AviaTor

Save Time, Save Lives

Annual Report **2022**

AVIATOR PROJECT. COM

COLOPHON

AviaTor

AviaTor Annual Report
INHOPE (Co-office)
Bos- en Lommerplein 280

1055 RW Amsterdam
The Netherlands
aviatorproject.com

DEAR READERS,

The fact that you are reading the second AviaTor annual report must mean that you have a more than average concern about the topic of online child sexual abuse and exploitation.

Children are at the core of our hearts and minds when we work on this topic on a day-to-day basis. The online world poses challenges for them, and it is up to us to make sure children are safe and protected from danger. Knowing what these challenges are and preventing risks for children is of the utmost importance in all our actions and policy.

2022 was another year of increased numbers of referrals worldwide, more sharing of (more severe) child abuse images amongst perpetrators and ever-growing demand for extra efforts from law enforcement and prosecution to arrest these offenders and abusers, take down websites, fora and boards where these images are shared, and to prevent them coming back again. We have seen an increase from 36.000 referrals in 2021 to 56.000 in 2022 in the Netherlands. A large number of these referrals contain so called “viral material” and may not pose a direct hands-on threat to children, but they do contribute to the negative effects the spread of images can have on victims. As much as possible should be taken offline to protect victims and make the internet a safer place.

With AviaTor, we are trying to become more efficient and take away a lot of the manual labour involved in handling referrals. We urge those member states that are currently working on these cases to examine their processes and see how much time is used up having to process known images time and time again. This is where AviaTor may be of assistance. It can save time and prevent your staff from being “over-exposed” to these images.

The need to step up our efforts Europe-wide is underpinned by the proposed EU legislation now under construction. We need a European resilience that not only fights abuse, but also prevents it from happening. Law enforcement and prosecution have to be strengthened to live up to the expectations European citizens have, and that will come with these proposals. Legislation can and will only work when we are able to hold those breaking the rules responsible and arrest and prosecute those abusing our children, on- and offline.

Don’t let legislation aimed at technology and its challenges take our focus away from the fact that it is people, not technology, that abuse children. The danger of hands-on sexual abuse is most often behind closed doors, in families and with relatives and with people the child knows. “Stranger danger” is an understandable and tempting message but must be balanced with the right prevention messages and attention to other types of danger.

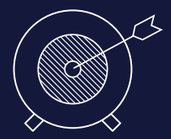
The Dutch Police are the lead on the AviaTor project. Together with the Belgian Federal Police and a consortium of partners, we have the privilege of incorporating our wishes and requirements into the project as much as possible, resulting in an almost tailor-made product. Wherever you may wish to participate in the project, or just use the ideas that were implemented, please contact the project management team.

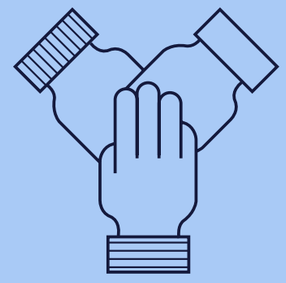
It is good to see so many countries are interested in participating in this unique project. Because only together will we be able to make a difference!

Ben van Mierlo

National coordinator for the fight against
Child Abuse Images and Transnational Child
Sex Offences Netherlands Police

Contents





CHAPTER 01

Before We Start

The value of AviaTor in the fight against CSAM and the purpose of this report.

BEFORE WE START

Introduction

AviaTor supports law enforcement agencies (LEAs) in their fight against online child sexual abuse and exploitation material (CSAM/CSEM) with innovative technological solutions, and a community of dedicated law enforcement officers and key specialists from different sectors.

The rapidly expanding amount of CSAM online is a vigorous problem at a global scale. The increasing mobile connectivity of people worldwide and constantly evolving technology have facilitated the significant rise of CSAM and grooming activities online within the past decade. Experts alert that not only is the volume of this material growing, but there is also an increase in the severity and level of violence against children.

Due to the nature and complexity of this crime, an international multistakeholder response is necessary. This response can only be efficient if proper tools and the newest technology, such as artificial intelligence (AI) and open-source intelligence (OSINT), is used. In order to effectively find and prosecute perpetrators who are using advanced technology to commit their crimes, law enforcement needs to have access to similar innovative tools. Without access to these resources, law enforcement faces a significant disadvantage in their efforts to identify, track and prosecute these criminals and save victims.

With this in mind, AviaTor has been designed to support law enforcement in the fight against child sexual abuse online. AviaTor offers a range of features that help in dealing with reports of CSAM more efficiently. Firstly, it provides automation and intelligence tools that help prioritise, assess, and process these reports. These tools assist in streamlining the initial investigative phase. Secondly, AviaTor integrates AI-assisted categorisation and automated online research using OSINT to support the pre-investigation process.

AviaTor also creates a supportive community consisting of law enforcement officers and experts who specialise in this area. This community serves as a platform for sharing best practices and exchanging valuable know-how and expertise. By fostering collaboration and knowledge-sharing, AviaTor strengthens the collective efforts in combating CSAM and promoting effective approaches within law enforcement.

This is the second AviaTor annual report out of a total of three reports published between 2022-2024. The overall goal of the annual reports is to provide the public and relevant stakeholders with insight into the project's developments. The primary focus of this report revolves around the statistics and practical use of AviaTor. In this report the readers will gain insights into the first released statistics based on the data retrieved from AviaTor users and learn about the recent CSAM modus operandi, as well as reporting trends based on the information given by law enforcement officers from Belgium, Greece, and Moldova.

As the newly proposed European Union (EU) Regulation laying down rules to prevent and combat child sexual abuse has raised numerous questions on its potential impact on the work of EU national law enforcement agencies, the European Commission has provided an exclusive interview about the Regulation and how it will influence the work of EU-based law enforcement agencies and AviaTor. This report provides a multi-perspective overview of the fight against CSAM covering statistical, technical, legal, and law enforcement.

GOOD TO KNOW

Acronyms & Abbreviations

- **AI** - Artificial Intelligence
- **API** - Application Programming Interface
- **AVIATOR** - Augmented Visual Intelligence and Targeted Online Research
- **CSAM** – Child Sexual Abuse Material[1]
- **ESP** – Electronic Service Provider
- **EU** – European Union
- **GDPR** – General Data Protection Regulation
- **ICSE** - International Child Sexual Exploitation database
- **ISF** - Internal Security Fund (European Commission)
- **ISFP** - European Union's Internal Security Fund
- **LEA** - Law Enforcement Agency
- **NCMEC** - The National Centre for Missing and Exploited Children
- **NLP** - Natural Language Processing
- **OSINT** - Open-Source Intelligence

[1] Child Sexual Abuse Material (CSAM) vs. child pornography

Sometimes CSAM is referred to as child pornography. However, the term "child pornography" should be avoided for the following reasons: the term child pornography fails to describe the true nature of the material and undermines the seriousness of the abuse from the child's perspective. Pornography is a term primarily used to describe material depicting adults engaged in consensual sexual acts distributed for the purposes of sexual pleasure. Using this term in the context of children risks normalising, trivialising and even legitimising the sexual abuse and exploitation of children. Child pornography implies consent, and a child cannot legally give consent. The term child pornography is still used in legislation in some countries. For this reason, CSAM is sometimes referred to as child pornography for legal purposes. In non-legal contexts, such as in media publications, the term Child Sexual Abuse Material (CSAM) should be used.

CHAPTER 02

The AviaTor Project

AviaTor has developed into a functioning tool with numerous features that correspond to the needs of LEAs. We provide insights into the developments and achievements so far.

A JOINT EFFORT

The AviaTor project

The Aviator project was successfully launched in 2019 with the help of the European Union's Internal Security Fund - Police (ISFP). The project team that was assembled consists of stakeholders from several disciplines. Considering the AviaTor tool is being developed specifically for law enforcement, the National Police of the Netherlands were asked to lead the project. Together with the Belgian Federal Police, they represent law enforcement and provide the project team with invaluable user feedback, testing results, and knowledge.

ZiuZ Visual Intelligence is the technology partner that develops the visual intelligence part of the AviaTor tool, as they specialise in image and video analyses for forensic investigations. Web-IQ, leader in OSINT solutions for law enforcement, is responsible for the other half of the development team. The team was then supplemented by Timelex, a law firm specialising in, among other subjects, the legal aspects of information technology and privacy and data protection in the EU, and DFKI, a research centre that conducts research on "human-centric AI." INHOPE (the International Association of Internet Hotlines) completes the project team, taking care of project management and communications.

The onboarding of more LEAs

The National Police of the Netherlands and the Belgian Federal Police were the first (test) users to have access to the AviaTor tool. Since then, numerous LEAs have joined the project and are currently either using or testing the tool. The number of participating LEAs grew to 18 in June 2023, from 11 in 2021, which means the project is on its course towards the target of at least 25 LEAs, including INTERPOL, by the end of the project in September 2024. AviaTor has expanded its global reach and has now users from Europe, Asia, and North America. The tool has generated significant interest, as evidenced by the developers delivering over 30 online demos in 2022.

The objectives set for the period of 2023-2024

- Achieve **full functionality** and long-term **sustainability** for AviaTor.
- Enhance the development of **advanced AI** technologies for text analysis and video analysis.
- **Foster collaboration** among LEAs, Europol, INTERPOL, and industry stakeholders.
- **Publish an annual report** for stakeholders, providing comprehensive statistics and insights on industry reporting.
- Onboard a minimum of **25 national LEAs**, enabling their utilisation of AviaTor.
- Conduct a thorough **legal review of EU laws** and policies that impact the project, ensuring compliance and alignment.

DEVELOPMENT

Technical progress

AviaTor is a comprehensive database tool equipped with AI and OSINT-powered prioritisation features for referrals from the National Centre of Missing and Exploited Children (NCMEC).

It is crucial to understand that the developers of AviaTor do not have access to the reports that the tool is specifically designed to process and sort. These reports contain illegal content and only law enforcement agencies have the authority to access them. Consequently, the development team heavily relies on the feedback provided by LEAs who use and test the AviaTor tool. They are the sole individuals capable of testing the software according to its intended purpose.

An additional important aspect to note is that AviaTor is installed as a standalone application. Rather than having a single universal version, each LEA user has their own uniquely configured version. They are not interconnected with one another, nor do they maintain any direct connection to the development team.

The AviaTor user group is requested to provide regular feedback to the development team as well as request changes to the software. The development team focuses on delivering the key developments as described below, as well as processing all the change requests they receive from law enforcement.

Key developments

During AviaTor's phase 2 (Sep 2021 – Sep 2024) the development teams focus on the following key developments.

1 Creating an AI classifier for text analysis.

2 Creating a more granular CSAM classifier and applying this classifier on video.

3 Creating face detection and grouping.

4 More advanced targeted online research.

5 Making AviaTor functionally complete and implementing new user requirements.

6 Make the interfaces in AviaTor available so LEAs can plug in their own modules and link to different databases.

1

Creating an AI classifier for text analysis

The AI classifier for text analysis has been under development and is ready for roll-out in quarter 3 (July-September) of 2023. The classifier will consist of the following:

- Coercion detection in text using keyword and sentence pattern spotting.
- Extraction of risk-related properties from free text (as opposed to structured fields).
- Improvement of job title risk classification.

2

Creating a more granular CSAM classifier and applying this classifier on video as well

The development of this more granular CSAM classifier is still in its early stages. The Dutch hotline Off Limits (previously known as EOKM) and Belgium hotline Child Focus will be assisting the development team by creating an annotated image dataset for training machine-learning classifiers.

3

Creating face detection and grouping

Development of this functionality is scheduled to take place in the upcoming year (2023).

4

More advanced targeted online research

Advancing the targeted online research will be the focus from quarter 3 of 2023.

The strategy for OSINT in AviaTor will be two-fold:

- Integrated online research capabilities, that can be used to prioritise reports directly in AviaTor, based on online risk and identification clues.
- Provide direct user access to OSINT tools to support cross-references and manual investigation work.

Further work will be done on:

- Cross matching reported email addresses and phone numbers with CSE-related Telegram and Discord activity.
- Add support cross-referencing other sources like TikTok and Omegle and extend coverage of Darknet CSE forums.
- Explore username matching with CPS.
- Allow users to start online investigations manually or conditionally.

5

Making AviaTor functionally complete and implementing new user requirements

Following user feedback from law enforcement users, multiple updates were implemented in 2022. Among other updates, the following can be listed:

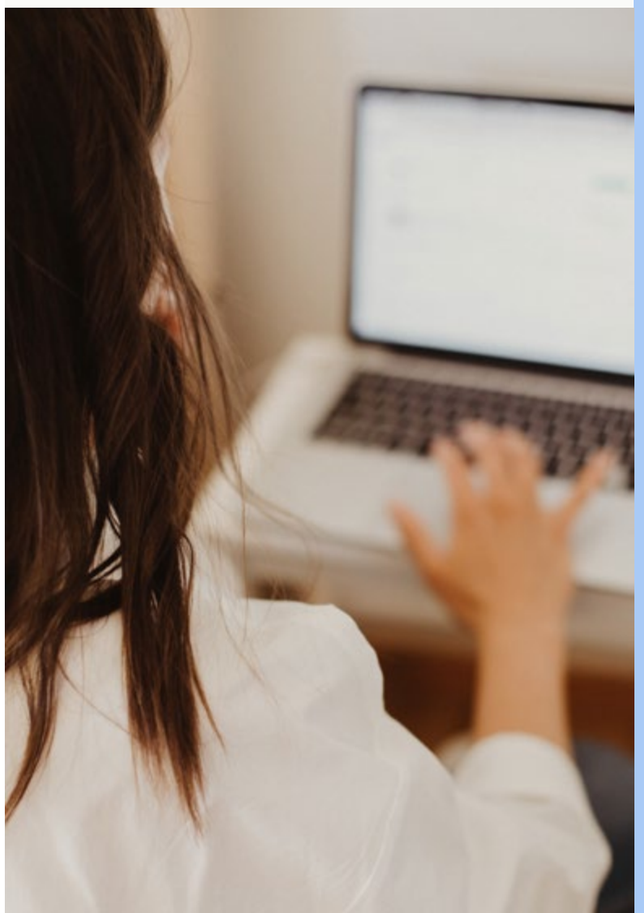
- Allow users to view and print a report in AviaTor including the results of targeted online research.
- Allow users to export an AviaTor investigation including results of targeted online research.
- Allow users to add and delete reports to an investigation.
- Allow users to set blurring as a global setting instead of on each individual page.
- Allow users to configure a scoring rule based on whether of targeted online research results contain a risk indicator.
- Allow users to recalculate the scores of existing reports and media when score settings are adjusted, or when a hash set is uploaded.
- Allow users to configure a score to indicate the likelihood of new content.

6

Making the interfaces in AviaTor available so LEAs can plug in their own modules and link to different databases

A generic plugin system was created which:

- Allows LEAs to write their own custom plugins connecting to AviaTor. These modules can consult local databases to feed the results back to AviaTor. A custom risk indicator can be created based on the outcome and displayed in AviaTor.
- Allows scoring rules to be configured for these modules.



CAPACITY BUILDING

Events and Communications

Aviator Seminar

The AviaTor Seminar took place on March 30th, 2023, in Brussels, Belgium. Around 60 experts working in the field of online child protection, from public and private sector (EU governmental organisations, law enforcement, civil society, safety tech and industry) participated at this networking event. The theme of the event was "The future of report prioritisation" and the overall goal was to facilitate the exchange of expertise and knowledge between relevant stakeholders from different sectors. Many key players in the fight against CSAM at a global level presented as speakers the newest trends, developments, and technology in their sector, among others: Uri Sadeh from INTERPOL, John Shehan from NCMEC, Annette Cassar from the European Commission, clinical expert and forensic psychologist Dr Michael Bourke, Cathal Delaney from Thorn, Ben van Mierlo from the National Police of the Netherlands, and Alexandre Dangréau from OVHcloud.

Peer-to-Peer learning events

Twice a year, the AviaTor user community comes together for peer-to-peer learning events. These events provide a platform for law enforcement officers with the specialisation in online crimes to exchange know-how on tools and techniques and share insights on the emerging trends. It is also a great opportunity for the AviaTor team to receive feedback from affiliated law enforcement officers as the end users of AviaTor tool.

The second AviaTor Peer-to-Peer learning event took place in September 2022 in Amsterdam, The Netherlands, with roughly 20 participants from LEAs and other organisations. During the event several topics were covered, such as the technical progress of AviaTor software, tricks and tips on using OSINT, and the recently created Universal Classification Schema. A specialist from the Dutch National Police shared insight on conducting OSINT investigations, and AviaTor affiliates shared their practical experience in handling the NCMEC reports and using the AviaTor tool.

The third AviaTor Peer-to-Peer event took place in Brussels, Belgium in March 2023, with about 30 participants. The focus of the event was on the prioritisation of CSAM reports and the national scoring mechanisms. AviaTor affiliates presented case examples to exchange know-how for processing CSAM reports and investigating these crimes. AviaTor partner Timelex provided participants with legal dos and don'ts when processing NCMEC reports, and further insights were given by DFKI on the challenges and solutions of cyber grooming detection.

Annual campaign 'Advance with AviaTor'

AviaTor has launched its annual campaign, titled "Advance with AviaTor," in June 2023. The campaign's primary focus is to acknowledge and highlight the significant variations in size, developmental stage, and available resources among national LEAs. Countries and LEAs possess unique and specific needs, which the AviaTor developers have personally observed while collaborating with different agencies. For smaller units, AviaTor may serve as their initial experience with database software, while larger and more advanced units aim to integrate AviaTor with their existing tools. The campaign is structured into three developmental levels, aiming to demonstrate how AviaTor can help advance at each level.

CHAPTER 03

Deep Dive Into AviaTor Data

AviaTor's development is driven by the invaluable feedback received from law enforcement using the tool. We provide insight into statistical data collected from three LEAs demonstrating the impact of AviaTor on the processing of NCMEC reports.

INTERPRETING DATA

Deep dive into AviaTor data

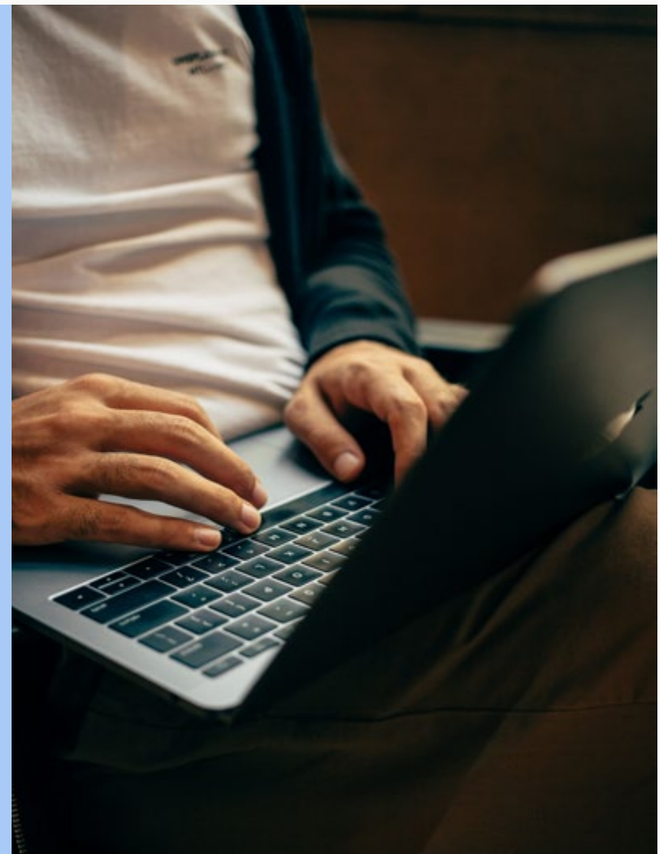
AviaTor's tagline is "Save time, save lives." During one of the early interviews, one investigator stated that "too much time is spent trying to find the things to investigate." AviaTor's mission is to reduce this time: to help police find those potential cases of ongoing abuse that are buried in the mountain of reports faster and to enable them to spend their valuable time on what matters most – identifying, rescuing, and safeguarding victims of online child exploitation and locating & stopping offenders.

The AviaTor project is now in its second phase and a number of LEAs are using the system to process NCMEC reports. To what degree is AviaTor reducing their workload? To answer this question, we gathered statistics from the local AviaTor system of three national LEAs. When it came to interpreting the data, numerous complexities and brain-twisters arose that will be highlighted throughout the article.

Using AviaTor can mean different things to different LEAs

At the start of the initial AviaTor project, European LEAs were interviewed about how they process NCMEC referrals.[1] Respondents were also invited to join the project as affiliates. These affiliate LEAs do not receive funding, but they are given free access to the software in exchange for regular feedback. At the time of writing, the AviaTor project has 16 affiliates, in addition to our two LEA project partners.

The affiliates are in different stages of AviaTor deployment. Prior to the actual software installation of AviaTor, agencies may need time to acquire the necessary hardware - AviaTor is installed locally - and approval for creating a database. Most agencies initially go through a testing phase before using AviaTor as a production system for processing referrals.

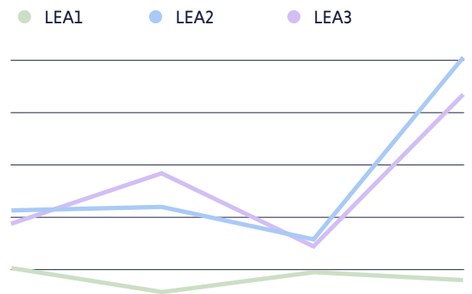


AviaTor is more than the actual tool and "using AviaTor" can mean different things to different LEAs. Some agencies, especially smaller workforces, implemented AviaTor as a complete database solution. Others use AviaTor as an upgrade to the existing internal workflow to tackle a growing number of referrals, or to find 'puzzle pieces' that could advance other CSE investigations. And lastly, a third group has joined AviaTor mostly for the community of experienced, dedicated law enforcement officers and other specialists in this field who meet multiple times a year for peer learning and networking activities.

To generate meaningful insights into agencies' workloads and how AviaTor helps to reduce the burden, we collected production statistics from three European[2] AviaTor instances at national law enforcement agencies: Belgium, Moldova, and Greece. The three agencies all started using AviaTor in production in 2022 and were able to process substantial numbers.

Comparing global figures with AviaTor and local data

Every year NCMEC publishes statistics about the number of referrals received from ESPs assigned to countries around the globe based on the IP address of the reported user. For Belgium and Greece, those 2022 statistics show that the number of referrals more than doubled compared to 2020 and 2021. The number for Moldova was lower than 2021, but higher than 2020.[3]



Not all these reports land on a police investigator's desk. In fact, the volume processed in AviaTor that forms the basis for the insights in this article, is much lower than the numbers published by NCMEC. The reason is that not all referrals are actually processed.

Country	Code	Continent	Population	2019	2020	2021	2022
Moldova	LEA1	Europe	2600000	10516	5993	9547	8372
Belgium	LEA2	Europe	11500000	21448	22154	15762	50255
Greece	LEA3	Europe	10500000	18911	28722	14616	43345

[1] This article uses 'NCMEC referrals' and 'NCMEC reports' interchangeably; elsewhere they may also be referred to as 'Cybertips'.

[2] Among the affiliates are national and regional law enforcement units from the EU, non-EU Europe, North America and Asia.

[3] Based on the Cybertipline Reports by Country published annually by NCMEC https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

Belgium

Although roughly 50.000 referrals were assigned to Belgium in 2022 according to NCMEC's Cybertipline Data, just under 20.000 were received at the federal department in Brussels. An even lower number is actually processed in AviaTor.

Three decision steps influence this funnel:

1. Belgium's referrals are first received and pre-processed at Europol.
2. Belgium does not process any referrals determined to be "informational" [4] by NCMEC.
3. After local assessment of imagery, reports that do not concern any illegal/punishable act according to Belgian law are excluded.

At the end of this process, 40%-45% of the referrals assessed in Belgium lead to the drafting of a police report.

Belgium is not an odd one out: the way referrals are processed varies across all LEAs. While some EU-based LEAs receive pre-processed referrals from Europol (like Belgium does), others receive the referrals directly via NCMEC's API. Another noteworthy procedural difference between LEAs is the reaction to minor offences. For instance, some LEAs apply a "three strikes" approach where all reports are fed into the system, but action is only taken on reported persons committing such an offense for the third time. This may still include shared viral material, which, although shared by many people, still concerns an actual child victim.[5]

Complicating factors in data collection and analysis

Before diving deeper into the AviaTor statistics, it is important to understand several factors that have impacted the collection of data and therefore also the resulting numbers presented in this report.

- As AviaTor is installed on the premises of the LEAs, the project team have no direct access to this data. To collect the relevant data, the LEAs were asked to run (and re-run) certain scripts on their installations and send back the results. It is important to stress that the information received by the project team contain aggregated statistics only, no personal or identifiable information was shared.
- There is a difference in the work process between the three LEAs. For example, as a result of the pre-selection procedure in Belgium not all incoming reports end up in AviaTor.
- The three LEAs did not start using AviaTor at the same time in 2022.
- When AviaTor is first installed, some agencies ingest reports from previous years as well so they can be used for cross-matching.
- AviaTor is still in development and new features were implemented throughout the year. Even if agencies were using AviaTor for the full year, some datapoints may not have been available for the full year.
- Reports from different platforms can differ in detail and format. The reported information depends on the reporting platform.
- Sometimes the exact meaning of a certain xml field is simply unknown to the project team.
- Some countries use AviaTor's full stack – meaning they use the database and workflow functionality, image/video categorisation and triage, whereas others had software already in place for sub-processes, like categorisation of images and videos.
- External factors can substantially delay the time between the potential crime taking place, the related report being processed at NCMEC, and law enforcement receiving the report. [6]
- In general, one must be very cautious when comparing NCMEC's global statistics with specific countries. The data in our sample is limited and it is impossible to rule out alternatives, such as possible skewness in the global distribution, where a few (large) countries heavily influence the global numbers.
- The number of reports does not necessarily correlate with the size of the problem, i.e., how much CSAM is distributed on a platform. A larger number of reports may be an indicator of better awareness, detection, and removal capabilities of ESPs. The volume of reporting can also be influenced by the characteristics of the platform[7] itself, such as end-to-end-encryption.

Even with all these factors in mind, the data from Belgium, Moldova, and Greece provide a number of fascinating insights into different processes, such as where the workload comes from and how AviaTor reduces it. The following analyses will focus on four key topics: Reporting ESPs, file types, uniqueness of reported files and uniqueness of reported persons.

4 'An informational report is one when the tech company provides insufficient information or where the imagery is considered viral and has been reported many times.' Ibid.

5 In some cases, a referral may even call for a completely different approach. For instance, when a referral was triggered by self-generated material (nudes) shared between minors, outreach, prevention or education may be more appropriate.

6 In December 2020 a special situation arose when, due to implementation of the EU's ePrivacy Directive, a number of ESPs temporarily halted reporting on EU citizens. This caused a large drop in the number of referrals early 2021 and a surge from retrospective reports later. It cannot be ruled out that any of this also impacted the workload in 2022. See also the legal article "The impact of the proposed CSAM Regulation" later on in this report.

7 The data refer to the electronic services provider, the actual platform or service may not always be distinguishable. Apple Inc, for example, submitted 234 reports. Apple provides several services including cloud storage and messenger services.

1. ESPs: Instead of WhatsApp, Discord completes the European top 5

In 2022, 236 different ESPs reported to NCMEC[8]. The distribution of reports over these ESPs is however extremely skewed:

- the top five ESPs provide over 90% of reports combined.
- 77 ESPs provided fewer than 10 reports each. Together they make up 0,0008% of the total.
- At least 1.100 connected ESPs did not submit any report.

Surprisingly, the three AviaTor LEAs fed reports into AviaTor from "only" 22 ESPs. None of the "bottom" 77 ESPs reporting to NCMEC make an appearance in the AviaTor statistics. A possible explanation for the remaining ESPs is that most of these are US-based companies that only provide their services domestically. The top 5 ESPs according to the AviaTor statistics are Facebook, Instagram, Omegle, Google, and Discord. They share a total of 85% of reports that were fed to AviaTor.

The AviaTor team sorted the ESPs by volume for each country. The resulting lists differ to some degree from NCMEC's global top 5. The main difference between the statistics of NCMEC and AviaTor seems to be that WhatsApp is overtaken by Discord in volume, even though all 3 European LEAs received referrals from both platforms. Regarding the statistics per individual country, it is interesting to see that in Belgium, Snapchat takes the first spot and Imgur comes in fourth, while neither of these two platforms are mentioned in the top 5 of any of the other participating countries nor NCMEC. Similarly, TikTok is only ranked in the top 5 in Moldova.

	NCMEC global	AviaTor total	Moldova	Belgium	Greece
Top 5 reporting ESPs	Facebook Instagram Google **WhatsApp** Omegle	Facebook Instagram Omegle Google **Discord**	Instagram Facebook **TikTok** Google **Discord**	**Snapchat** Facebook Instagram **Imgur** Google	Facebook Instagram Omegle **Discord** Google
Share of total	94%	85%	96%	80%	88%

Another notable difference is the overall percentage of Facebook and Instagram reports as set out below. The share of the total volume by Facebook is much lower than NCMEC's global average, while Instagram's share is larger, with the exception of Belgium.

	NCMEC global	AviaTor total	Moldova	Belgium	Greece
Facebook reports as a % of total	67%	35%	38%	24%	35%
Instagram reports as a % of total	16%	30%	42%	12%	26%

[8] To date more than 1,500 ESPs are registered to make reports, and 17% of these are non-U.S. based companies who voluntarily choose to report to the CyberTipline. In 2022, only 236 companies actually submitted CyberTipline reports and just 5 ESPs (Facebook, Instagram, Google, WhatsApp, and Omegle) accounted for more than 90% of the reports. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

Taking into account that in Belgium a (large) number of reports have been put aside before being fed into AviaTor at one of the decision steps, the difference between Facebook's 67% global share and 24% share in Belgium can be (in part) attributed to those reports not containing a punishable act according to the local jurisdiction.

2. File types: 99% of reported files are images or videos

Among the causes of variation between referrals are differences in how ESPs report and which information about a user is available on a platform, but also the reported content. All LEAs mentioned that some reports contain hundreds of (unknown) images or videos, whereas other reports contain a single (known) image.

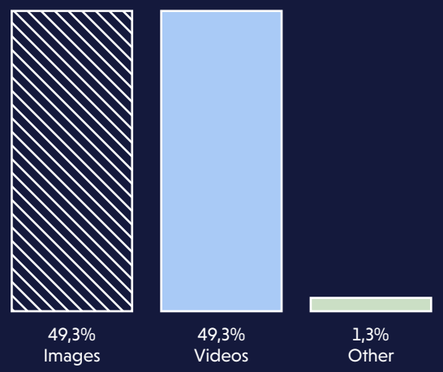
Of the files processed in AviaTor, by far the majority of are videos and images: in the AviaTor sample 99% of files are images or videos. Among images the most common format is jpg (> 70%) whereas videos are overwhelmingly (>96%) in mp4 format.

In their combined total, Moldova, Belgium, and Greece fed as many video files as image files into their AviaTor installations. In total the three countries processed more than 290.000 files, on average over 12 files per report, although that number is mostly driven by Greece. Belgium and Moldova are closer to the global average of 3 files per report.

Reports may also contain chat: a text file in which a discussion is captured, potentially concerning grooming. Text files occur in less than 1% of referrals. A small remainder consists of audio files, messages (such as forwarded emails) or zip files.

Videos and text are generally more labour-intensive to process than images. Text may also be "embedded" in other report fields, for instance in the 'Additional information' field. Those instances are not counted here.

Types of reported content



Country	Images	Videos	Other
Moldova	61%	38,5%	0,5%
Belgium	42,8%	55,8%	1,3%
Greece	48,8%	49,8%	1,4%
AviaTor total	49,3%	49,3%	1,3%
NCMEC global	55,9%	42,7%	1,4%

3. Unique files: Hundreds of referrals containing the same

Reports can be triggered by human detection, meaning a user of the platform or a moderator flags the potentially abusive content. Automatic detection is more common, either using content classifiers (AI), but mostly by comparing hashes with databases of known CSAM.

A hash of an image or video is a unique fingerprint. Several hashing technologies are used in identifying CSAM:

↗ Exact matching using MD5 or SHA-1: files with the same value are identical.

↗ Similarity comparison with PhotoDNA, PDQ or F1: used to find the same or similar images or videos regardless of changes to e.g., colour, size, or metadata. Based on the proximity of the values.

A 2020 analysis by Facebook on images and videos reported that, during a two-month period, "more than 90% of this content was the same as or visually similar to previously reported content. And copies of just six videos were responsible for more than half of the child exploitative content we reported in that time period." [9]

A large share of viral content is marked as "informational" by NCMEC and may not be further processed by law enforcement. But despite going viral, an image or video can still constitute abuse and warrant an investigation.

In interviews with LEA leading up to the development of the AviaTor system, most of them mentioned that they regularly received hundreds of referrals containing the same file. In AviaTor, MD5, SHA-1, F1, and/or PhotoDNA values are calculated for images and videos in all reported files. These files are then de-duplicated for assessment, meaning that if the same file is received a hundred times, LEAs see and categorise it only once. AviaTor users can also include hash databases of known CSAM to automatically categorise any incoming duplicates.

To assess how much impact de-duplication has on the workload, we asked the Belgian, Greek, and Moldovan LEA for the number of unique image content, based on PhotoDNA. This means that, independent of resizing or other small alterations, it can be determined how many of the same or similar images were received by the agencies.

Greece

In Greece all reports are processed centrally with AviaTor. During the year 2022, reports from previous years have also been inserted. That means that the counts of duplicate files and identifiers not only tells us about the calendar year 2022, but also how many duplicates are re-processed over the years.

Moldova

In Moldova, NCMEC reports are registered as "Information about a possible crime" and all reports are processed with AviaTor. A direct connection to NCMEC's API means new reports are imported daily without pre-selection. The "archive" of previous years has not been imported - yet.

[9] Preventing Child Exploitation on Our Apps, https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps

As the percentages of unique image content are not the same for all agencies, the impact will vary, but these early results show that local deduplication on content can eliminate roughly 30%-50% of duplicated files from the classification process. The largest percentage of duplicates (just over 50% are not unique) is found in Greece, where cross-matching includes pre-2022 reports. But this is still not as high as NCMEC's global 61,9% duplicates.

Taking into account that all three LEAs started using AviaTor in 2022, these are very promising numbers that confirm AviaTor is successful at what it was designed to do – (de)prioritise reports so that LEAs would have more time and resources for actual investigations.

Country	Unique image content based on PhotoDNA	Duplicate
Moldova	70,1%	29,9%
Belgium	68,1%	31,5%
Greece	49,8%	50,2%
NCMEC global	38,1%	61,9%

An important premise for determining the impact is that the AviaTor database of each LEA is isolated from the others: there is no cross-matching between the three and uniqueness of files is determined only in comparison with the other files in that country's database.

Let's say a particular illegal image is shared 100 times and generates 100 reports. If these reports end up at 100 different agencies, the fact that it was sent 100 times is irrelevant: in the local situation there are no duplicates. On the other hand, if all 100 instances end up at the same agency, de-duplication is a major time saver.

This is the reason why the percentages of Moldova, Belgium, and Greece are higher than the global percentage – because NCMEC receives all images at a global scale, they receive all 100 copies in the example above, resulting in the highest percentage of duplication.

4. Unique identifiers: up to 57% of person identifiers have a match in the database

As previously mentioned, some agencies use a "three-strikes" approach where minor offenses are not actioned until a third report on the same person is received. Multiple reports for the same individual are a common occurrence. If a user uploads four illegal videos one after the other, this can result in four NCMEC reports. In fact, the chances of this may increase with better/faster detection mechanisms.[10] Even if this is not the case, people often have a presence on multiple platforms and the same person may be reported by different ESPs.

When police open an investigation into a reported person, all relevant reports will be included. AviaTor includes cross-matching of identifiers such as email addresses, phone numbers, screen names, and IP addresses to create a cluster of reports that belong to the same person.

Identifiers may not always be correct or unique: information may be faked, the same screen name on a different platform may belong to a different person, and not all fields may be filled out in each report. Nevertheless, the number of unique identifiers can be considered an estimate of the number of distinct persons.

[10] During a 2022 conference presentation in Lisbon, Portugal, Google explained how their detection mechanism could flag an illegal video already during the upload, which can actually lead to more reports.

In the analysis we looked at unique identifier-combinations: the number of times that the combination of a screen name, email and phone number appeared in reports.

Whereas the same image or video can be sent to many agencies around the world, it is less likely that persons are reported in multiple countries.

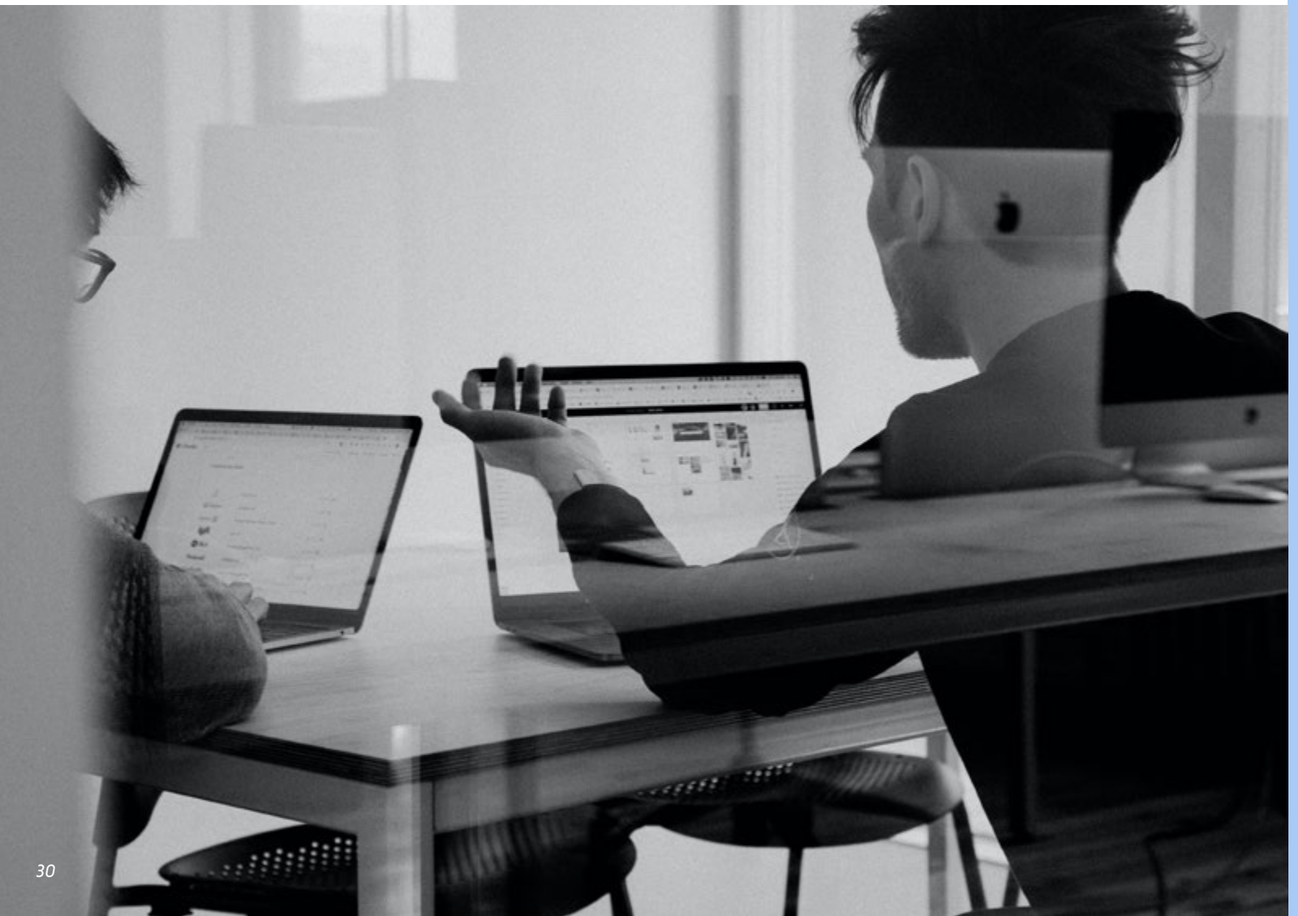
↗ In Moldova, 89% of identifier-combinations are unique. This implies that 11% of the reports have a match in the database, meaning they share the same associated screen name, phone number, and email address with other reports.

↗ In Belgium, 67% of identifier-combinations are unique, which means that 33% of the reports have a match in the database. A larger share of the reports received were submitted multiple times and cross-matching and clustering will have a larger impact.

↗ In Greece, 43% of identifier-combinations are unique and 57% have a match in the database.

The main difference between the use of AviaTor in Greece compared to the other two countries is the inclusion of pre-2022 reports in the Greek system. Unlike Belgium, where a pre-selection process is conducted, Greece fed all 2022 reports as well as pre-2022 reports directly into AviaTor without any filtering or exclusion.

The above underscores the importance of timestamping the reports concerning the same suspect. A viable solution would be for the AviaTor team to develop a "timeline" feature to enable LEAs to track historical information regarding the suspect.



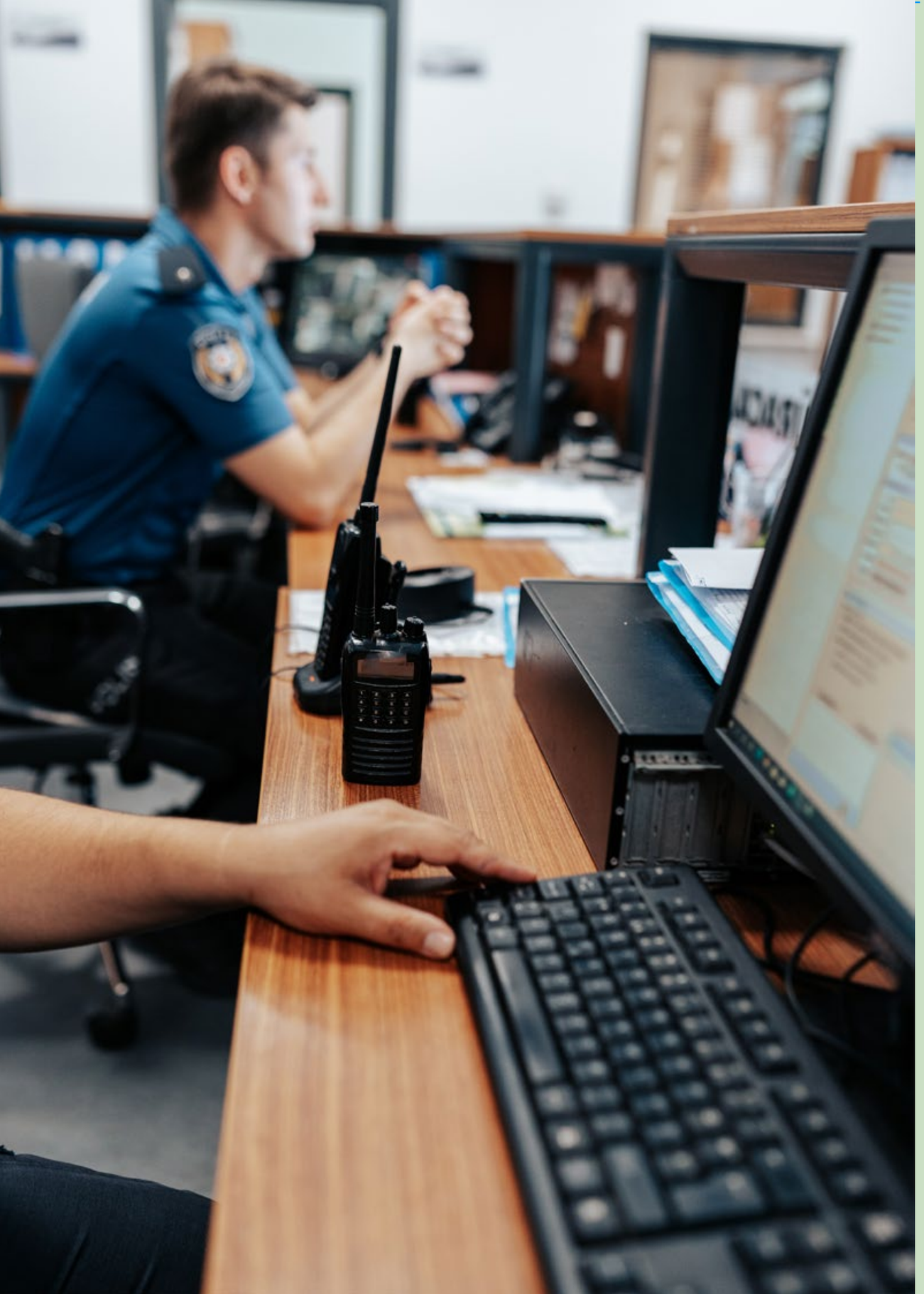
Conclusion

The initial statistics obtained from AviaTor show that in 2022, three out of the 16 AviaTor affiliated LEAs combined fed nearly 25,000 reports containing 300,000 files into AviaTor. Of the files, 99% consisted of images and videos. The reports originated from 22 different ESPs, with the top five ESPs being responsible for 85% of the imported reports in AviaTor. With less than a year of being in use, AviaTor proved valuable by de-duplicating files for the affiliated agencies. The percentage of duplicated files varied between 30% and 50%, indicating a significant time saver if duplicate files no longer need to be assessed and the LEA analyst can focus on previously unseen content.

Another noteworthy feature of AviaTor which had great impact on the work of LEAs was the cross-matching and the linking of information pertaining to reported persons (such as screen names, phone numbers and email addresses). Greece serves as an excellent example, as the automatic cross-matching feature produced identifier matches for 60% of the reports. By automatically linking reports on the reported person, LEAs can faster estimate risk and detect imminent threats, which in turn helps them to reach victims quicker and prevent criminals from committing further crimes. In addition to that, AviaTor serves as a valuable tool for LEAs to collect evidence.

The outlined statistics confirm that AviaTor is on track to be of enormous support to LEAs in triaging reports. However, the analysis also made clear that due to the variation in information reported by the ESPs and different procedures of LEAs in processing reports, analysing AviaTor data is complex. The European Union's move towards standardised reporting requirements for ESPs should greatly impact the ability to generate meaningful statistics and monitor trends.

Moving forward, the AviaTor team plans to gather more statistics from more affiliate users, enabling the generation of comprehensive workflow-related statistics, such as the number of reports that were deemed actionable and contained illegal content according to the national legislation. The acquiring of more data from a wider range of agencies, will support the identification of trends associated with risk, the usability of online research findings and their correlation with case outcomes.
The insights will contribute to enhancing the overall effectiveness of the AviaTor platform, but may also drive higher-level policy decisions and lead to preventional barriers.



LAW ENFORCEMENT

CHAPTER 04

Interview: Practical Use of AviaTor

AviaTor has been in use in Moldova since 2021. Artur Degteariov, head of the Cyber Crime Unit in Moldova, provides us with insight into their daily practical use of the tool and the impact it has had on their work process.

FROM THE FIELD

LAW ENFORCEMENT

Interview: The practical use of AviaTor

Artur Degteariov is the head of the section responsible for tackling online child sexual abuse within the Directorate for cybercrime investigations of Moldova. The unit has been actively using AviaTor since 2021 and contributing to its development. With a career spanning over a decade, Artur has made significant contributions to combatting organised crime, human trafficking, and, most notably, online child abuse and exploitation. In 2013 Artur joined the newly established cybercrime team in Moldova, where he has since exclusively focused on combatting online child abuse and exploitation.

The Cyber Crime Unit now includes six officers dedicated to safeguarding the online well-being of children across the nation. The unit covers all cases in Moldova, including a small regional unit in Chișinău, the capital city. Following the Europol model, the cybercrime team is divided into specialised sections that address cyber-dependent crimes, online fraud, and online child sexual abuse. The team includes a group of first responders who play a critical role in providing swift support and intervention.

What is the number of NCMEC reports that the Moldovan police received in 2022 and have you seen a growth in numbers in the last years?

On an annual basis, we receive approximately 5000-6000 reports from NCMEC. We began receiving reports from them directly in 2016, and since then, the number of incoming reports has remained relatively consistent. We evaluate the numbers every semester and focus on actionable reports. Over time, we have developed the ability to quickly identify reports that require action. In the past, we also spent resources investigating some of the cases that ultimately turned out to be mistakes or misjudgements of the suspect, rather than instances of individuals possessing CSAM for sexual gratification. So now we strive to avoid such situations by quickly identifying actionable reports and concentrating solely on those involving the abuse of children and/or obtaining sexual gratification from their exploitation.

Regarding the numbers, I would say that there is currently no significant increase. During the COVID-19 pandemic, there was a surge in reports due to increased file sharing, but it did not translate into a proportional rise in CSAM. Rather, more individuals were sharing the same existing material.

A large portion of reports contain viral content (usually between 1-5 files per case) which was shared for shock value rather than for sexual gratification. In such cases, we carefully analyse the activity to decide whether an investigation is necessary. For instance, if someone forwards two known CSAM images from their mobile device, we generally do not take immediate action. However, if the situation involves grooming, self-generated content, or new material, we always start an investigation. The same applies when an individual shares significant amounts of CSAM over an extended period.

Are you worried about your department's capacity when it comes to processing NCMEC reports in the future?

At the moment I think we have sufficient capacity within our unit. Although sometimes when we seize devices or have lots of material to examine, it can be terribly busy. Our goal is to increase our capacity to cover an increasing range of areas within the online environment. The amount of material discovered on devices has gone up, with instances of up to 20 terabytes (TB) of data being found on a seized device. This takes up significant resources for a thorough examination. Additionally, investigating grooming techniques and perpetrator behaviour requires intensive human investigation, consuming considerable time and capacity.

We are obligated to examine seized material thoroughly, but we are constrained by legislative time limitations on search and seizure. We must analyse all material and arrive at a conclusion in time; otherwise, we are obliged to return the seized hardware – for example mobile phones. If incriminating evidence is discovered, the devices are presented in criminal court as evidence for the corresponding case. This can involve millions of images and videos.

How has the landscape of CSAM reporting evolved in Moldova over the past decade?

The evolution of social networks and the internet has played a significant role. As certain online spaces gain popularity, particularly among the younger demographic, abusers are drawn to these platforms in search of potential victims.

In the first stages, we were investigating many cases related to Skype, as it was one of the few platforms offering video conferencing capabilities at the time. However, various social networks such as Facebook, Instagram, and Snapchat currently provide this feature. There are even instances where we encounter unfamiliar social networks that we had not previously seen. Different national and cultural groups use different online platforms for online communications. For instance, Balti, the second largest city in Moldova, which is in the northern region of the country where Russian is predominantly spoken, shows a preference for Russian social networks.

Have you noticed any trends in reported CSAM?

Occasionally we receive anonymous reports through the helpline, where victims themselves report their cases but prefer to remain unidentified.

Throughout the period from 2021 to 2022, we saw an increase in cases involving self-generated content. However, the frequency of such cases appears to have thankfully gone down recently. We conducted

awareness campaigns and engaged in activities aimed at drawing attention to the issue, which contributed to the decrease in these cases.

Currently, one of the primary tactics employed by perpetrators is sextortion. They masquerade as children, trying to groom or deceive their targets. Once the victims share compromising material, the perpetrators exploit it to coerce them into supplying more.

How does your department use AviaTor and how does the tool support or influence your workflow process?

Initially, we used Aviator through a virtual server. However, we recently transitioned to a physical server and installed AviaTor on it. We employ AviaTor for processing all NCMEC reports. AviaTor significantly aids us in prioritising reports and finding repeat offenders. Moreover, it helps the identification of perpetrators who own substantial amounts of material.

Comparing our current usage of AviaTor to how we processed NCMEC reports in the past, the utilisation of AviaTor proves to be much more streamlined. The workflow and necessary steps have become more efficient, requiring less manual labour. It also reduces the reliance on the individual officer's memory, as AviaTor automatically links cases for us, even if significant periods of time separate them. This feature greatly assists in proving malicious intent when prosecuting these offenders.

In your opinion, what is the most helpful feature or strength of AviaTor?

AviaTor offers valuable functionalities that contribute to our work. Firstly, it supplies a comprehensive overview of the volume of material, allowing us to assess the scope of the investigation. Furthermore, AviaTor aids in identifying recurring offenders, and the display of IP addresses enables quick identification of proxy usage.

The software allows for swift image viewing and user activity analysis, which is highly convenient. The inclusion of OSINT capabilities is of great significance. AviaTor helps us determine the status of social media profiles, whether they are still active or suspended. In cases where a profile has been suspended, it becomes crucial for us to act quickly and try and retrieve any available screen captures or evidence. Consequently, the suspension of a social media profile can elevate the priority level of a case.

However, when it comes to prioritisation between reports, it is hard to decide which indicator is the most important within AviaTor, as it differs per case. For example, in the case of grooming where there is a real child victim, the number of materials found is not truly relevant – we will start an investigation regardless. While in other cases, the amount of content found could lead to us deciding whether to open an investigation.

Do you consider AviaTor to be user-friendly?

Yes, the tool has significantly increased our report processing capabilities, making it approximately five times faster compared to manual methods. In the initial stages of receiving NCMEC reports, we relied on manual review and analysis, which was a time-consuming process.

"The most notable advantage is that AviaTor allows us to prove connections between reports from the present and the past, which would be nearly impossible for a human to remember."

If you had to advise other law enforcement agencies about whether to use AviaTor - what would be the strongest benefits in your opinion?

The most notable advantage is that AviaTor allows us to prove connections between reports from the present and the past, which would be nearly impossible for a human to remember. The software enables cross-matching of information that might otherwise go unnoticed. This capability surpasses human memory ability and greatly enhances our investigative capabilities.

"As new platforms appear and more children access the online space, the task of safeguarding children in the digital environment becomes increasingly challenging."

What do you envision for the future of law enforcement's handling of CSAM and what potential risks and challenges do you anticipate?

The rapid pace of technological advancement applies not only to legitimate applications but also to offenders. As new platforms appear and more children access the online space, the task of safeguarding children in the digital environment becomes increasingly challenging. The expanding memory ability of devices helps with the easier dissemination of harmful material. To effectively address these evolving threats, it is crucial to continuously adopt innovative technologies for detection and investigation. Failure to keep pace with technological advancements may pose significant challenges in the future.

Also, the sheer volume of digital material poses a considerable storage challenge. Anticipating the technology that will be utilised in the future presents difficulties, making it challenging to develop long-term storage solutions for the digital evidence accumulated during investigations.

Do you have any success stories you can share from the field?

We encountered a distressing case involving grooming that was reported through Instagram. The severity of the case and its violent nature prompted us to conduct an in-depth analysis, during which AviaTor proved invaluable. The software enabled us to find if the offender was previously known and revealed other cases associated with CSAM. Despite meeting challenges with mismatched IP addresses, as the perpetrator used different or dynamic IPs, AviaTor eased a swift identification process. It aided us in understanding the primary activities of the individual involved.

As a result of our efforts, we successfully found and apprehended the individual responsible, leading to his conviction. The prompt identification made possible by AviaTor played a crucial role in ensuring justice was served.

Artur Degteariov

Head of the section responsible for tackling online child sexual abuse within the Directorate for cybercrime investigations of Moldova

LAW

CHAPTER 05

The Legislative Proposal

The EU's legislative proposal aims to prevent and combat CSA. The European Commission provides answers to some of the most frequently asked questions about the draft Regulation.

FROM THE EC

LAW

Our legislative proposal to counter child sexual abuse

Last year the European Commission proposed a new regulation to prevent and combat child sexual abuse within the European Union. This has raised numerous questions among key stakeholders in the field of child safety, including LEAs, on the possible impact it might have on the current procedures and workflows. In this article, we hear from the European Commission as they answer some of the most frequently asked questions concerning this newly proposed regulation.

What is the EU's legislative proposal?

On May 11th, 2022, the European Commission published a proposal for a Regulation laying down rules to prevent and combat child sexual abuse (hereinafter the "proposal"). The Proposal would have a twofold objective: firstly, to introduce mandatory obligations for service providers, secondly to create a new EU Agency to prevent and combat child sexual abuse.

What is the status of the negotiations?

As of summer 2023, the Proposal is currently being negotiated at the European Parliament, with the LIBE Committee in the lead, and at the Council, under the Swedish presidency at the time of this paper.

Can you expand on the detection obligation?

The detection obligations only occur where the risk assessment has indicated a significant risk of misuse of the service for the purpose of online child sexual abuse, notwithstanding the mitigation measures taken by the provider.

↗ Member States will need to designate national authorities in charge of reviewing the risk assessment and the mitigating measures proposed by the service provider to prevent child sexual abuse online.

↗ Where such authorities determine that a significant risk remains, they can ask a court or an independent administrative authority to issue a detection order for known or new child sexual abuse material or grooming to address any remaining significant risk in a targeted manner.

Detection orders are therefore limited in time, subject to strict procedural safeguards, and target a specific type of offence on a specific service.

Which material do the detection obligations cover?

The detection obligations cover: known material, new material, and grooming.

↗ Known material (re-uploaded photos and videos that have been previously identified as child sexual abuse material)

↗ New material (photos and videos not previously identified)

↗ Grooming (a practice where child sexual abuse offenders build a relationship of trust and emotional connection with children in order to manipulate and sexually exploit and abuse them).

In line with the central objective of the proposal to better protect children, the identification of grooming only concerns interpersonal communications where it is known that one of the users is a child.

Which indicators will be used to detect the material?

Detection can only be based on the set of indicators of online child sexual abuse kept by the EU Centre under the control of national law enforcement authorities. The law enforcement authorities are therefore one of the main actors to ensure that reliable indicators will be utilised. The Commission believes that this will strongly contribute to improving the effectiveness and transparency of the detection process.

How will the reports be structured?

The Commission's proposed legislation contains an Annex with templates on detection, reporting and removal orders, to ensure that minimum information will have to be included in the reports. These Annexes were created following a series of consultations with law enforcement prior to the creation of the Proposal. The minimum information present in the reports will ensure that reports are more actionable for law enforcement, thereby potentially improving reporting standards globally.

How will the EU Centre help law enforcement?

The EU Centre will work with companies and law enforcement to help them exchange information and best practices, providing oversight, transparency, and accountability. The EU Centre will closely support law enforcement, so that they can act on reports and save children as quickly as possible.

↗ The EU Centre will receive, and process reports from providers of any child sexual abuse materials or solicitation of children detected on their services and will share them with the competent law enforcement authorities and Europol, unless they are submitted in error. We would expect there to be a rapid response from the moment the reports are received by the EU Centre to when they arrive at law enforcement.

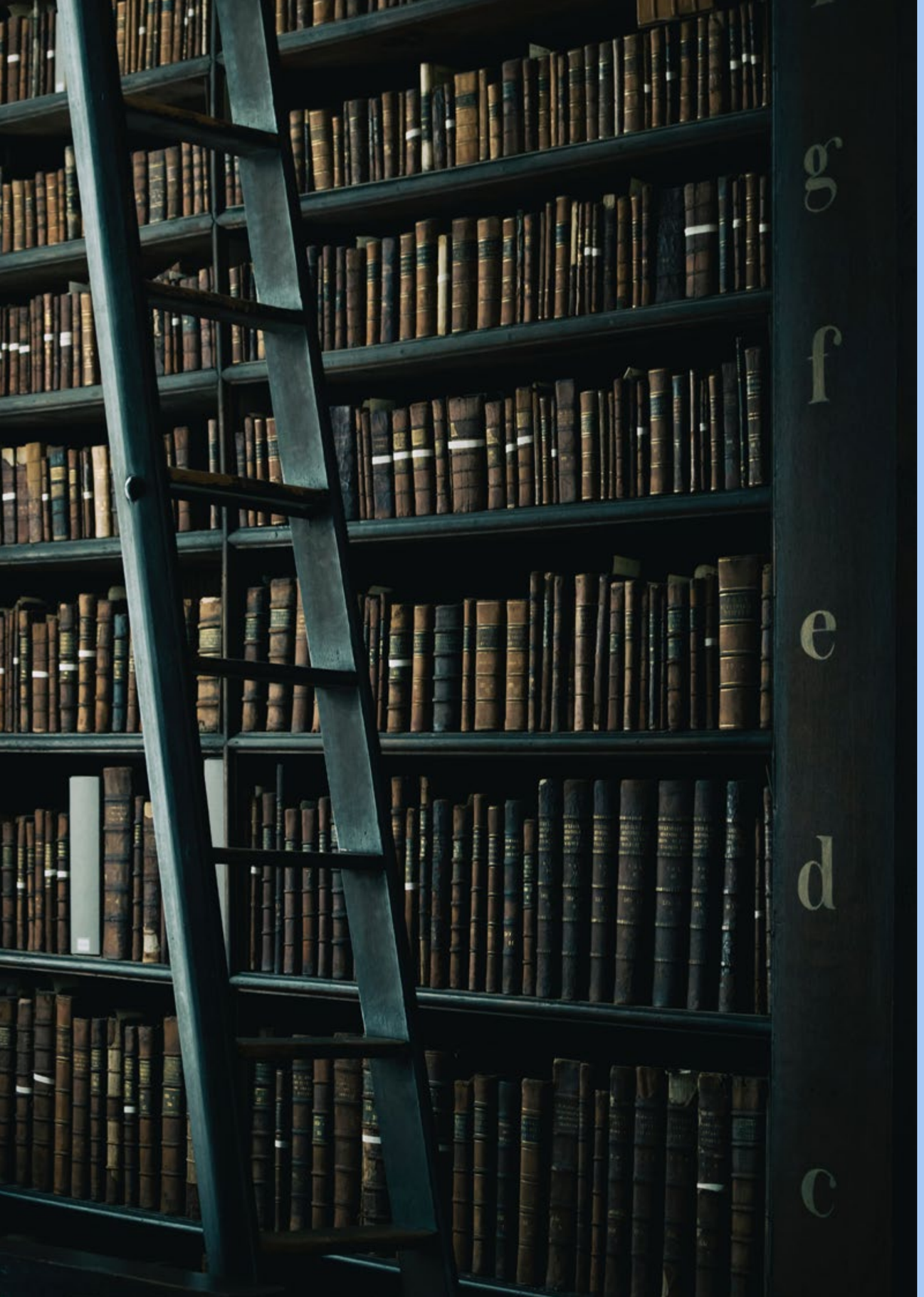
↗ The EU Centre will function as an important safeguard by preventing false positives from being reported to law enforcement, ensuring visibility on the effectiveness of detection measures, transparency, and accountability of the process. This means that reports being sent to law enforcement would be clearer and at less risk of false positives.

Will the EU Centre conduct research work?

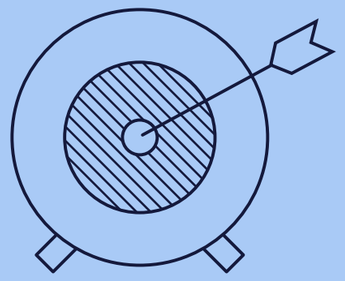
The EU Centre could serve as a knowledge hub for sharing best practices and research work on prevention, assistance to victims, investigations, and prosecutions. Law enforcement could have brand new opportunities for collaborating with the EU Centre in terms of sharing expertise. This will ultimately benefit all parties including the functioning of Member States' apparatus to counter this heinous crime.

How will the proposed Regulation interact with your 2011 Directive?

The proposed Regulation supports and builds upon the implementation of the 2011 Directive. The Directive is aimed at harmonising the criminal legislation of EU Countries. A revision of the Directive is in progress. We expect this work to be finalised by the end of 2023.



LAW



CHAPTER 06

The Regulation's Impact

The proposed CSAM Regulation will influence the workflow of LEAs as well as the AviaTor tool. We take a deep dive into the possible consequences.

DEEP-DIVE

LAW

The impact of the proposed CSAM Regulation on the AviaTor Project

The context of the proposal

The Proposal is a response to the growing demand for more effective measures in the fight against child sexual abuse material in the EU. Studies showed that the EU was hosting the most CSAM worldwide.[11] The Proposal is part of the 2020 EU strategy for a More Effective Fight Against Child Sexual Abuse.

An unintended and unwanted side-effect of the rise of application-based electronic communication services, such as WhatsApp, Instagram, and Messenger, was that it provided predators with the means to effectively disseminate CSAM to a larger audience. Luckily, the application providers responded diligently by commencing voluntary detection, reporting and removal of CSAM from their platforms. In 2018, the EU changed the definition of "electronic communication services" by broadening the scope of that definition in the European Electronic Communications Code to also include number-independent interpersonal communication services (i.e., services that do not require a phone number). [12] The EU motivated this decision by referring to the growing importance of these services. The result of this change in definition was that number-independent interpersonal communication services like WhatsApp, Facebook Messenger, Snapchat, and others, were suddenly classified as electronic communication services. This, in turn, meant that these services had to comply with the confidentiality obligations set forth in the 2002 ePrivacy Directive.[13] These obligations ensure that providers of electronic communication services must keep communication between two or more participants private and confidential. In layman's terms: they are not allowed to process personal data relating to the communication facilitated by their services. The result was that ESPs like WhatsApp and Snapchat, and web-based e-mail services were now prohibited from voluntarily detecting CSAM on their services and reporting it to competent authorities.

In order to provide the possibility for service providers to continue voluntary detection of CSAM on their services, the EU decided to implement an interim CSAM Derogation in July 2021.[14] The Derogation is a temporary Regulation which exempts certain providers from the confidentiality obligations in the ePrivacy Directive for the purposes of continuing their voluntary detection efforts. It must be stressed that the CSAM Derogation only provides for the possibility for ESPs to continue using voluntary detection tools in order to specifically detect and report CSAM. It does not entail an obligation to implement any detection technology.

The CSAM Derogation provides only a temporary solution and the following issue still needed to be tackled: how to ensure that providers can and must take effective measures against CSAM on their services and platforms, while reconciling these measures with the fundamental rights of all users of these services and platforms? The proposed CSAM Regulation is an instrument intended to provide a permanent and robust solution for this problem.[15] It is the European Commission's attempt to respond to the numerous legal and ethical concerns that have been voiced after the adoption of the Interim derogation to the ePrivacy Directive, i.e., lack of legal basis for the voluntary processing, the scope and application of the proposed safeguards, etc. [16]

The influence of the proposed CSAM Regulation on the workflow of EU-based LEAs

The proposed CSAM Regulation will establish a new EU body called the "EU Centre," which shall, among many other responsibilities, act as the receiving and processing entity for CSAM reports by ESPs providing services within the EU.[17] The EU Centre is obliged to forward all CSAM reports, that have not been considered as "manifestly unfounded," [18] to competent national law enforcement agencies or, where applicable, to Europol. Therefore, the main influence of the proposed CSAM Regulation on the work of LEAs will come from the creation of the EU Centre and its given tasks.

The EU Centre will act as an EU centralised body for the facilitation of detecting, reporting, and removing of CSAM. One of the main ways in which it will fulfil this mission is by ensuring that the reports on online child sexual abuse received by LEAs contain sufficient information to initiate an investigation and allowing them to act. Through the harmonised reporting mechanism, the proposed CSAM Regulation will provide clear rules for ESPs on, among others, which information should be included in a report (e.g., content data, IP-address, information concerning identity of the user, etc.). This in turn should improve the quality and relevance of the reports received by LEAs, which should result in LEAs being able to focus their limited capacity on actionable reports (meaning it leads to an investigation) as much as possible.

In addition, the EU Centre can give EU-based LEAs access to their database of indicators in case this is needed for investigation purposes. This database will include indicators consisting of digital identifiers to detect the dissemination of known or new CSAM or the solicitation of children. The database will hold a list of uniform resource locators and other additional information to facilitate the use of the indicators, such as language identifiers and identifiers allowing for a distinction between different types of files. In case police investigators want to access this database, they must file an official request and upon approval, they will be granted access to the information specifically relevant to their investigation.

The impact on CSAM reports and the role of AviaTor

The new obligation for ESPs active within the EU to detect and report CSAM on their services will most likely lead to an increase in CSAM reports received by the EU-based LEAs. The EU Centre is designed to filter through the reports and forward only "good quality" reports to law enforcement, which should lead to a decrease in non-actionable reports being sent to LEA. An increase in reports, on the other hand, could take place considering the number of new ESPs that will fall under the new reporting obligation, who have never before been obligated to report CSAM found on their servers. These are not only EU-based ESPs, but also ESPs from outside the EU and the US, that are offering their services within the EU.

[11] Source: Europe remains 'global hub' for hosting of online child sexual abuse material | IWF

[12] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[13] Article 5 (1) (confidentiality of communications) and article 6 (traffic data) of the ePrivacy Directive.

[14] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

[15] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.

[16] European Data Protection Supervisor, Opinion 7/2020 on the proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online

[17] Article 45 of the proposed CSAM Regulation

[18] This term is used in the legislation and will be interpreted by the EU Centre.

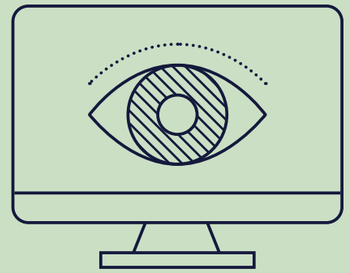
Therefore, EU-based LEAs could potentially face an increase in their workload when it comes to processing CSAM reports. As several LEAs are already struggling with the high volume of these reports, and have reached the limits of their capacity, it is of utmost importance to support them with prioritisation and workflow streamlining tooling. AviaTor has been developed to support law enforcement with managing high volumes of CSAM reports through prioritisation functionalities, while being fully customisable by the user. With the support of AviaTor, LEAs can determine which reports are high priority as well as identify lower priority reports such as the ones containing viral material.

Another point to take into consideration is that even though a central reporting entity on EU grounds is welcomed, one should not forget the already existing CSAM reporting mechanisms that are in place: the International Association of Internet Hotlines (INHOPE) for public reporting, and the National Centre for Missing and Exploited Children (NCMEC) for industry reporting. As the exact cooperation and interaction between the EU Centre and the existing organisations is still being defined in the legislative procedure, industry and organisations are voicing concerns about the risk of duplication of reports being reported to LEAs in the EU. This means that either the EU Centre or EU-based LEAs will have to filter the duplicated reports coming from different international stakeholders. This is where AviaTor can provide the perfect tool for European LEAs and the EU Centre. AviaTor is created to help in classifying, prioritising, and de-duplicating CSAM reports. One of the functionalities in AviaTor is the detection of duplicated reports by grouping similar reports together (content is labelled as duplicates or near duplicates), and therefore making the de-duplication work of police officers or analysts significantly easier.

Last, the proposed Regulation states that the EU Centre shall maintain and operate a database of indicators (see hashes/AI classifiers).[19] The centralised hash list maintained by the EU Centre should be applauded as it will allow users to rely on a database of hashed material which is known to be illegal in the EU, therefore also limiting the existence of false positives. This again provides opportunities for AviaTor, as the EU Centre hash list can also be integrated into the AviaTor database.

[19] Article 44 Proposed Regulation

TECHNOLOGY



CHAPTER 07

Cyber Grooming Detection

AviaTor has the potential to integrate AI and machine learning techniques to detect and prevent cyber grooming by analysing patterns, behaviours, and content. We look at recent research into the detection of cyber grooming and discuss the challenges that come with that.

MACHINE-LEARNING

TECHNOLOGY

Cyber grooming detection within AviaTor

When children and teenagers use mobile devices and social media, there is a higher risk of them encountering online harassment. One particular risk they face is called cyber grooming, where a person tries to manipulate and exploit a potential victim for sexual purposes, both online and offline. In this report, we provide a brief overview of the latest advancements in detecting cyber grooming. We discuss the current methods used and highlight the challenges in detecting signs of cyber grooming in chat logs. Lastly, we present our ongoing research within the AviaTor project in this area.

Introduction

When an adult befriends a child online with the intention of sexually abusing them, it's often referred to as cyber grooming. Sometimes different terms like **enticement of children, solicitation of children for sexual purposes or sextortion** are used, but they have similar meanings.

Cyber grooming is when an adult tricks a child online by pretending to be their friend and gaining their trust, with the intention of sexually exploiting or abusing them. Online enticement is when someone uses the internet to convince or tempt a child into engaging in sexual activity. Cyber grooming focuses on building a relationship and gaining trust over time, while online enticement involves persuading or luring a child into sexual activity using online communication. Sextortion is when someone uses sexual images or videos to force or blackmail someone into doing sexual acts or providing more sexual material. However, people often use these terms interchangeably.

It has become easier to contact potential victims due to the widespread use of social media platforms. A study by the Pew Internet Project conducted in 2009 found that 15% of children aged 12 to 17 received sexually suggestive photos or videos.[20] During the Covid-lockdown for a three-month period, [21] the British police reported 1,220 cases of sexual communication with a child.

When it comes to cyber grooming, there are specific steps that perpetrators often follow. First, they identify and choose potential victims. Then they try to make contact through digital communication. Next, they employ tactics like flattery, sympathy, and other methods to build a relationship with the victim and gain their trust. For instance, they might pretend to have similar interests or share information about hobbies, family, or social situations. These tactics help manipulate the victim by relating to their problems, building rapport, and ultimately establishing trust. They may also attempt to isolate the child from their family and friends.

Teenagers are often approached by perpetrators in direct communication using social media. These platforms can include popular social media tools like Facebook, chat applications, web forums, or even computer games. In this report, we provide a summary of the latest advancements in cyber grooming detection. We discuss the current challenges involved and outline our ongoing research in developing cross-lingual cyber grooming detection, as integrated into the AviaTor tool.

Related work on cyber grooming detection

Linguistic analysis of chat protocols

In Antonsen's Master's thesis (2021), an analysis of linguistic clues related to cyber grooming is analysed. The study involved participants who were asked to determine whether specific conversations were considered as cyber grooming or not. The findings revealed certain patterns in cyber grooming conversations. For instance, these conversations often contain explicit content, with predators frequently asking questions about age, age gaps, meeting possibilities, sharing pictures, clothing, and alternative communication methods like phone or direct chat. Age information is usually freely exchanged between the victim and perpetrator. Predators are trying to ensure privacy and often ask victims if parents or other household people are currently at home. Communication often drifts into sexual content and the predator asks about performing a specific (sexual) action or roleplaying. Furthermore, predators are eager to arrange in-person meetings and use a variety of nicknames (e.g., honey, darling, etc.) for referring to the victim.

Within the dataset, non-cyber grooming chats typically lack sexual content and instead focus on genuine interest in the other person or engage in small talk about topics like sports, hobbies, or school. Interestingly, during the evaluation process, human evaluators mistakenly identified around 7% of regular conversations as instances of cyber grooming. Some of these false positives contained sexual content, highlighting the challenge of distinguishing between legal and illegal chat conversations.

In Shannon's analysis (2008), 315 Swedish police reports related to cyber grooming were examined, covering the period from January 2004 to September 2006. The reports were classified into four main categories, and similar linguistic characteristics were observed as in Antonsen's study (2021). For instance, the language used by perpetrators was often flattering, and they attempted to establish various modes of communication while striving for secrecy. It was also observed that some perpetrators posed as model scouts and requested different pictures to build a portfolio. In certain cases, blackmail was used to coerce victims into sending more pictures. Interestingly, it was common for perpetrators to claim to be younger than they actually were (e.g., a 37-year-old pretending to be 25 years old). The analysis found that approximately 90% of the victims were female, with over 60% falling within the age range of 11 to 14. Some of the victims were dealing with serious family issues or facing bullying at school.

Machine learning perspective

Recent advancements in natural language processing, specifically the transformer architecture, have significantly accelerated research in this field. These advanced architectures have shown improvements in various areas of natural language processing (NLP). For example, they are better at understanding context, learning from limited examples, and working with multiple languages.

What's interesting is that these models acquire multilingual capabilities by training them on large amounts of unlabelled text in multiple languages. Afterward, the models are fine-tuned for specific tasks, such as identifying cyber grooming, and can perform these tasks in different languages.

In the early stages of cyber grooming detection, researchers like Villatoro-Tello et al. (2012) used a method called "bag-of-words." This approach involved representing the documents using a term-frequency/inverse document frequency weighing scheme and using support vector machines for classification.

Later, various machine learning techniques were compared by different researchers to detect cyber grooming in chat logs. These techniques included logistic regression, Naïve Bayes, support vector machines, convolutional neural networks and more. The goal was to find the most effective method for identifying instances of cyber grooming in chat conversations.

Researchers have applied transformer-based approaches to the PAN'12 dataset and achieved an F1 score of 97%. Meanwhile, it is argued that the objective should not only be to detect cyber grooming in chats, but also to prevent it by identifying malicious behaviour as early as possible. They propose redefining the task to prioritise early alerts, rather than waiting until the entire conversation has been analysed. This would make it possible to promptly warn parents about unusual conversation patterns. However, for the AviaTor project, we assume access to complete chat reports after a report has been filed with NCMEC. Therefore, the task of early cyber grooming detection can be disregarded in this context.

Problems with long texts and available data

Working with long text

One major drawback of the transformer architecture is its complexity when it comes to processing large texts. The attention mechanism used in transformers has a quadratic complexity, which means it can only handle a specific length of input. For example, BERT-based models typically have a limit of 512 sub-piece tokens. However, chat conversations are usually much longer than that. How to deal with text longer than 512 tokens is a currently open research question.

One simple approach is to truncate the document, assuming that the first 512 tokens contain enough information for accurate classification. However, in the case of chat conversations, this assumption may not hold true because the initial part of the conversation, where people are getting to know each other, can be similar in both cyber grooming and non-cyber grooming messages.

Another approach is to divide the text into smaller parts or chunks and feed each chunk separately to the model for classification. More complex models have been developed to reduce the complexity of the attention operation and allow for a larger context to be included. However, even these models have an upper limit on the number of tokens they can process (e.g., 2048 sub-piece tokens), so they still cannot handle arbitrarily long text. Finding a solution for working with texts longer than the input size of the selected transformer model is currently an area of ongoing research.

Availability of data

To develop algorithms that can detect cyber grooming behaviour in chats, manually labelled data is needed. However, obtaining such data is challenging due to the illegal nature of cyber grooming. To our knowledge, the only freely available resource for this purpose is the Perverted Justice website.[22] This website collects chat logs from volunteers who pose as children and engage in conversations with sexual predators. The collected chat logs are then handed over to law enforcement for legal action.

Besides ethical questions, it is currently unclear if these chat logs reflect real cyber grooming behaviour, as the volunteers mimic children's behaviour. Another major problem is that Perverted Justice only collects chats in English language, but cyber grooming occurs in all spoken languages.

One of the few freely available datasets for studying cyber grooming is the PAN'12 dataset. The authors of this dataset gathered English chat logs from various websites and marked predatory lines in the conversations. The dataset consists of a mixture of predatory chats obtained from Perverted Justice and non-predatory conversations collected from other chat platforms like Omegle and IRC channels.

In the PAN'12 dataset, only about 2.5% of the segments are identified as cyber grooming, reflecting the belief that cyber grooming constitutes only a small portion of overall chats. The non-cyber grooming data in the dataset also includes discussions about cybersex to make it more challenging to differentiate between different types of content.

Mcghee et al. (2011) developed the ChatCoder2-corpus, by scraping almost 500 chats from Perverted Justice. A subset of 155 chats was segmented and messages were categorised into one of three phases: approach, exchange of personal information and actual grooming. These phases were based on the recommendations provided in Olson et al. (2007). It's important to note that

the ChatCoder2-corpus was specifically developed to study linguistic properties and does not include instances of non-cyber grooming behaviour.

Cheong et al. (2015) use real chat protocols collected from a massive online multiplayer game to detect real cyber grooming behaviour. Unfortunately, this dataset is not available to the public.

Current status within the AviaTor project

In the AviaTor project, we conducted a thorough analysis of existing research and gathered publicly available datasets. Unfortunately, we were only able to obtain the PAN'12 dataset because the creators of ChatCoder2 were unwilling to share the data with research groups outside of academia.

Currently, we have translated all the PAN'12 chat-conversations into the three target languages German, French, and Dutch, using a state-of-the-art machine translation model published by Meta-research, which is freely available. We chose these specific languages based on their relevance to the AviaTor project. German and French are widely spoken languages in the European Union, and we have native speakers of all three languages involved in our project. The translation process took approximately 72 hours using a dedicated graphics processing unit accelerator (RTX 6000).

In the first step of our project, we trained a BERT-based classifier using English training data. We fine-tuned the classifier and used document truncation, which means we only considered a specific portion of the chat text. The classifier performed very well, achieving an accuracy of 99.9% on the test data. This high accuracy was expected because of the distribution of the classes in the data.

In our upcoming experiments, we plan to train multi-lingual transformer models using the English training data. We will then evaluate these models using both the original English chat protocols and the translated versions. This will help us estimate the models' ability to understand multiple languages without specifically being trained on them. We have several ideas to further improve this approach, such as using sliding window techniques instead of truncation, incorporating few-shot learning by using translated training examples, or explicitly indicating the authors' languages to the language model. These improvements will enhance the effectiveness and flexibility of our system.

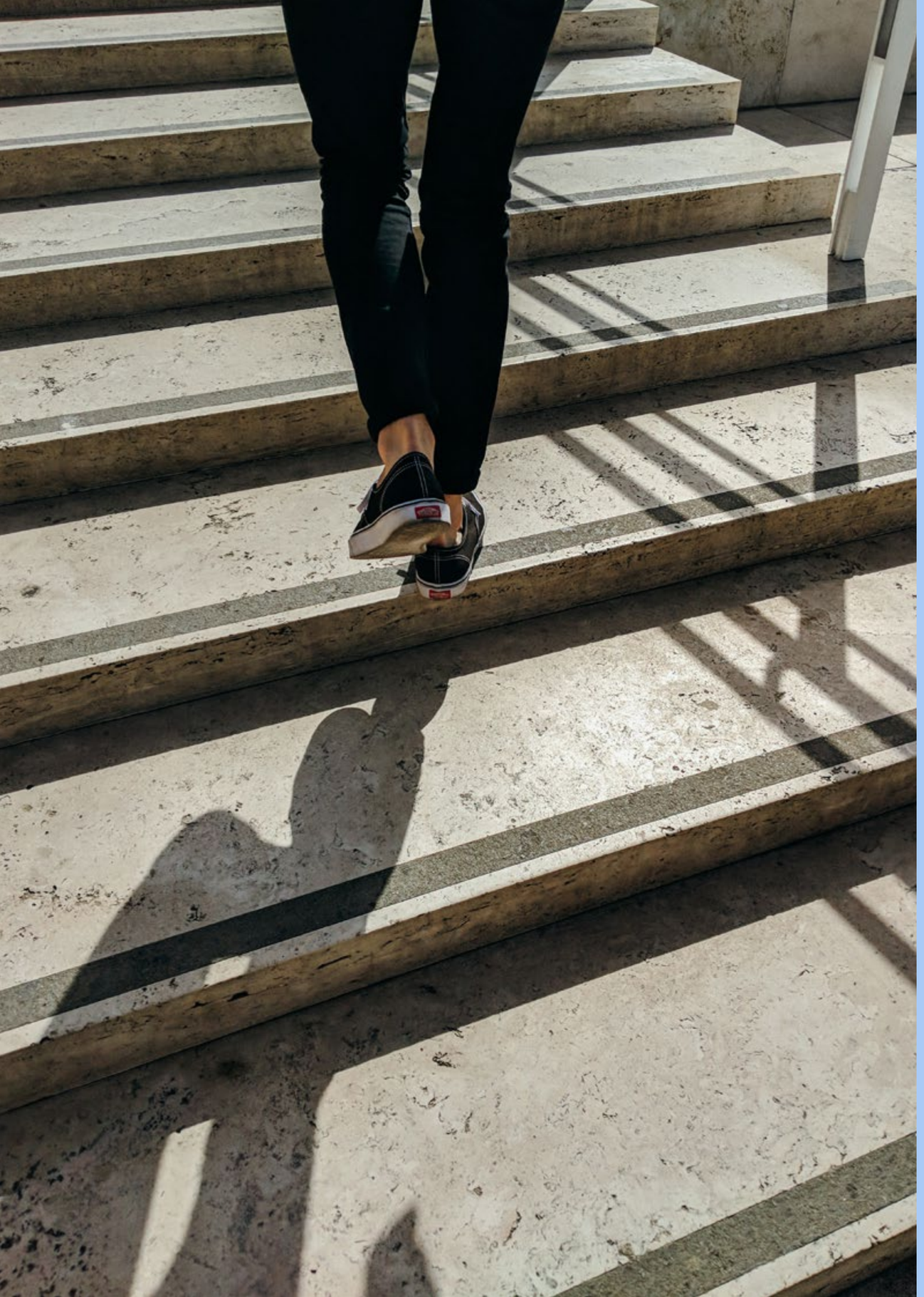
Our next step is to evaluate our system using real data provided by LEAs. We will share our model with them so they can use it in their investigations. To enhance the usability of our system, we aim to incorporate explainable AI methods. These methods will highlight the relevant messages exchanged between the perpetrator and victim in the chat conversations. This feature will help investigators to quickly identify and assess the importance of the classified chat messages. By providing this contextual information, we aim to improve the efficiency and effectiveness of the system in detecting and preventing cyber grooming incidents.

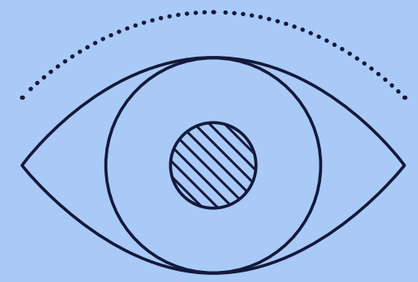
Currently, we are working on creating behavioural tests to assess the performance of our multilingual model. These tests are designed to simulate various linguistic aspects commonly found in cyber grooming conversations. The goal is to determine whether our model can accurately identify and capture these specific linguistic features. By translating these tests into multiple languages, we can systematically evaluate the model's ability to recognise these linguistic properties across all four languages being studied. This process will provide valuable insights into the model's effectiveness and language coverage in detecting cyber grooming behaviour.

[20] https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting-major-findings/

[21] https://www.nspcc.org.uk/about-us/news-opinion/2020/instagram-grooming-crimes-children-lockdown/

[22] http://www.perverted-justice.com/





CHAPTER 08

The Way Forward

Why the growing stream of reports can also be seen as an opportunity to improve in the future.

THE FUTURE OF AVIATOR

The way forward

Reporting is an important instrument to gain insight into the size and nature of the CSAM problem: to understand where and how CSAM material is shared and to monitor developments in the underlying abuse modus operandi and the technology that is used to facilitate and share CSAM.

With that knowledge, barriers can be created to prevent the spread of CSAM, perpetrators can be identified and arrested, and victims can be safeguarded to prevent further abuse.

This second annual report shows that the number of CSAM reports will continue to rise sharply in the coming decade. Not only because of the growing stream of reports from NCMEC, but also because of future reports in response to the upcoming EU Regulation and the arrival of the EU Centre.

The fact that the number of reports is increasing is partly because the abuse and sharing of CSAM is growing, and with it the number of victims and perpetrators. There are hundreds of millions of children who will take their first steps in the online world in the coming decade, at an increasingly younger age. Although this generation will hopefully have more and more resilience and will apply the lessons learned together with their parents and environment to be safer online, we are currently seeing an increase in self-generated CSAM and sextortion. Potential offenders will continue to have plenty of opportunities to approach these children and will keep using the internet to share CSAM material and encourage abuse.

On the other hand, the expected growth in the number of reports is caused by new detection and reporting rules in Europe and other regions, a growing number of parties reporting to NCMEC and improved detection capabilities.

Where the growing stream of reports is often seen as a problem, we at AviaTor would like to turn this into an opportunity. An opportunity for even better insight into what is happening, even better intelligence to make the right decision for prioritisation, investigation, prevention, and policy.

But that is only possible with the right tools, agreements, cooperation, and capacity in place. The AviaTor team is determined to make an important contribution to this in the coming years.

We see it as our role to provide LEAs with the right tools to efficiently process their CSAM reports and extract information that delivers maximum impact. We have learned that we must start with simple tools that work well and support the daily work of our users. As we improve these tools and learn more about the workflows of our users, we integrate more innovative techniques, like AI and OSINT. Together, this creates a strong and durable combination for the future.

Artificial Intelligence (in the form of image, video, and text analysis) helps us to assist the human user to work even more efficiently and to cope with the growing number of reports. But it also helps to reduce contact with the burdensome material, and to discover connections that are impossible for a human to find manually.

While the possibilities of AI will continue to expand in the coming years, it is very important within the domain of CSE to pay full attention to the trustworthiness of the AI techniques we use.

Also, we see that generative AI is used by perpetrators to generate sexual abuse imagery of existing and/or fictive children. We need to develop insights and legislation for this material and explore (AI) techniques that allow LEA to discriminate between actual abuse and AI-generated content.

Crime, CSAM, perpetrators, and victims are online. All reports in AviaTor come from parties that offer services on the internet. Therefore, it is essential to have the online context of a report in order to make the right decisions. Open Source Intelligence will allow users to find connections, assessing risks and discovering clues for identifying perpetrators and victims and prioritising the work. It is our strategy to give AviaTor users even better access to AviaTor's OSINT capabilities and to continue to develop support for new online environments, in line with their national legislation.

Although AviaTor is a stand-alone tool that runs on-premises at each member state, we believe that AviaTor facilitates collaboration in many ways. AviaTor as a tool is a landing place for sharing best practices and developing standards. Technical partners, legal experts and LEAs work together in the AviaTor team. With them, and with future partners such as the EU Centre, we discover which problems we have to solve today and which challenges we need to address for tomorrow, and where the differences and similarities between the member states lie.

Reports that are processed by AviaTor have already come a long way: they are created by ESPs, reported to NCMEC, then send to the LEA (potentially via Europol). Cooperation throughout the chain to improve this process has become more important than ever and deserves even more attention in the future. We may soon be able to set a good example here in Europe.

We are working with our partners on a sustainability plan that will support the further development, roll-out, and operation of Aviator after the end of the current ISF-P project.

We are therefore convinced that AviaTor will be one of the important tools for Europe in the fight against online CSAM in the coming decade.

There is no time to waste, we have to act now.

Mathijs Homminga

Founder & CTO of Web-IQ

CHAPTER 09

Meet the Partners

The AviaTor project is unique due to its relatively small team. The project partners have exceptional expertise in their fields, making the development process fast, focused, and agile.

THE TEAM

Meet the Partners

AviaTor is a project that brings together two prominent technological companies specialising in visual intelligence and OSINT, ZiuZ Forensic and Web-IQ. These companies are renowned for their expertise in these fields, and they collaborate to develop the AviaTor tool.

Additionally, AviaTor collaborates with a growing number of LEAs across the EU. Currently, the project is led by National Police of the Netherlands that demonstrate their commitment and leadership in advancing investigative technologies. The Belgian Police are another crucial partner that share their expertise/skills and resources to the project.

In order to further enhance the project's capabilities and legal framework, AviaTor involves an additional legal partner – Timelex. Timelex is highly specialised law firm that brings legal knowledge and guidance to ensure compliance and ethical considerations throughout the project. Another crucial AviaTor partner is DFKI, the AI research centre worldwide that contributes its cutting-edge research and technological advancement to drive innovation. Lastly, INHOPE plays a vital role in addressing online safety issues and promoting cooperation in combating CSAM.

This collaboration between the project partners forms a robust and multidisciplinary team, leveraging their respective expertise to develop AviaTor tool to assist LEAs in combatting illegal online content.

The National Police of the Netherlands

The National Police of the Netherlands are the project lead of the AviaTor project. They have been using AviaTor since the first version in 2019. The NPN is also one of the two main practitioners in the project. As such, they are responsible for defining, prioritising, and approving the functionality that will make AviaTor complete. In addition, they are responsible for composing the data sets needed to train the AI developed in the project and will have IT personnel participating in the development. Their role is crucial as they can provide the partners with the specific knowledge of the challenges at hand from a LEA perspective, and the necessary feedback on the proposed solutions.

The Belgian Federal Police

The Belgian Federal Police have been part of the AviaTor team since the first version in 2019 and are highly involved in the AviaTor project through providing insights and input for the development and testing latest updates. The Belgian Federal Police are the other main practitioner within the project.

ZiuZ Forensic

ZiuZ Forensic develops high-grade products with visual intelligence technology to help innovate forensic investigations. ZiuZ Forensic solutions make a worldwide impact and contribute to solving societal issues by enabling law enforcement agencies to analyse and categorise large amounts of visual data in child abuse investigations.

ZiuZ Forensic works in close cooperation with universities, NGOs, companies, and research institutes. They're constantly looking for new technologies to develop their products and services. Next to traditional pattern recognition and image analysis technologies, they explore machine learning, deep learning, and artificial intelligence technologies.

Web-IQ

To fight online child abuse, human trafficking and fraud, law enforcement agencies and the financial services industry need the best open-source intelligence. Web-IQ provides its partners with leading OSINT solutions to make the world a better place. They believe that law enforcement agencies should have the best online intelligence tools and data available to help them in their fight against serious crimes, thereby making the world a better place.

Web-IQ is an active private sector partner of the Virtual Global Taskforce: the international collaboration of law enforcement agencies, non-governmental organisations, and industry partners to protect children from online and offline sexual exploitation. Their role as development partner within the project is to enrich reports with data other than images/video content (e.g., text-based and online data), develop AI for text analysis and building the user interface.

DFKI – The German Research Centre for Artificial Intelligence

DFKI conducts research on "human-centric AI" in the major ground-breaking areas of AI research and applications with a focus on socially relevant topics and scientific excellence. They are convinced that AI technologies can help in meeting the great societal challenges we face such as man-made climate change, social injustices, and dangerous diseases. As the largest independent AI research centre worldwide, they initiate, realise, and support many activities to develop reliable and trustworthy AI.

In this project, they will advise on the selection and creation of necessary datasets, as well as the use of machine learning approaches.

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

Timelex

Timelex is a leading niche law firm specialising in the legal aspects of information technology (IT), privacy & data protection (GDPR), intellectual property, and media and electronic communications. Every day they strive to match law and innovation. Timelex is an independent law firm operating from the capital of the European Union, working with an extensive network of leading law firms across the globe with similar profiles.

Founded in 2007, Timelex has grown into a leading law firm with strong market recognition. This is illustrated by the fact that they are consistently ranked as a top-tier and leading law firm in international law firm rankings such as Legal 500 and Chambers based on feedback from clients and other national and foreign lawyers. In the framework of AviaTor Timelex, as a law firm, will provide legal advice to the project and selects the most appropriate legal instruments to accommodate effective collaboration.

TIMELEX

INHOPE

INHOPE is the global network of hotlines combatting online CSAM. The network consists of 52 hotlines in 48 countries (as of April 2023) that provide the public with a way to anonymously report illegal content online with a focus on CSAM. Reports are reviewed by trained content analysts who review and classify the reported material. If confirmed illegal, law enforcement agencies will be advised, and a Notice and Takedown order will be sent to the relevant hosting provider so that the content is removed from the digital world as rapidly as possible.

Within the AviaTor project, they are responsible for marketing and communication, website development, creating campaigns, organising the capacity-building events and this annual report. INHOPE provides relevant feedback on the new working process and tooling from an international point of view (regarding the intake of reports through hotlines).

INHOPE

This project was funded by the European Union's Internal Security Fund – Police

The content of this annual report represents the views of the author only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

AviaTor

Annual Report of 2022
by INHOPE Association

Learn more and support us at
aviatorproject.com