain underestimated. However, it would seem that the socio-psychological impacts are more important to victims than the financial impacts. In addition, although the needs of cyber victims are similar to those of victims of traditional crime, recognition of victim status is not always present, suggesting a lack of knowledge or specialised staff to assist victims of cybercrime. We also observed that although various systems have been implemented, some are not yet ready for a cross-border phenomenon such as cybercrime and to deal with its long-term impacts. Victim support should be more thoroughly developed and given more consideration in criminal policies.

The third point is the cooperation and the coordination between stakeholders. A multitude of stakeholders are active in the field of cybercrime prevention or repression. Collaborations are gradually emerging, but synergies are still weak. Through this report, we identified several challenges for CSOs that could perhaps be remedied with the establishment of more systematic and formalised cooperation between various actors. Indeed, the extent of the cybercrime phenomenon and its cross-border dimension mean that each stakeholder cannot find a solution individually and that partnerships must be developed, and action taken together.

The last point refers to European research projects. It was noted that multiple projects have been funded and implemented, but there is a lack of capacity to reach the right audience based on the results. It would therefore be relevant to reflect on how to improve the mechanisms for disseminating any findings so that they can be used in the development of public policy and impact society.

In conclusion, the report has provided a broad overview of perceptions from CSOs and other stakeholders. Further efforts should address the methodology used to determine the socio-psychological impacts of cybercrime and how to respond to them. Moreover, future research should focus on new prevention strategies that fall in line with technological developments and consumption habits and on how to prevent the normalisation of cybercrime. Lastly, more effort should be put toward enhancing the evaluation process for prevention programmes.

References

Aebi, Marcelo F., Stefano Caneppele and Lorena Molnar, *Measuring Cybercrime in Europe: The Role of Crime Statistics and Victimisation Surveys - Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union*, Eleven, The Hague (Netherlands), 2022.

Aiken, Mary, Julia Davidson and Philipp Amann, *Youth Pathways into Cybercrime*, London, Paladin Capital Group, 2016.
https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf

Associação Portuguesa de Apoio à Vítima APAV, *Training Manual: Specialised Support to Victims of Cybercrime*, 2021.
https://apav.pt/publiproj/images/publicacoes/Training_Manual_EN.pdf

Brewer, Russel, Melissa de Vel-Palumbo, Alice Hutchings, Thomas Holt, Andrew Goldsmith and David Maimon, *Cybercrime prevention: Theory and applications*, Springer, Cham (Switzerland), 2019.

Buil-Gil, David and Yongyu Zeng, "Meeting you was a fake: investigating the increase in romance fraud during COVID-19", *Journal of Financial Crime*, Vol. 29, Issue 2, March 2021, pp. 460-475. https://doi.org/10.1108/JFC-02-2021-0042

Caneppele, Stefano, Christine Burkhardt, Amandine da Silva, Lachlan Jaccoud, Fabian Muhly and Sandra Ribeiro, *Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels*, Université de Lausanne, 2022.

Chesney, Robert, and Danielle Keats Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security", *California Law Review*, Vol. 107, 2019, pp.1753-1820. https://doi.org/10.15779/Z38RV0D15J

Council of Europe, Convention on Cybercrime, ETS 185, Budapest, 23.11.2001.
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe - Treaty Office. Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime Status as of 5/7/2022. 2022
https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

EU Centre of Expertise for Victims of Terrorism. Annex to EU Handbook on Victims of Terrorism, January 2021.
https://ec.europa.eu/info/sites/default/files/law/annex_to_eu_handbook_on_victims_of_terrorism_2021_01_15_en.pdf

da Silva, Amandine, Christine Burkhardt and Stefano Caneppele, "Challenges in Measurement of cybercrime", 2022.
https://www.ccdriver-h2020.com/_files/ugd/0ef83d_5612d75012b64b6e993c0fd9368ed36b.pdf

Gercke, Marco, *Understanding cybercrime: Phenomena, challenges and legal response*, ITU Telecommunication Development Sector, 2012.
http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Leukfeldt, Eric. R., Raoul Notté and Marijke Malsch, "Exploring the Needs of Victims of Cyber-dependent and Cyber-enables Crimes", *Victims & Offenders*, Vol. 15, Issue 1, 2020, pp. 60-77.
https://www.tandfonline.com/doi/pdf/10.1080/15564886.2019.1672229?needAccess=true

Paillé, Pierre, and Alex Mucchielli, *L'analyse qualitative en sciences humaines et sociales*, Armand Colin, Paris (France), 2013, pp. 231-313.

Phillips, Kirsty., Julia C. Davidson, Ruby Farr, Christine Burkhardt, Stefano Caneppele and Mary P. Aiken, "Conceptualising Cybercrime: Definitions, Typologies and Taxonomies", *Forensic Sciences*, Vol. 2, Issue 2, April 2022, pp. 379-398.
https://www.mdpi.com/2673-6756/2/2/28/html

Ramos, Elsa, *L'entretien compréhensif en sociologie*, Armand Colin, 2015, pp. 45-111.

Reep-van den Bergh, Carin M. M., and Marianne Junger, "Victims of cybercrime in Europe: a review of victim surveys", *Crime science*, Vol. 7, No. 5, 2018.
https://doi.org/10.1186/s40163-018-0079-3

Scamwatch. *Scam statistics, Dating & Romance*. 2022, 26 July.
https://www.scamwatch.gov.au/scam-statistics?scamid=13&date=2022

Suler, John, "The online disinhibition effect", *Cyberpsychology & behavior*, Vol. 7, Issue 3, June 2004, pp. 321-326. https://doi.org/10.1089/1094931041291295

Udris, Reinis, "Cyberbullying among high school students in Japan: Development and validation of the Online Disinhibition Scale", *Computers in Human Behavior*, Vol. 41, December 2014, pp. 253-261. https://doi.org/10.1016/j.chb.2014.09.036

Whitty, Monica T., "Do you love me? Psychological characteristics of romance scam victims", *Cyberpsychology, behavior, and social networking*, Vo. 21, Issue 2, February 2018, pp. 105-109. https://doi.org/10.1089/cyber.2016.0729

Annex

Annexe 1 Interview schedule used with civil society organisation representatives

Preliminary remarks

The interview schedule is split into six parts (A to F):

- *General questions* (Part A)
- The *cybercrime phenomenon*, including current and future trends, obstacles and challenges, social/political/economic impacts, etc. (Part B)
- *Cybercrime prevention*, including the role of CSOs/LEAs/companies, the effectiveness and gaps of prevention programme, etc. (Part C)
- *Cybercrime investigation*, including the role of CSOs, cooperation with LEA, etc. (Part D)
- The *dissemination of EC funded research projects*, including dissemination mechanism, ethical issues, confidence in EU organisation, etc. (Part E)
- *Conclusion* (Part F)

Parts A, B and F must be included in all interviews. Then, you have to choose another part – between parts C to E – depending on the profile of the CSO.

For each part, the interviewer should be flexible in the discussion: he/she may choose the most appropriate questions, according to the context and the person interviewed.

Introductory text (example)

"Thank you for taking the time to be interviewed today. The interview will last for about one hour. First, let me introduce myself, I am [*name*], a [*title*] at [*institution*], and we are conducting these interviews to get the views of key stakeholders on cybercriminality in the EU. Just a reminder that this interview is being recorded, and as we are now starting, we will start the recording now. Some housekeeping - these interviews will be anonymous and confidential so please refrain from disclosing any personal and confidential information and please refrain from disclosing any information that is sensitive in nature. Within this interview, we are going to ask for your opinions on cybercrime phenomenon and [*name the interview parts you have chosen to include*]. You will also be given the opportunity to add any information at the end of the interview. If you do not have any questions, we are going to begin with a few brief questions about yourself and your experience".

A. Introduction – General questions

1. Please name your position and responsibilities within the CSO
2. Tell me about your educational background?
3. Approximately how many years have you worked in this field and in this CSO?
4. Could you please describe the main activity of your CSO?
5. What kind of stakeholders/actors does the CSO cooperate with in its current work?
6. Is there any cooperation between the CSO and LEAs? Please give us an example.
7. How does the CSO deal with cybercrime? What objectives and interests are being pursued?
8. Have you ever been involved in research work in cybercrime? Please give us an example.
9. Has the CSO ever implemented programmes regarding cybercrime? Please give us an example.
10. Has the CSO ever participated in international or national cybercrime prevention programmes? Please give us an example.

B. Perception of cybercrime phenomenon

1. In the last 3 years, according to your opinion, what are the most recurrent manifestations of cybercrime?
2. In your opinion, how will cybercrime evolve in the coming months?
3. What sources of information do you use in your current work?
4. Is the CSO's field of activity affected by cybercrime? If yes, please explain how this threat has evolved in the last 3 years.
5. Are you familiar with the concept of cybercrime as a service? Please explain how your CSO is using this concept in its current work.
6. How is the CSO's field of activity impacted by cybercrime as a service?
7. Does the CSO deal with youth engagement in cybercrime? If yes, could you please describe how?
8. In your opinion, what are the main pressing issues your CSO is currently facing regarding cybercrime?
9. In your opinion, what are the main challenges related to cybercrime that your CSO will have to overcome in the future?
10. From your point of view, which type of cybercrime has the most serious impact on individual victims, from a psychological and economic perspective? Please explain your choice.
11. From your point of view, which type of cybercrime has the most serious impact on companies? Please explain your choice.

12. From your point of view, what is the actual risk that European governments stability and democratic system may be threatened by cybercrime attacks? Please give us an example if possible.

C. The role of CSO in cybercrime prevention

1. According to your experience, what is the role of CSOs in preventing cybercrime? Please indicate what the society should expect and what it should not expect.
2. In your opinion, what are the key elements of an effective prevention programme? Please provide examples and explain us why you considered the initiatives successful.
3. What type of prevention projects is CSO supporting and would support in the future?
4. Is there any cooperation between CSO and companies regarding cybercrime prevention? If yes, please describe the scope of this collaboration, and its strong and weak points.
5. Is there any cooperation between CSO and LEAs regarding cybercrime prevention? If yes, please describe the scope of this collaboration, and its strong and weak points.
6. Are there any other problems and gaps regarding cybercrime prevention programmes? (ethical, security, regulation issues)
7. What legal changes would enable CSOs to participate better in cybercrime prevention activities?

D. Cybercrime Investigation – CSOs' role regarding cybercrime and cybersecurity matters

1. According to your experience, what is the role of CSOs in reporting cybercrime and cybersecurity issues to LEAs?
2. How does the cooperation work with LEAs? If any, please describe the cooperation models implemented, and its strong and weak points.
3. According to your experience, what is the role of CSOs in monitoring cybercrime and cybersecurity situation?
4. What legal changes would enable CSOs to support better in cybercrime investigation activities?

E. Dissemination of Horizon/EC funded research projects and use of the results of such projects

1. Has your CSO participated in any Horizon or EC funded research projects? Please give us an example.
2. Do you use Horizon/EC funded project results in your current work? Please give us an example.
3. [*if the interviewee answered "yes" to the first question of this Part E*] According to you, what are the main ethical issues in research projects funded by Horizon/EC?

4. [*if the interviewee answered "yes" to the first question of this Part E*] In your opinion and concerning the ethical issues in research project, what improvements could be made in the future that could increase confidence in EU organisations?

F. Conclusion

1. Is there anything you would like to add on the topic?
2. Do you know any other CSOs involved in the fight against cybercrime that we could also interview?

Conclusion text (example)

Thank you again for taking the time to take part in this study. Your response will go towards academic reports or publications – findings will be reported in aggregate with occasional use of verbatim excerpts (pseudonyms will of course be used to maintain confidentiality and anonymity). We are going to turn off the audio recording - the interview is now concluded.

Annexe 2 Interview schedule used with Stakeholder board members

Preliminary remarks

The interview schedule is split into five parts (A to E):

- *General questions* (Part A)
- The *cybercrime phenomenon*, including current and future trends (Part B)
- *CSOs' role regarding cybercrime and cybersecurity matters*, including challenges and limitations of CSO involvement in crime prevention, cooperation with LEAs, etc. (Part C)
- The *dissemination of EC funded research projects*, including ethical issues, confidence in EU organisation, etc. (Part D)
- *Conclusion* (Part E)

For each part, the interviewer should be flexible in the discussion: he/she may choose the most appropriate questions, according to the context and the person interviewed.

Introductory text (example)

"Thank you for taking the time to be interviewed today. The interview will last for about 30 minutes. First, let me introduce myself, I am [*name*], a [*title*] at [*institution*], and we are conducting these interviews to get the views of key stakeholders on cybercriminality in the EU. Just a reminder that this interview is being recorded, and as we are now starting, we will start the recording now. Some housekeeping - these interviews will be anonymous and confidential so please refrain from disclosing any personal and confidential information and please refrain from disclosing any information that is sensitive in nature. Within this interview, we are going to ask for your opinions on cybercrime phenomenon. You will also be given the opportunity to add any information at the end of the interview. If you do not have any questions, we are going to begin with a few brief questions about yourself and your experience".

A. Introduction – General questions

1. Please name your position and responsibilities within [*name the organisation*]
2. Approximately how many years have you worked in this field and in this organisation?

B. Perception of cybercrime phenomenon

1. In the last 3 years, according to your opinion, what are the most recurrent manifestations of cybercrime?
2. In your opinion, how will cybercrime evolve in the coming months?

C. CSOs' role regarding cybercrime and cybersecurity matters

1. In your opinion, what is the role of CSOs in preventing cybercrime?
2. In your opinion, what are the main challenges and limitations of CSO involvement in crime prevention? (ethical, security, regulation issues)
3. In your opinion, what legal changes would enable CSOs to participate better in cybercrime prevention activities?
4. In your opinion, what is the role of CSOs in reporting cybercrime and cybersecurity issues to LEAs?
5. In your opinion, what is the role of CSOs in monitoring cybercrime and cybersecurity situation?
6. In your opinion, what legal changes would enable CSOs to support better in cybercrime investigation activities?

D. Dissemination of Horizon/EC funded research projects and use of the results of such projects

1. Do you use Horizon/EC funded project results in your current work? Please give us an example.
2. According to you, what are the main ethical issues in research projects funded by Horizon/EC?
3. In your opinion and concerning the ethical issues in research project, what improvements could be made in the future that could increase confidence in EU organisations?

E. Conclusion

1. Is there anything you would like to add on the topic?
2. Do you know any CSOs involved in cybercrime prevention or cybercrime monitoring that we could interview?

Conclusion text (example)

Thank you again for taking the time to take part in this study. Your response will go towards academic reports or publications – findings will be reported in aggregate with occasional use of verbatim excerpts (pseudonyms will of course be used to maintain confidentiality and anonymity). We are going to turn off the audio recording - the interview is now concluded.

Annexe 3 Information sheet and consent form

CC-DRIVER

Information Sheet and Consent Form

The purpose of this Participant Information Sheet and Consent Form is to provide you with the information that you need to consider in deciding whether to participate in this research project.

1. WHAT IS CC-DRIVER?

The CC-DRIVER research project is a €5 million, three-year Horizon2020 project examining the drivers of cybercriminality in the EU, with a special focus on the factors that lead young people to cybercrime. CC-DRIVER is aimed at these key goals:

1. Study cybercrime-as-a-service and develop cybercrime investigation tools for LEAs.
2. Understand drivers of new forms of cybercriminality.
3. Create an online questionnaire to assess the vulnerability of young people to cybercrime.
4. Support the harmonisation of cybercrime legislation across EU states by developing policy toolkits.
5. Maintain European societal values and fundamental rights.

2. WHAT IS THE COMPOSITION OF THE PROJECT CONSORTIUM?

The consortium consists of 13 partners, including law enforcement agencies (LEAs), SMEs, industrial high-tech companies and academic institutes. The consortium brings together experts with complementary skills, including leaders in key technology areas impacting the fight on cybercrime.

3. THE RESEARCH ACTIVITY

If you choose to participate in this research activity, you will be asked to participate in a one-to-one interview that will be conducted online (via Microsoft Teams). During the interview you will be asked about a few different topics. To give an example of the type of content; you may be asked your opinions about cybercrime trends, cybercrime prevention programme, cybercrime investigation or dissemination of EC funded research project. There are no foreseen risks or adverse experiences anticipated as a result of this study.

4. WHAT ARE THE CONFIDENTIALITY/DATA PROTECTION RULES IMPLEMENTED BY CC-DRIVER?

All data processing performed by CC-DRIVER partners will be in conformity with the H2020 rules on the processing of personal data and with the EU General Data Protection Regulation 2016/679.

The interview will be recorded, transcribed and anonymised. Information that could identify participants will be removed from the transcript prior to being analysed by CC-DRIVER partners. CC-DRIVER partners will securely store the audio files on password protected devices. Audio files will be permanently destroyed once the transcript is completed and validated. The signed information sheet and consent form will be securely stored on password protected devices and will be destroyed when they are no longer needed, or five years after the end of the project.

No personal data will be shared beyond the CC-DRIVER consortium without your consent. The results of this project may be disseminated, in form of a; peer reviewed journal, internal report, presentation to participants and/or relevant community groups, and as a books and/or book chapter. Data and findings will be reported as a group, in a summary form, that may include excerpts or case studies, however the utmost care will be taken to ensure that data is appropriately anonymised and de-identified, to ensure confidentiality.

5. WHAT PERSONAL DATA WILL BE COLLECTED FROM YOU?

In this research activity, we will only process your personal data where you consent. You can remove your consent at any time.

- A recording of your interview. This is collected so that we can record your views for later analysis. The recording will be permanently destroyed once the transcript is completed and validated.
- Your e-mail address. This is collected so we can contact you.
- Your name, if you provide it, will be used to enable you to exercise your rights regarding your personal data. It will be recorded on your informed consent form.

- Your signature. This is collected to confirm that you understand the meaning of giving your consent to participate in the research activity. It will be recorded on your informed consent form.
- Your rank/position, organisation, and the country of your organisation will, if you consent, be processed so that they can be included in research work for the European Commission and for scientific publications.

These data will be archived and destroyed when they are no longer needed, or five years after the end of the project (whichever is sooner).

6. WHAT ARE YOUR RIGHTS AS A DATA SUBJECT?

In accordance with principles of research ethics and the EU data protection framework, you have rights regarding how your personal data is processed. Here are your rights and how we can fulfil them:

- Rights to access personal data processed about you, and the right for these data to be in a portable form – If you request access to personal data that we hold about you, we will provide you with these data in an easily accessible format.
- Right to rectify personal data held about you – If you think the personal data that we hold about you is inaccurate or incomplete, you can correct or complete it.
- Right to restrict the processing of your personal data – If you want to restrict the way we process your personal data, you can request that we do so.
- Right to request your personal data is erased – If you want us to delete your personal data from our systems, you can request that we do so.
- Right to confidentiality and anonymity – Due to the nature of this study, an interview-based study, participation and information cannot be anonymised at source. However, your responses will be anonymised, deidentified and will be reported as part of an anonymised sample. We will ensure that interview transcripts do not contain any names or identifying information, it will either be removed or replaced with pseudonyms. Publications arising from this research will contain anonymised data only.
- Right to leave the research activity – Your participation in this research is voluntary. If you wish to withdraw from participating in this research activity, you can do so at any time without negative consequences and your personal data will not be processed.

If requests to exercise these rights are excessive, malicious, impossible to fulfil, or require a disproportionate effort, we may reject some requests in accordance with data protection legislation.

7. CONSENT FORM

By ticking the consent boxes below, I acknowledge that I will participate in these activities voluntarily. I understand that my participation will involve providing my views on cybercrime orally and these will be recorded and collected by researchers.

I understand the following:

- I have read the information explaining the project and understand how this research activity will collect and process my views and my personal data if I choose to provide it.
- I will be asked to provide professional or personal views on cybercrime phenomenon, cybercrime prevention programme, cybercrime investigation and dissemination of EC funded research projects.
- I have the right to ask questions about my participation and receive clear answers before making any decision.
- I understand that I should only share the information that I am legally allowed to share, and that I should not disclose any confidential information which I do not have the right to disclose.
- My participation is voluntary, and I may refuse to answer any questions I do not wish to discuss. I am free to end my participation at any time with no negative consequences.
- My responses to this interview are recorded and the audio file will be kept on a password protected device. The audio file will be permanently destroyed once the transcript is complete and validated.
- Where my personal data is processed digitally, this will be on device that are password-protected. The record of personal data will be destroyed when they are no longer needed, and in any case five years after the end of the project (whichever is sooner).
- My personal data will not be transferred to third parties.
- If the information I provide is used for the writing of a piece of work to be delivered to the European Commission, or scientific research paper, the consortium will remove my name from that information so that my identity and views remain confidential (unless attribution is required and I have consented to it).
- I have been made aware of my rights regarding my personal data and how to exercise them.
- I have been given the contact details of the research team and I have been informed that I am free to contact them with any queries about the research or the project:
    - For more information on the CC-DRIVER project, you should contact David Wright, CC-DRIVER Project Coordinator, david.wright@trilateralresearch.com
    - For more information on this research activity, you should contact Professor Stefano Caneppele, University of Lausanne, stefano.caneppele@unil.ch
    - For more information on the processing of your personal data, you should contact Pablo Diaz Venegas, University of Lausanne, PabloAndres.DiazVenegas@unil.ch

I f you agree to participate in this study, please tick the two boxes

My participation is voluntary. I have not been pressured or coerced in any way to provide answers to this interview.

I agree that my responses to this interview can be used by the CC-DRIVER Consortium for their work in the project, and my responses can be used for scientific research papers.

Please tick the appropriate box
As a participant to the study:

I agree to be identified by name, position and affiliation in the research.

I do not wish to be identified by name, but I can be cited anonymously by position.

I do not wish to be identified by name, but I can be cited anonymously by affiliation.

I do not wish for my name, position, and affiliation to be identified.

Full Name:
Affiliation (organisation):
Signature:
Date:
Email (only provide this if you consent to being contacted to follow up on your answers to this interview):
Position/rank in your organisation (only provide this if you consent to its being included in work submitted to the European Commission and scientific research papers):