HOW CSAM OFFENDERS ARE ADAPTING TO NEW TECHNOLOGY – EPISODE 2

SEASON 4

INTRODUCTION

Carlota: Welcome to Season 4 of "The Europol Podcast," the official podcast of the EU Agency for Law Enforcement Cooperation. This season, we look at the emerging threats and key developments in the field of cybercrime.

Episode 2: "How CSAM Offenders are adapting to new technology." In this episode, we look at how individuals involved in child sexual exploitation are broadening their criminal activities, increasing opportunities for abuse, and making the exchange of material more efficient and lucrative.

To understand how this works, I speak with Danny van Althuis, Head of Team at Europol. He explains how financial sexual extortion continues to surge, detection of AI and challenges it poses for law enforcement, and the importance of victim safeguarding. Our conversation was recorded during a Europol live expert session. Because the live Q&A already took place, it is no longer possible to ask questions. Take a listen.

Hi, everyone. Welcome. It's great to have you here. I'm Carlota, and today we're talking about how offenders involved in child sexual exploitation are adapting to new technology. It's a heavy topic, but it's a very important one, and I'm not doing it alone. I'm here with Danny van Althuis, Head of Team at Europol, and he has more than 10 years of experience working to protect children, victims of child sexual exploitation and abuse. Welcome, Danny. How are you today?

Danny: Thank you very much. I'm doing fine. Thank you.

Carlota: So, before we dive in, for people who've never come across you or your team, could you run us through what your day-to-day is like at Europol?

Danny: Yeah. So, I work at AP TWINS, the Analysis Project Twins within the European Cybercrime Centre, and we are solely focused on the fight against online and offline child sexual abuse cases. So our team consists of 17 people, divided over 4 different sections, and we deliver victim identification support, analysis support, technical support, and strategical support, all in relation to the fight against child sexual abuse material.

Carlota: Okay. Thank you for that overview.

I'm sure everyone's super interested in knowing more about your work, and they'll have lots of questions at the end of the session after your presentation. For everyone who's watching or listening, this session is a part of a series we're running around the IOCTA, which is the Internet Organised Crime Threat Assessment. It's Europol's flagship report on cybercrime. We've been publishing it every year for over a decade, and it's based on operational insights from law enforcement from across the EU and beyond, and it also has input from industry and academia. And one thing that the report shows year after year is that offenders are adapting really quickly. They're often adapting faster than legislation and sometimes even faster than tech companies themselves.

This year's IOCTA report points to a disturbing rise in online sexual exploitation, with offenders leveraging things like encrypted platforms, AI-generated content, and monetisation models to expand their criminal operations. And in a moment, Danny will be discussing these new technologies, the monetisation of child sexual abuse material. We will have around 15 to 20 minutes for the Q&A, so we will try to get through as many questions as we can. And with that being said, Danny, the floor is yours.

OVERVIEW OF ONLINE CHILD SEXUAL EXPLOITATION & MAIN THREATS

Danny: Yeah. Well, thank you for the introduction, and thank you for allowing me to join this deep dive into the online child sexual exploitation chapter of the IOCTA 2026.

In the next 20 minutes, I want to do more than only summarise the chapter, and I want to translate the main developments in a more operational picture. So what is changing, why does it matter for law enforcement, and where the most important opportunities lie for interventions.

And the central message of this chapter is that online child sexual exploitation is evolving into an adaptive criminal ecosystem. New technologies are increasing scale, concealment, and speed, while offenders continue to innovate in how they exploit victims, monetise abuse, and organise online.

In the IOCTA 2026, 4 developments stand out, in particular the continued rise of sexual extortion, the increased monetisation of CSAM, as you mentioned, the growing role of end-to-end encrypted environments, and the expanding use of AI-generated or synthetic child sexual abuse material. And today, for the people who are watching, the key question is not only what offenders are doing. The question is where we can intervene earlier, faster, and more effectively to safeguard children.

And the best way to understand this chapter is to see these developments in a chain or interconnected. And this chain often starts with self-generated sexual material, and that material may be shared voluntarily or under pressure, through manipulation, or in circumstances where a child does not fully understand the consequences. And once an image has been shared, the child loses control over it. It can be copied, redistributed, traded, manipulated, uploaded, and the loss of control that creates leverage. Offenders can use material to demand additional content, money, compliance with increasingly harmful requests.

And at the same time, offenders are increasingly turning child sexual abuse material, or CSAM, into a commodity on platforms, subscription models, cryptocurrency payments, and live distance child abuse services. And that creates new opportunities for financial gain and attracts new types of offenders.

End-to-end encrypted environments facilitate networking, grooming, contact exchange, and migration between platforms where the risks are increasing. And finally, AI adds another layer on top, synthetic child sexual abuse material. It increases volume, complicates triage, creates uncertainty, and the pressure on the victim is then enormous. So this is not a collection of separate trends. It is a connected, exploited ecosystem.

And why does this matter? This chain is describing the way it is driven in 4 different developments, and that is, in our opinion, at this moment, shaping today's threat landscape. It is sexual extortion, increasing monetisation of child sexual abuse material, offender use end-to-end encrypted environments, and the growing availability of AI-generated or synthetic child sexual abuse material.

Each of these developments creates a distinct investigative and safeguarding challenge, but together, they reinforce one another.

They show why online child sexual exploitation can no longer be viewed solely as a content moderation problem.

It simultaneously is a child protection issue, a cybercrime issue, a financial intelligence issue, and a data challenge. And let us look now at each of these developments in a little bit more detail.

SEXUAL EXTORTION AND CONTENT ESCALATION

Sexual extortion deserves particular attention because it's one of the clearest examples on how online harm can escalate very, very quickly. In the IOCTA report that the online distribution of self-generated sexual abuse material continued usually since 2022. Because once shared, again, the child loses control. And even in the initial sharing, it does not start as a criminal process. It can become that because it is the basis of extortion.

We see that the National Centre for Missing and Exploited Children, NCMEC, they give us cyber tips related to financial extortion or sexual extortion has increased over 70% since 2024. And that figure matters because it is demonstrating a scale, a huge scale. This is no longer an isolated phenomenon.

Children may feel overwhelmed, ashamed, and frightened, and they may comply with demands because they believe it's the only way to regain control. But the demands, of course, continues.

And sextortion is a process, not a single incident. It often starts with targeting and contact, then it moves slowly into grooming, content capture, then threatening, in the end, maybe monetisation, and of course, continuous abuse. And this cycle, enabled by common online tools like encrypted messaging, private groups, cloud storage, payment services, and disposable accounts.

And investigators must look beyond the image itself and identify the wider network, infrastructure, and money flows behind all this abuse.

For investigators, the challenge is identifying the extortion process early. Behind every single report may be multiple victims, organised groups, payment trails, or cross-platform activity.

MONETISATION MODELS AND STREAMING PLATFORMS

The second major development that we see is monetisation. And historically, many offender communities were built upon trust, reputation, and status. And the IOCTA highlights a significant shift. Financial gain is becoming increasingly more important, and the report identifies several platforms selling child sexual abuse material in 2025. Some operate even as a marketplace.

Others function as scams, targeting offenders themselves. Either way, they demonstrate how child sexual abuse material is increasingly packaged, advertised, and monetised using models similar like other cybercrime markets.

And a strong example of that is KidFlicks, a child sexual abuse material or streaming material platform, and that was dismantled in 2025. Between 2021 and 2025, it accumulated over 1.8 million registered users and approximately about 80,000 uploaded videos. So again, 1.8 million users and more than 80,000 videos. Users could obtain access through platform activity or cryptocurrency payments.

And the investigation involved authorities from more than 35 countries and resulted in over 1,400 suspects being identified and arrested. And those numbers illustrate both the scale of the problem and the opportunities for disruption, because monetisation creates infrastructure, it creates accounts, payment flows,

subscription, administrations, hosting service, and financial traces. And all of these can generate investigative leads.

The operational takeaway is very simple. Monetisation increasingly links child sexual exploitation to cybercrime, cryptocurrency, and online criminal services, requiring a broader investigative approach.

Live distance child abuse remains an important part of the monetisation picture. It demonstrates that online child sexual exploitation is not only about material that already exists online, it also can evolve real-time orchestration of abuse.

A consumer may be in one country, the facilitator in another country, and the victim in a third country.

And the abuse can occur live, on demand, and repeatedly. And we know that prices for live-streamed abuse sessions can be as low as 15 United States dollars, with victims often abused multiple times a day to maximise earnings.

And we see that EU-based consumers continue to purchase live-streamed abuse involving victims located primarily outside of the EU, although cases involving victims within the EU are also identified.

The Philippines remained a significant hotspot, but the report stresses that victims are likely located in many other countries as well. And for investigators, these cases create a difficult evidential environment. There may be limited stored material, limited traces, and a strong need for a rapid international cooperation if a child or a victim is identified.

And the key point is live-distanced child abuse directly connects to online demand with a physical abuse. The objective is not only to identify consumers, but also to locate and safeguard children as quickly as possible.

ENCRYPTED COMMUNICATION ENVIRONMENTS & CRIMINAL CONVERGENCE

Third major development is the role of end-to-end encrypted messaging applications. And these applications are no longer merely communication tools, they have become offender environments.

They are used for grooming, networking, CSAM exchange, operational coordination, and offender education.

And some encrypted groups function much like dark web forms, providing social structure, reputation systems, access control, and knowledge sharing. They also lower the barrier to entry because offenders do not require specialist technical knowledge or participate. And the groups frequently migrate between different applications, creating a moving target for investigators.

The IOCTA also highlights the COM network as an example of convergence between child sexual exploitation, extortion, cybercrime, and heavy violence.

Many participants are minors themselves, and motivations vary considerably. Some offenders seek sexual gratification. Others are driven by status, belonging, financial gain, ideological influences, or simply the desire to create harm and chaos.

This is important because it demonstrates that not all online child sexual exploitation is driven by traditional offender motivation. In some communities, the objective is influence, reputation, intimidation, or disruption, with sexual exploitation becoming a tool among many.

The grooming process often starts with online spaces frequented by young people, including gaming environments and communities where vulnerable children seek support.

Trust is established before coercion begins. And for investigators, this convergence matters because a CSE investigation increasingly intersects with cybercrime, extortion, and again, cryptocurrency and violent environments.

So the response cannot sit in one silo.

SYNTHETIC CSAM AND GENERATIVE AI

The 4th development, and I already mentioned it, is synthetic child sexual abuse material. AI tools are becoming easier to access and increasingly capable. Investigations involving AI-generated material are already emerging across multiple platforms. Fully synthetic material can be generated from text prompts.

Partially synthetic material can modify genuine images of children.

And the latter creates a particular challenge because a real victim may be altered, sexualised, or placed in a completely different context. At the same time, offender communities are exchanging prompts, technical guidance, and operational security advice to improve the outputs and avoid detection. Specialised sub-fora on the dark web are entirely devoted to the production, distribution, and exchange of this AI-generated material. To give you an example, a dark web board with over 165,000 members exclusive on the training how to use AI to create child sexual abuse. And we find that on laptop after seizures in prompts, low-rank adaption models, and tools to train and refine AI models.

And these fora serve as a knowledge hub where beginners and experts collaborate. And the challenge is not simply that more material is being created. The challenge is the uncertainty. Investigators must determine whether a child is real, whether a child is being altered, where it's in obvious real danger.

And let us be totally clear. Users adapt open source AI models by training them on existing child sexual abuse material, bypassing the built-in safety mechanism to generate realistic AI-generated material.

There is no boundary to fantasy, risking that further increase of hand-on abuse severity that we see happen over the last years.

IOCTA highlights a subscription-based offender community providing access to AI-generated child sexual abuse material. And that case involved approximately 1,500 members, customers from 29 countries, and we identified 273 suspects.

The lesson is clear. AI-generated CSAM is not a technological issue. It is a community issue, a commercial issue, but also an investigative issue.

INVESTIGATIVE CHALLENGES AND KEY GAPS

If we translate the chapter into investigative consequences, 4 gaps stand out. The first is the velocity gap. Offenders can launch, scale, migrate, and adapt faster than traditional investigative and judicial processes. Extortion can escalate within hours. Groups can move between applications, platforms can disappear and reappear, and synthetic material can be produced in volumes.

And the second is a data gap.

End-to-end encryption, short of inconsistent data retention, and jurisdictional barriers and platform migration can delay access to evidence. And by the time a request is made, relevant data may no longer be available, or it is difficult to connect to the right person, device, or account.

Investigators and analysts face more material, including first generation child sexual abuse material, redistributed self-generated material, and synthetic content.

And any time we have to make sure that it is not a real victim that is in real harm.

The 4th is the convergence gap. Online sexual exploitation increasingly intersects with fraud, cryptocurrency, and cybercrime services, and getting more and more involved in extremist communities with violent online networks. And a single investigation can therefore require expertise both in child safeguarding, digital forensics, social media analysis, financial tracing, cyber intelligence, but also behaviour analysis.

And this changes the bottleneck. The question is not simply whether law enforcement can find illegal material. The deeper question is whether law enforcement can extract meaning, identity, evidence quickly enough from a more concealed and fast-moving ecosystem.

INTERVENTION STRATEGIES AND DISRUPTION

So where can we interrupt this chain?

The first intervention points is prevention and victim support. Children affected by sexual extortion often feel shame and fear. They may delay reporting because they think they will be blamed, because they believe that offenders will stop if they just comply.

Clear, accessible support can reduce that isolation, and the IOCTA highlights Help4U,

a platform created by Europol and Centric to support children and teenagers facing online sexual abuse or other harmful online behaviour. It gives guidance to rights, online safety, and practical next steps, and it also supports parents, teachers, and other professionals. And the priority is to identify children who are currently at risk.

The third intervention point is cooperation with online service providers.

Faster referrals, better prevention of data, preservation of data, lawful access where possible, and consistent retention policies can make a difference between a missed opportunity and a safeguarded child.

The 4th intervention point is financial tracing. Monetisation is harmful because it fuels demands, but it also can generate leads. And cryptocurrency payment subscription models, scam sites, hosting arrangement, and payment flows can reveal the networks.

The 5th and the last,

these cases increasingly require investigative work with not only old-fashioned investigators. We need cybercrime specialists, financial intelligence specialists, behavioural analysis experts, and digital forensic teams. We also need prosecutors to be on the topic, platform contacts, and international partners, because no single discipline sees the whole picture as it is alone.

The common threat is speed. The response need to be faster than the offender's ability to coerce a child, move a group, or delete data or generate new material.

Q&A: EMOTIONAL TOLL, VICTIM IDENTIFICATION & AI DETECTION

Carlota: Thank you, Danny. What do you say we go straight ahead to get the Q&A session started?

Danny: Yes, absolutely. Absolutely.

Carlota: So, there's a couple of personal questions I think are a good starting point for the discussion.

Danny: Personal questions?

Carlota: Yes.

Danny: Okay.

Carlota: Well, not too personal, don't worry.

But what is it like to work directly with CSAM material on a daily basis, and how do you cope with the emotional toll of it all?

Danny: Yeah. Yeah. So, as Head of Team, I am in a position where I do not view the material on daily basis. But within the team, there are colleagues whose daily job is absolutely viewing the material. And we try to be as close to each other as possible, so if there is something that is bothering you, there is no boundary or no threshold that you can speak out on that, because everybody realises that there might be a media file that you have to watch to investigate that might trouble you.

Carlota: Mm-hmm.

Danny: And we have a twice a year mandatory resilience assessments, where we speak to professionals. And on the other hand, we have a lot of freedom. So if your day is over in the watching the material, we can decide that, and we have enough other work to do as well. So we have a lot of freedom to move between the investigative on the material itself or do something else.

Carlota: Okay.

And talking more about progress within this field, what does success look like in this line of work? How do you measure it?

Danny: Oh, that's very simple. A safeguarded victim.

Carlota: There's a few questions about the content itself. There's one on synthetic content. In your experience, how much of the synthetic CSAM content is based on real children?

Danny: There are 2 different things to this. So we see existing children being placed in a sexual environment, so child sexual abuse material created by the use of a child. We see fully generated AI material.

But in both situations, we have to realise that the creation of AI-generated material, even if the victim does not exist, you could say, "Okay, the victim does not even exist. Why would you bother?" Because we know that for the creation of this kind of material, the models are trained on existing real child sexual abuse material.

And of course, if there is a non-existing child, it is difficult for us to identify, is it a real child, yes or no? Because in the end, our main focus is still victim-centric. We have to make sure that we are 100% sure that it's not an actual child. And the quality of the material is so good nowadays for the best professionals that we have, and

we host several times a year victim identification task forces where we fly in from all over the world, the world's best victim identification specialist, it's getting increasingly more difficult to identify if something is AI-generated, AI-altered, or a non-existing child.

Carlota: Speaking of AI software, has the profile of suspects producing CSAM changed due to the ease of use and availability of AI?

Danny: Yeah, absolutely. So I think if you go back in time when the first large language models were capable of creating synthetic material in general, so not only CSAM, but if you want to create a synthetic image, you had to do more and more. You had to create better prompts. Now you can go to a community where you can just, yeah, download the prompts, get educated by the people who are on those forums as well.

And we see that the models or the fine-tuning models are getting distributed amongst them also. So you can find well-trained models in seizures of different persons.

Carlota: Okay, yeah.

We have a couple of questions more focused on law enforcement now. How much of the CSAM detection can be automated, and how much of it has to be manually reviewed?

Danny: In the end, we have to determine by a professional if something is child sexual abuse material.

What we do and what we are working hard is to make sure that we can automate the process of clustering and predetermination to make the work of the specialist easier. You can imagine if we have a seizure where we have 1.5 or 2 million media files that we have to assess, that it would be very, very helpful for us to have an automated assessment so that the specialist needs less time to make a final decision whether something is child sexual abuse material or not, and if it consists of the same victim or the same perpetrator. So in the end, it will always be a decision by a human, but technology, of course, increases the speed where the amount of decisions can be made.

Carlota: And regarding the work of researchers, what can the research community do to help stop CSAM? Are there technical challenges faced by frontline investigators?

Danny: Yeah, so we have the network where we work in is very connected. So law enforcement internationally is connected. We work very closely with NGOs. We have a good relationship with researchers, universities all around the world. And in that connection, we try to assist each other in work. And we benefit a lot from universities and from NGOs and other private partners, because in the end, as law enforcement, especially within Europol, we also see the huge value of public-private partnerships. And we do that broad, from financial institutions to the financial intelligence units, but also the universities, the technical universities, and a lot of NGOs with a lot of technical capabilities as well.

Carlota: Working together—

Danny: Yeah, absolutely

Carlota: —in the end, the bottom line.

Danny: Absolutely.

Carlota: And related to that, how can social media intelligence help with CSAM detection?

Danny: ... social media intelligence and the way that you could have technological possibilities on social media platforms.

Carlota: Yes.

Danny: Yeah, so that is evolving. So there is a lot of initiatives on how to make open source intelligence or social media intelligence more beneficial for us. We follow that. We use some of those parts as well. The only thing is that if we want to use a tool on social media, it needs to be compliant with a lot of European data protection rules, because then we would be online. So the social media detection, we are a lot of depending on the information that the social media platforms themself give through NCMEC to the member states. And we assist the member states, at this moment, 26 within Europe, by receiving that referral from NCMEC, which I mentioned in the presentation as well. And then we can enrich that data for the member state, and then we send the referral out to the member state.

Carlota: Yeah. And speaking of kind of social media environments, online environments, you mentioned gaming in your presentation, gaming platforms. Do you see any special developments in the gaming environment, and how can gaming environments be made safer? What advice would you have for gaming companies?

Danny: So predators are there where they think they can attract children. And that was even before there was social media or the internet. People were working in swimming pools, working in kindergartens. We see all these different things from the past as well. So there is nothing different in that. The only thing is the amount of possibilities are increasing because now you can go to a chat room within a game or within a gaming platform, and you will not only have 10 children to try to talk to, you have maybe 100 or 200 or maybe 1,000 children that you can try to talk to and try to groom and try to lure into your fantasy. And I think gaming platforms do realise that and have to keep realising that as well, and to make sure that there's a proper age control so that there is no need for an adult speaking to a unknown minor. And also, the moderation, I think in the end, they are also responsible that some things should not be possible to discuss within that communication environments that they create.

Carlota: Yeah, I agree.

So let's go a bit more into the modus operandi questions. How much are these developments driven by access to encrypted chat tools and/or the dark web?

Danny: Yeah, both. So the first big adaption, of course, was adapted to the dark web, the Onion router, for instance, where it became more easy to use the Tor network because it was just an executable that you could easy install on whatever platform you are. And that makes, of course, the anonymity bigger. Then the chat applications started to move towards end-to-end encryption, and that means that it is now even easier to do it from your phone because a lot of those applications are end-to-end encrypted. So we see that move. In the past, we saw a group of perpetrators solely focusing on what we called in the dark web, and we had a distinction between the people who start using the end-to-end encryption platforms. Now we see intersections. We see people move from one place to the other place and also very easily change between the different platforms. As soon as they have the idea that something might not be safe or there is any risk, they just move to a new platform.

Carlota: Yeah.

We have another question about the live streaming of CSAM from the criminal law perspective. How does Europol tackle this type of offence?

Danny: Yeah. So Europol itself supports countries in their investigations, in whatever investigation concerning, in our area, between crimes against children. So that means that we try to facilitate as good as possible all information, all intelligence that can lead to the identification of a facilitator in the country where the abuse takes place, or to the perpetrator in whatever European member state or third-party country as it is. But at the same time, we are also developing future possibilities, because in the end, if you would have a good view on what possibilities there are in, like, what kind of payment flows there are, we try to identify that as well. So we cooperate very well with financial institutions to see if there is possibility for those financial institutions to identify red flags within their payment system, because they have due diligence to do anyway. Also to give those referrals to the financial intelligence units to law enforcement. And we play a, I call it a role, that we would receive that information, enrich that information, and then disseminate it to the countries where the information needs to be.

Carlota: Speaking of help for different countries, we have a question from someone who's seen the Help4U website, says it looks great.

Danny: Thank you.

Carlota: What if the kid that needs help is not from one of the listed countries inside Help4U?

Danny: Yeah. So Help4U at this moment is expanding. So, at this moment, I think we have added X countries only this year. So, as far as Europol concerns, this is not a Europe-based website. And there's a lot of communication ongoing at the moment to start to have the website Help4U also being available for children in other countries. The only thing is that we have to make sure that everything is then also precisely tailored, because it's not only translation in a language. We also have to make sure that if you get guidance, that the guidance is correct. If guidance changes in a country, you have to be sure that if a child gets a report, you can get your help here, that that link is actually still working. So, we do it carefully because we want to make sure that if you follow a guideline, that the guideline is good, but we try to onboard as many countries as possible. And at this moment, we are working at least with 12 countries who have already shown interest to be a part of the Help4U ecosystem.

Carlota: That's great.

Danny: Yeah.

Carlota: The more it grows, the better.

Danny: Oh, yeah. Absolutely.

Carlota: Speaking of working together, how can law enforcement agencies adapt their investigative techniques to counter AI-generated CSAM?

Danny: Yeah, that is the 1 million-dollar question. It's a very good question. So, we do a lot of international cooperation. So Europol at itself, its sole purpose is to collaborate internationally. So that's why we have these 44 nationalities and these 50 agencies within this one building in The Hague. So we work a lot together. We see each other a lot online in instances where we do sprints on huge data sets to determine whatever crime area handled within this building. And that also means that we have proper channels. Without going too deep in that, of course, you can imagine we have proper channels where also on the technical side of our work, we collaborate very well. So, to give you an idea, within AP TWINS, we have also the technical section, as I said. Within the technical section, we have development capacity. So not only the forensic, the old-fashioned computer forensic capacity, we also have development capacity. And that means that that development

capacity collaborates with their network in the international community, but also with universities, also with NGOs who have also those capabilities to get the most out of technological possibilities. So we do that, but to go in depth on what we are exactly doing is not the right platform at this moment.

Carlota: Okay. So, we're coming to the end of the time we have for this, so this is the last question.

Danny: Yeah.

Carlota: I want to end with this one. Given the critical role of voluntary detection by online platforms and identifying and reporting CSAM, what safeguards are needed to protect children right now?

Danny: Can you rephrase that, please? Sorry.

Carlota: Given the critical role of voluntary detection by online platforms in identifying and reporting CSAM, what safeguards are needed to protect children?

Danny: Yeah. So, for us, as crimes against children investigators, we are responsible for the safety, security, and future of children. They don't have the ability to make the proper decision once they get a friend request or a chat request or whatever. So I think us as adults, including the people who are developing and maintaining social media platforms, have to make sure that there is proper safeguards within the technology, within the platforms that they have. So, it is safety by design, privacy by default. So no reason to talk with somebody who is an adult who is not within your family circle, for instance. I think proper age verification could be there. And in the end, have some form of detection of unwanted behaviour within your platform. Because in the end, there is no social media platform who wants to create a location where their platform can be used for criminal activity in general. So I think there's a very good reason for a platform itself to have some kind of detection if something is criminal. And I think that should be the main message. We are, as adults, responsible for safety and the possibility for every child to grow up without violence, sexual violence, or whatsoever.

WRAP-UP

Carlota: Thank you.

You've heard all about how CSAM offenders are adapting to new technology as highlighted in our annual Internet Organised Crime Threat Assessment Report. If you would like to know more about the key cyber threats affecting the EU, including child sexual abuse material, ransomware, and online fraud schemes, you can listen to all the episodes of this season on whichever platform you use. And if you liked the episode, consider giving us a like, subscribing, or sharing the podcast with others. You can find links to the Internet Organised Crime Threat Assessment, or IOCTA Report, and the other resources mentioned in the show notes. Thank you very much for listening. We will see you soon.

Note: This transcript was generated using automated transcription technology and edited for accessibility purposes. It may contain minor errors or inaccuracies.