ERA
european.law

Preventing Child Sexual Abuse

Role of law enforcement agencies and the internet industry

Tallinn, 21-22 October 2021

UP GRADE
YOUR LEGAL EXPERTISE

Criminal Law

Professional Training (CPD)
www.era.int

Speakers & Chairs

Laviero Buono, Head of European Criminal Law, ERA, Trier

Rainer Franosch, Prosecutor, Deputy Director-General for Criminal Law and Criminal Procedure, Wiesbaden

Catherine Garcia-van Hoogstraten, Director, Responsible Technology, European Government Affairs Corporate, External and Legal Affairs, Microsoft, Brussels

Jaroslaw Konczyk, Criminal Investigator, Human Trafficking Department, National Police Headquarters, Warsaw

Eneli Laurits, District Prosecutor, Estonian Prosecutor's Office, Tallinn

Tuuli Lepp, Counsellor for Justice Affairs, Permanent Representation of Estonia to the EU, Brussels

Mick Moran, Garda Liaison Officer, Irish Embassy, Paris

Taavi Pern, Chief State Prosecutor, Estonian Prosecutor's Office, Tallinn

Karin Talviste, State Prosecutor, Estonian Prosecutor's Office, Tallinn

Nina Vaaranen-Valkonen, Executive Director, Senior Specialist, Psychotherapist Suojellaan Lapsia ry/Protect Children

Margus Veem, Psychologist, Personal Rehabilitation Programme, Viljandi County Hospital

Celine Verheijen, Project coordinator children´s rights and sexual exploitation, Defence for Children /ECPAT The Nederland, Amsterdam

Régis Villette, Head, French National Centre for Victim Identification on Child Sexual Exploitation Material Analysis, Ministry of Interior, Caserne Lange, Pontoise

Samantha Woolfe, Global Partnerships and Development Manager, INHOPE, Amsterdam

With the support of the Internal Security Fund – Police Programme 2014-2020 of the European Union

Key topics

- European and international legal instruments to fight child sex abuse material
- Measures against advertising abuse opportunities and sexual exploitation of children in travel and tourism
- Preventive intervention programmes or measures
- Intervention programmes or measures on a voluntary basis in the course of or after criminal proceedings

Language
English

Event number
321DT37f

Organiser
ERA (Laviero Buono) in cooperation with the Estonian Prosecutor's Office

www.era.int

PREVENTING CHILD SEX ABUSE

Thursday, 21 October 2021

08:30 Arrival and registration of participants

09:00 Welcome and introduction to the programme
Taavi Pern & Laviero Buono

I. INTRODUCTORY SESSION

09:05 **Fighting child sex abuse: an overview of the legislation and policy in place**
Tuuli Lepp

09:30 **Online child abuse and travelling child sex offenders: what is the link, what has been done by the travel and tourism sector and why are people reluctant to report?**
Celine Verheijen

10:00 Discussion

10:15 **Work carried out by the law enforcement authorities to prevent child sexual abuse**
Régis Villette

11:00 Discussion

11:15 Coffee break

Chair: *Régis Villette*

11:45 **Child sexual abuse online: the work of international organisations raising awareness, reducing the risks and removing the content**
Samantha Woolfe

12:30 Discussion

12:45 Lunch

II. LAW ENFORCEMENT AGENCIES' EXPERIENCES WITH REGARD TO THE PREVENTION AND THE FIGHT AGAINST CHILD SEX ABUSE MATERIAL

Chair: *Samantha Woolfe*

14:15 **Investigations in the darkweb to detect child sexual abuse material**
Rainer Franosh

15:00 Discussion

15:15 **Victim identification efforts based on analysis of child sexual abuse material**
Jaroslaw Konczyk

15:45 Discussion

16:00 Coffee break

Chair: *Laviero Buono*

16:30 **Preventing child sexual abuse material: experiences in Estonia**
Eneli Laurits

17:15 Discussion

17:30 End of the first day

19:30 Dinner

Objective

Online child sexual exploitation is a constantly evolving phenomenon and is shaped by developments in technology. Mobile connectivity and the development of pay-as-you-go streaming solutions, which provide a high degree of anonymity to the viewer, are furthering the trend in the commercialisation of child sexual abuse material.

This seminar aims to assess and debate legal measures to prevent and combat the production, processing, possession and distribution of child sexual abuse material on the internet. Particular emphasis will be placed on the dialogue between law enforcement agencies and the internet industry.

Who should attend?

Judges, prosecutors, lawyers in private practice, law enforcers, ministry officials and representatives of victims' support and children's rights organisations from Estonia, Latvia, Lithuania, Sweden and Finland ("Regional approach")

Location

Hotel Europa
Paadi Street 5
10151 Tallinn
Estonia

Participation fee

€ 140

Your contacts

Laviero Buono
Head of Section
E-Mail: LBuono@era.int

Liz Greenwood
Assistant
E-Mail: egreenwood@era.int
Tel.: +49 (0)651 9 37 37 - 322

Friday, 22 October 2021

III. PREVENTING AND FIGHTING CHILD SEXUAL ABUSE MATERIAL: THE ROLE OF THE PRIVATE SECTOR

Chair: *Karin Talviste*

09:30 **Cooperation between law enforcement authorities and the internet industry to fight child sexual abuse: case studies**
Mick Moran

10:15 **Leading technical solutions to prevent and combat child sexual abuse**
Catherine Garcia-van Hoogstraten

10:45 Discussion

11:00 Break

IV. INTERVENTION PROGRAMMES OR MEASURES ON A VOLUNTARY BASIS IN THE COURSE OF OR AFTER CRIMINAL NATIONAL PROCEEDINGS

Chair: *Laviero Buono*

11:30 **Dark Web investigations in child sexual abuse material**
Nina Vaaranen-Valkonen

12:00 **Preventing and minimising the risks of repeated offences of a sexual nature against children: experiences to share**
Margus Veem

12:30 Discussion

12:45 End of seminar and lunch

For programme updates: **www.era.int**
Programme may be subject to amendment.

Apply online for this seminar:
www.era.int/?130869&en

About the project

This seminar is part of a large-scale project sponsored by the European Commission under the “Internal Security Fund – Police” Programme. It consists of six events to take place in Lyon, Tallinn, Cracow, Zagreb, Trier and Lisbon.

CPD

ERA programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). This event corresponds to **8 CPD hours**.

This programme has been produced with the financial support of the Internal Security Fund – Police Programme 2014-2020 of the European Union.

The content of this programme reflects only ERA’s view and the Commission is not responsible for any use that may be made of the information it contains

More information at:
www.era.int

Apply online for

PREVENTING CHILD SEXUAL ABUSE

Tallinn, 21-22 October 2021 / Event number: 321DT37f/eg

Europäische Rechtsakademie
Academy of European Law
Académie de Droit Européen
Accademia di Diritto Europeo

Terms and conditions of participation

Selection

1. The number of places available is limited (40 places). Participation will be subject to a selection procedure. Selection will be first come first served and according to nationality.
2. This Project implements a "regional approach", hence this event is only open for participants from Estonia, Latvia, Lithuania, Sweden and Finland.
3. Applications should be submitted before **15 September 2021**.
4. A response will be sent to every applicant after this deadline. **We advise you not to book any travel or hotel before you receive our confirmation**.

Registration Fee

5. €140 including documentation, lunches and dinner.

Travel expenses

6. Travel costs up to €350 (if your place of work is more than 100km from the venue) can be reimbursed by ERA upon receipt of the original receipts, tickets, boarding passes, invoices after the seminar. Participants are asked to book their own travel and accommodation. These rules do not apply to representatives of EU Institutions and Agencies who are supposed to cover their own travel and accommodation. Participants are advised of the obligation to use the most cost-efficient mode of transport available and to read the travel reimbursement information sheet carefully.

Accommodation

7. Maximum 2 hotel nights can be reimbursed by ERA, only upon receipt of the original hotel invoice, up to €110.00 per night including breakfast, if your place of work is more than 100km from the venue.

Other services

8. Two lunches, beverages consumed during the event and the seminar documents are offered by ERA. One dinner is also included.

Participation

9. Participation at the whole conference is required and your presence will be recorded.
10. A list of participants including each participant's address will be made available to all participants unless ERA receives written objection from the participant no later than two weeks prior to the beginning of the event.
11. The participant's address and other relevant information will be stored in ERA's database in order to provide information about future ERA events, publications and/or other developments in the participant's area of interest unless the participant indicates that he or she does not wish ERA to do so. A certificate of attendance will be distributed at the end of the conference.

Apply online for "Preventing Child Sexual Abuse":

www.era.int/?130869&en

Venue

Hestia Hotel Europa
Paadi Street 5
10151 Tallinn
Estonia

Language

English

Contact Person

Liz Greenwood
Assistant
egreenwood@era.int
+49 (0)651 9 37 37 - 322

An overview of the EU legal and policy instruments to fight child sex abuse

Tuuli Lepp

Counsellor for Justice Affairs

Permanent Representation of Estonia to the EU

21.10.2021, Tallinn, Estonia

With the support of the Internal Security Fund-Police Programme
of the European Union 2014-2020

1

Content

What is already there?

- (UN Convention on the rights of the Child)
- CoE Lanzarote Convention
- Directive 2011/93/EU
- Council Conclusions from 2019
- EU strategy for a more effective fight against child sexual abuse 2020-2025
- Connected legislative instruments and policy documents

What is yet to come?

- New instruments

2

Council of Europe Lanzarote Convention

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention; CETS 201)
- Adopted in Lanzarote, Spain in 2007, entered into force in 2010
- All 47 Council of Europe Member States are parties to the Convention (+Tunisia)
- Holistic response to sexual violence against children through prevention, protection, prosecution and promotion of national and international cooperation
- The Lanzarote Committee:
  - monitoring the implementation of the Convention
  - recommendations
  - capacity-building activities (study-visits, conferences etc.)

3

Directive 2011/93/EU

- Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (OJ L 335, 17.12.2011.) "Child Sexual Abuse Directive".
- The first comprehensive EU legal instrument:
  - establishing minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children and child sexual abuse material,
  - covering the prevention,
  - investigation and prosecution of offences, and
  - assistance to and protection of victims.

4

Directive 2011/93/EU

- Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (COM/2016/0871)
- Report assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (COM/2016/0872)

Council Conclusions of 8 October 2019 on combatting the sexual abuse of children

- *12. The Council considers industry, and in particular online platforms, to be a key contributor to preventing and eradicating child sexual abuse and exploitation, including the swift removal of child sexual abuse material online. Notwithstanding current efforts, the Council notes that more must be done to counter technical, legal and human challenges that hamper the effective work of competent authorities.*
- *13. The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law. Furthermore, cooperation between national law enforcement authorities, Internet providers, Europol and Interpol should be intensified in accordance with the applicable legal framework, for instance by devising mechanisms for the encrypted exchange of information. This could allow for continuous monitoring of the network for identifying and blocking sites containing the sexual exploitation of children and placing them on the lists of forbidden sites. In particular, the Council emphasises the importance of ensuring that new technological developments do not adversely impact on the ability to block child sexual abuse material online. In this regard, the Council urges industry to engage with relevant stakeholders as appropriate.*
- The Council invites online service providers to remove or disable access to contents identified as child sexual abuse material online as soon as possible after becoming aware of such content. It calls on the Commission to propose measures to address this growing challenge. (p 14)
- Council recognises the necessity of setting out a multi-stakeholder approach and invites the Commission to consider further action to support prevention-related initiatives. (p 15)

EU strategy for a more effective fight against child sexual abuse 2020-2025

- Comprehensive response to the growing threat of child sexual abuse both offline and online, by improving prevention, investigation, and assistance to victims.
- Includes 8 initiatives to put in place a strong legal framework for the protection of children and facilitate a coordinated approach across the many actors involved in protecting and supporting children.
- The key actions to be taken:

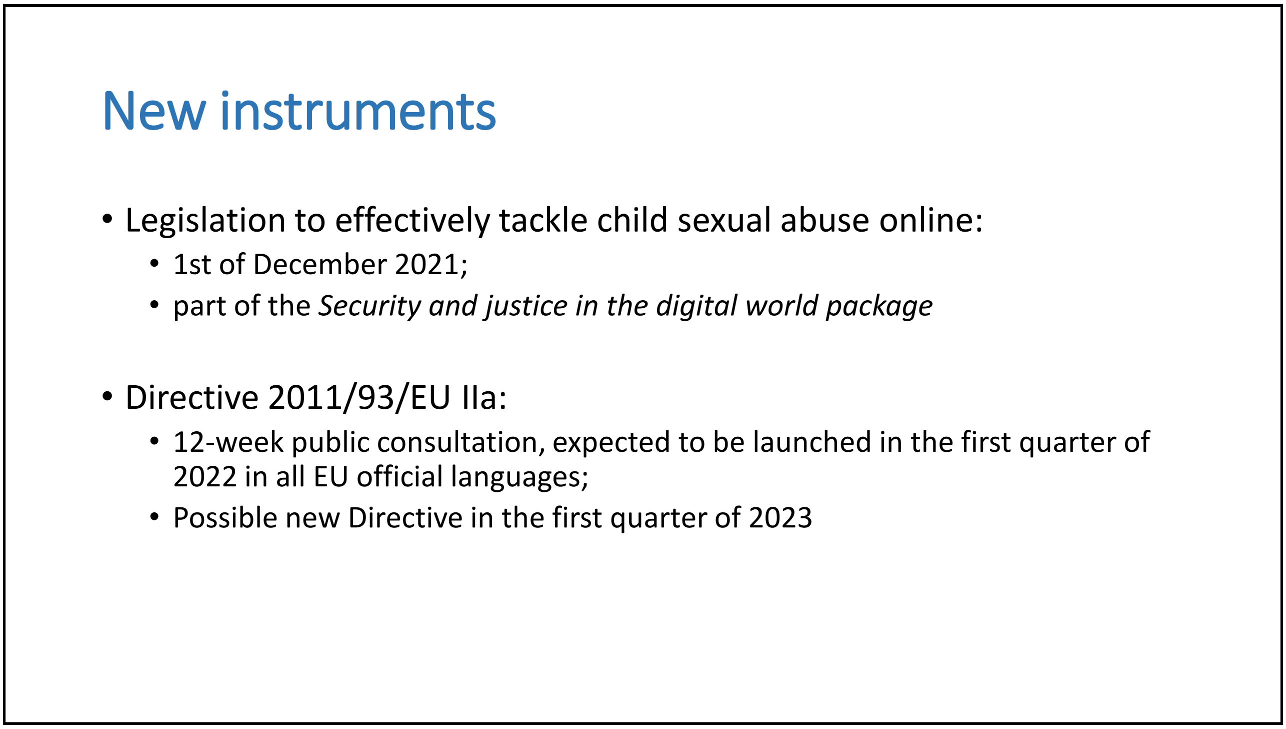
  1. ensure complete implementation of current legislation, notably Directive 2011/93/EU;
  2. ensure that EU laws enable an effective response;
  3. identify legislative gaps, best practices and priority actions;
  4. strengthen the law enforcement efforts at national and EU level;
  5. enable EU countries to better protect children through prevention;
  6. establish a European centre to prevent and counter child sexual abuse;
  7. galvanise industry efforts to ensure the protection of children in their products;
  8. improve protection of children globally through multi-stakeholder cooperation.

7

Connected legislative instruments and policy documents

- EU Security Union Strategy COM/2020/605
- European Strategy for a Better Internet for Children COM/2012/0196
- Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime
- European Parliament Resolution of 26 November 2019 on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child
- 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
- e-evidence proposals (COM/2018/225 and COM/2018/226)
- retention of telecom data

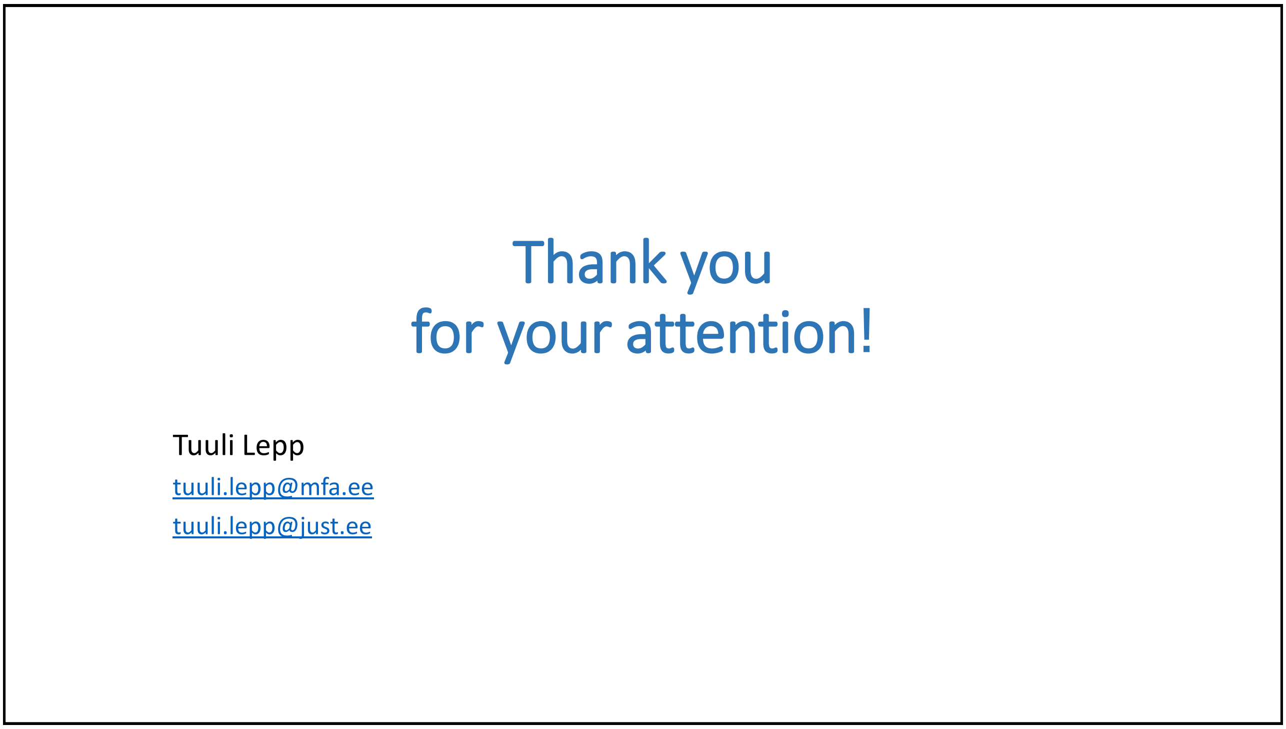
8



New instruments

- Legislation to effectively tackle child sexual abuse online:
  - 1st of December 2021;
  - part of the *Security and justice in the digital world package*
- Directive 2011/93/EU IIa:
  - 12-week public consultation, expected to be launched in the first quarter of 2022 in all EU official languages;
  - Possible new Directive in the first quarter of 2023

9



Thank you for your attention!

Tuuli Lepp

tuuli.lepp@mfa.ee

tuuli.lepp@just.ee

10

DEFENCE for CHILDREN

With the support of the Internal Security Fund-Police Programme
of the European Union 2014-2020

Online child sexual abuse and travelling child sex offenders

Celine Verheijen
Defence for Children-ECPAT Netherlands

ERA Professional Training
21 October 2021

DON'T LOOK AWAY

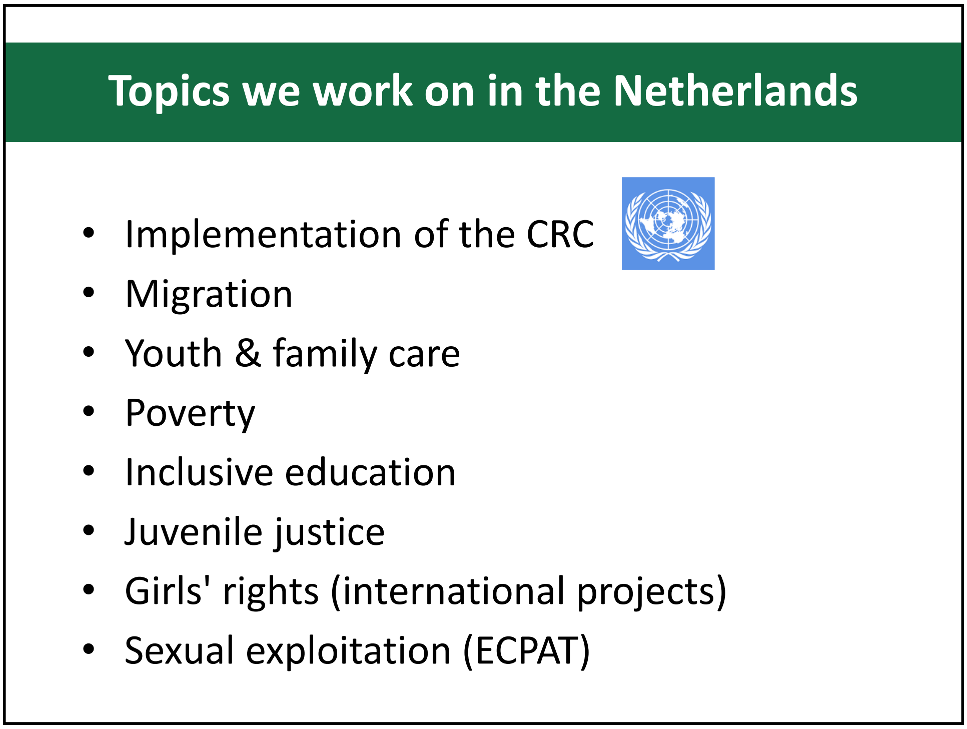
MELD!

1

Defence for Children - ECPAT

DEFENCE for CHILDREN

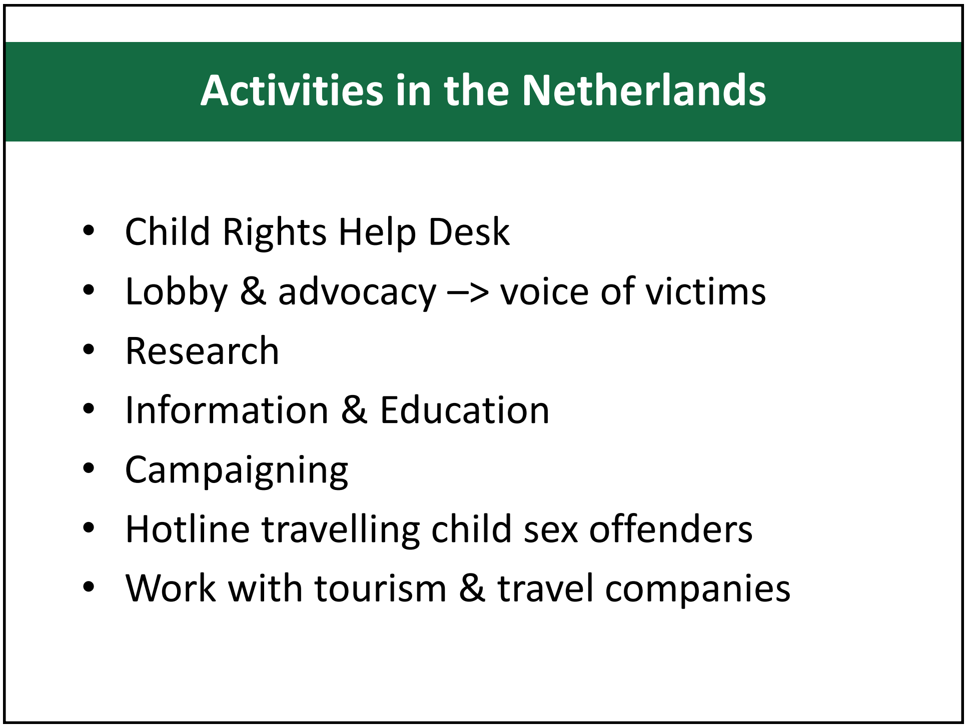
2



Topics we work on in the Netherlands

- Implementation of the CRC
- Migration
- Youth & family care
- Poverty
- Inclusive education
- Juvenile justice
- Girls' rights (international projects)
- Sexual exploitation (ECPAT)

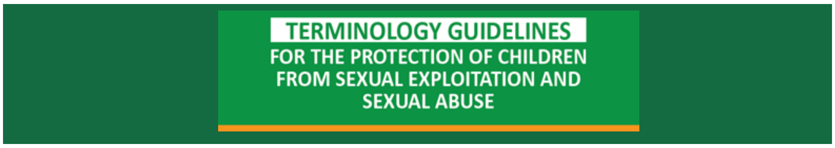
3



Activities in the Netherlands

- Child Rights Help Desk
- Lobby & advocacy –> voice of victims
- Research
- Information & Education
- Campaigning
- Hotline travelling child sex offenders
- Work with tourism & travel companies

4



TERMINOLOGY GUIDELINES
FOR THE PROTECTION OF CHILDREN
FROM SEXUAL EXPLOITATION AND
SEXUAL ABUSE

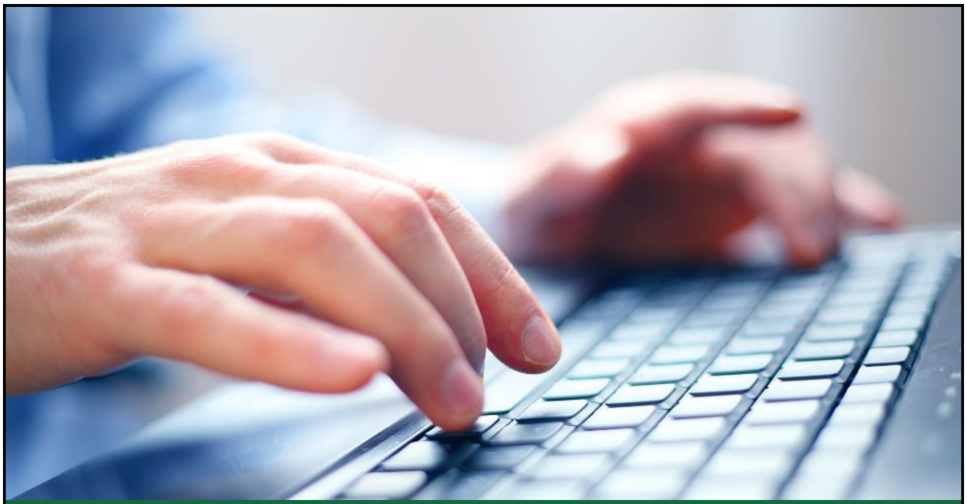
Terms to avoid	Preferable terms
• Child prostitution	• Exploitation of children in prostitution
• Child pornography	• Online child sexual abuse material
• Child sex tourism	• Sexual exploitation of children in travel and tourism

5

Questions for today

- What is the link between online sexual abuse and travelling child sex offenders?
- What is the role of the travel and tourism sector in the protection of children against sexual exploitation?
- Why are people reluctant to report suspicions of sexual exploitation when travelling abroad?

6



LINKAGE BETWEEN ONLINE CHILD SEXUAL ABUSE AND TRAVELLING CHILD SEX OFFENDERS

DON'T LOOK AWAY

7

Linkages

Travelling child sex offenders use the internet:

- To come in contact with potential victims
  - Online grooming
- Record and share material of child sexual abuse
- Continue abuse after they returned home

Social media networks, dating sites, darkweb, livestream

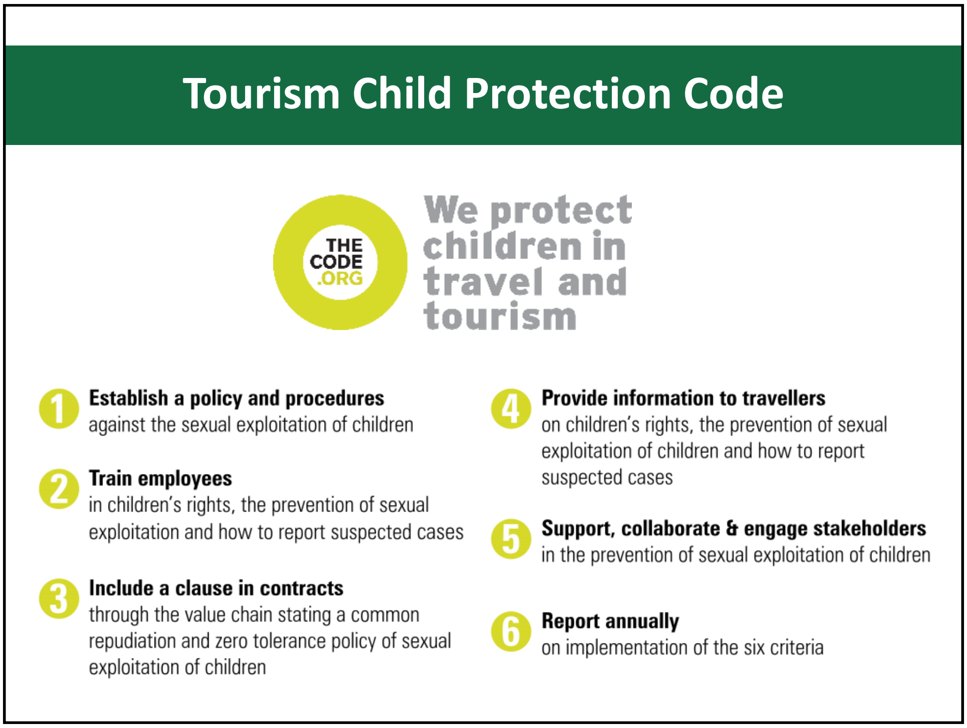
8

ROLE OF THE TOURISM SECTOR

MULTI-STAKEHOLDER COOPEATION

DON'T LOOK AWAY

9



Tourism Child Protection Code

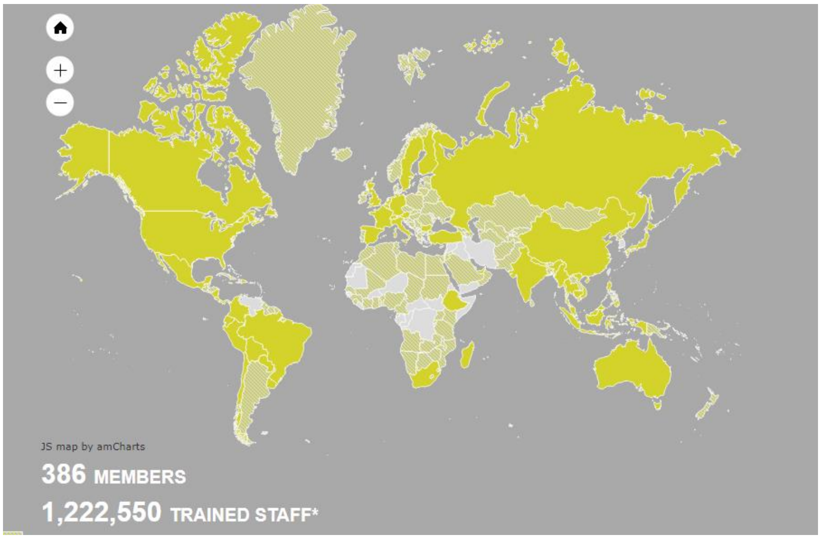
THE CODE .ORG

We protect children in travel and tourism

1. **Establish a policy and procedures** against the sexual exploitation of children
2. **Train employees** in children's rights, the prevention of sexual exploitation and how to report suspected cases
3. **Include a clause in contracts** through the value chain stating a common repudiation and zero tolerance policy of sexual exploitation of children
4. **Provide information to travellers** on children's rights, the prevention of sexual exploitation of children and how to report suspected cases
5. **Support, collaborate & engage stakeholders** in the prevention of sexual exploitation of children
6. **Report annually** on implementation of the six criteria

10

Members



386 MEMBERS

1,222,550 TRAINED STAFF*

11

Some members

ACCORHOTELS Feel Welcome

CARLSON℠ HOTELS WORLDWIDE

Marriott. HOTELS & RESORTS

IHG® Hotels & Resorts

WYNDHAM HOTEL GROUP

RHG RADISSON HOTEL GROUP™

RCD HOTELS

Hilton HOTELS & RESORTS

DELTA AIR LINES

IBERIA

Luxair

easyJet holidays

ABTA Travel with confidence

DRV

Uber

National. ATESA

KUONI

FOX World Travel

DER Touristik

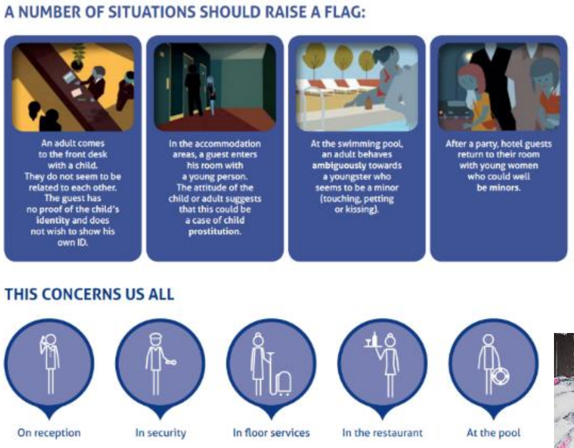
JTB

BCD travel

ITB The World's Leading Travel Trade Show®

12

Accor WATCH Program



A NUMBER OF SITUATIONS SHOULD RAISE A FLAG:

An adult comes to the front desk with a child. They do not seem to be related to each other. The guest has no proof of the child's identity and does not wish to show his own ID.

In the accommodation areas, a guest enters his room with a young person. The attitude of the child or adult suggests that this could be a case of child prostitution.

At the swimming pool, an adult behaves ambiguously towards a youngster who seems to be a minor (touching, petting or kissing).

After a party, hotel guests return to their room with young women who could well be minors.

THIS CONCERNS US ALL

WATCH
We Act Together for Children

PLANET 21
THE ACCOR SUSTAINABLE DEVELOPMENT PROGRAM

Witness of a suspicious situation?
Don't look away, inform one of our employees.

13

Don’t Look Away campaign

- Cooperation between: Ministry, police, tourism & travel sector, ngo’s
- On national levels and international 8 countries: GE, FR, AT, PL, BE, CH, LU, NL
- Goal: Increase cooperation between relevant stakeholders and quantity and quality of reports

14

Online reporting platform

www.dontlookaway.report

17

Research in 5 countries

Literature review

Online survey

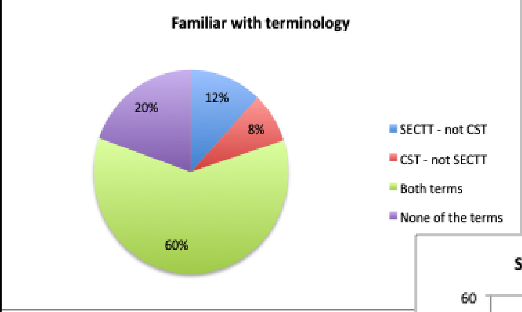
Country	AT	BE	FR	GE	NL	Total
Number of respondents	120	392	134	143	292	1,081

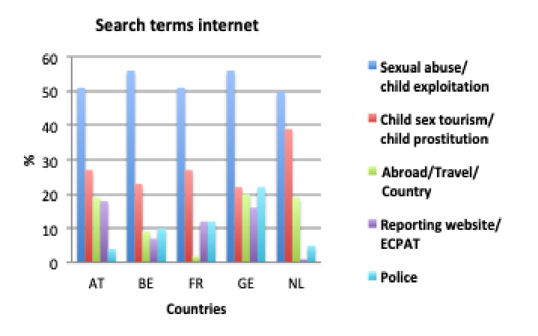
Focus group discussions (90 participants)

- Experts
- Tourism professionals
- Youngsters

18

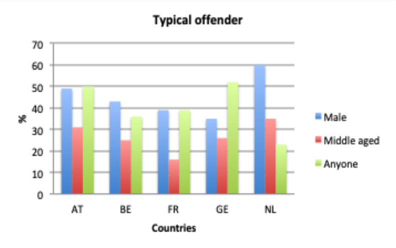
Terminology

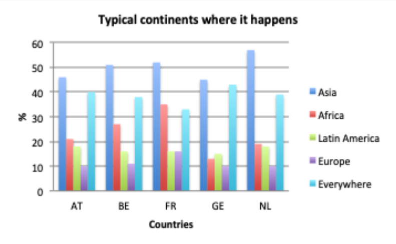


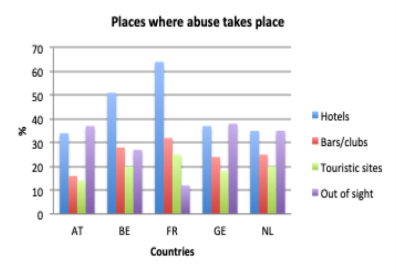


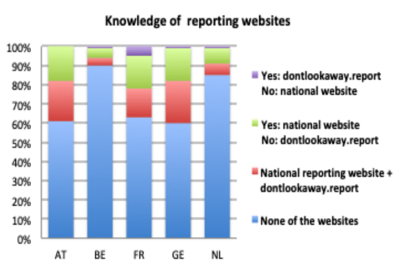
19

Knowledge of the subject









20

Situations witnessed

"A tourist we met was totally insinuating the fact of having an affair with a child."

"There were very young looking girls scantily dressed at a bar that gave massages."

- 22% of the respondents of survey witnessed suspicious situation(s) (N = 183)
- Together they witnessed 250-300 potential victims

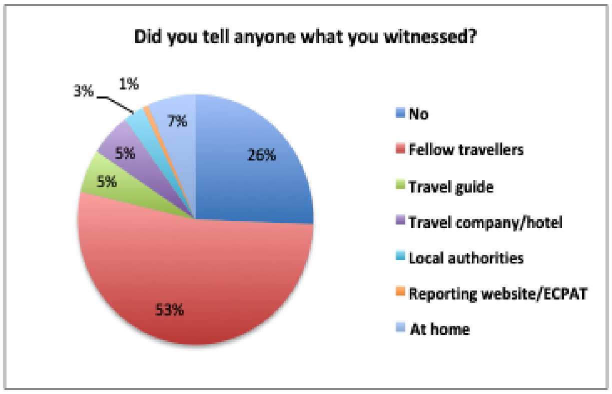
"At the exit of a hotel I saw 2 elderly men hand in hand with 2 young women who seemed minor."

"I saw a Western looking man with a relatively young woman at breakfast in a hotel. The girl was dressed very provocative."

"A man was touching a young girl in an obscene manner in a restaurant. She said: 'you have to wait until we are hidden'."

21

Actions taken



22

Obstacles

- Not being sure, fear of false accusations
- Fear of misinterpretation the situation
- Fear of interfering in someone’s personal life
- Afraid of getting the child(ren) into trouble
- No possibility to report anonymously
- Lack of knowledge on further involvement in the case
- Afraid of getting involved in criminal activities
- Lack of trust that the police will act on the report
- No access to Wifi and forgetting to report later or afraid that it would be too late
- Being in a lazy holiday mode, not interested
- Tourists don’t expect to see this and don’t want to be confronted with this during vacation

23

How to increase reporting?

- Knowing what happens with a report
- Knowing the role of the reporter after reporting
- Examples of success stories
- Possibility to report anonymously
- Confidence that reporting does not mean immediate arrest
- Access to easy reporting possibilities
- Confidence that they will receive feedback after a report
- Knowing that little information can also be useful for the police
- Knowing that it can be reported at police in own country

24

Thank you for your attention!

www.protectingchildrenintourism.org

25

ERA – October 21st 2021

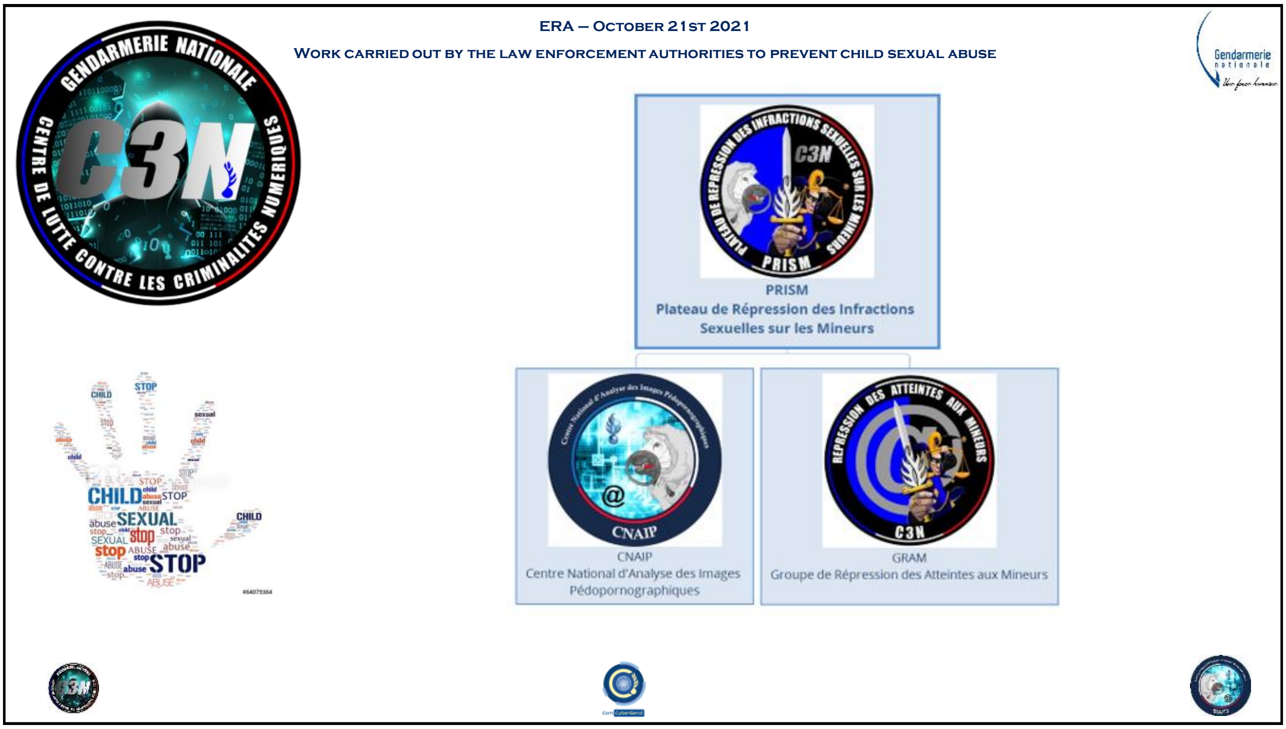
Work carried out by the law enforcement authorities to prevent child sexual abuse

With the support of the Internal Security Fund-Police Programme of the European Union 2014-2020

ERA – October 21st 2021

Work carried out by the law enforcement authorities to prevent child sexual abuse

3



ERA – October 21st 2021

Work carried out by the law enforcement authorities to prevent child sexual abuse

PRISM
Plateau de Répression des Infractions Sexuelles sur les Mineurs

CNAIP
Centre National d'Analyse des Images Pédopornographiques

GRAM
Groupe de Répression des Atteintes aux Mineurs

Gendarmerie nationale
GENDARMERIE NATIONALE
C3N
CENTRE DE LUTTE CONTRE LES CRIMINALITES NUMERIQUES
PLATEAU DE REPRESSION DES INFRACTIONS SEXUELLES SUR LES MINEURS
PRISM
Centre National d'Analyse des Images Pédopornographiques
CNAIP
REPRESSION DES ATTEINTES AUX MINEURS
C3N
CHILD
SEXUAL
ABUSE
STOP

4

PLAN

1/ Child-abuse perpetrators :

1.1 / Overview of various type of child-abuse perpetrators

1.2 / Type of networks

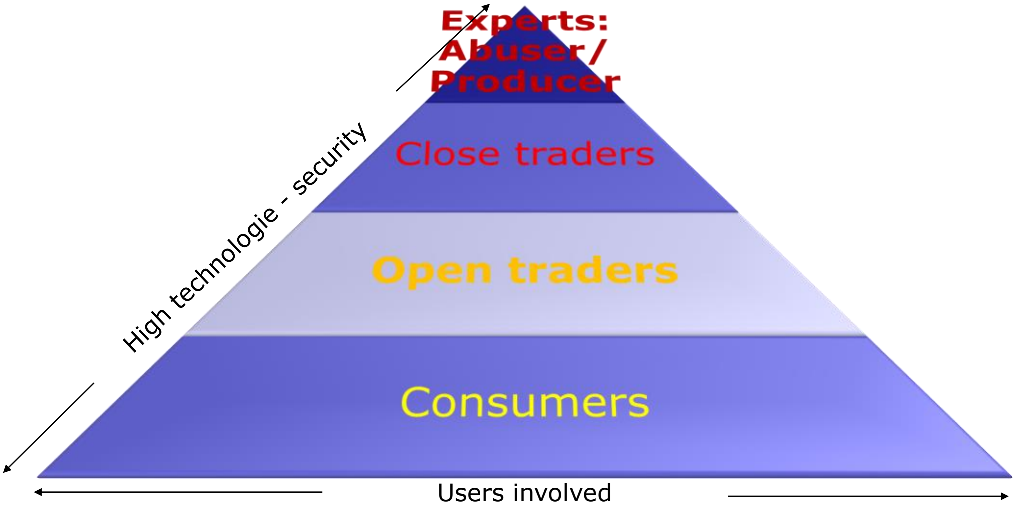
1.3 / Type of victims

2 / 2 types of investigations :

2.1. / focused on tracking perpetrators

2.2 / VID focus

CHILD ABUSE PERPETRATORS

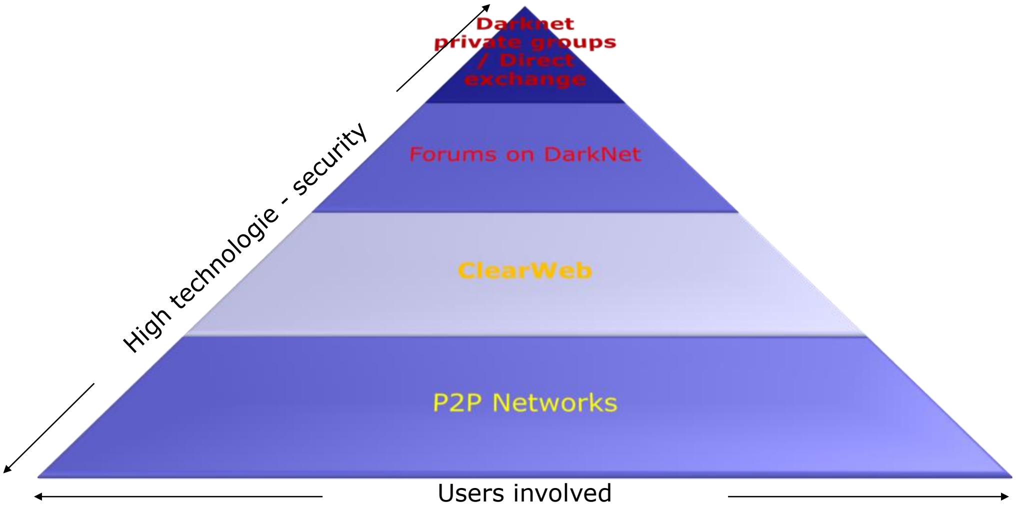


Crédits : Mick Moran

ERA – October 21st 2021

Work carried out by the law enforcement authorities to prevent child sexual abuse

CHILD ABUSE PERPETRATORS


Darknet private groups / Direct exchange
Forums on DarkNet
ClearWeb
P2P Networks
High technologie - security
Users involved

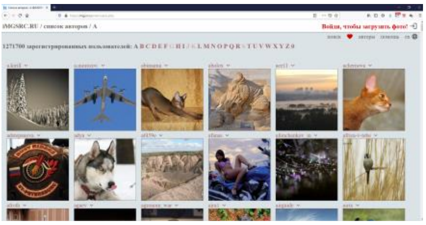
Crédits : Mick Moran

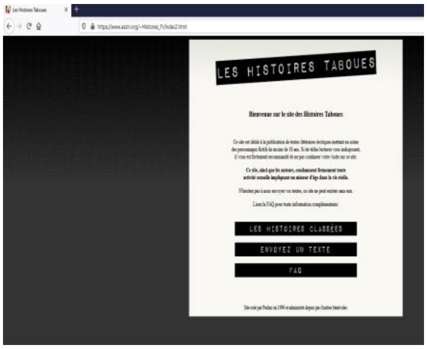
ERA – October 21st 2021

Work carried out by the law enforcement authorities to prevent child sexual abuse

CHILD ABUSE PERPETRATORS

ClearWeb




LES HISTOIRES TABOUES

Bienvenue sur le site des Histoires Taboues

Ce site est dédié à la publication de textes littéraires érotiques mettant en scène des personnages fictifs de moins de 18 ans. Si de telles lectures vous indisposent, il vous est fortement recommandé de ne pas continuer votre visite sur ce site.

Ce site, ainsi que les auteurs, condamnent fermement toute activité sexuelle impliquant un mineur d'âge dans la vie réelle.

N'hésitez pas à nous envoyer vos textes, ce site ne peut exister sans eux.

Lisez la FAQ pour toute information complémentaire.

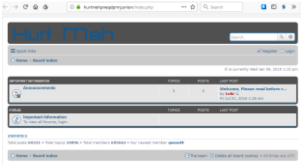
LES HISTOIRES CLASSÉES

ENVOYEZ UN TEXTE

FAQ

Site créé par Pedan en 1999 et administré depuis par d'autres bénévoles.

DarkWeb

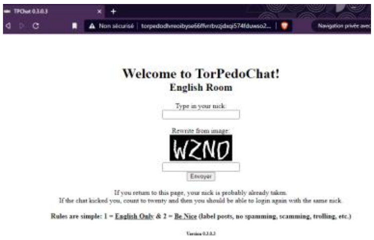


CHILD ABUSE PERPETRATORS

ClearWeb

DarkWeb

TOX



TPChat 0.3.0.3

Non sécurisé | torpedodhvreoibyse66ffvrrbvzjdxqi574fduwso2...

Navigation privée avec

Welcome to TorPedoChat!

English Room

Type in your nick:

Rewrite from image:

WZNO

Envoyer

If you return to this page, your nick is probably already taken.
If the chat kicked you, count to twenty and then you should be able to login again with the same nick.

Rules are simple: 1 = English Only & 2 = Be Nice (label posts, no spamming, scamming, trolling, etc.)

Version 0.3.0.3

CHILD ABUSE PERPETRATORS

Online

≠

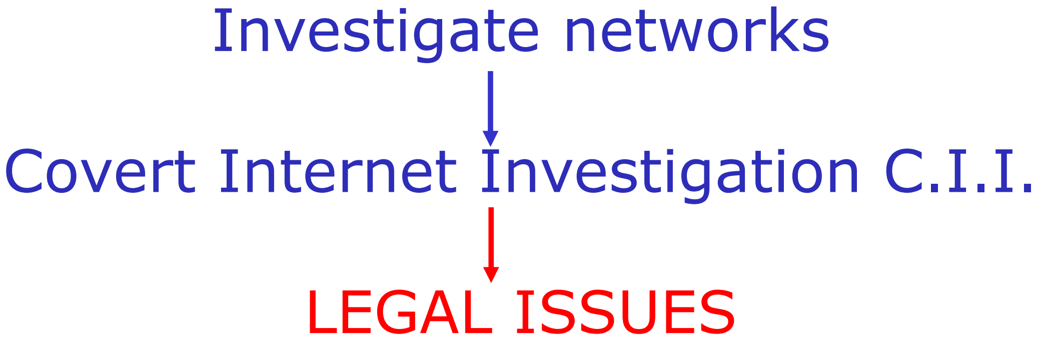
In Real Life

2 TYPES OF INVESTIGATION

Focused on tracking perpetrators

2 TYPES OF INVESTIGATION

Focused on tracking perpetrators



Investigate networks

Covert Internet Investigation C.I.I.

LEGAL ISSUES

French legislation regarding C.I.I.

Art 230-46 Code of Criminal Procedure

Alows to:

- **Participate in electronic exchanges**
- To **extract or preserve the data** and any **element of proof**
- **After Judge or Prosecutor agreement**, acquire any content, product, substance, sample or service, including illegal content, or **transmit in response to an express request for illegal content**

2 TYPES OF INVESTIGATION

Focused on tracking perpetrators

Investigate relationship of an identified abuser

↓

Investigation and Forensic analysis

↓

COOPERATION NEEDED

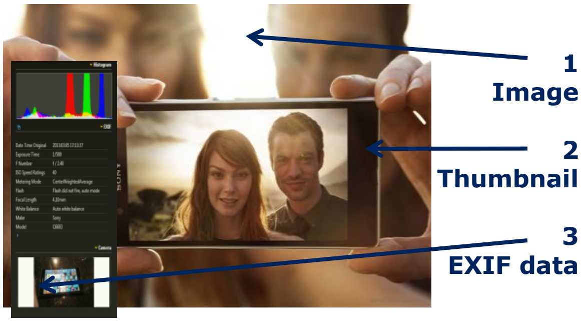
2 TYPES OF INVESTIGATION

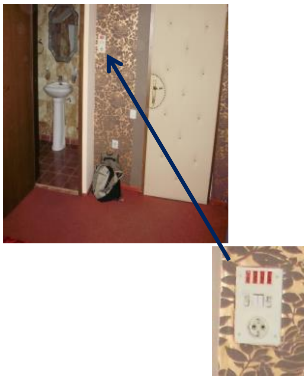
Victim Identification focus

2 TYPES OF INVESTIGATION

Victim Identification focus

Investigate data retrieved from C.I.I.





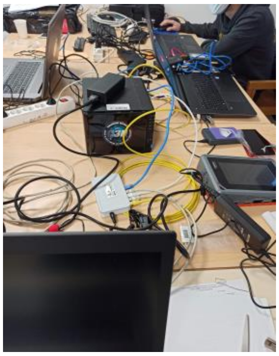
ERA – October 21st 2021

Work carried out by the law enforcement authorities to prevent child sexual abuse

2 TYPES OF INVESTIGATION

Victim Identification focus

Investigate data retrieved from house search

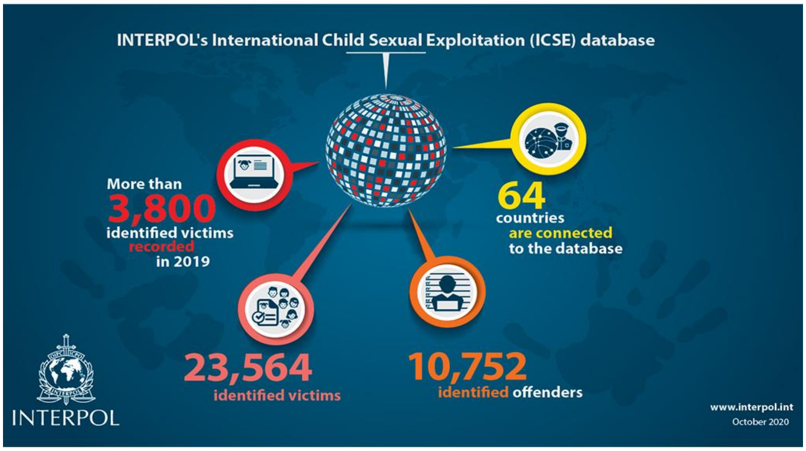


ERA – October 21st 2021

Work carried out by the law enforcement authorities to prevent child sexual abuse

2 TYPES OF INVESTIGATION

Victim Identification focus - ICSE



INTERPOL's International Child Sexual Exploitation (ICSE) database

More than 3,800 identified victims recorded in 2019

64 countries are connected to the database

23,564 identified victims

10,752 identified offenders

INTERPOL

www.interpol.int
October 2020

CONCLUSION

Victim Centric approach

Cooperation needed

THANKS

COMCYBERGEND/ C3N / CNAIP

+33 1 71 66 40 54 ADJ VILLETTE
cnaip.dc.scrcgn@gendarmerie.interieur.gouv.fr

Darknet Investigations

Preventing Child Sexual Abuse

Tallinn, 21-22 October 2021

With the support of the Internal Security Fund-Police Programme
of the European Union 2014-2020

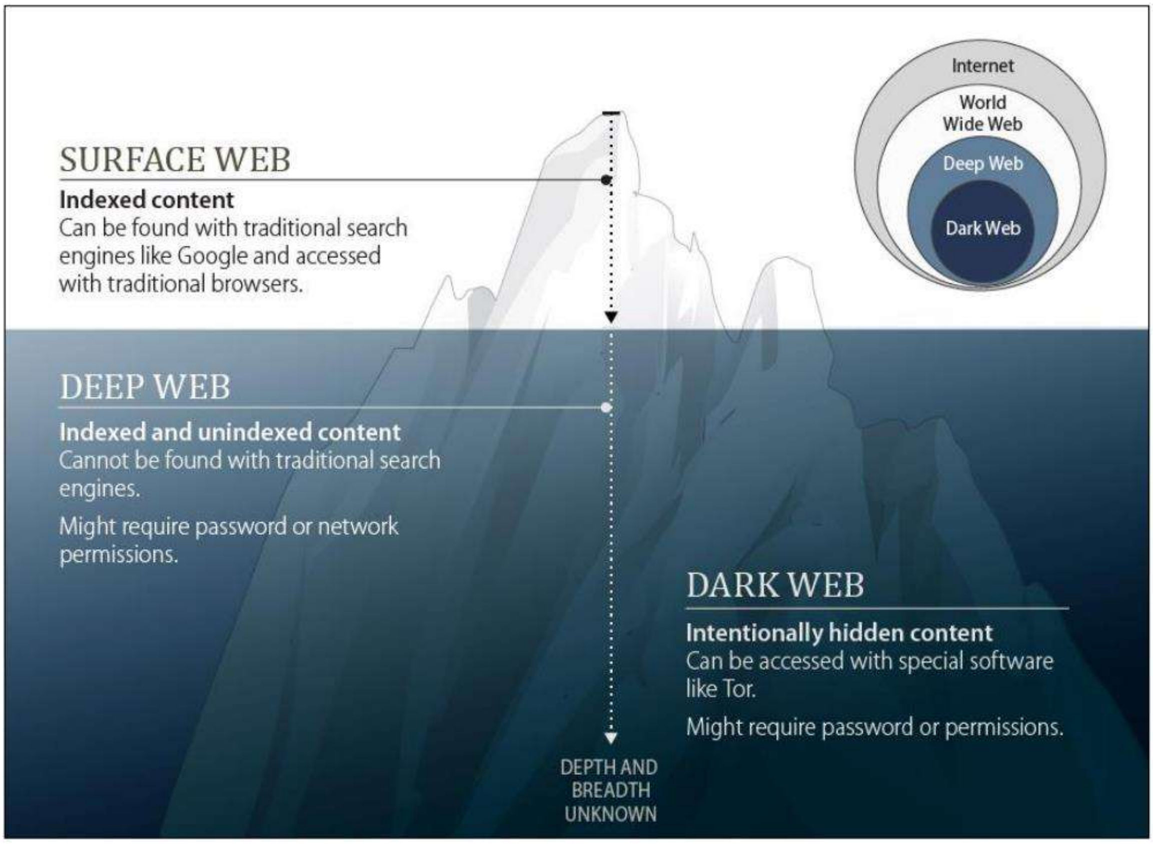
Rainer Franosch
Deputy Director-General, Department for Criminal Law, Cybercrime Division
Ministry of Justice of the German Federal State of Hesse

Cybercriminal’s techniques and other obstacles

To prevent an investigation, cybercriminals

- Use anonymization and encryption
- Eliminate or obfuscate evidence
- Use anonymous online data storage
- Use compromised computers in different countries to thwart investigation
- Take advantage of the different or conflicting legislation and legal codes and procedures
- Introduce doubt about the collected evidence in the prosecution process or in trial

Layers of the Internet



SURFACE WEB

Indexed content

Can be found with traditional search engines like Google and accessed with traditional browsers.

DEEP WEB

Indexed and unindexed content

Cannot be found with traditional search engines.

Might require password or network permissions.

DARK WEB

Intentionally hidden content

Can be accessed with special software like Tor.

Might require password or permissions.

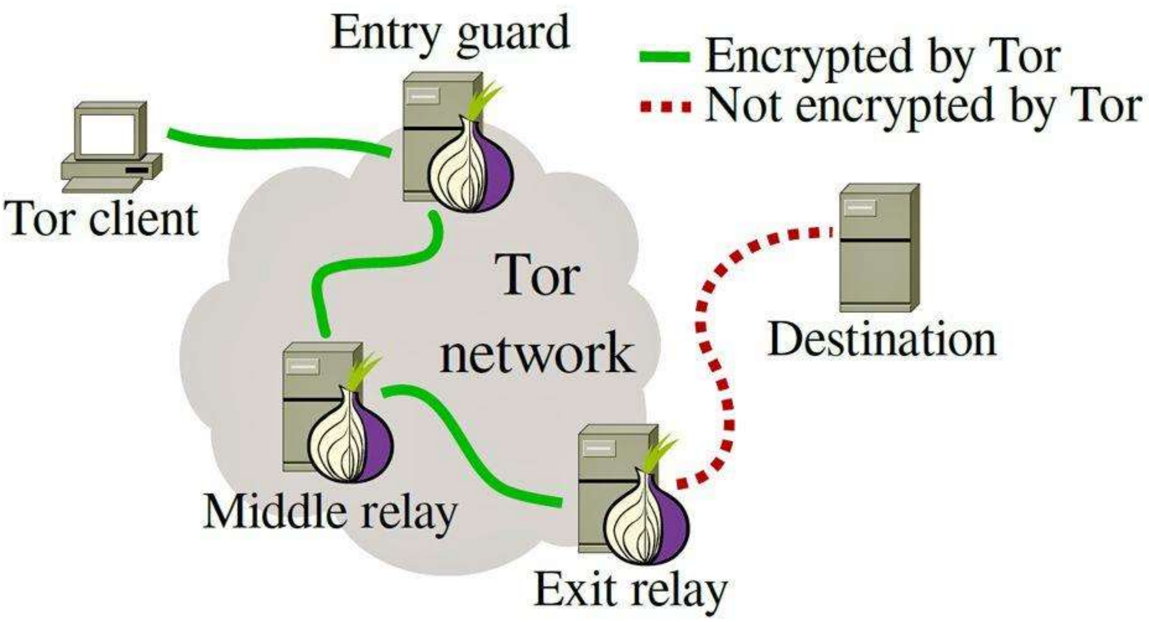
Source: Congressional Research Service (CRS).

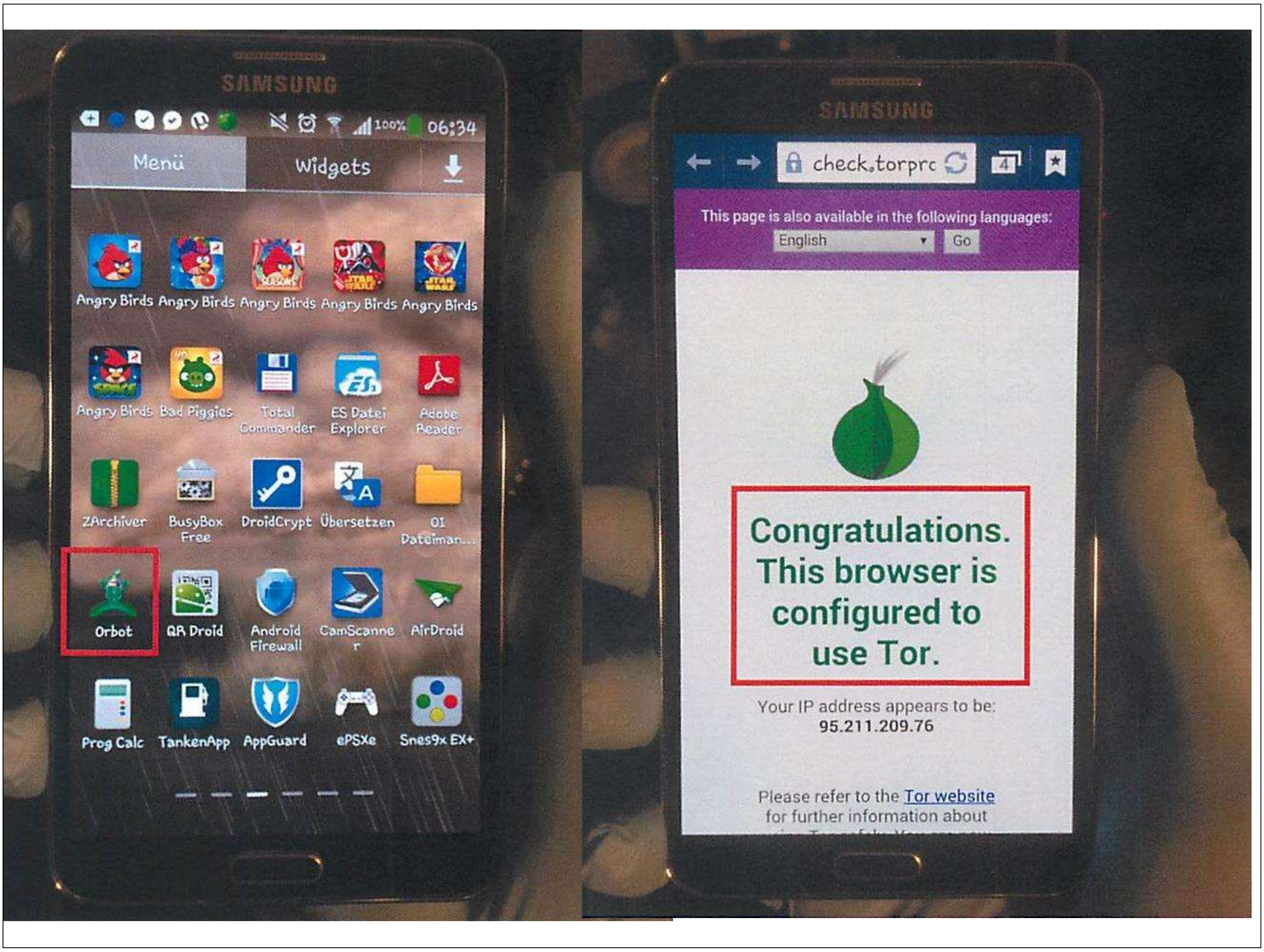
Note: Proportions in the figure may not be to scale.

The Onion Router - TOR

- TOR = Acronym for The Onion Router
- Free software for enabling anonymous communication
- Originally developed on behalf of the U.S. intelligence community
- Use of the TOR software bounces a user’s communications around a distributed network of relay computers
- Users can remain anonymous
- Activities can remain untraceable
- Resources can remain hidden

The Onion Router - TOR





This page is also available in the following languages:

English ▾ Go

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 95.211.209.76

Please refer to the Tor website for further information about

TOR Hidden Services (the „Darknet“)

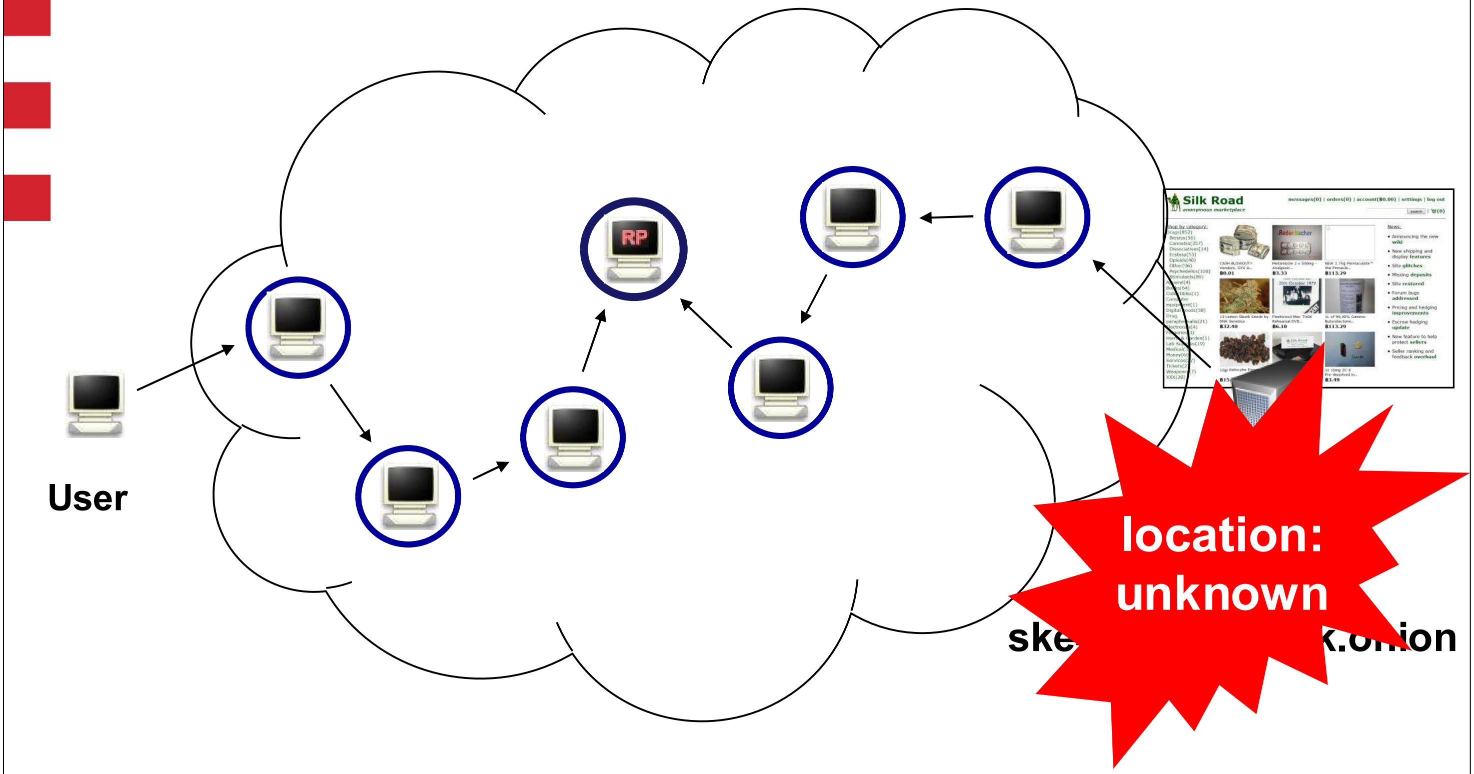
- Hide physical location of service by using a rendezvous point.

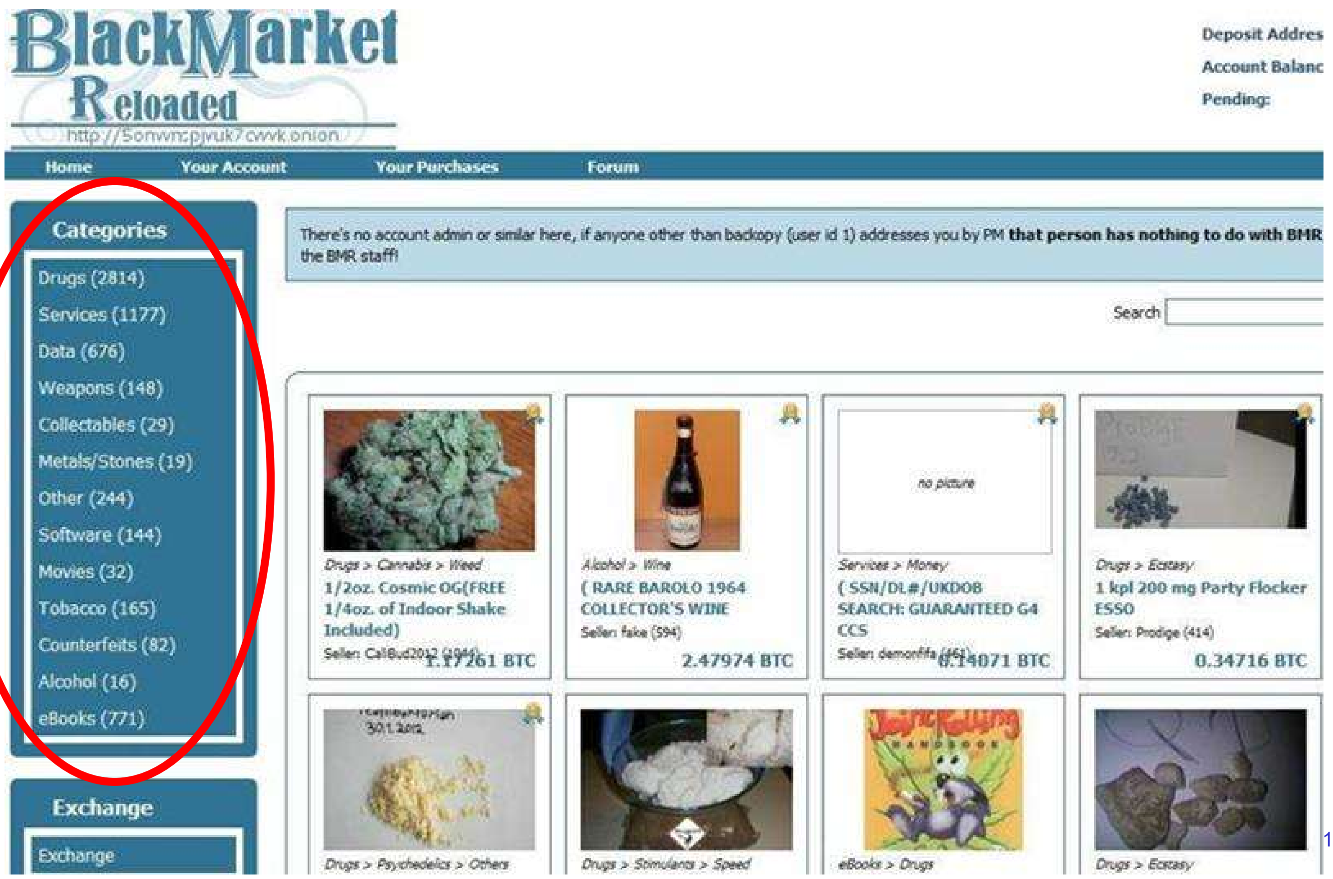
- Dark net marketplaces operate on the dark net. These sites are generally only accessible through the input of specific addresses into a TOR browser.

- The dark net marketplaces function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, victims of human trafficking, CSAM and other illicit goods.

- Within the Darknet both web surfers and website publishers are entirely anonymous.

TOR Hidden Services (the „Darknet“)





BlackMarket Reloaded
http://5onwnspjvuk7cwvk.onion

Deposit Addres
Account Balanc
Pending:

Home | Your Account | Your Purchases | Forum

Categories
- Drugs (2814)
- Services (1177)
- Data (676)
- Weapons (148)
- Collectables (29)
- Metals/Stones (19)
- Other (244)
- Software (144)
- Movies (32)
- Tobacco (165)
- Counterfeits (82)
- Alcohol (16)
- eBooks (771)

Exchange
- Exchange

There's no account admin or similar here, if anyone other than backopy (user id 1) addresses you by PM **that person has nothing to do with BMR** the BMR staff!

Search

Drugs > Cannabis > Weed
1/2oz. Cosmic OG(FREE 1/4oz. of Indoor Shake Included)
Seller: CaliBud2012 (1044)
1.17261 BTC

Alcohol > Wine
(RARE BAROLO 1964 COLLECTOR'S WINE
Seller: fake (594)
2.47974 BTC

no picture
Services > Money
(SSN/DL#/UKDOB SEARCH: GUARANTEED G4 CCS
Seller: demonffa (461)
0.14071 BTC

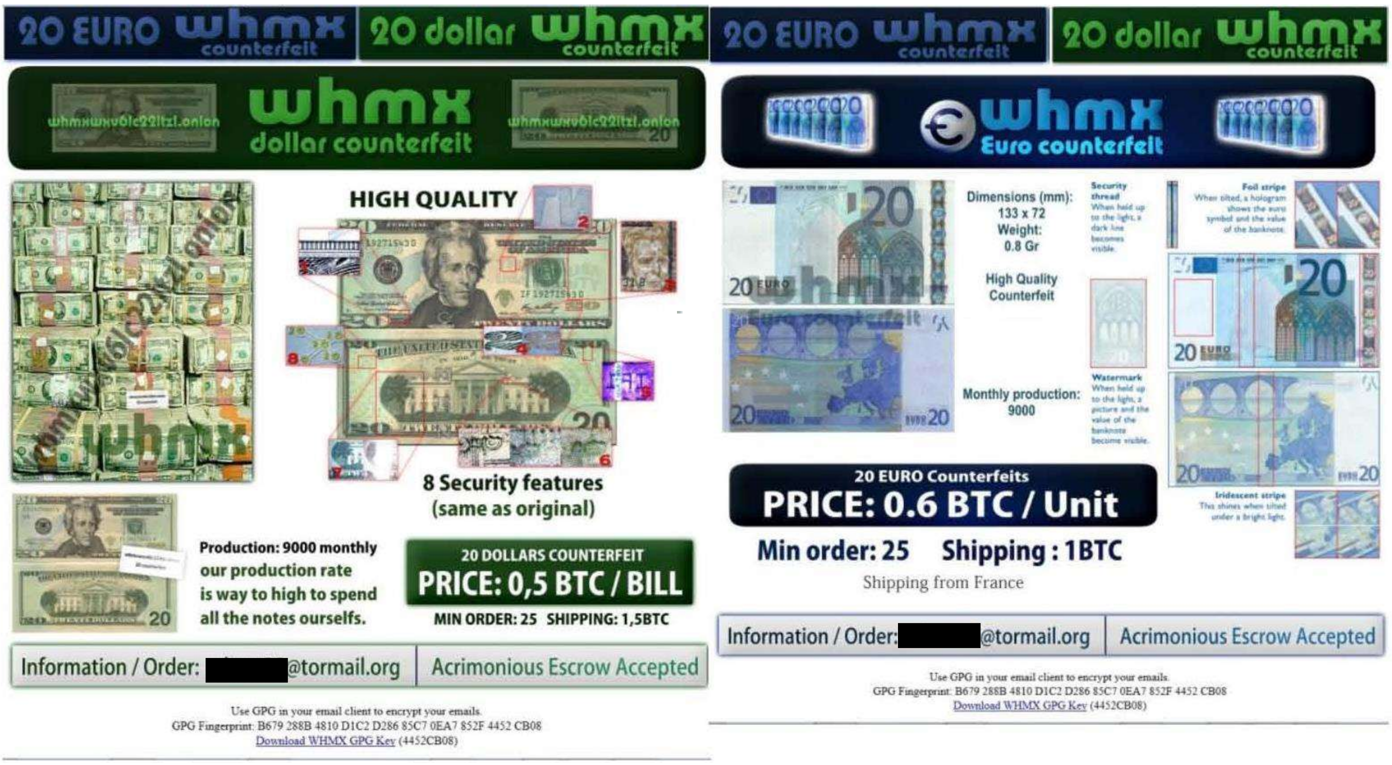
Drugs > Ecstasy
1 kpl 200 mg Party Flocker ESSO
Seller: Prodige (414)
0.34716 BTC

Drugs > Psychedelics > Others

Drugs > Stimulants > Speed

eBooks > Drugs

Drugs > Ecstasy



8 Security features (same as original)

Production: 9000 monthly our production rate is way to high to spend all the notes ourselfs.

20 DOLLARS COUNTERFEIT
PRICE: 0,5 BTC / BILL
MIN ORDER: 25 SHIPPING: 1,5BTC

Information / Order: [redacted]@tormail.org | Acrimonious Escrow Accepted

Use GPG in your email client to encrypt your emails.
GPG Fingerprint: B679 288B 4810 D1C2 D286 85C7 0EA7 852F 4452 CB08
Download WHMX GPG Key (4452CB08)

Dimensions (mm): 133 x 72
Weight: 0.8 Gr

High Quality Counterfeit

Monthly production: 9000

Security thread When held up to the light, a dark line becomes visible.

Foil stripe When tilted, a hologram shows the euro symbol and the value of the banknote.

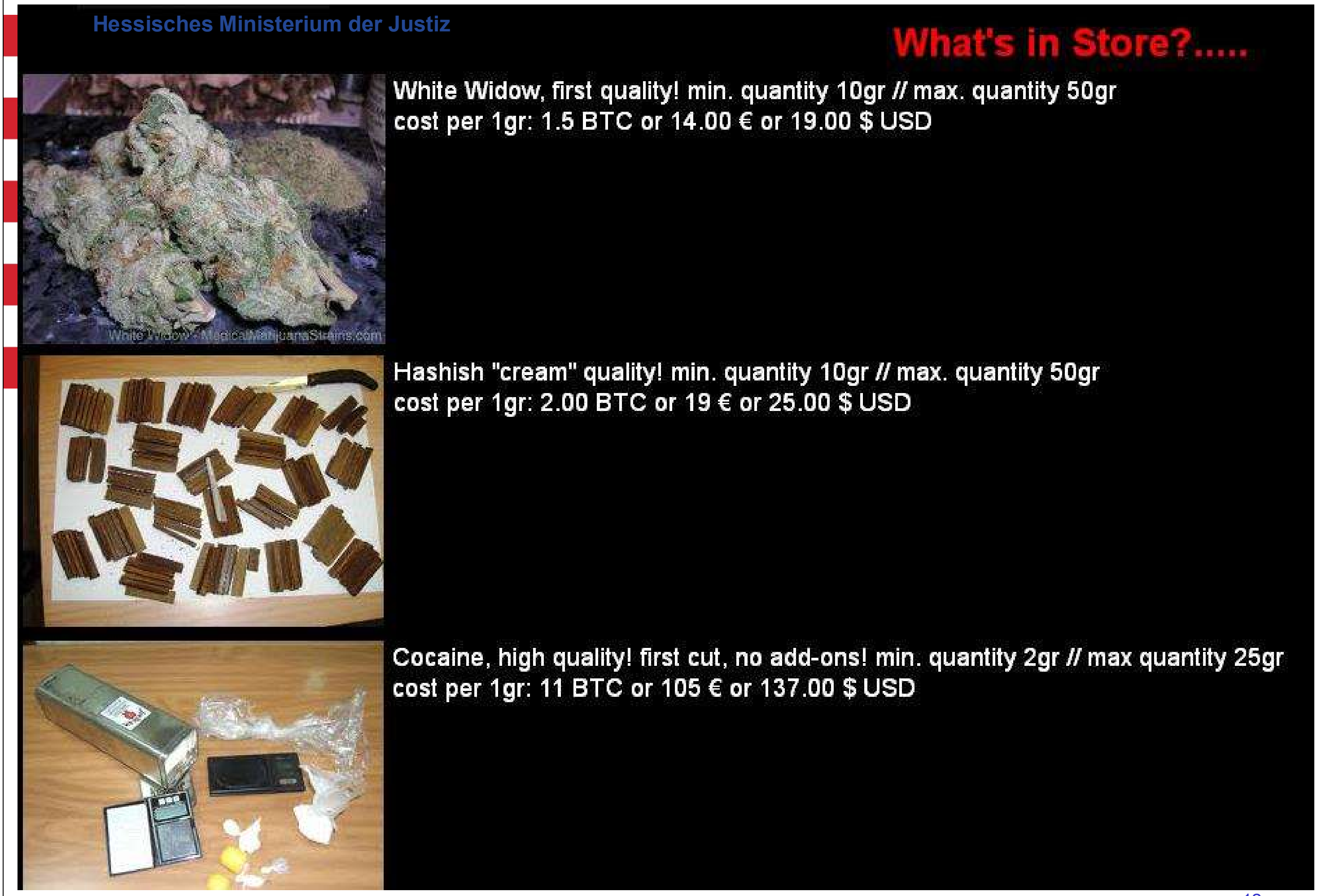
Watermark When held up to the light, a picture and the value of the banknote become visible.

Iridescent stripe This shines when tilted under a bright light.

20 EURO Counterfeits
PRICE: 0.6 BTC / Unit
Min order: 25 Shipping : 1BTC
Shipping from France

Information / Order: [redacted]@tormail.org | Acrimonious Escrow Accepted

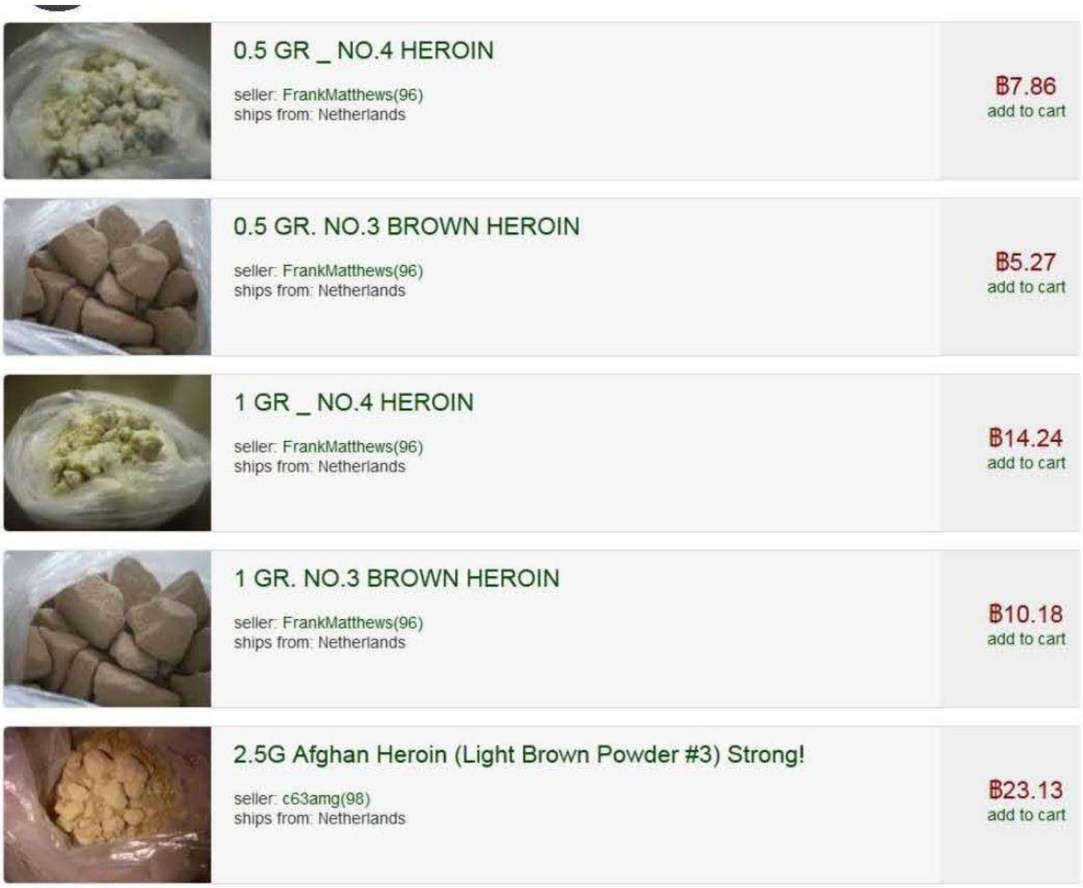
Use GPG in your email client to encrypt your emails.
GPG Fingerprint: B679 288B 4810 D1C2 D286 85C7 0EA7 852F 4452 CB08
Download WHMX GPG Key (4452CB08)


What's in Store?.....

White Widow, first quality! min. quantity 10gr // max. quantity 50gr
cost per 1gr: 1.5 BTC or 14.00 € or 19.00 $ USD

Hashish "cream" quality! min. quantity 10gr // max. quantity 50gr
cost per 1gr: 2.00 BTC or 19 € or 25.00 $ USD

Cocaine, high quality! first cut, no add-ons! min. quantity 2gr // max quantity 25gr
cost per 1gr: 11 BTC or 105 € or 137.00 $ USD



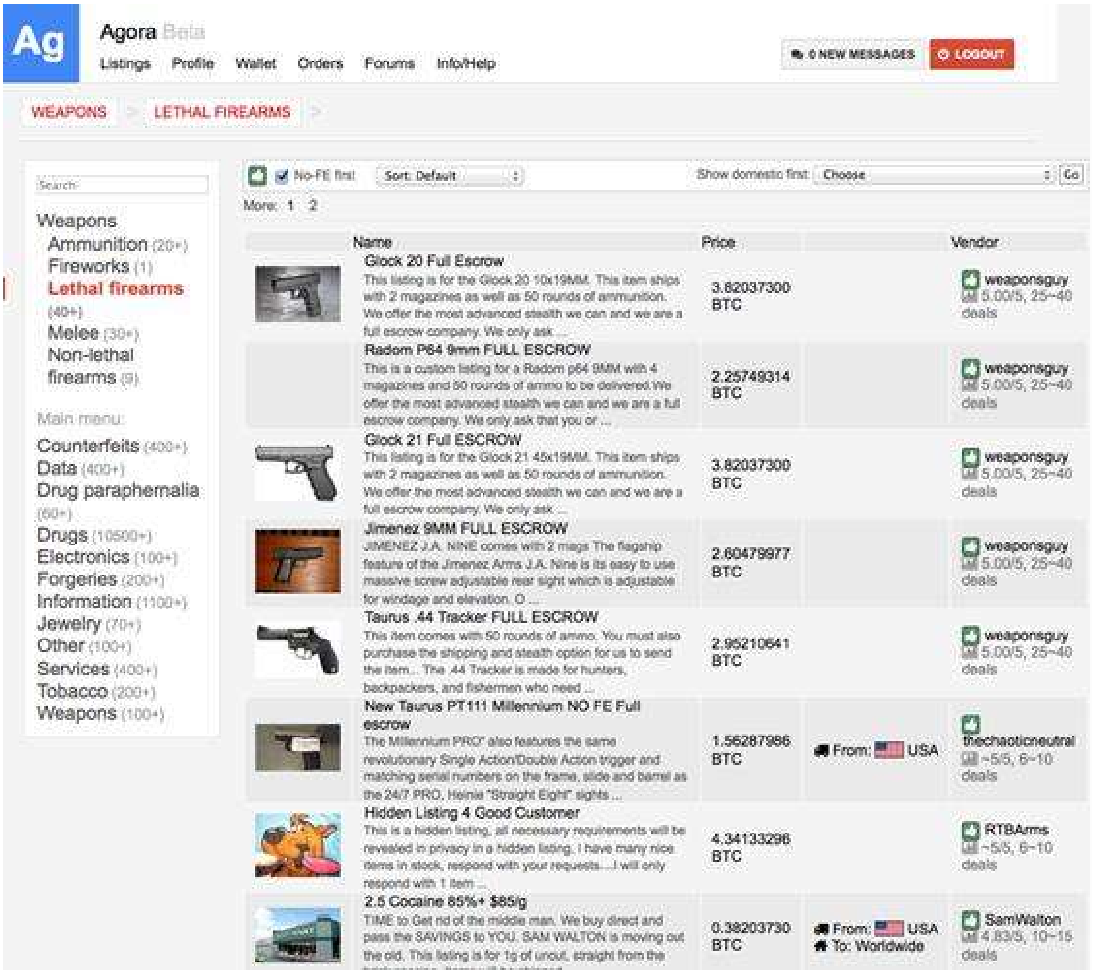
0.5 GR _ NO.4 HEROIN
seller: FrankMatthews(96)
ships from: Netherlands
Ƀ7.86
add to cart

0.5 GR. NO.3 BROWN HEROIN
seller: FrankMatthews(96)
ships from: Netherlands
Ƀ5.27
add to cart

1 GR _ NO.4 HEROIN
seller: FrankMatthews(96)
ships from: Netherlands
Ƀ14.24
add to cart

1 GR. NO.3 BROWN HEROIN
seller: FrankMatthews(96)
ships from: Netherlands
Ƀ10.18
add to cart

2.5G Afghan Heroin (Light Brown Powder #3) Strong!
seller: c63amg(98)
ships from: Netherlands
Ƀ23.13
add to cart



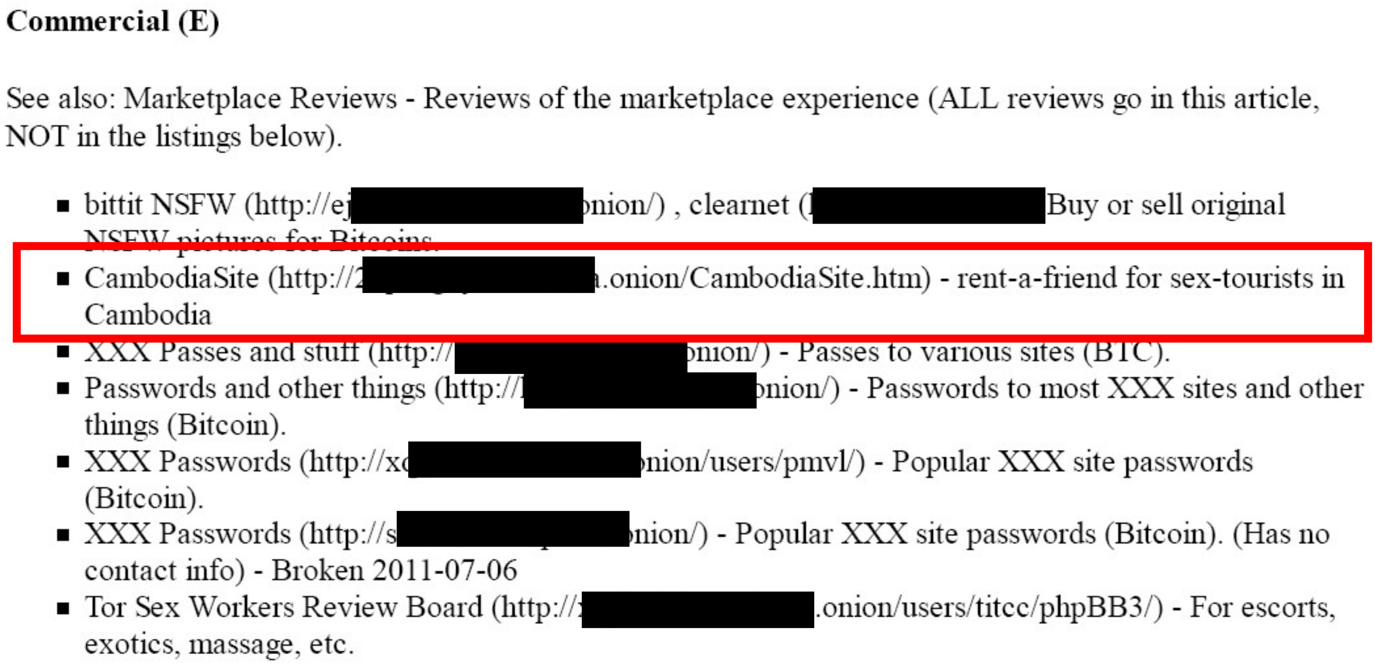
Weapons
Ammunition (20+)
Fireworks (1)
Lethal firearms (40+)
Melee (30+)
Non-lethal firearms (9)

Main menu:
Counterfeits (400+)
Data (400+)
Drug paraphernalia (60+)
Drugs (10500+)
Electronics (100+)
Forgeries (200+)
Information (1100+)
Jewelry (70+)
Other (100+)
Services (400+)
Tobacco (200+)
Weapons (100+)

☑ No-FE first
Sort: Default
Show domestic first: Choose
Go

More: 1 2

Name	Price		Vendor
Glock 20 Full Escrow This listing is for the Glock 20 10x19MM. This item ships with 2 magazines as well as 50 rounds of ammunition. We offer the most advanced stealth we can and we are a full escrow company. We only ask ...	3.82037300 BTC		weaponsguy 5.00/5, 25~40 deals
Radom P64 9mm FULL ESCROW This is a custom listing for a Radom p64 9MM with 4 magazines and 50 rounds of ammo to be delivered.We offer the most advanced stealth we can and we are a full escrow company. We only ask that you or ...	2.25749314 BTC		weaponsguy 5.00/5, 25~40 deals
Glock 21 Full ESCROW This listing is for the Glock 21 45x19MM. This item ships with 2 magazines as well as 50 rounds of ammunition. We offer the most advanced stealth we can and we are a full escrow company. We only ask ...	3.82037300 BTC		weaponsguy 5.00/5, 25~40 deals
Jimenez 9MM FULL ESCROW JIMENEZ J.A. NINE comes with 2 mags The flagship feature of the Jimenez Arms J.A. Nine is its easy to use massive screw adjustable rear sight which is adjustable for windage and elevation. O ...	2.60479977 BTC		weaponsguy 5.00/5, 25~40 deals
Taurus .44 Tracker FULL ESCROW This item comes with 50 rounds of ammo. You must also purchase the shipping and stealth option for us to send the item... The .44 Tracker is made for hunters, backpackers, and fishermen who need ...	2.95210641 BTC		weaponsguy 5.00/5, 25~40 deals
New Taurus PT111 Millennium NO FE Full escrow The Millennium PRO" also features the same revolutionary Single Action/Double Action trigger and matching serial numbers on the frame, slide and barrel as the 24/7 PRO, Heinie "Straight Eight" sights ...	1.56287986 BTC	From: USA	thechaoticneutral ~5/5, 6~10 deals
Hidden Listing 4 Good Customer This is a hidden listing, all necessary requirements will be revealed in privacy in a hidden listing. I have many nice items in stock, respond with your requests....I will only respond with 1 item ...	4.34133296 BTC		RTBArms ~5/5, 6~10 deals
2.5 Cocaine 85%+ $85/g TIME to Get rid of the middle man. We buy direct and pass the SAVINGS to YOU. SAM WALTON is moving out the old. This listing is for 1g of uncut, straight from the	0.38203730 BTC	From: USA To: Worldwide	SamWalton 4.83/5, 10~15 deals



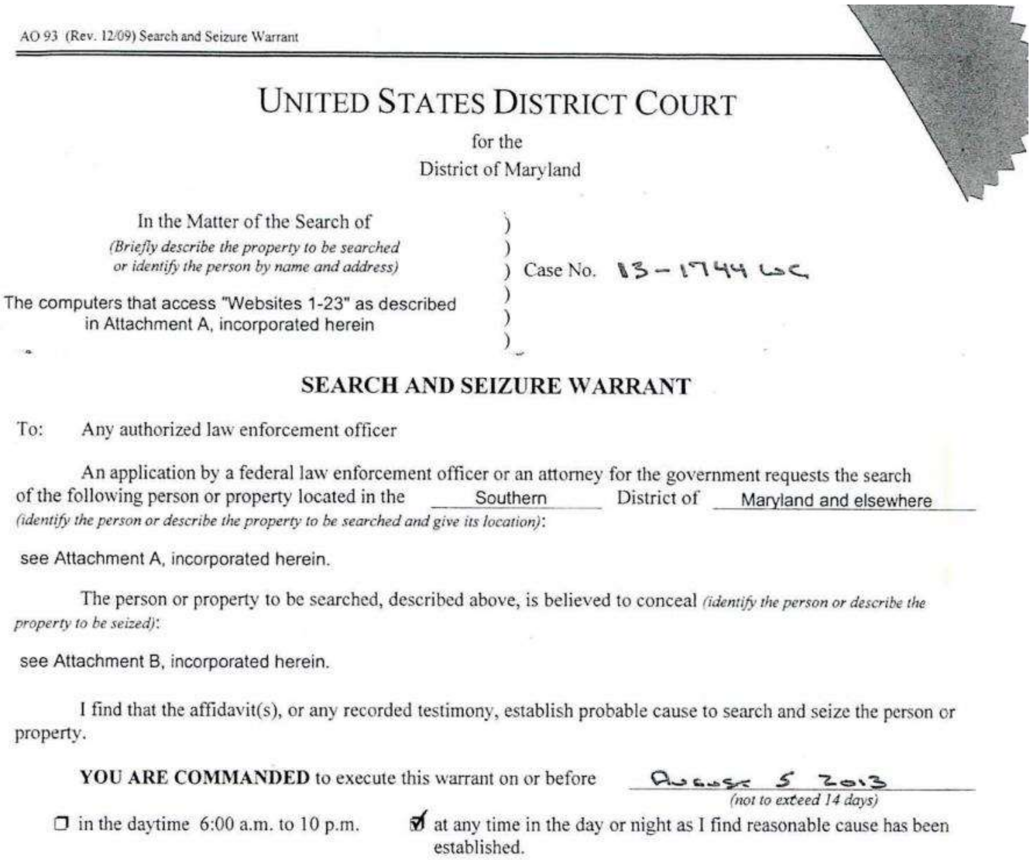
Commercial (E)

See also: Marketplace Reviews - Reviews of the marketplace experience (ALL reviews go in this article, NOT in the listings below).

- bittit NSFW (http://ej[redacted]onion/) , clearnet ([redacted]Buy or sell original NSFW pictures for Bitcoins.
- CambodiaSite (http://2[redacted].onion/CambodiaSite.htm) - rent-a-friend for sex-tourists in Cambodia
- XXX Passes and stuff (http://[redacted]onion/) - Passes to various sites (BTC).
- Passwords and other things (http://[redacted]onion/) - Passwords to most XXX sites and other things (Bitcoin).
- XXX Passwords (http://xc[redacted]onion/users/pmvl/) - Popular XXX site passwords (Bitcoin).
- XXX Passwords (http://s[redacted]onion/) - Popular XXX site passwords (Bitcoin). (Has no contact info) - Broken 2011-07-06
- Tor Sex Workers Review Board (http://[redacted].onion/users/titcc/phpBB3/) - For escorts, exotics, massage, etc.

Case Studies

Operation DOWNFALL (Freedom Hosting)



AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT
for the
District of Maryland

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The computers that access "Websites 1-23" as described in Attachment A, incorporated herein
) Case No. 13-1744 WC

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Maryland and elsewhere *(identify the person or describe the property to be searched and give its location)*:

see Attachment A, incorporated herein.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

see Attachment B, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before August 5 2013
(not to exceed 14 days)

□ in the daytime 6:00 a.m. to 10 p.m. ☑ at any time in the day or night as I find reasonable cause has been established.

Operation DOWNFALL – a technical approach

- **In 2013, the FBI seized a server hosting numerous child sexual abuse material (CSAM) sites on the Tor network.**
- **Instead of shutting it down, FBI continued to run it from a government site in the District of Maryland for about 10 days.**
- **LEA determined that simply shutting down the sites was not sufficient, as users would migrate to different websites.**
- **LEA decided that in an international investigation every effort should be taken to identify as many users as possible.**

Operation DOWNFALL – a technical approach

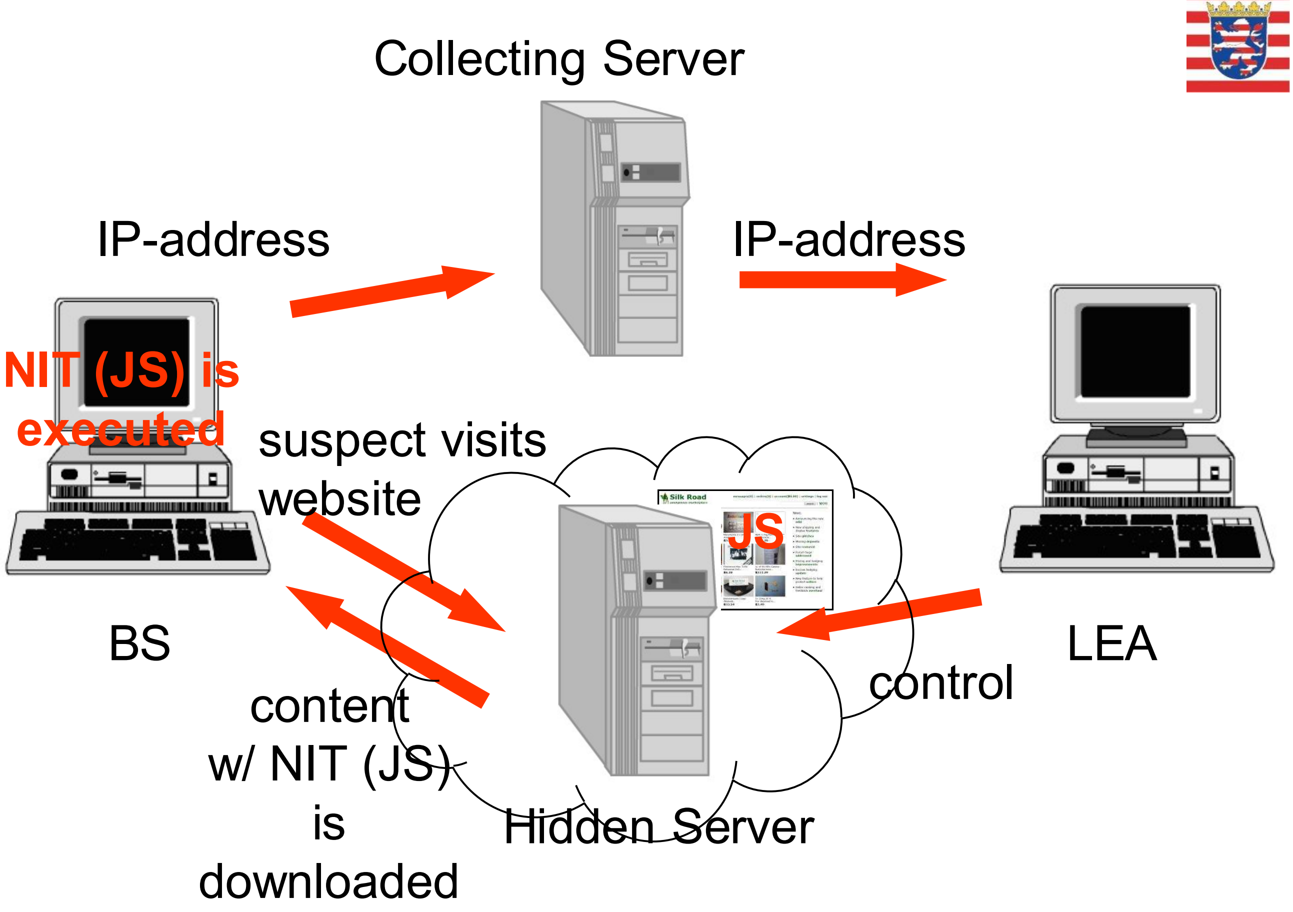
- During the site seizure, LEA deployed a network investigative technique (NIT) that gathered identifying information from users’computers.
- According to researchers, the code exploited a security hole in Firefox to identify users of the Tor Browser Bundle. Mozilla confirmed the code exploited a critical memory management vulnerability in Firefox that had been publicly reported on 25 June 2013, and which had been corrected for the latest version of the browser.

Operation DOWNFALL – a technical approach

- For technical reasons, the measures taken by the police caught the attention of the counterpart quite promptly, so that after the publication of several warning messages by the users, hardly any criminally relevant activities took place on the monitored pages.
- The single NIT warrant, executed in Maryland, U.S.A., implicated more than 70.000 users worldwide.
- 300 could be de-anonymized, 15 were German defendants.

Network Investigative Technique (NIT)

Computer code that when deployed to a person's computer, causes that computer to send to the government its actual IP address and other related information



Collecting Server

IP-address

IP-address

NIT (JS) is executed

suspect visits website

JS

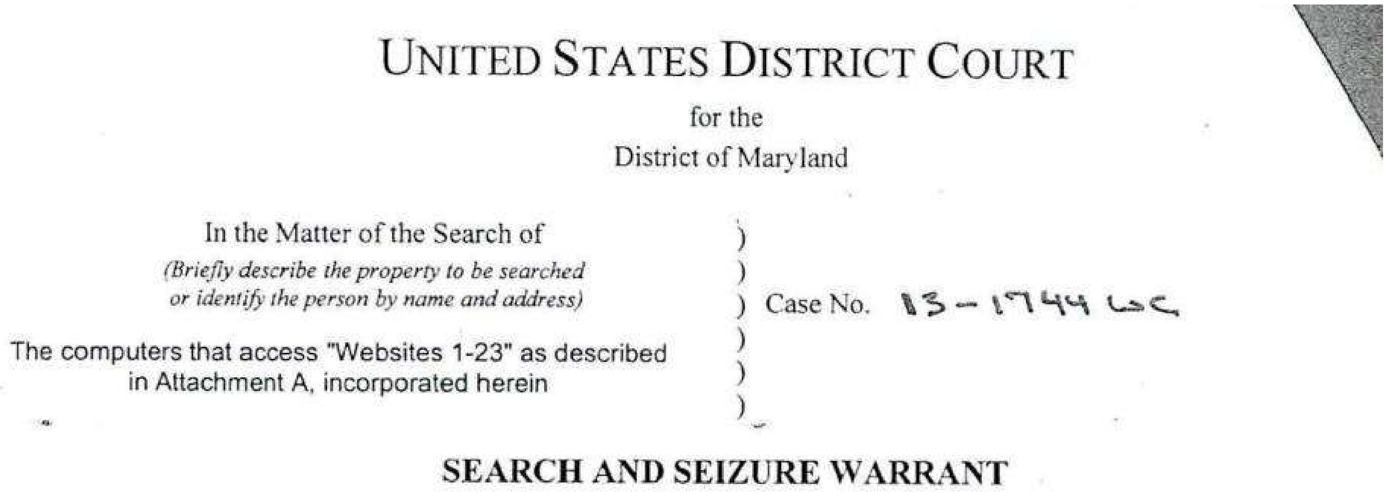
BS

LEA

control

content w/ NIT (JS) is downloaded

Hidden Server



UNITED STATES DISTRICT COURT

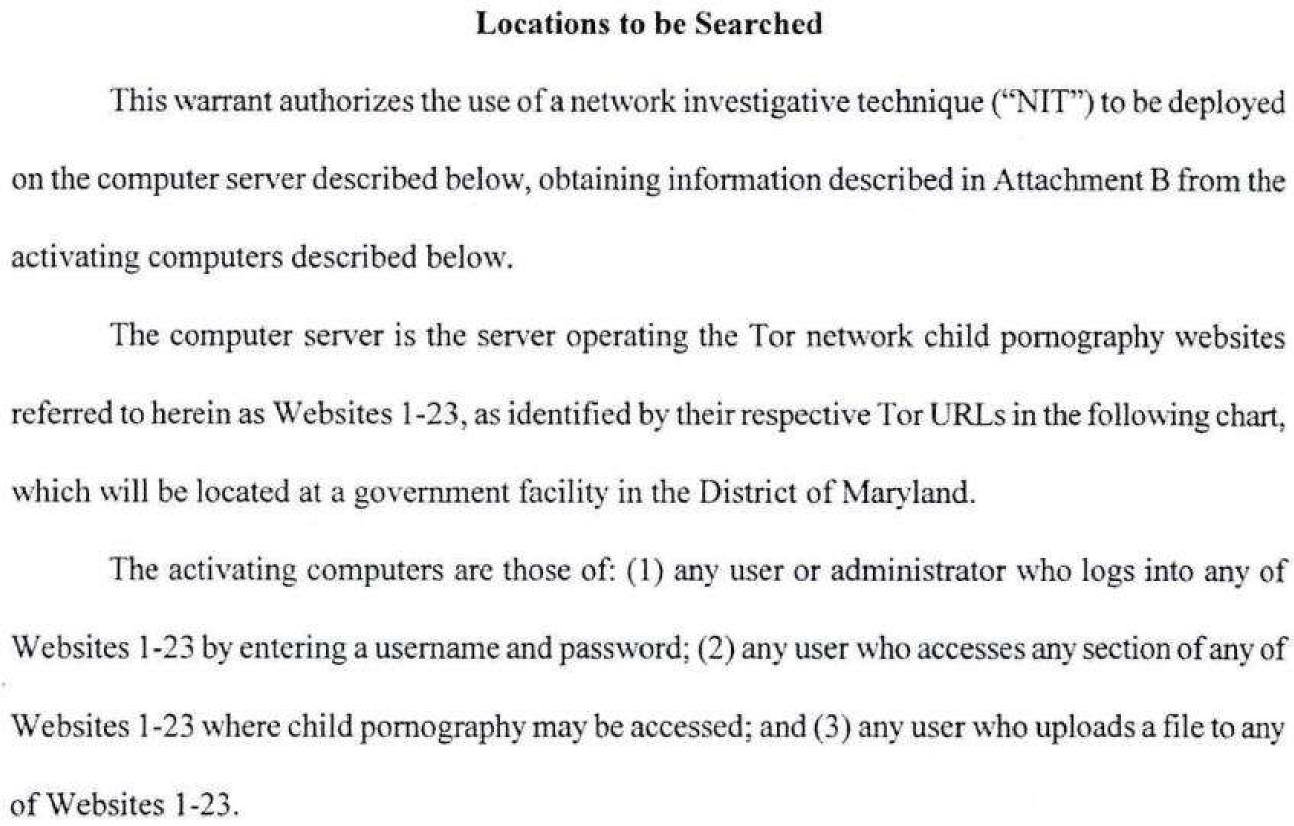
for the
District of Maryland

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The computers that access "Websites 1-23" as described in Attachment A, incorporated herein

Case No. 13-1744 WC

SEARCH AND SEIZURE WARRANT

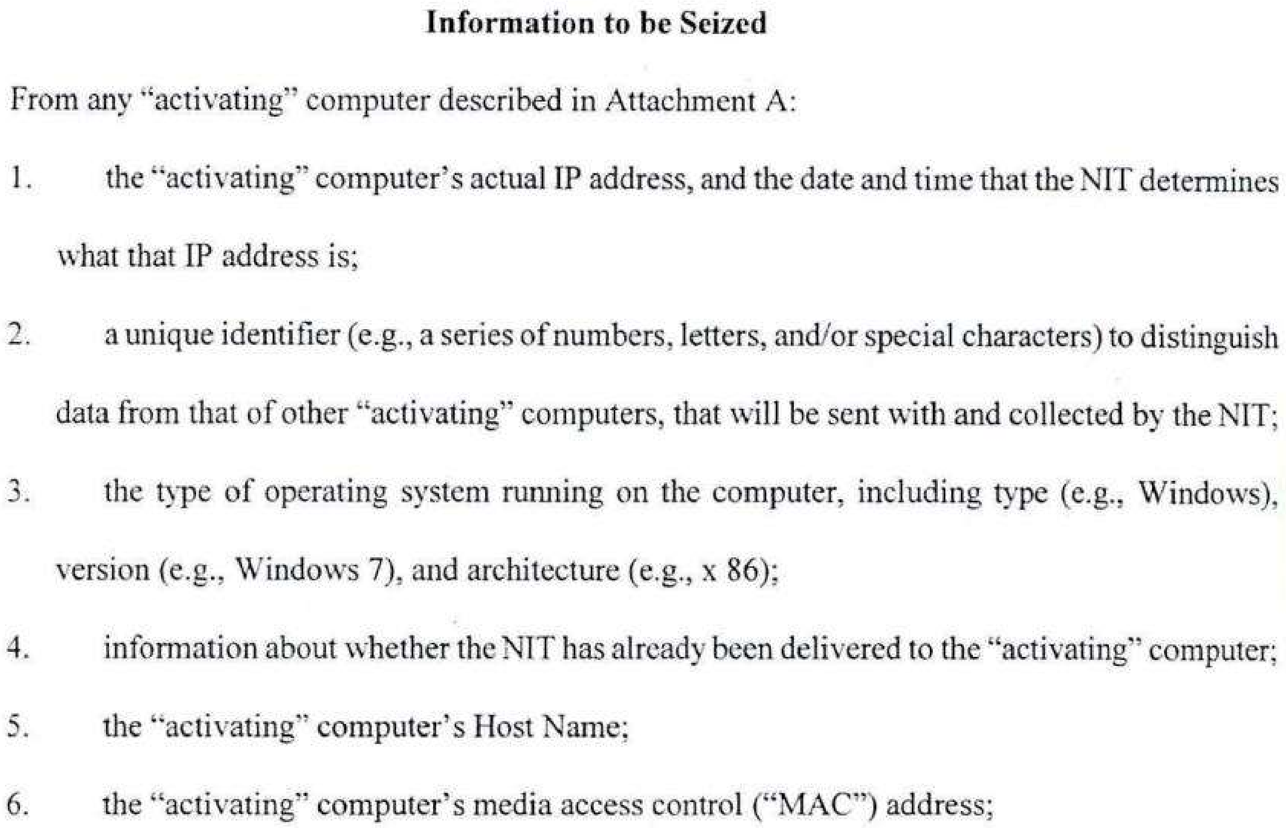


Locations to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography websites referred to herein as Websites 1-23, as identified by their respective Tor URLs in the following chart, which will be located at a government facility in the District of Maryland.

The activating computers are those of: (1) any user or administrator who logs into any of Websites 1-23 by entering a username and password; (2) any user who accesses any section of any of Websites 1-23 where child pornography may be accessed; and (3) any user who uploads a file to any of Websites 1-23.

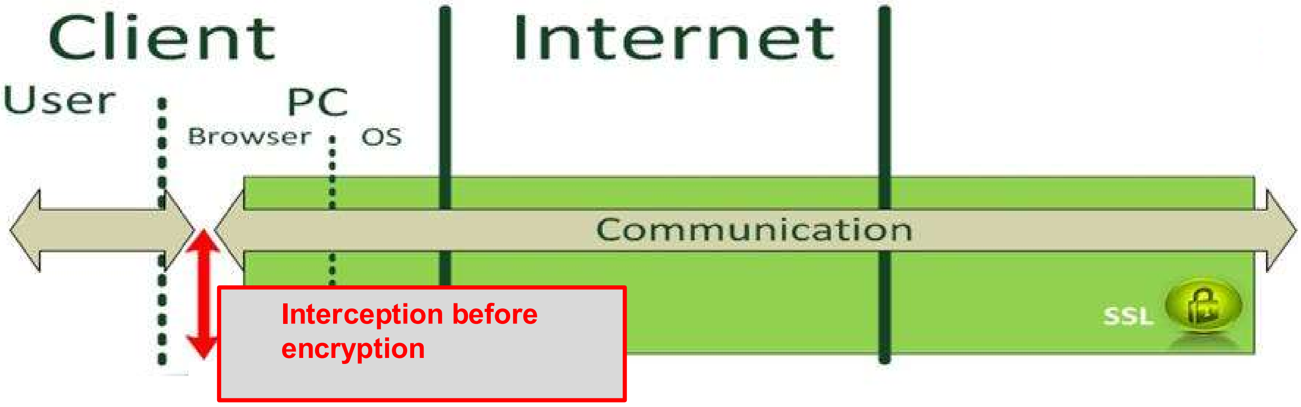


Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's media access control ("MAC") address;

Source TC interception – usage of NIT



Interception before encryption

NIT – Technical issues

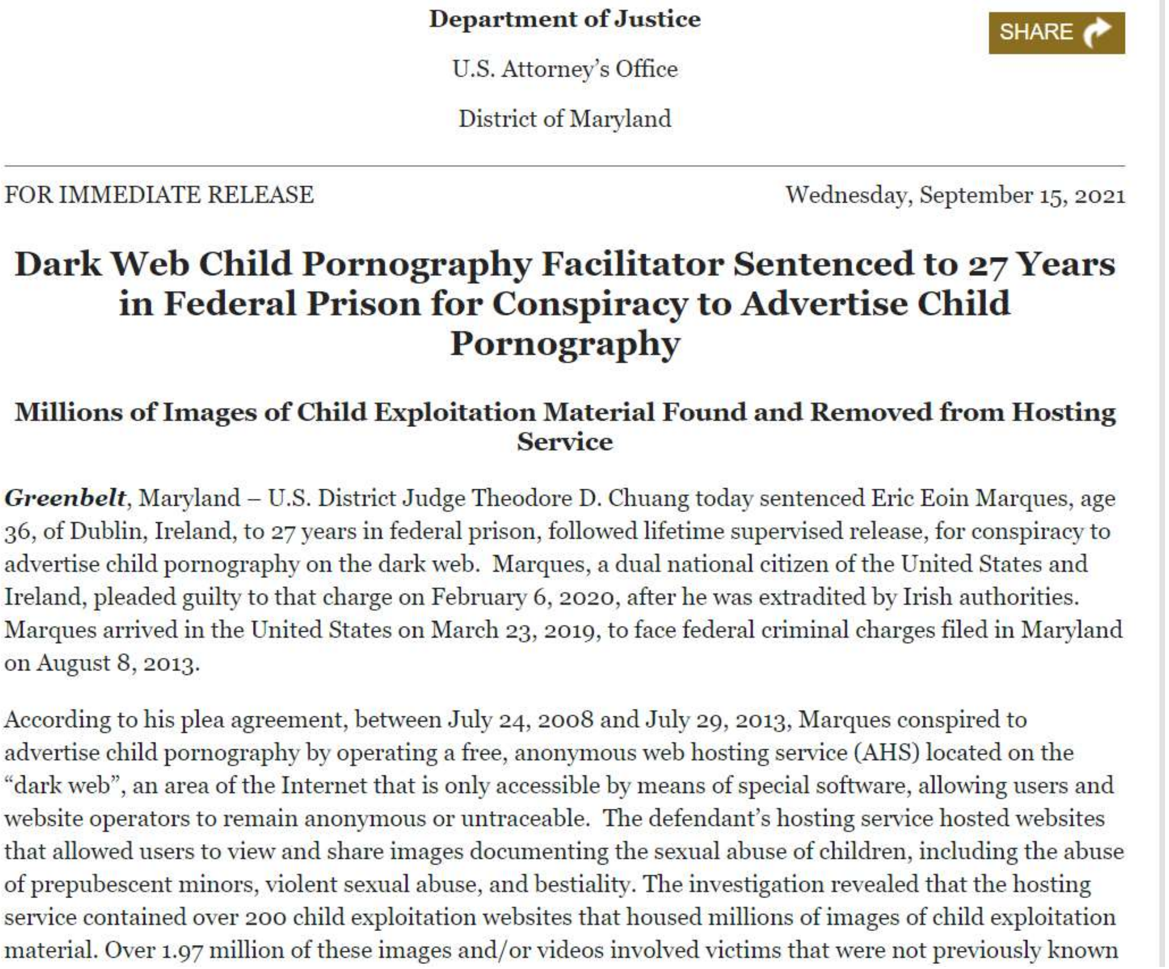
- **Commercial product or a tool developed by LE itself?**
- **How to install on the suspects device?**
- **How to remove from the suspects device?**
- **How to avoid Communications Insecurity:**

"Wiretapping is an important investigative tool, but solving law enforcement's difficulties should not come at the expense of increasing cybersecurity vulnerabilities."

Susan Landau in: „Patriots Debate: Contemporary Issues in National Security Law",
http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online.html

NIT – Legal issues

- **Defense challenged the admissability of the IP-addresses acquired by the NIT.**
- **Initial suspicion sufficient?**
- **Was the NIT a proper LEA technique or one used by an intelligence service?**
- **At that time, there was no legal basis for an online search in the German procedural code. Was the usage of the NIT wire tapping or an online search?**
- **Does the operation of the CSAM sites by LEA create a procedural impediment ("fruit of the poisoness tree")?**



Department of Justice

U.S. Attorney's Office

District of Maryland

FOR IMMEDIATE RELEASE

Wednesday, September 15, 2021

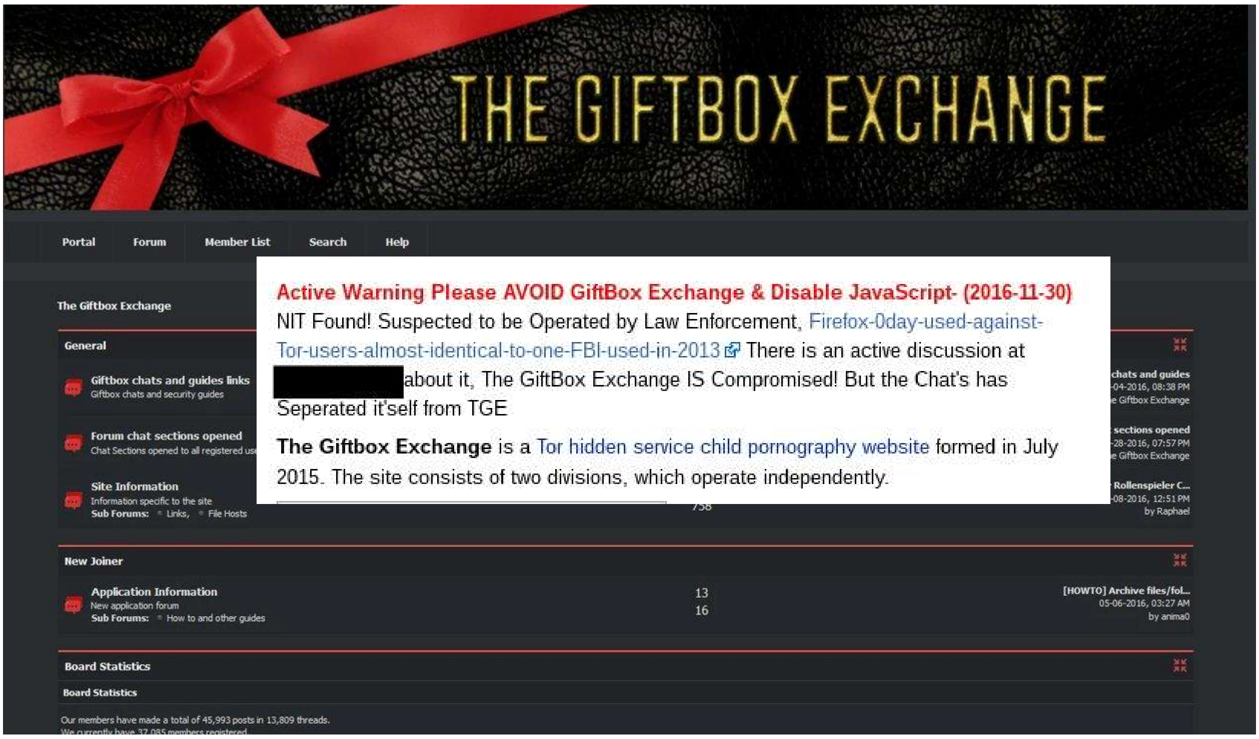
Dark Web Child Pornography Facilitator Sentenced to 27 Years in Federal Prison for Conspiracy to Advertise Child Pornography

Millions of Images of Child Exploitation Material Found and Removed from Hosting Service

Greenbelt, Maryland – U.S. District Judge Theodore D. Chuang today sentenced Eric Eoin Marques, age 36, of Dublin, Ireland, to 27 years in federal prison, followed lifetime supervised release, for conspiracy to advertise child pornography on the dark web. Marques, a dual national citizen of the United States and Ireland, pleaded guilty to that charge on February 6, 2020, after he was extradited by Irish authorities. Marques arrived in the United States on March 23, 2019, to face federal criminal charges filed in Maryland on August 8, 2013.

According to his plea agreement, between July 24, 2008 and July 29, 2013, Marques conspired to advertise child pornography by operating a free, anonymous web hosting service (AHS) located on the "dark web", an area of the Internet that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. The defendant's hosting service hosted websites that allowed users to view and share images documenting the sexual abuse of children, including the abuse of prepubescent minors, violent sexual abuse, and bestiality. The investigation revealed that the hosting service contained over 200 child exploitation websites that housed millions of images of child exploitation material. Over 1.97 million of these images and/or videos involved victims that were not previously known

Operation ARTEMIS (The Giftbox Exchange / Elysium) – a combined approach



Active Warning Please AVOID GiftBox Exchange & Disable JavaScript- (2016-11-30)

NIT Found! Suspected to be Operated by Law Enforcement, Firefox-0day-used-against-Tor-users-almost-identical-to-one-FBI-used-in-2013 There is an active discussion at [redacted] about it, The GiftBox Exchange IS Compromised! But the Chat's has Seperated it'self from TGE

The Giftbox Exchange is a Tor hidden service child pornography website formed in July 2015. The site consists of two divisions, which operate independently.

Our members have made a total of 45,993 posts in 13,809 threads.
We currently have 37,085 members registered.

“Those Who Live by Anonymity, Die by Anonymity”

“Criminals are attracted to the dark net and Bitcoin due to the perceived anonymity that these technologies provide. TOR browsers and other programs limit law enforcement’s ability to track IP traffic back to the target. Dark net marketplaces by their very nature are unfriendly to law enforcement. (…) The use of these anonymizing technologies gives criminals a sense of invulnerability.

And that is how we get them.

As any experienced investigator will attest, de-anonymizing criminals on the internet is as much a matter of psychology as technology.”

Matthew J. Cronin, Hunting in the Dark: A Prosecutor’s Guide to the Dark Net and Cryptocurrencies, 66 U.S. ATT’Y BULL. (July 2018), p. 65 et seq.

“Those Who Live by Anonymity, Die by Anonymity”

“Dark net operators rely heavily on the powerful shield of anonymity that the dark net and cryptocurrencies provide them. Use their greatest asset against them. Just as agents cannot immediately identify a dark net target, the dark net target cannot identify an agent. Cloaked in the same anonymous technology, a well-trained federal agent can infiltrate any dark net criminal community. Operating undercover on the dark net, agents are able to generate tremendous amounts of information about their targets, potentially becoming a target’s valued customer or even a “friend.” That is especially true when an undercover agent gains access to an account with significant criminal transaction history (and thus digital street cred) or, even better, has longstanding ties to the target.”

Matthew J. Cronin, Hunting in the Dark: A Prosecutor’s Guide to the Dark Net and Cryptocurrencies, 66 U.S. ATT’Y BULL. (July 2018), p. 65 et seq.

Operation ARTEMIS

- In May 2016, Australian LEA (Taskforce ARGOS) were being offered access to the account details of a European moderator of the CSAM darknet site “The Giftbox Exchange” by a third-party LEA.

- This European agency sought out Taskforce ARGOS due to the stricter regulations placed on controlled operations in its own jurisdiction.

- At the same time, another CSAM forum, “Child’s Play”, was founded.

- Officers monitoring the Giftbox Exchange suspected a connection with Child’s Play due to a range of similarities in messages posted by Giftbox Exchange moderator CuriousVendetta and Child’s Play founder WarHead.

Operation ARTEMIS

- Both usernames could be traced to a Canadian man, Benjamin Faulkner, who was subsequently arrested along with Giftbox Exchange founder Patrick Falte in Montpelier, Virginia, on 1 October 2016.

- U.S. LEA was able to extract the passwords for Child’s Play from Faulkner, which were then passed on to Taskforce ARGOS and allowed them to take over control over the CSAM site.

The „ELYSIUM“-investigation

- At the beginning of 2017, the Australian police took over the account of the moderator of the website The Giftbox Exchange on the Darknet and came across a German who was already planning another CSAM site called “Elysium”.

- The Cybercrime Prosecution Centre of the State of Hesse (ZIT), a specialized unit of the General Public Prosecutor's Office in Frankfurt am Main took over the investigation.

- In June 2017, the site Elysium was shut down by the authorities. So far, 14 suspects and 29 victims have been identified and images have been found that pointed to perpetrators in Germany.

The „ELYSIUM“-investigation

- After locating the server of the Elysium platform, German law enforcement commenced electronic surveillance of the server and defendant one as well as undercover operations.

- The surveillance measures included uploading avatar images to confirm the server location as well as surveillance of messages sent.

- This helped identify defendants one and two.

- Additionally, in 2016 the German Bundeskriminalamt was sent abuse images of defendant three from which the image of a fingertip and, hence, the fingerprint of the abuser could be deduced thereby identifying defendant three.

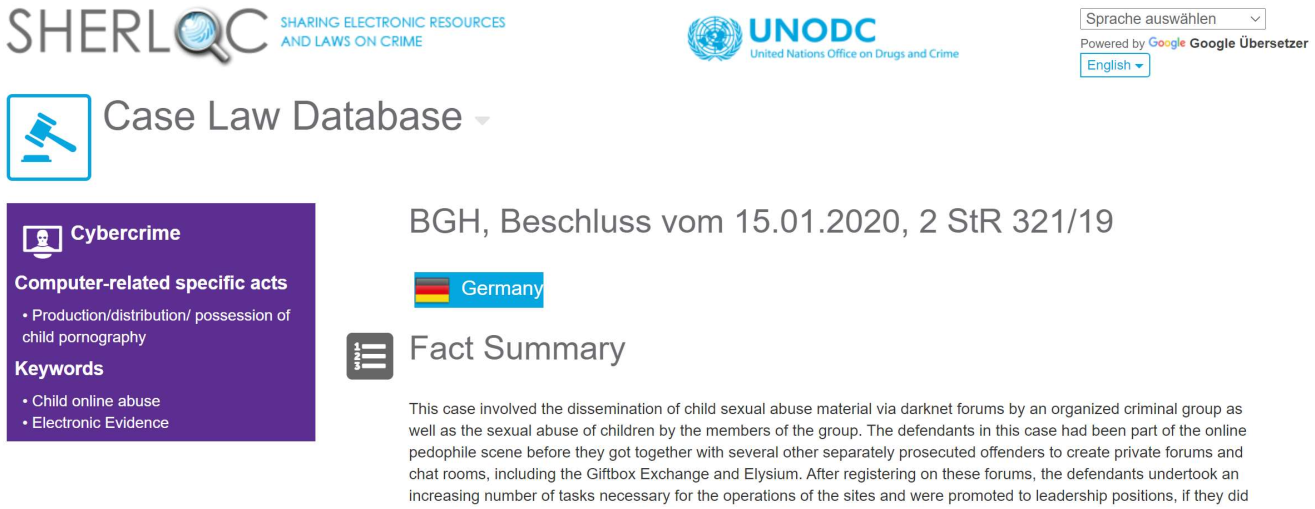
-

- By locating an in-memoriam site for the at-that-point-already-arrested defendant one, defendant four could be identified.

The „ELYSIUM“-investigation

- **The well-documented case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group.**
- **The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium.**

The „ELYSIUM“-investigation



SHERLOC SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME
UNODC United Nations Office on Drugs and Crime
Sprache auswählen
Powered by Google Google Übersetzer
English

Case Law Database

Cybercrime

Computer-related specific acts

- Production/distribution/ possession of child pornography

Keywords

- Child online abuse
- Electronic Evidence

BGH, Beschluss vom 15.01.2020, 2 StR 321/19

Germany

Fact Summary

This case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group. The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium. After registering on these forums, the defendants undertook an increasing number of tasks necessary for the operations of the sites and were promoted to leadership positions, if they did

New German legislation: police is now allowed to distribute fictual (computer generated) CSAM for the purpose of arresting perpetrators

Section 184b (5) of the German Penal Code (StGB) was supplemented by p. 2:

„Paragraph 1, numbers 1 and 4, shall not apply to official acts within the scope of criminal investigation proceedings if the act relates to child pornographic content that does not reflect an actual event and was also not produced using a picture recording of a child or juvenile, and the clarification of the facts would otherwise be futile or substantially impeded“

New German legislation: police is now allowed to distribute fictual (computer generated) CSAM for the purpose of arresting perpetrators

The offence exception is flanked by Section 110d of the German Code of Criminal Procedure (StPO), which provides that operations require

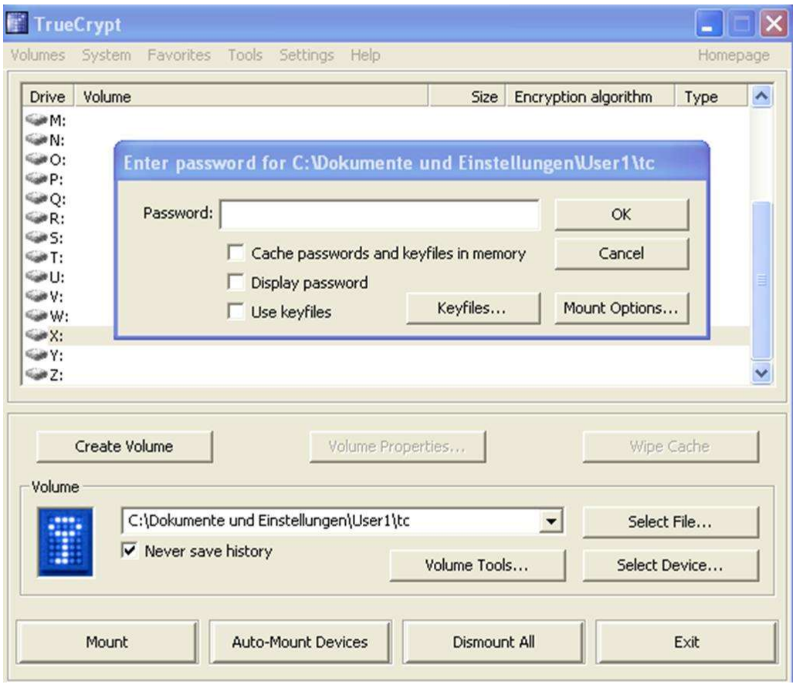
- A court order (in case of imminent danger, the consent of the public prosecutor's office is sufficient, but that the measure must be terminated unless there is a court order is given within three working days);

- It must be stated in the application by the PPO that the acting police officers have been comprehensively prepared for the operation; and

- The court order must be given in writing and be limited in time.

Case study - Encryption of storage media

- In Germany, a suspect is not obliged to hand over the credentials for encrypted storage media.



Enter password for C:\Dokumente und Einstellungen\User1\tc

Password:

☐ Cache passwords and keyfiles in memory

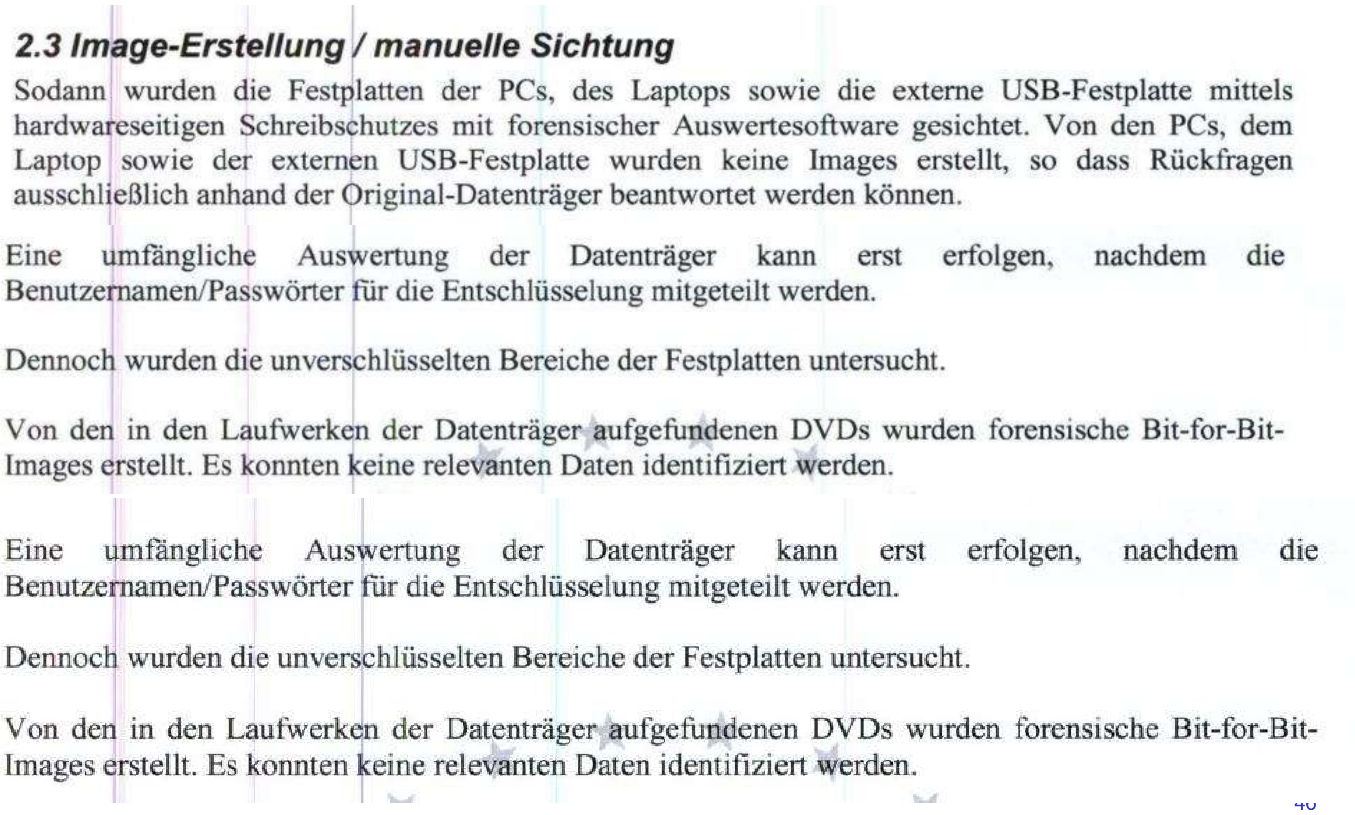
☐ Display password

☐ Use keyfiles

Volume: C:\Dokumente und Einstellungen\User1\tc

☑ Never save history

Without password: decryption of an encrypted device impossible



2.3 Image-Erstellung / manuelle Sichtung

Sodann wurden die Festplatten der PCs, des Laptops sowie die externe USB-Festplatte mittels hardwareseitigen Schreibschutzes mit forensischer Auswertesoftware gesichtet. Von den PCs, dem Laptop sowie der externen USB-Festplatte wurden keine Images erstellt, so dass Rückfragen ausschließlich anhand der Original-Datenträger beantwortet werden können.

Eine umfängliche Auswertung der Datenträger kann erst erfolgen, nachdem die Benutzernamen/Passwörter für die Entschlüsselung mitgeteilt werden.

Dennoch wurden die unverschlüsselten Bereiche der Festplatten untersucht.

Von den in den Laufwerken der Datenträger aufgefundenen DVDs wurden forensische Bit-for-Bit-Images erstellt. Es konnten keine relevanten Daten identifiziert werden.

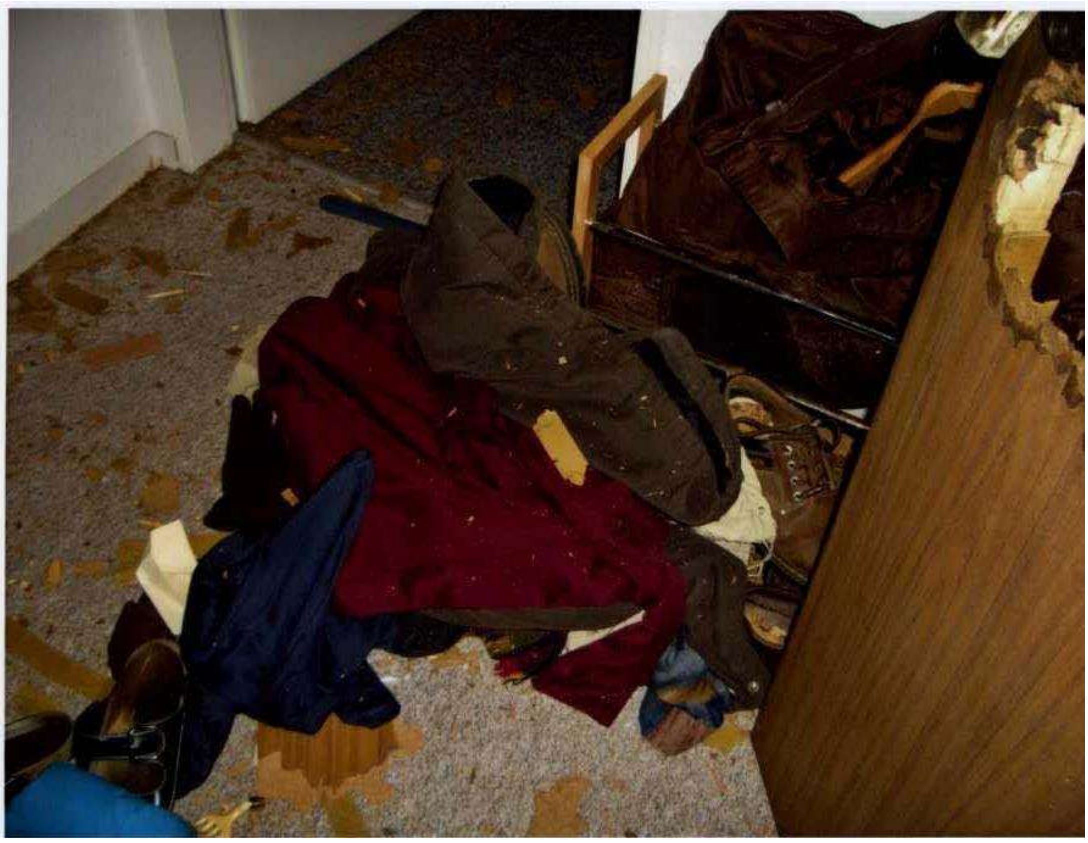
Eine umfängliche Auswertung der Datenträger kann erst erfolgen, nachdem die Benutzernamen/Passwörter für die Entschlüsselung mitgeteilt werden.

Dennoch wurden die unverschlüsselten Bereiche der Festplatten untersucht.

Von den in den Laufwerken der Datenträger aufgefundenen DVDs wurden forensische Bit-for-Bit-Images erstellt. Es konnten keine relevanten Daten identifiziert werden.

Solution: „No-Knock-Raid“: Interception of TC to check online activity…

… and then abruptly entering the premises with SWAT (example: use of explosives to open the door)



Legal basis for „No-Knock-Raids“

- In some legislations a special „no-knock“ warrant is needed.

- Judges may lawfully issue "no-knock" warrants where circumstances justify a no-knock entry, e.g. to prevent

  + physical harm to the officers or other persons,
  + the destruction of relevant evidence,
  + the escape of a suspect

- No-knock warrants have been controversial:

  + proportionality?
  + cases, where armed homeowners, believing that they are being invaded, have shot at officers, resulting in deaths on both sides

Discussion

Discussion

"Law enforcement agencies should be able to hack. It can be a legitimate and effective investigative technique. There is nothing inherently wrong with the government compromising computer systems. But appropriate procedural protections are vital, and present practices leave much room for improvement"

J. Mayer, Government Hacking, Yale Law Journal (2018), p. 570 et seq.

Discussion

"While the covert activities of Taskforce ARGOS are protected in the Queensland legal system, it remains in doubt as to if this intelligence can be lawfully used in jurisdictions where such methods would be deemed unlawful. In cases in which a police investigation is tarnished by unlawful conduct, most jurisdictions apply some form of the fruit of the poisonous tree doctrine that would rule evidence gathered by illegal means as inadmissible in a criminal trial."

Bleakley, Paul (2018), "Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks." The Police Journal: Theory, Practice, Principles, 92 (3) . pp. 221-236

Discussion

“Prohibit the practice of “forum shopping” in joint investigations and joint investigation teams:

The Draft Protocol should be limited to investigative measures that are authorised under the domestic laws of all participating Parties and, in particular, the domestic law applicable to the territory where the investigation is carried out. This is necessary to prevent forum shopping activities that could undermine fundamental rights protections under domestic law and international human rights law.”

Joint Civil Society Response to the provisional draft text on “Joint investigation teams and joint investigations” of the Cybercrime Convention Committee (T-CY), Dec. 2020, https://edri.org/wp-content/uploads/2020/12/CivilSocietySubmission_CoEProtocolBudapest_5thround.pdf

Thank you for your attention!
Questions? Remarks?

With the support of the Internal Security Fund-Police Programme
of the European Union 2014-2020

Fighting CSAM.

Don’t ignore it,
Report it!

INHOPE

1

Child sexual abuse online: the work of international organisations raising awareness, reducing the risks and removing the content

Don’t ignore it,
Report it!

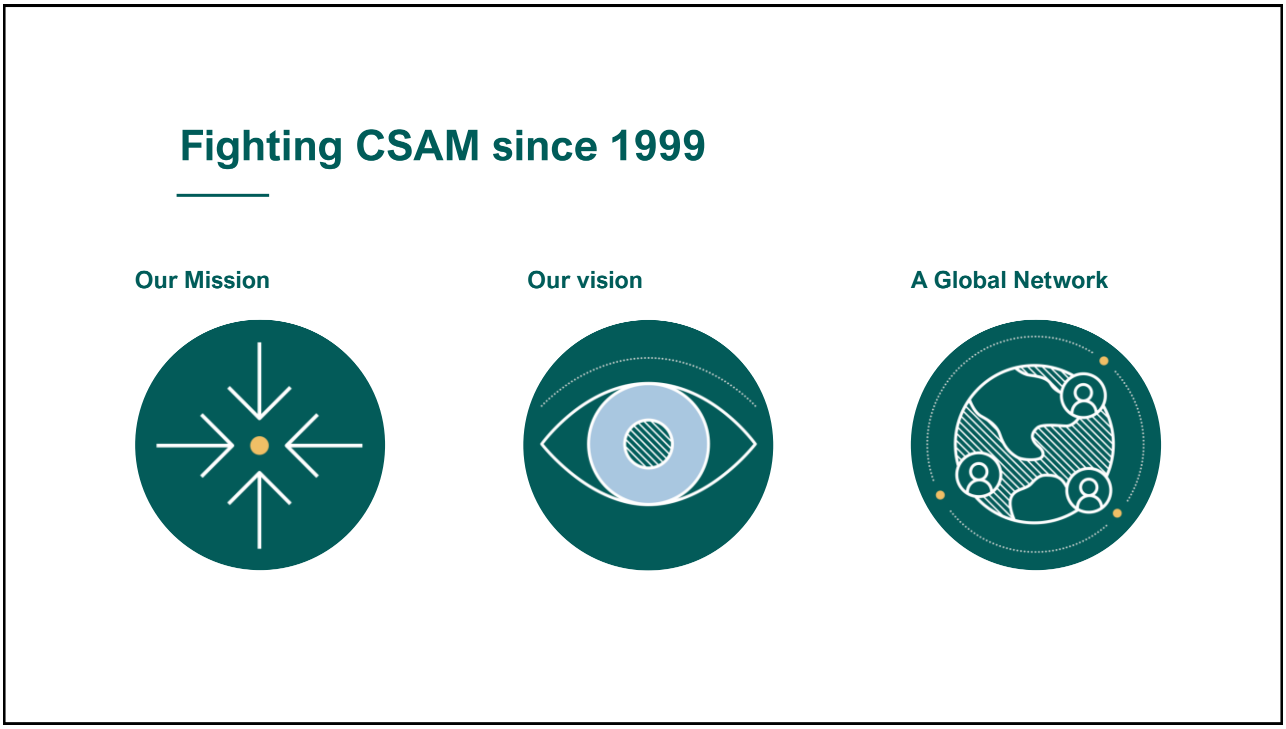
INHOPE

2

01

The story of INHOPE

3



Fighting CSAM since 1999

Our Mission

Our vision

A Global Network

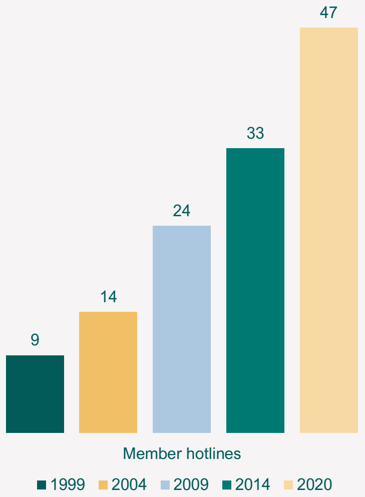
4

Who we are

INHOPE is the **global network** combatting online Child Sexual Abuse Material (CSAM).

The network consists of 47 hotlines in 43 countries (as of December 2020) that **provide the public with a way to anonymously report illegal content** online with a focus on CSAM.

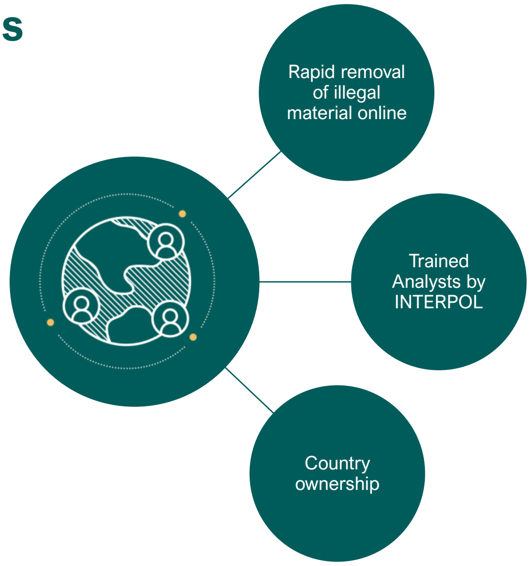
Reports are reviewed by **hotline content analysts trained by INTERPOL** who classify the illegality of the material, which is then shared with the national law enforcement agency and a Notice and Takedown order is sent to the relevant hosting provider. Confirmed CSAM is removed via the countries Notice and Takedown procedure.



5

The role of our hotlines

A hotline enables the public to anonymously report online material they suspect may be illegal. A hotline analyst will investigate the report and, if confirmed illegal, they act to have the content removed from the internet as rapidly as possible.

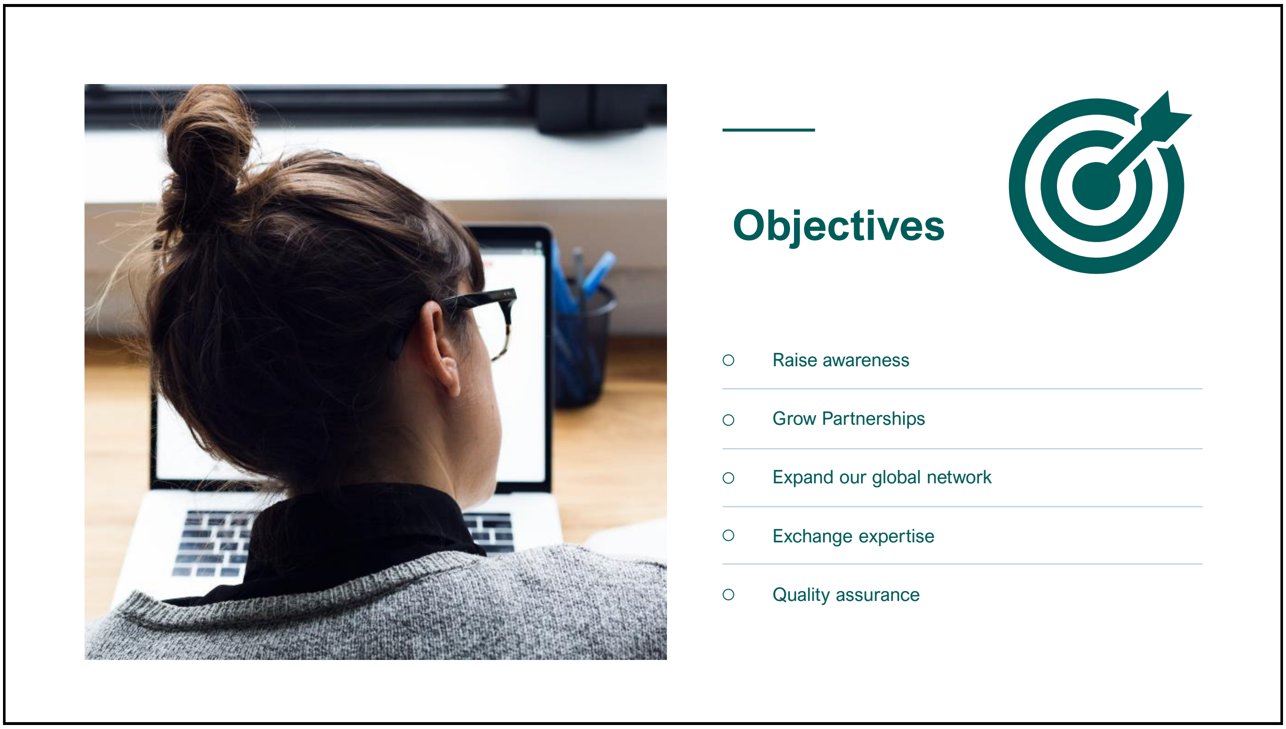


Rapid removal of illegal material online

Trained Analysts by INTERPOL

Country ownership

6



Objectives

- ○ Raise awareness
- ○ Grow Partnerships
- ○ Expand our global network
- ○ Exchange expertise
- ○ Quality assurance

7

02

INHOPE Projects

8

Better Internet for Kids

- Reducing risk
- Better Internet for Kids is a European Commission funded initiative aiming to create a better internet for Europe's children and youth https://www.betterinternetforkids.eu/
- Safer Internet Centers in every country consist of hotlines, helplines and awareness raising centers
- Insafe coordinates the network of awareness centers, helplines and youth panels
- INHOPE coordinates the network of hotlines.

Funded by
the European Union

9

What is ICCAM & Why is it important?
- removing content fast

How ICCAM works

- Concept
- Ecosystem
- Functionalities
- Requirements

ICCAM aims to

- Provide a secure exchange of CSAM reports between hotlines
- Enhance hotlines' capacity
- Facilitate image/video hashing/fingerprinting and crawling technologies
- Streamline hotlines' workflow and content assessment
- Escalate "new" CSAM
- Reduce number of duplicates
- •Feeds INTERPOL's ICSE database

Who created ICCAM

- ICCAM was developed by INHOPE and Ziuz Forensics with funding from the European Commission

Funded by
the European Union

10

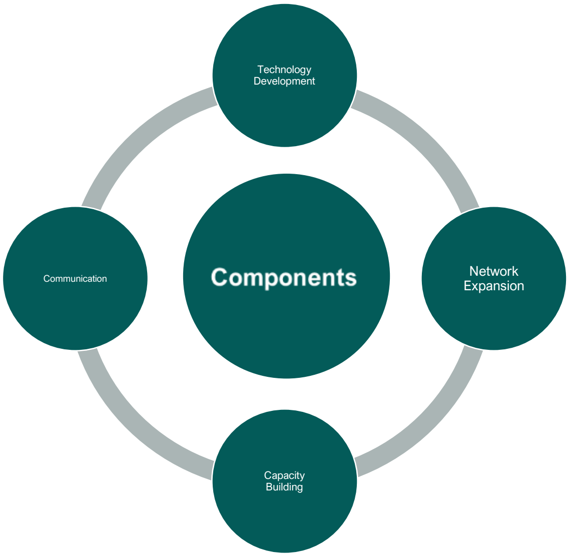
Save time,
Save lives
Improve assessment workflow
A
B
C
Long-term practical Solutions
Funded by the European Union's Internal Security Fund
EU project

The AviaTor Project

- Efficient tool to prioritise processing industry reports received by the National Centre for Missing and Exploited Children (NCMEC) in the USA
- Automation and intelligence to support law enforcement agencies (LEAs)
- Configurable to the needs of LEA
- Automatically crawls online sources for additional information for investigations (in accordance with the national legal requirements.)

11

End Violence Against Children



Project ESCAPE

- Donor: End Violence Against Children Fund
- Partners: INHOPE and ZiuZ
- Timeline: Oct 2020- Sept 2022
- Enhanced technology, Report Box, 4 new hotlines
- Communication toolkits & tailor-made training

12

Network Expansion

Initiatives that expand our reach are essential. In some instances local organisations approach INHOPE to establish a national hotline and in others we approach them.

INHOPE uses its **Country Assessment Framework Tool** to understand which should be priority countries for the establishment of a hotline.

13

Timeline for creating your INHOPE hotline

INHOPE

Once a request to establish a hotline is received, INHOPE conducts a country review using a country assessment framework.

INHOPE undertakes a due diligence mission to establish if La Strada is fit for purpose.

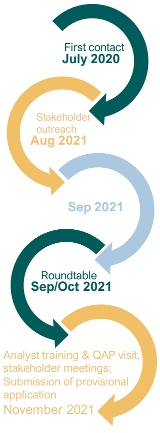
If La Strada is appropriate for a hotline, INHOPE organises a meeting to provide an overview of what a hotline does, the INHOPE network of hotlines, including a discussion of expectations from both parties.

Approx. time period:
July 2020 first meetings with commitment to apply for INHOPE membership December 2021

INHOPE schedules monthly meetings with La Strada. During this period, INHOPE assists with:
- Organisation of a roundtable with relevant stakeholders;
- Preparing La Strada to operate a hotline with the support of templates and best practices developed by the network of hotlines;
- Preparation of La Strada's application for INHOPE membership.

INHOPE holds a **Report Box** Training for La Strada. The technical manual can be downloaded **here.**

Both INHOPE and La Strada together start to **plan the timeline** for the stakeholder roundtable. The stakeholder roundtable should take place between months 7 and 11.



First contact
July 2020

Stakeholder outreach
Aug 2021

Sep 2021

Roundtable
Sep/Oct 2021

Analyst training & QAP visit, stakeholder meetings; Submission of provisional application
November 2021

A large amount of energy and time needs to be invested in the first six months of setting-up a hotline in any country. Timelines differ per hotline. INHOPE will assist you through all the steps laid out here to succeed in the development of a hotline in your country. #reportit!

La Strada

START: La Strada contacts INHOPE and expresses interest to establish a national hotline. *The process to establish an INHOPE hotline is started here - congratulations!*

La Strada schedules a meeting with the national law enforcement agency (LEA) to introduce and explain the role of a hotline. Ultimately the hotline requires an official agreement with LEA e.g., Memorandum of Understanding. This agreement allows La Strada to analyse online CSAM and send it on to LEA and to industry for rapid removal. LEA outreach can take a long time so this must be started as soon as process commences. INHOPE assists as necessary.

Approx. time period:
August-November 2021

In addition to LEA, La Strada must start to gather support and written letters from:
- Government departments (e.g., Ministries of Interior, Education, Digital Transformation);
- Technology Industry (e.g., hosting providers, social media platforms, telecommunications companies and manufacturers)
- NGOs in child advocacy and child protection space
INHOPE will supply example letters to La Strada.

Approx. time period:
August-November 2021

La Strada ensures a web-reporting form is in place and informs INHOPE. Examples include eco Germany Hotline Web-Reporting and Spanish Hotline Web-Reporting. INHOPE will provide a template and best practices for a web-reporting form.

14

Timeline for creating your INHOPE hotline cont'd.

INHOPE

Communications Guidance
INHOPE's Communications team assists La Strada with awareness-raising campaigns and publicity of the newly-established hotline. This includes guidance and advice on launching a general hotline campaign to ensure that the national public are aware of the need to report online CSA.

Quality Assurance Visit
INHOPE conducts a Quality Assurance visit to assess the hotline's operations on:

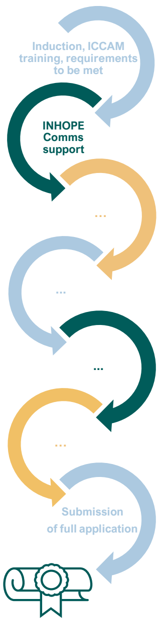
- Report handling
- Cooperation with key stakeholders
- Visibility
- Staff Welfare
- Physical & IT security
- Membership compliance.

Approx. time period:
Due to COVID-19 all Hotline Training meetings of 2021 are online.

Hotline Training Meeting
La Strada is invited to the bi-annual INHOPE Hotline Training Meeting to learn and exchange best practices with other INHOPE hotlines.

Training
INHOPE conducts CORE Training and INTERPOL Content Assessment Training for the new provisional member La Strada.

Full Membership Application
If the provisional member, La Strada, is ready, their application for full membership is discussed with INHOPE's Network Expansion Task Group. The Task Group can recommend the hotline for **full** membership to INHOPE network.


Induction, ICCAM training, requirements to be met
INHOPE Comms support
...
...
...
...
Submission of full application

La Strada

Approx. time period:
September-November 2021

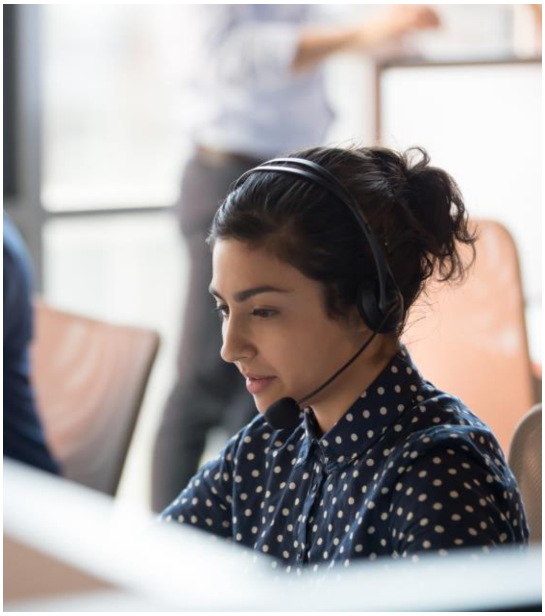
Quality Assurance visit
La Strada welcomes INHOPE to conduct a Quality Assurance visit to determine whether or not La Strada is ready to apply for provisional membership at INHOPE.

INHOPE Annual General Meeting
One month prior to an INHOPE Annual General Meeting (AGM), La Strada must meet all requirements of the Provisional Membership Checklist. La Strada's application for membership is voted upon during the Annual General Meeting by INHOPE members. The hotline La Strada is a provisional member of INHOPE.

Recommendations and requirements
The hotline improves its operations according to the recommendations made during the Quality Assurance Visit and reports back to INHOPE.

Full Membership Application
The provisional member, La Strada, meets all criteria for full membership and submits its application at least one month before the next Members Meeting.

15



Training

○ CORE Training

○ Content Assessment/ICCAM Training at INTERPOL

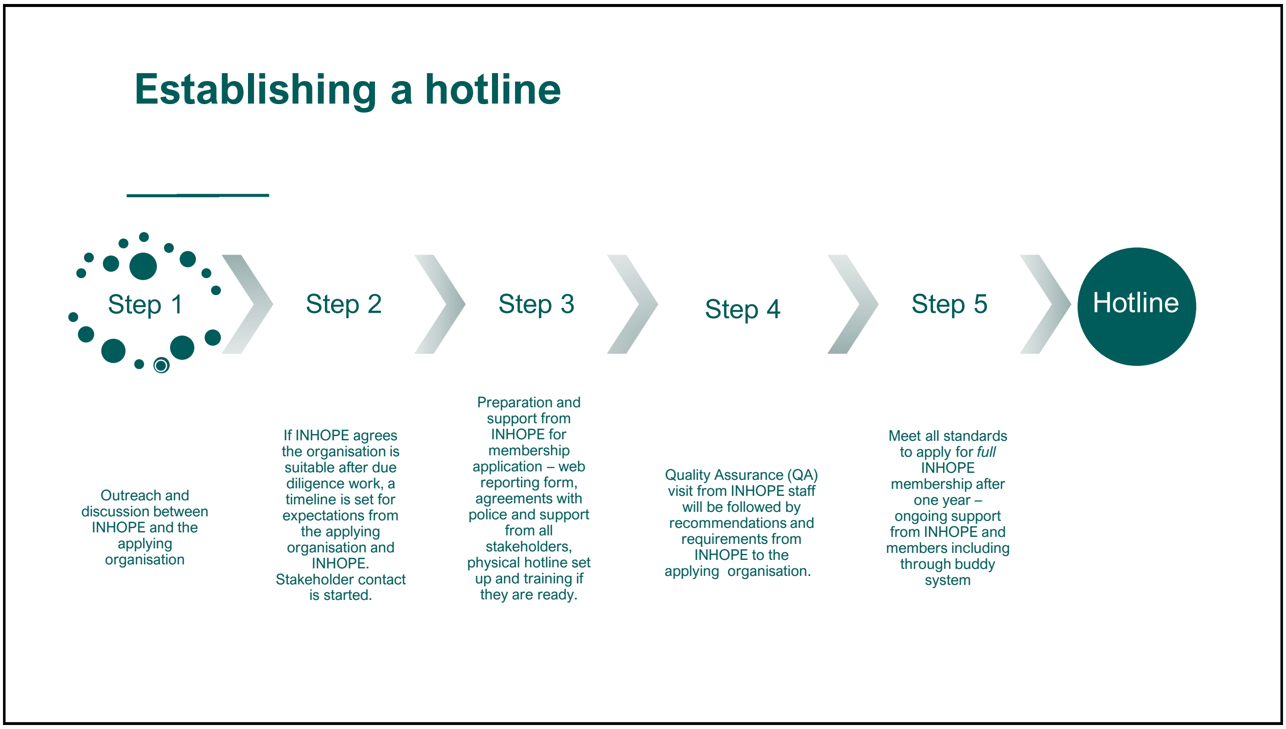
○ Online learning management system

○ Workshop for advanced analysts

○ INHOPE Slack platform and Buddy hotlines

○ Monthly Q&A and Mindfulness sessions for analysts

16



Establishing a hotline

Step 1: Outreach and discussion between INHOPE and the applying organisation

Step 2: If INHOPE agrees the organisation is suitable after due diligence work, a timeline is set for expectations from the applying organisation and INHOPE. Stakeholder contact is started.

Step 3: Preparation and support from INHOPE for membership application – web reporting form, agreements with police and support from all stakeholders, physical hotline set up and training if they are ready.

Step 4: Quality Assurance (QA) visit from INHOPE staff will be followed by recommendations and requirements from INHOPE to the applying organisation.

Step 5: Meet all standards to apply for *full* INHOPE membership after one year – ongoing support from INHOPE and members including through buddy system

17

03

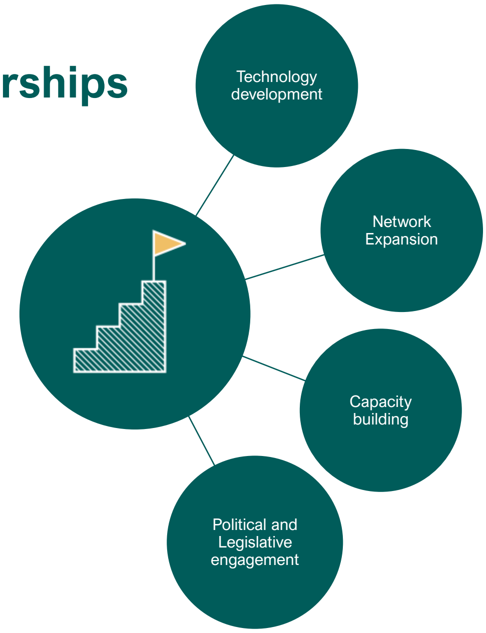
Partnerships: organisations fighting CSAM with INHOPE

18

Key to Success - Partnerships

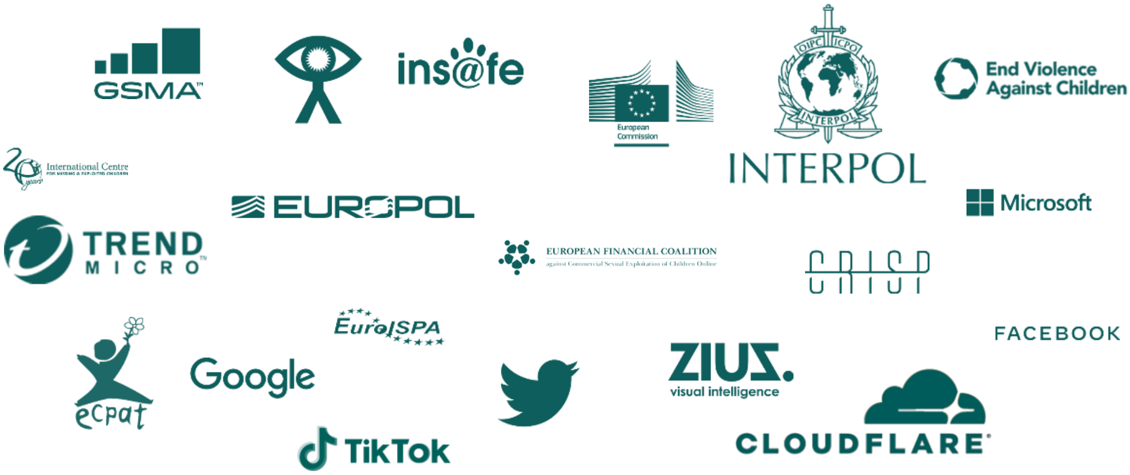
INHOPE works with partners who also believe in our mission to combat Child Sexual Abuse Material online by growing and supporting our global network of hotlines using a multi stakeholder approach.

Our partnerships enable and strengthen the hotline-corporate relationship to protect the public, as well as victims of online abuse by issuing notices for rapid removal of confirmed CSAM.



19

Partnerships



20

Events & Activities

INHOPE Summit

Packed with presentations from industry experts, and panel discussions, INHOPE's Annual Summit brings together like-minded individuals from technology, law enforcement and industry partners to ensure that INHOPE's network of 46 hotlines continue to remove online CSAM as rapidly as possible.

- Most effective channels for invitations 30% WOM, 23.33% newsletters, 20% direct mail.
- 2,515 organic website visits and 420 organic article reads.
- 160+ attendees
- 4.6/5 from survey respondents.
- Increased awareness of CSAM and the role that both hotlines and industry play.
- New discussions and collaborations.

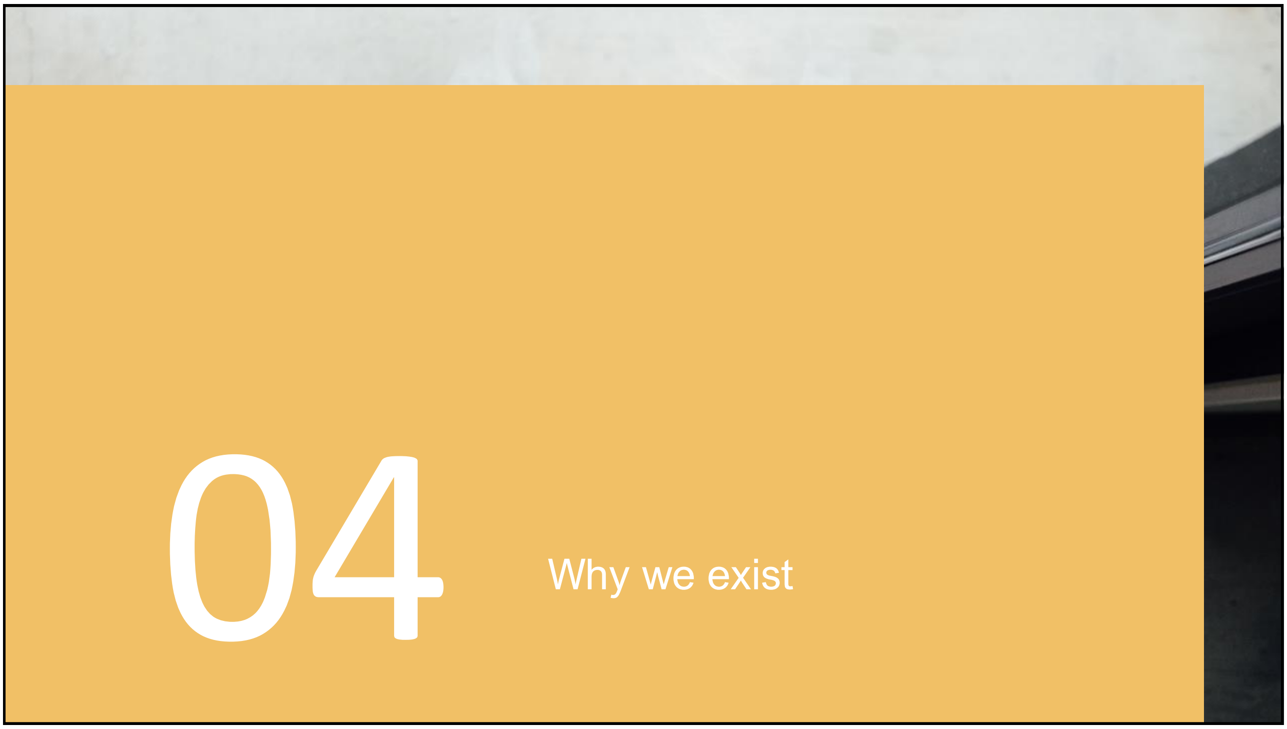
Expert Insights

With 500+ registered attendees working for over 200 different organisations and based in nearly 50 countries, the Expert Insights season was an opportunity for a truly global meeting of minds, all looking for ways to strengthen their collaboration with others and exchange ideas.

These INHOPE webinars are tailored to facilitate greater collaboration among those working in the fight against Child Sexual Abuse Material (CSAM).

- Analysts processing reports of CSAM
- Law Enforcement involved in investigating cybercrime and child sexual abuse cases
- Policy advisors in private companies and governmental bodies
- Technology specialists and those developing tools to detect CSAM and process reports
- Academics researching the latest trends and offender patterns in CSAM sharing
- Communications and marketing teams spreading the word about online child protection
- Psychologists and counsellors working directly with offenders and survivors

21

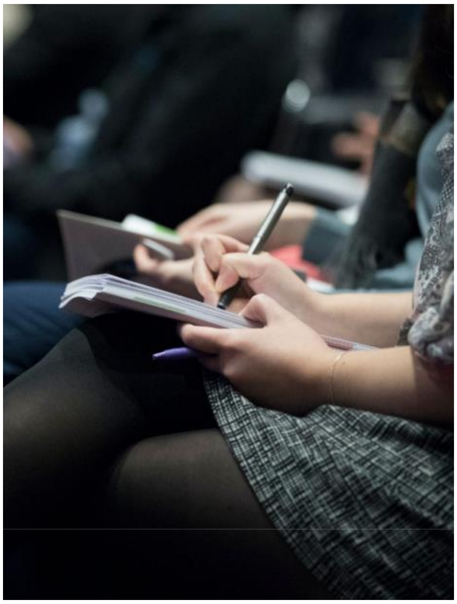


04 Why we exist

22

Exchanging Expertise

- INHOPE builds capacity of hotlines worldwide by organising Hotline Training Meetings, Focus Groups and the INHOPE summit for tech companies, policy experts and decision-makers
- INHOPE organises seasonal webinars
- Hold bi-annual training meetings for hotline managers and analysts
- INHOPE runs a monthly members newsletter, quarterly partner newsletter, and updates/insights mailing lists

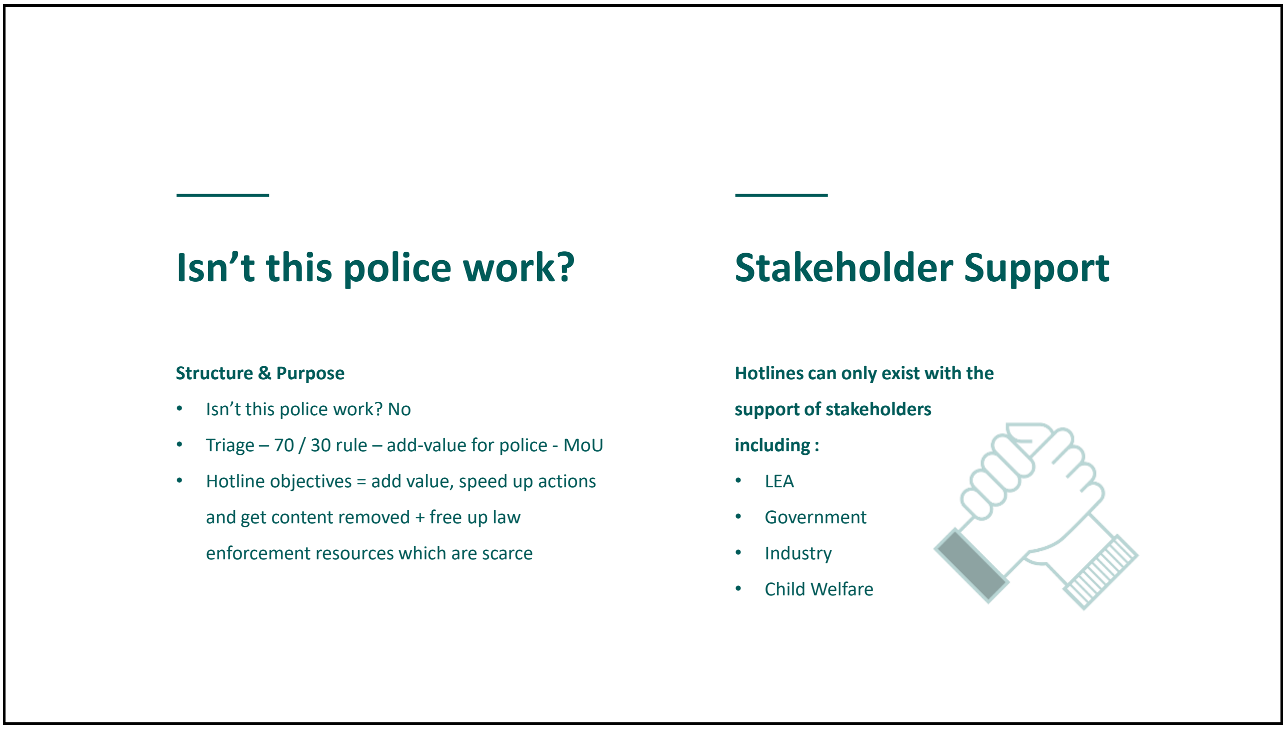


23

VALUE – training, supporting and linking our hotlines and national LE

- CSAM is **transnational**, crosses borders, jurisdictions – thus policies and actions aimed at mitigating risks relating to CSAM demand international collaboration
- The INHOPE Network provides the possibility to **exchange reports legally**
- BPPs, training, support and hotlines support each other, buddy systems, change legislation
- **ICCAM system** – allows for instant exchange of reports when hosted in other countries (often multiple)
- **Fast action to remove content** due to international network – speed is crucial
- Get evidence preserved so police can investigate

24



Isn't this police work?

Structure & Purpose

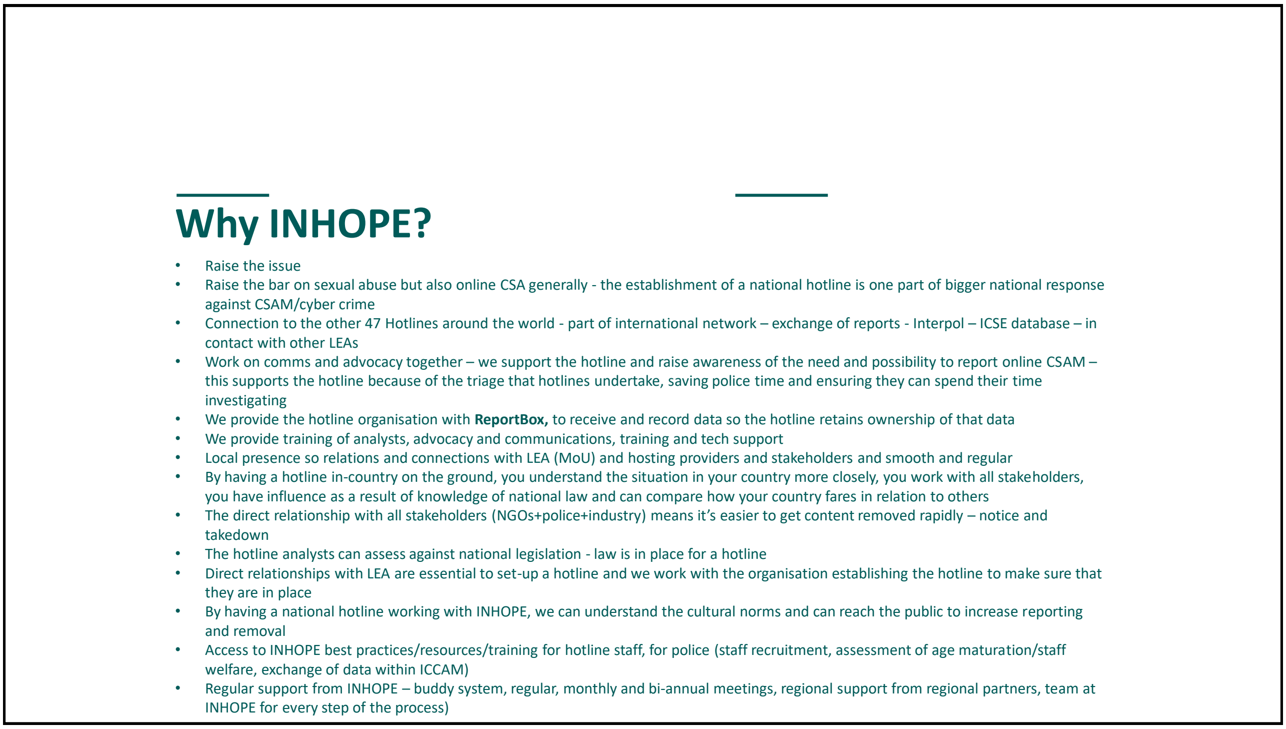
- Isn't this police work? No
- Triage – 70 / 30 rule – add-value for police - MoU
- Hotline objectives = add value, speed up actions and get content removed + free up law enforcement resources which are scarce

Stakeholder Support

Hotlines can only exist with the support of stakeholders including :

- LEA
- Government
- Industry
- Child Welfare

25



Why INHOPE?

- Raise the issue
- Raise the bar on sexual abuse but also online CSA generally - the establishment of a national hotline is one part of bigger national response against CSAM/cyber crime
- Connection to the other 47 Hotlines around the world - part of international network – exchange of reports - Interpol – ICSE database – in contact with other LEAs
- Work on comms and advocacy together – we support the hotline and raise awareness of the need and possibility to report online CSAM – this supports the hotline because of the triage that hotlines undertake, saving police time and ensuring they can spend their time investigating
- We provide the hotline organisation with **ReportBox,** to receive and record data so the hotline retains ownership of that data
- We provide training of analysts, advocacy and communications, training and tech support
- Local presence so relations and connections with LEA (MoU) and hosting providers and stakeholders and smooth and regular
- By having a hotline in-country on the ground, you understand the situation in your country more closely, you work with all stakeholders, you have influence as a result of knowledge of national law and can compare how your country fares in relation to others
- The direct relationship with all stakeholders (NGOs+police+industry) means it's easier to get content removed rapidly – notice and takedown
- The hotline analysts can assess against national legislation - law is in place for a hotline
- Direct relationships with LEA are essential to set-up a hotline and we work with the organisation establishing the hotline to make sure that they are in place
- By having a national hotline working with INHOPE, we can understand the cultural norms and can reach the public to increase reporting and removal
- Access to INHOPE best practices/resources/training for hotline staff, for police (staff recruitment, assessment of age maturation/staff welfare, exchange of data within ICCAM)
- Regular support from INHOPE – buddy system, regular, monthly and bi-annual meetings, regional support from regional partners, team at INHOPE for every step of the process)

26

Why you should care about having a hotline ?

- Because the INHOPE network reduces the risk of children becoming victims of CSAM – supply/ demand
- The sooner it is removed from the internet preventing re-sharing / copying and minimising continual revictimisation
- Law enforcement (nationally) are advised rapidly
- Interpol victim ID team advised of any new material directly through ICCAM
- ICCAM means less duplication - less trauma for analysts
- ICCAM feeds ICSE database
- ICCAM makes us more efficient - it delivers real time data

How will we help you?

- We make sure that you know have everything in place to set-up a hotline about your national hotline and we never stop supporting you!
- We help coordinate meetings with all your stakeholders and we join the meetings
- We do everything we can to make sure that the Hotline is allowed to operate effectively
- We provide you with an advocacy and communications toolkit and playbook
- We train your staff (INHOPE and INTERPOL and then every six months they have three days of training)

27

End Violence Against Children

INHOPE’s vision is a world free of Child Sexual Abuse Material.

INHOPE

28

Thanks for listening.

Samantha Woolfe
Partnerships and Network Expansion Lead
samantha.woolfe@inhope.org

INHOPE

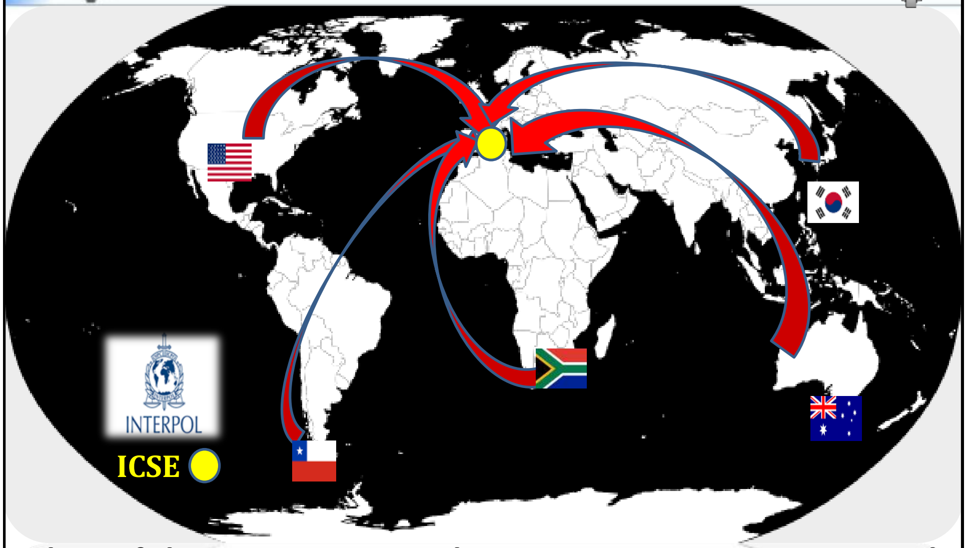
National Police Headquarters
Criminal Bureau

Victim identification efforts based on analysis of the child abuse material

With the support of the Internal Security Fund-Police Programme of the European Union 2014-2020

1

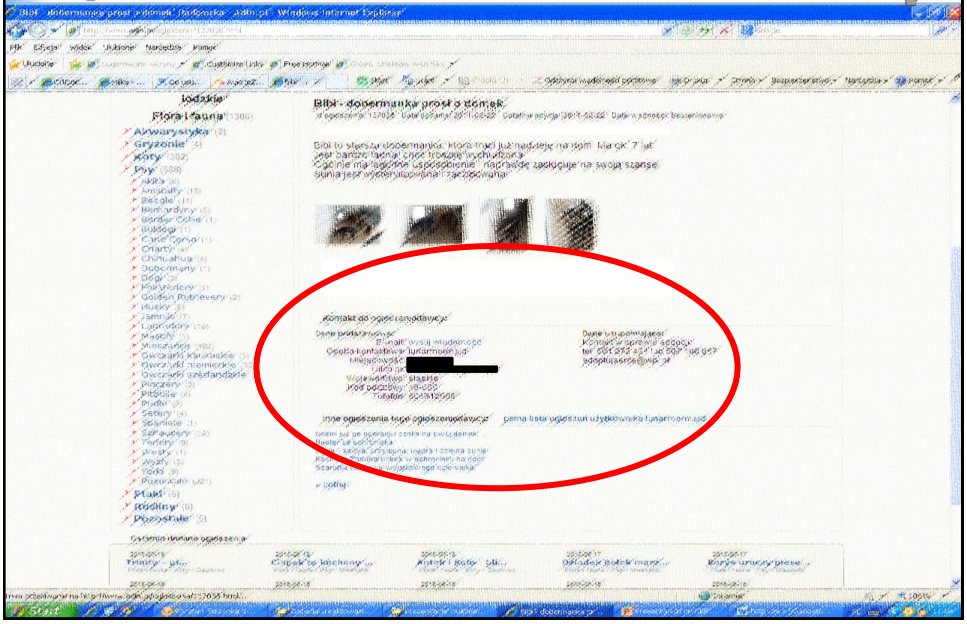
National Police Headquarters
Criminal Bureau



Flow of the CAM to Interpol ICSE Data Base – International Child Sexual Exploitation Data Base

2

National Police Headquarters
Criminal Bureau



Bibi - dobermanka prosi o domek, Radomsko - Adin.pl - Windows Internet Explorer

łódzkie
Flora i fauna (300)
- Akwarystyka (5)
- Gryzonie (4)
- Koty (382)
- Psy (888)
  - Akita (6)
  - Amstaffy (18)
  - Beagle (11)
  - Bernardyny (5)
  - Border Collie (1)
  - Buldogi (1)
  - Cane Corso (1)
  - Charty (4)
  - Chihuahua (4)
  - Dobermany (7)
  - Dogi (3)
  - Foksteriery (1)
  - Golden Retrievery (2)
  - Husky (8)
  - Jamniki (7)
  - Labradory (18)
  - Mastify (5)
  - Mieszańce (192)
  - Owczarki kaukaskie (5)
  - Owczarki niemieckie
  - Owczarki szetlandzkie
  - Pinczery (3)
  - Pitbulle (6)
  - Pudle (2)
  - Setery (4)
  - Spaniele (1)
  - Sznaucery (12)
  - Teriery (9)
  - Westy (1)
  - Wyżły (3)
  - Yorki (9)
  - Pozostałe (21)
- Ptaki (5)
- Rośliny (6)
- Pozostałe (5)

Bibi - dobermanka prosi o domek

Id ogłoszenia: 137038 Data dodania: 2011-02-22 Ostatnia edycja: 2011-02-22 Data ważności: bezterminowo

Bibi to starsza dobermanka, która traci już nadzieję na dom. Ma ok. 7 lat, jest bardzo ładna, choć troszkę wychudzona. Ogólnie ma łagodne usposobienie, naprawdę zasługuje na swoją szansę. Sunia jest wysterylizowana i zaszczepiona.

Kontakt do ogłoszeniodawcy:

Dane podstawowe:
E-mail: wyślij wiadomość
Osoba kontaktowa: lunarmorm.pd
Miejscowość: [redacted]
Województwo: śląskie
Kod pocztowy: [illegible]
Telefon: [illegible]

Dane uzupełniające:
Kontakt w sprawie adopcji:
tel. [illegible]
[illegible]@wp.pl

Inne ogłoszenia tego ogłoszeniodawcy: pełna lista ogłoszeń użytkownika lunarmorm.pd

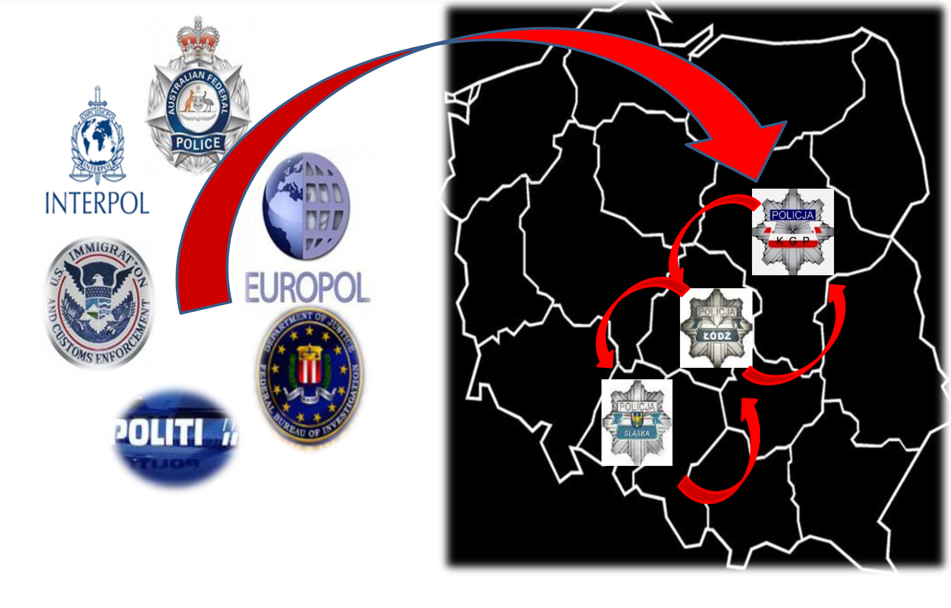
[illegible]

« cofnij

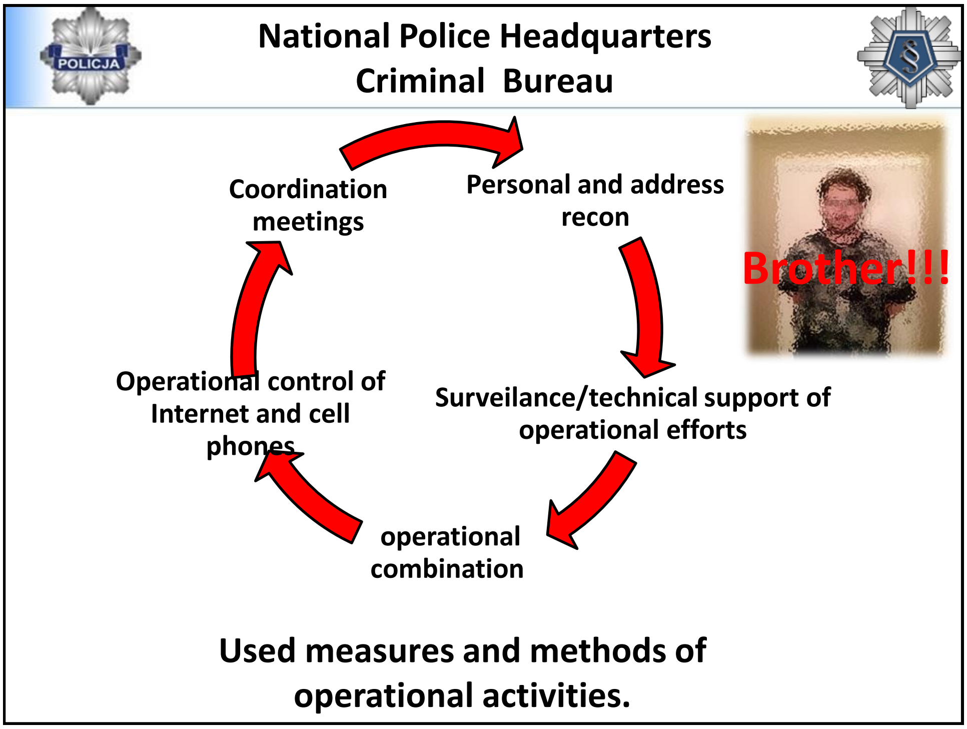
Ostatnio dodane ogłoszenia

Trinity - pi... | Czapek to kochany... | Kotek i Bolo... | Dołądek Bolek mazz... | Boryś uroczy piese...

National Police Headquarters
Criminal Bureau



INTERPOL
AUSTRALIAN FEDERAL POLICE
EUROPOL
IMMIGRATION AND CUSTOMS ENFORCEMENT
FEDERAL BUREAU OF INVESTIGATION
POLITI
POLICJA K G P
POLICJA ŁÓDŹ
POLICJA ŚLĄSKA



National Police Headquarters
Criminal Bureau

Coordination meetings

Personal and address recon

Surveilance/technical support of operational efforts

operational combination

Operational control of Internet and cell phones

Used measures and methods of operational activities.

15

National Police Headquarters
Criminal Bureau

The same carpet as on ICSE series

The same linoleum as on ICSE series

Arrested on 31 August 2015

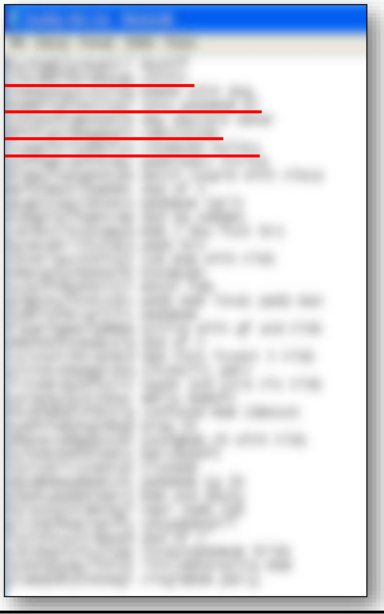
The same bed

The same bike

Execution of the search warrant – the flat where the suspect abused his sister

16

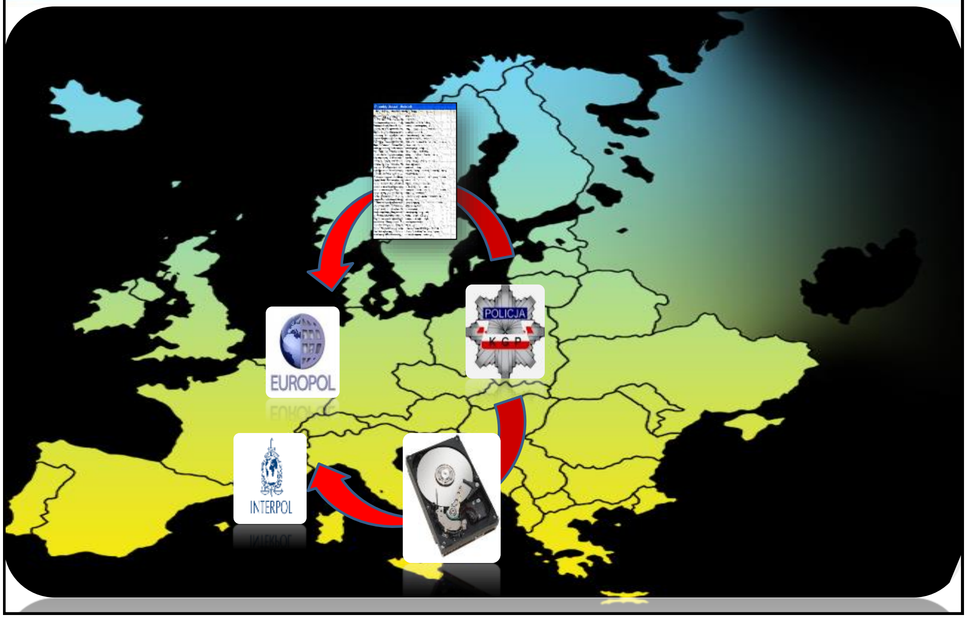
National Police Headquarters
Criminal Bureau



Seizure of the Torchat buddy-list – list of suspect’s contacts. At least four next perpetrators from Poland.

17

National Police Headquarters
Criminal Bureau

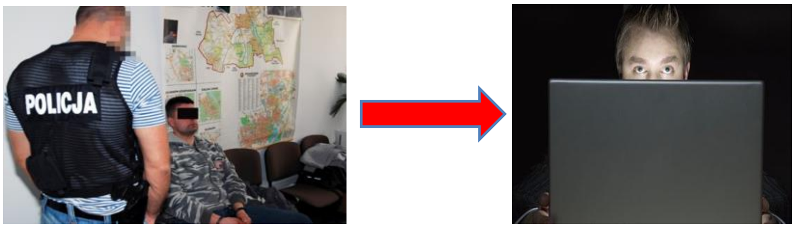


18

National Police Headquarters
Criminal Bureau

Next steps in the investigation:

Organization of the proceedings experiment in the frame of on-going investigation - under Police control the live chat of the suspect on TorChat (as “gravi”) and other services he used in his criminal activity such as pedo-bulletin boards in TOR network.



19

National Police Headquarters
Criminal Bureau

The most promising results of the experiment:

- **establishment of the contact with “voinic” again;**
- **obtaining and seizure of CAM sent to our suspect by „voinic”;**
- **obtaining information about two additional Polish hands-on abusers;**
- **obtaining data leading to „voinic” identification;**
- **uploading of seized CAM into ICSE DB: part of the material completely new.**

20

National Police Headquarters
Criminal Bureau

(21:38:27) voinic: I'll be in KRK (*Cracow*) in December, we may meet if you want
(21:39:02) myself: what time, cause I want to go to my parents for Christmas
(21:39:17) voinic: before Christmas, second week
(21:39:50) myself: well, I'll be not far away
(21:40:33) myself: you planning to bring some girl? so we don't get bored
(21:40:54) voinic: mmm, that would be cool :)
(21:41:18) voinic: we may go to aqua park to have a look
(21:41:44) voinic: or simply we gonna watch movies in the hotel

(21:42:21) myself: such a girl would be a nice present for Santa clause day or for Christmas, just tie in a bow and put under the Christmas tree
(21:43:59) myself: and in the aqua park you can have a great view ;)
(21:44:21) voinic: so, for example on Sunday the 6th before afternoon when the kids are
(21:54:03) myself: about this meeting we shall arrange in one day or you staying longer?
(21:54:23) voinic: I'll be there for whole week

23

National Police Headquarters
Criminal Bureau

(22:06:20) voinic: on Sunday the 6th from 11 a.m. I'll be at the aqua park which is at Good Sheppard Street.
(22:07:43) voinic: I'll have deep blue towel and black shower cap with yellow oval emblem
(22:08:14) myself: ok I'll try to be there, but first I must collect the money
(22:08:41) voinic: I'll pay you back for the train ticket and aqua park ticket if you want
(22:09:35) myself: shit man, thanks, in such situation I'll be there for sure
(22:10:03) voinic: relax
(22:10:54) voinic: take swimming trunks and towel with you :)
(22:11:13) voinic: I see that caps are not mandatory
(22:12:02) myself: ok, I'll take orange towel and I'll wait for you about 11 at..?
(22:12:30) voinic: inside
(22:13:18) voinic: every 15 minutes I will check the place opposite to the dragon

24

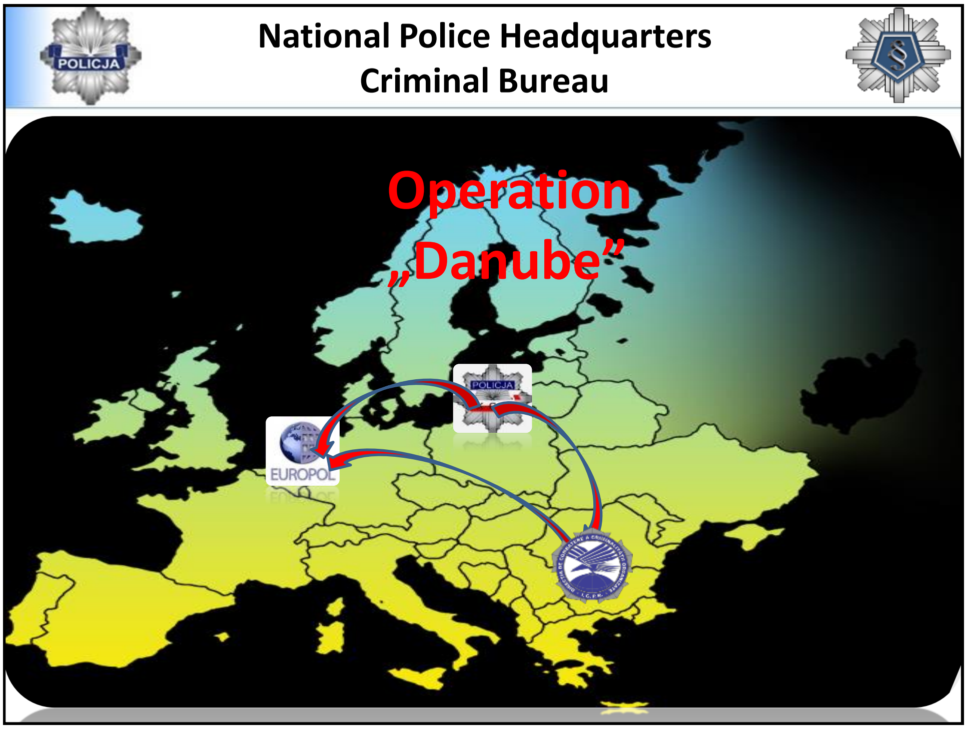
National Police Headquarters
Criminal Bureau

(22:13:53) myself: this dragon, it’s some kind of a fountain?
(22:14:02) voinic: yes
(22:14:26) voinic: opposite there is also fitness room at the first floor
(22:14:52) voinic: it’s under the middle window
22:18:37) voinic: when you already recognize me or I recognize you, I will ask if you know what the way to pay for the sauna is
(22:19:07) voinic: and you will say that you don’t know but you heard it is not worthy to go there

Conducting Police surveillance at the aqua park and positive identification of „voinic” – 27yo project coordinator and PR manager in Polish Institute in Bucharest (part of Polish Embassy) in Romania.

National Police Headquarters
Criminal Bureau

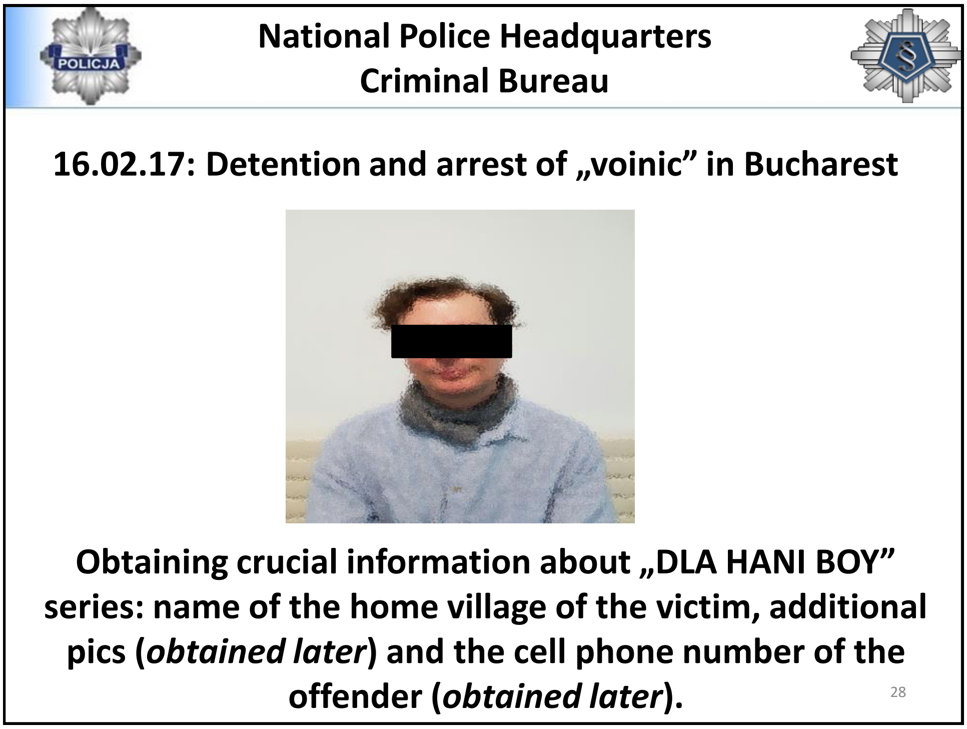
- establishment of operational and procedural cooperation with Romanian colleagues (Police and Prosecutor Office);
- „voinic” case linked to operation „Downfall 2”
- ongoing investigation;
- identification efforts focused on new ICSE series (DLA HANI BOY, etc.);
- new links and cases – operation „Danube”



National Police Headquarters
Criminal Bureau

Operation „Danube"

27



National Police Headquarters
Criminal Bureau

16.02.17: Detention and arrest of „voinic" in Bucharest

Obtaining crucial information about „DLA HANI BOY" series: name of the home village of the victim, additional pics (*obtained later*) and the cell phone number of the offender (*obtained later*).

28

28

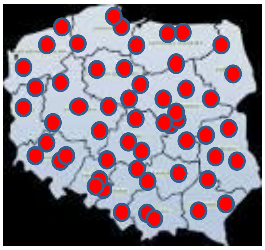
National Police Headquarters
Criminal Bureau

Follow – up of the both operations

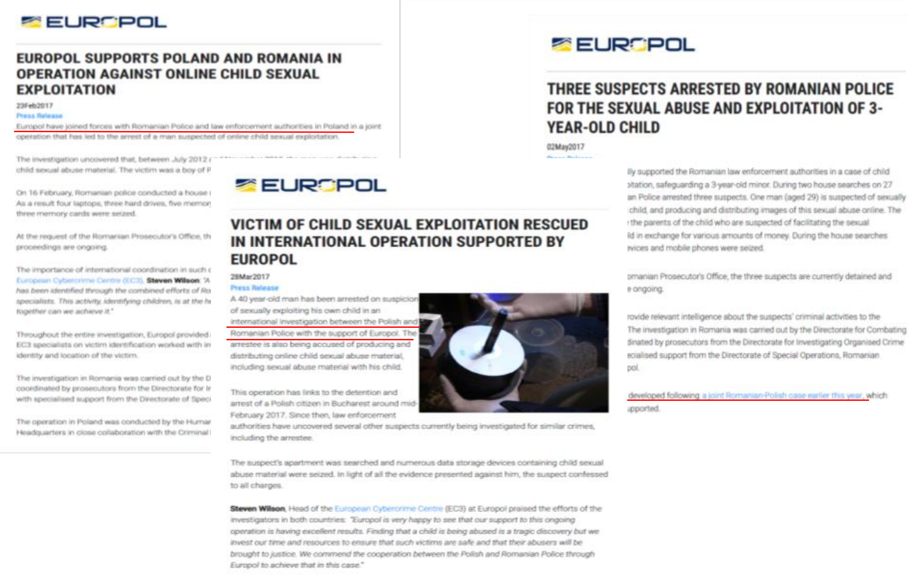
So far (5 May 2021) in the frame of the investigation 90 individuals have been detained from whom

- 42 have been temporarily arrested,
- 34 are under the surveillance of Police,
- 29 are banned to leave the country,

84 000 PLN (approx. 18750 euro) has been seized.



National Police Headquarters
Criminal Bureau



EUROPOL

EUROPOL SUPPORTS POLAND AND ROMANIA IN OPERATION AGAINST ONLINE CHILD SEXUAL EXPLOITATION

23Feb2017

Press Release

Europol have joined forces with Romanian Police and law enforcement authorities in Poland in a joint operation that has led to the arrest of a man suspected of online child sexual exploitation.

The investigation uncovered that, between July 2012 a
child sexual abuse material. The victim was a boy of P

On 16 February, Romanian police conducted a house
As a result four laptops, three hard drives, five memor
three memory cards were seized.

At the request of the Romanian Prosecutor's Office, th
proceedings are ongoing.

The importance of international coordination in such c
European Cybercrime Centre (EC3), **Steven Wilson**: "A
has been identified through the combined efforts of Ro
specialists. This activity, identifying children, is at the he
together can we achieve it."

Throughout the entire investigation, Europol provided
EC3 specialists on victim identification worked with in
identity and location of the victim.

The investigation in Romania was carried out by the D
coordinated by prosecutors from the Directorate for In
with specialised support from the Directorate of Speci

The operation in Poland was conducted by the Human
Headquarters in close collaboration with the Criminal

EUROPOL

THREE SUSPECTS ARRESTED BY ROMANIAN POLICE FOR THE SEXUAL ABUSE AND EXPLOITATION OF 3-YEAR-OLD CHILD

02May2017

lly supported the Romanian law enforcement authorities in a case of child
oitation, safeguarding a 3-year-old minor. During two house searches on 27
an Police arrested three suspects. One man (aged 29) is suspected of sexually
child, and producing and distributing images of this sexual abuse online. The
the parents of the child who are suspected of facilitating the sexual
ld in exchange for various amounts of money. During the house searches
evices and mobile phones were seized.

omanian Prosecutor's Office, the three suspects are currently detained and
e ongoing.

rovide relevant intelligence about the suspects' criminal activities to the
The investigation in Romania was carried out by the Directorate for Combating
dinated by prosecutors from the Directorate for Investigating Organised Crime
ecialised support from the Directorate of Special Operations, Romanian
pol.

developed following a joint Romanian-Polish case earlier this year, which
upported.

EUROPOL

VICTIM OF CHILD SEXUAL EXPLOITATION RESCUED IN INTERNATIONAL OPERATION SUPPORTED BY EUROPOL

28Mar2017

Press Release

A 40 year-old man has been arrested on suspicion of sexually exploiting his own child in an international investigation between the Polish and Romanian Police with the support of Europol. The arrestee is also being accused of producing and distributing online child sexual abuse material, including sexual abuse material with his child.

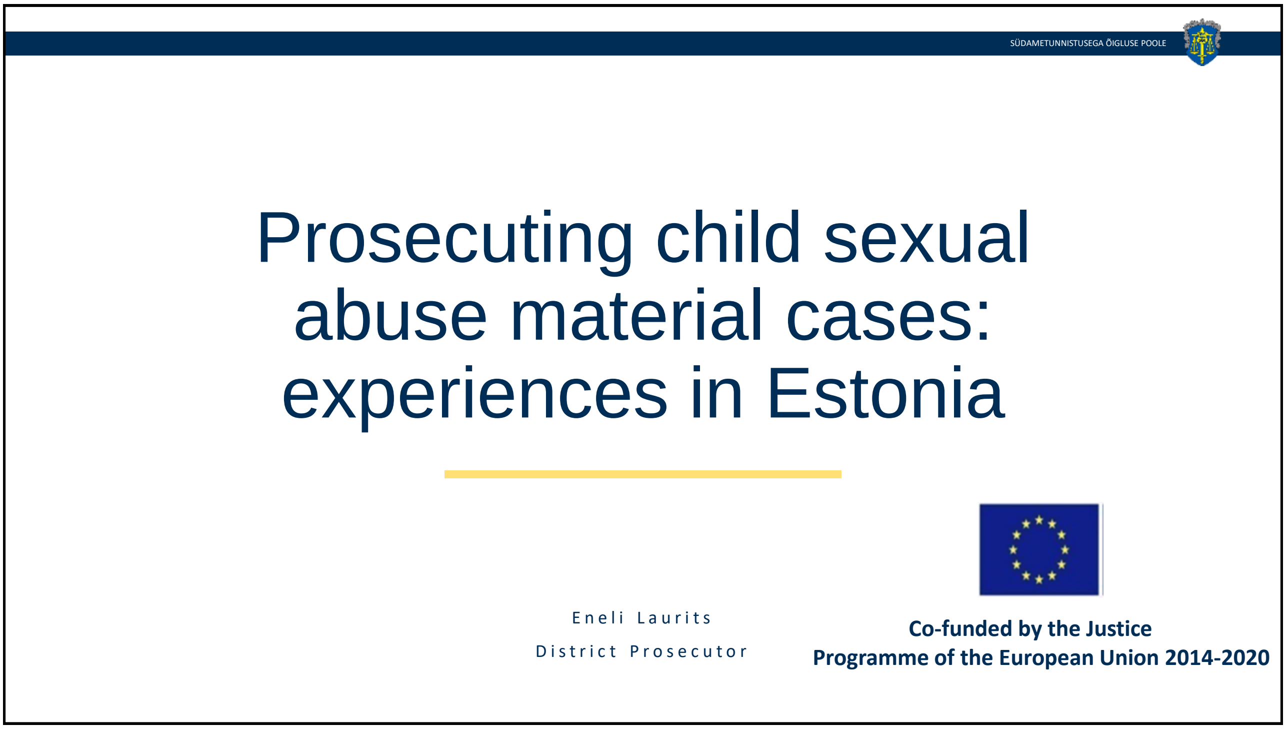
This operation has links to the detention and arrest of a Polish citizen in Bucharest around mid-February 2017. Since then, law enforcement authorities have uncovered several other suspects currently being investigated for similar crimes, including the arrestee.

The suspect's apartment was searched and numerous data storage devices containing child sexual abuse material were seized. In light of all the evidence presented against him, the suspect confessed to all charges.

Steven Wilson, Head of the European Cybercrime Centre (EC3) at Europol praised the efforts of the investigators in both countries: *"Europol is very happy to see that our support to this ongoing operation is having excellent results. Finding that a child is being abused is a tragic discovery but we invest our time and resources to ensure that such victims are safe and that their abusers will be brought to justice. We commend the cooperation between the Polish and Romanian Police through Europol to achieve that in this case."*

THANK YOU FOR YOUR ATTENTION

Lt Col. Jarosław „Jerry” Kończyk
Human Trafficking Department
Criminal Bureau
National Police Headquarters



SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

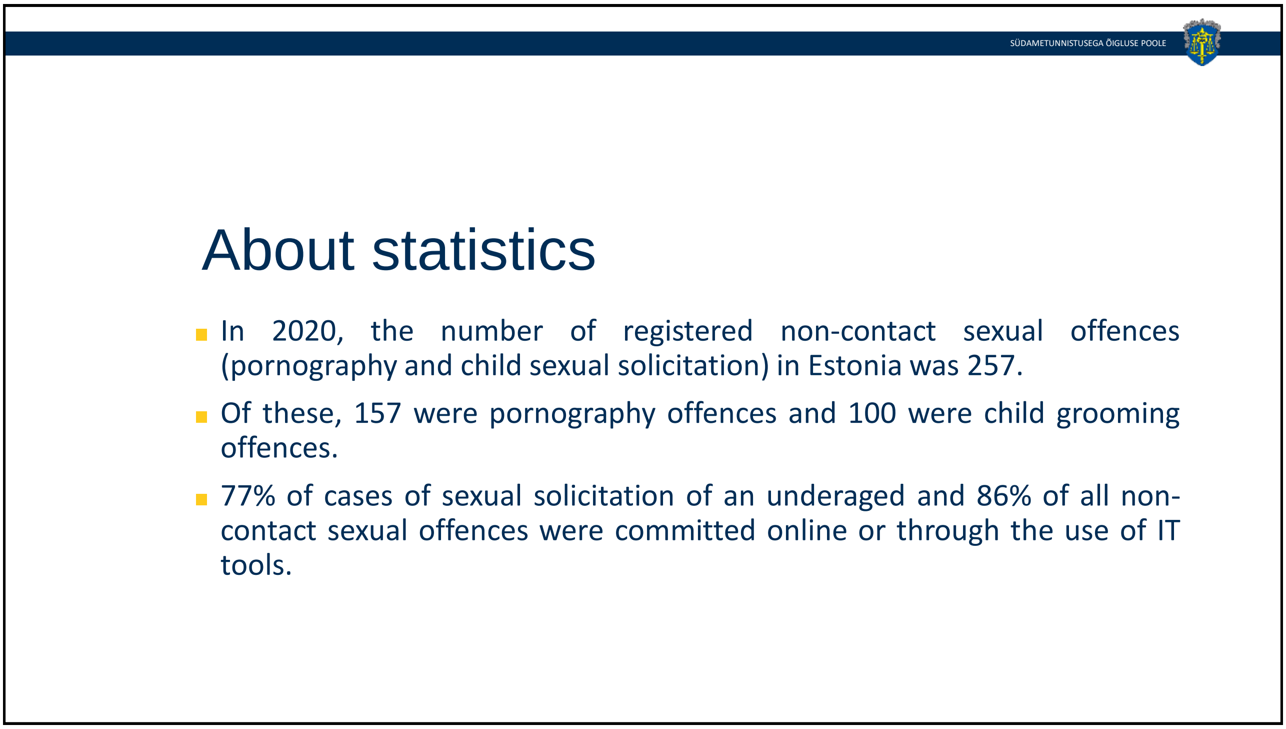
Prosecuting child sexual abuse material cases: experiences in Estonia

Eneli Laurits

District Prosecutor

Co-funded by the Justice Programme of the European Union 2014-2020

1



SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

About statistics

- In 2020, the number of registered non-contact sexual offences (pornography and child sexual solicitation) in Estonia was 257.
- Of these, 157 were pornography offences and 100 were child grooming offences.
- 77% of cases of sexual solicitation of an underaged and 86% of all non-contact sexual offences were committed online or through the use of IT tools.

2

SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Estonian Penal Code » 178:
manufacture of works involving child pornography or making child pornography available

Manufacture, acquisition or storing, handing over, displaying or making available to another person in any other manner of **pictures, writings or other works or reproductions of works** depicting a person of less than eighteen years of age in a pornographic situation, or a person of less than fourteen years of age in a pornographic **or** erotic situation, is punishable by a pecuniary punishment or up to three years' imprisonment

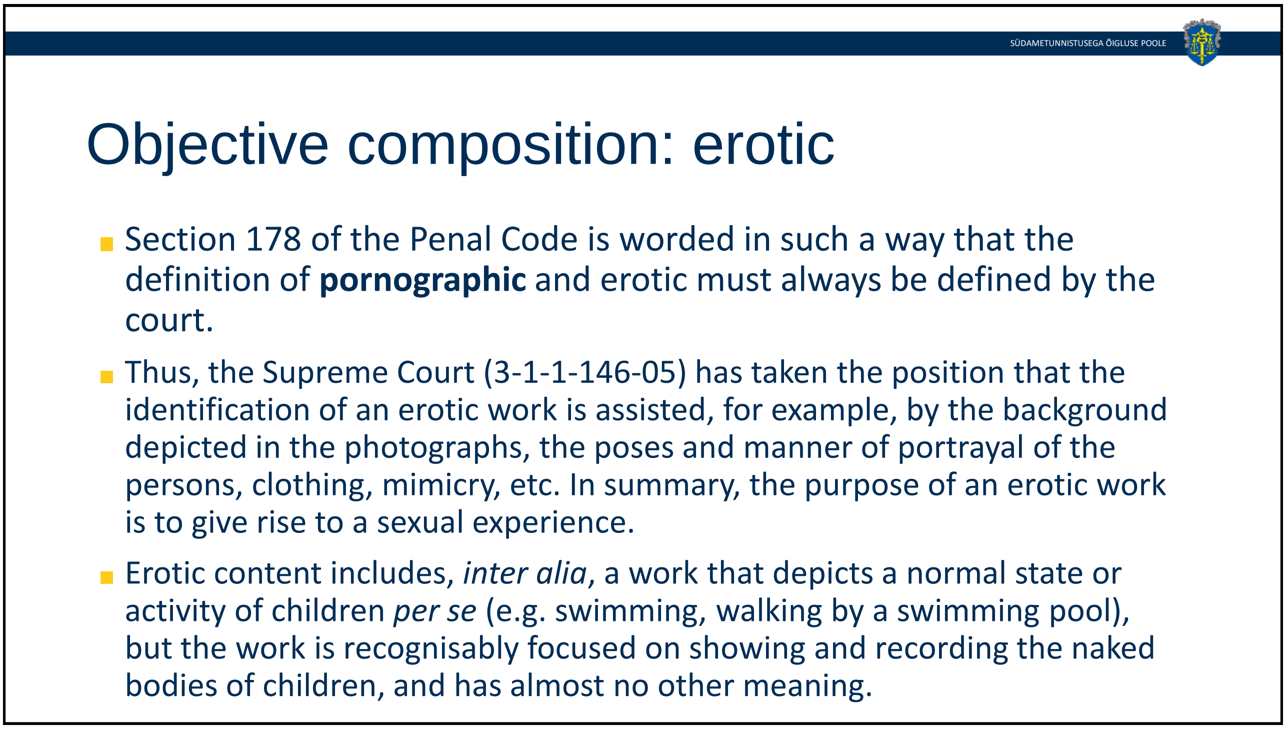
3

SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Objective composition: child?

It has been accepted in the court case-law that this wording makes it possible to understand the legislator's intention to criminalise the creation and handling of erotic or pornographic works **depicting persons who are recognisably** children.

4

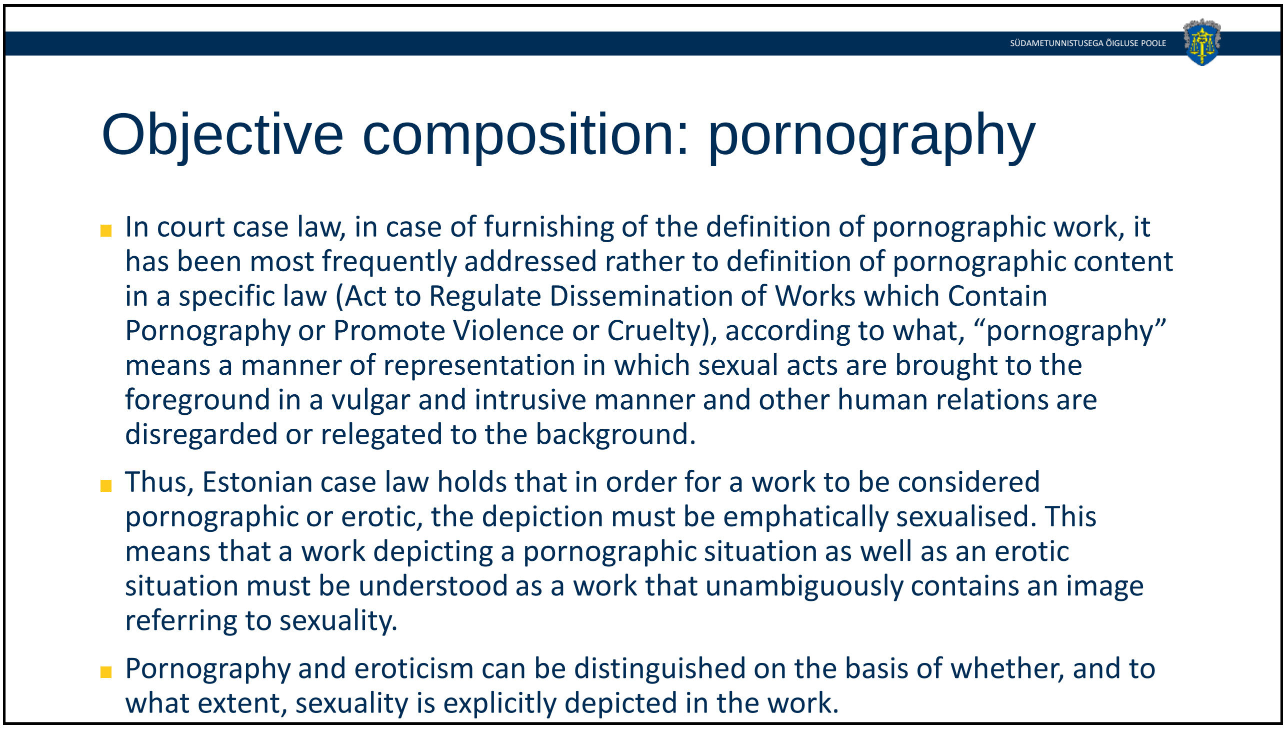


SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Objective composition: erotic

- Section 178 of the Penal Code is worded in such a way that the definition of **pornographic** and erotic must always be defined by the court.
- Thus, the Supreme Court (3-1-1-146-05) has taken the position that the identification of an erotic work is assisted, for example, by the background depicted in the photographs, the poses and manner of portrayal of the persons, clothing, mimicry, etc. In summary, the purpose of an erotic work is to give rise to a sexual experience.
- Erotic content includes, *inter alia*, a work that depicts a normal state or activity of children *per se* (e.g. swimming, walking by a swimming pool), but the work is recognisably focused on showing and recording the naked bodies of children, and has almost no other meaning.

5



SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Objective composition: pornography

- In court case law, in case of furnishing of the definition of pornographic work, it has been most frequently addressed rather to definition of pornographic content in a specific law (Act to Regulate Dissemination of Works which Contain Pornography or Promote Violence or Cruelty), according to what, “pornography” means a manner of representation in which sexual acts are brought to the foreground in a vulgar and intrusive manner and other human relations are disregarded or relegated to the background.
- Thus, Estonian case law holds that in order for a work to be considered pornographic or erotic, the depiction must be emphatically sexualised. This means that a work depicting a pornographic situation as well as an erotic situation must be understood as a work that unambiguously contains an image referring to sexuality.
- Pornography and eroticism can be distinguished on the basis of whether, and to what extent, sexuality is explicitly depicted in the work.

6

Objective composition: pornography

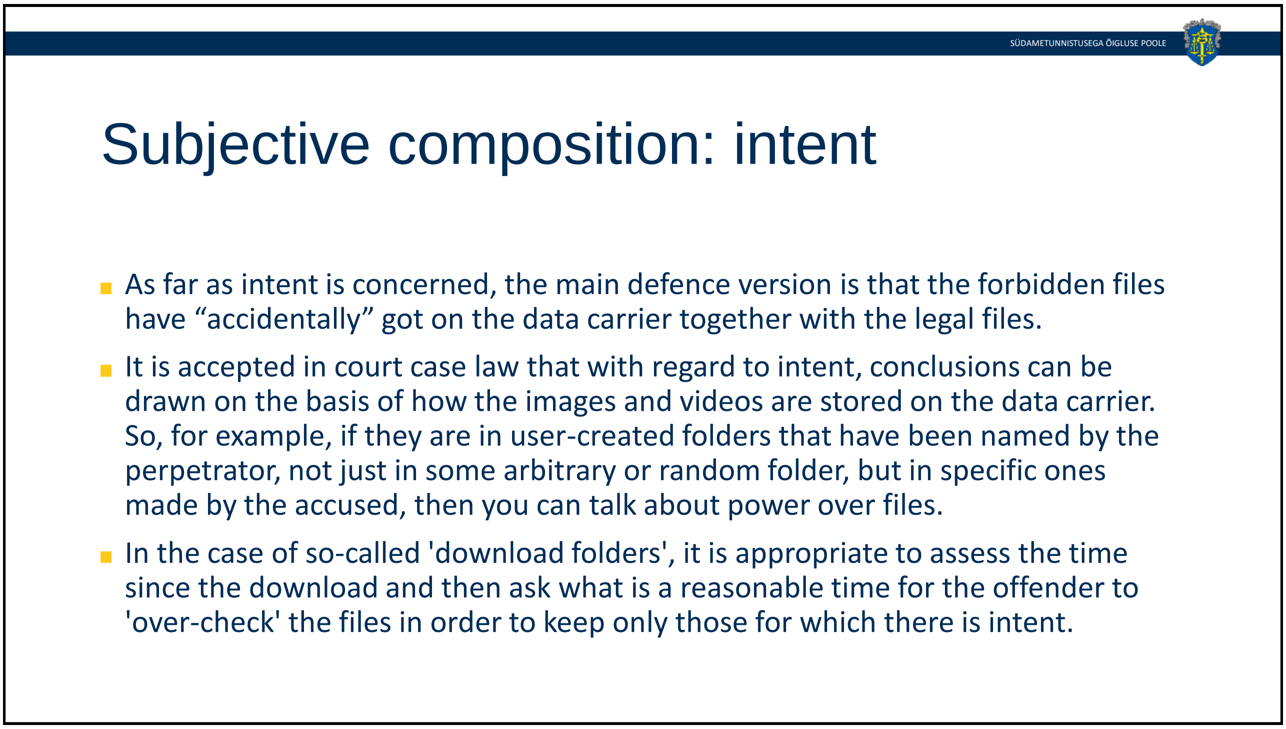
- Criticism: with regard to the aforementioned definition of pornography, the Tallinn Circuit Court has stated that it is not really applicable in criminal law, because it does not comply with **the principle of specification** of criminal law.
- All three of the characteristics used to describe pornographic imagery are inherently subjective and non-measurable. Their application inevitably leads to unacceptable arbitrariness in criminal law.

7

Objective Composition

- The objective constituent element of the provision does not require that the work created must be arousing to the perpetrator or that he must have viewed the work.
- Nor does the provision of Estonian law require an analysis of whether the work has any **artistic value**. Objectively, it has no meaning.

8

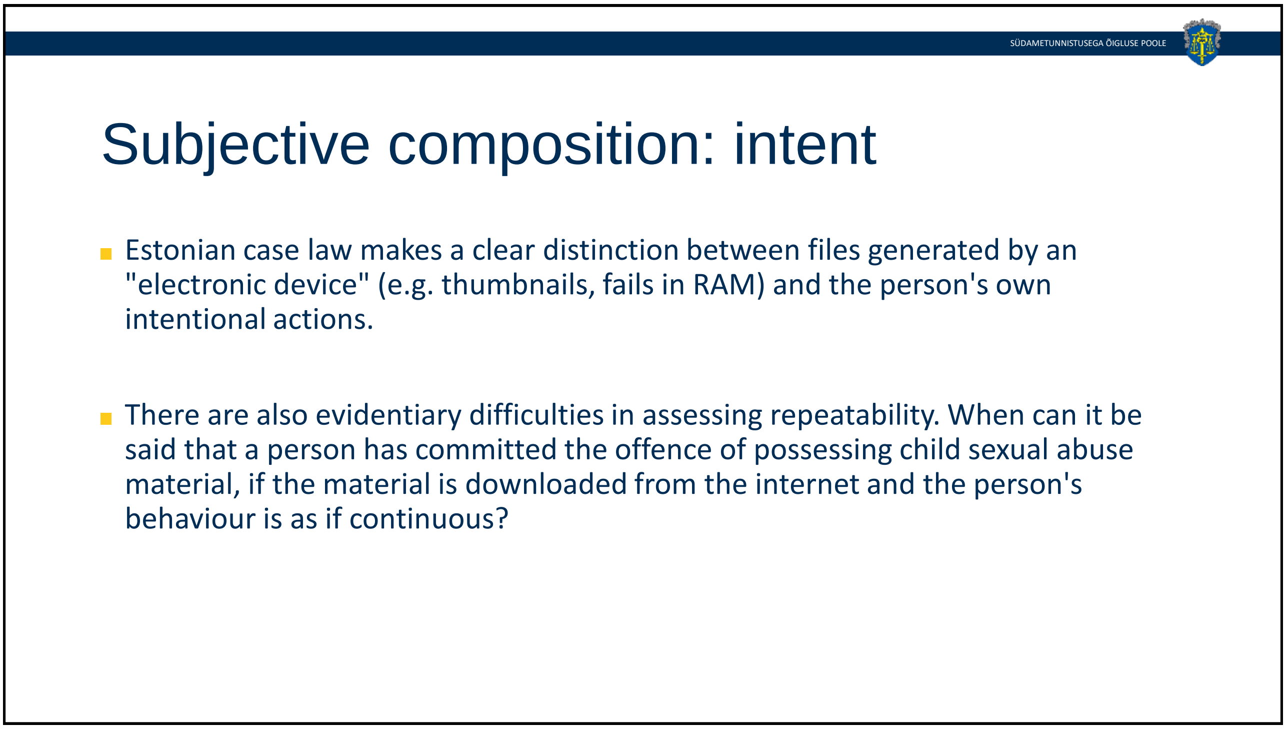


SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Subjective composition: intent

- As far as intent is concerned, the main defence version is that the forbidden files have “accidentally” got on the data carrier together with the legal files.
- It is accepted in court case law that with regard to intent, conclusions can be drawn on the basis of how the images and videos are stored on the data carrier. So, for example, if they are in user-created folders that have been named by the perpetrator, not just in some arbitrary or random folder, but in specific ones made by the accused, then you can talk about power over files.
- In the case of so-called 'download folders', it is appropriate to assess the time since the download and then ask what is a reasonable time for the offender to 'over-check' the files in order to keep only those for which there is intent.

9

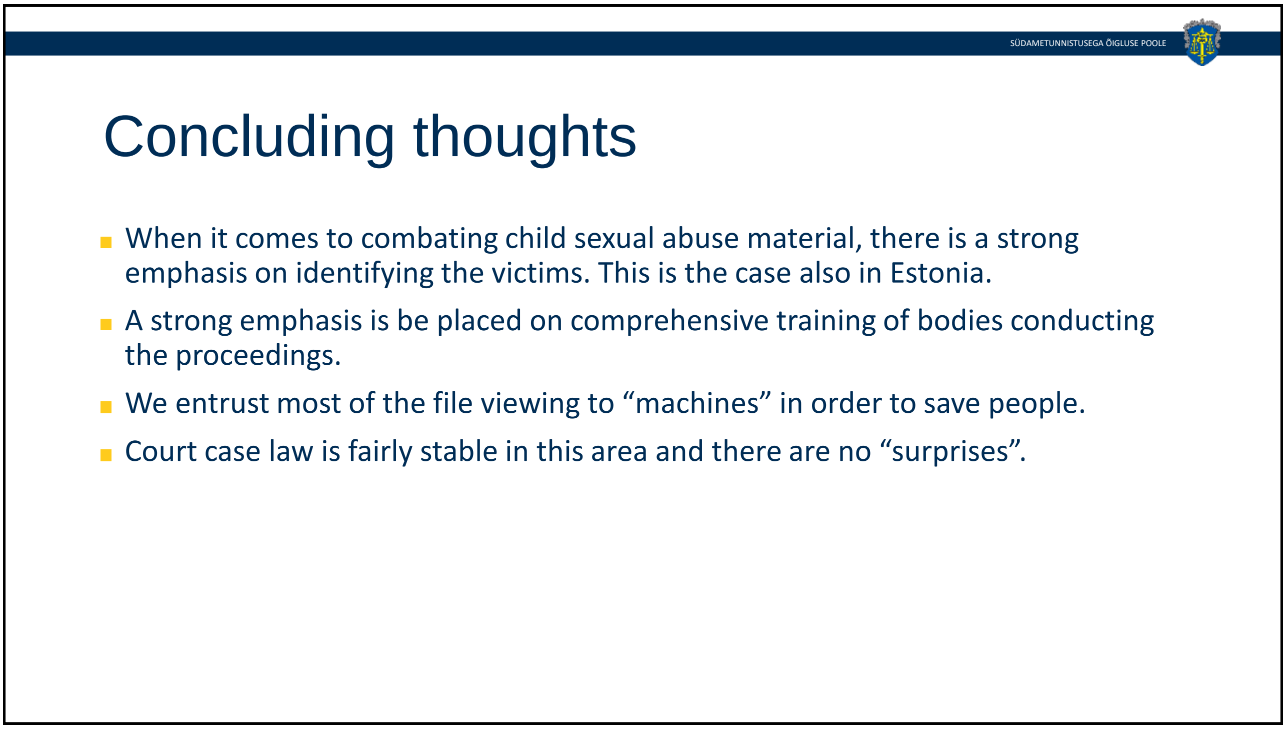


SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Subjective composition: intent

- Estonian case law makes a clear distinction between files generated by an "electronic device" (e.g. thumbnails, fails in RAM) and the person's own intentional actions.
- There are also evidentiary difficulties in assessing repeatability. When can it be said that a person has committed the offence of possessing child sexual abuse material, if the material is downloaded from the internet and the person's behaviour is as if continuous?

10

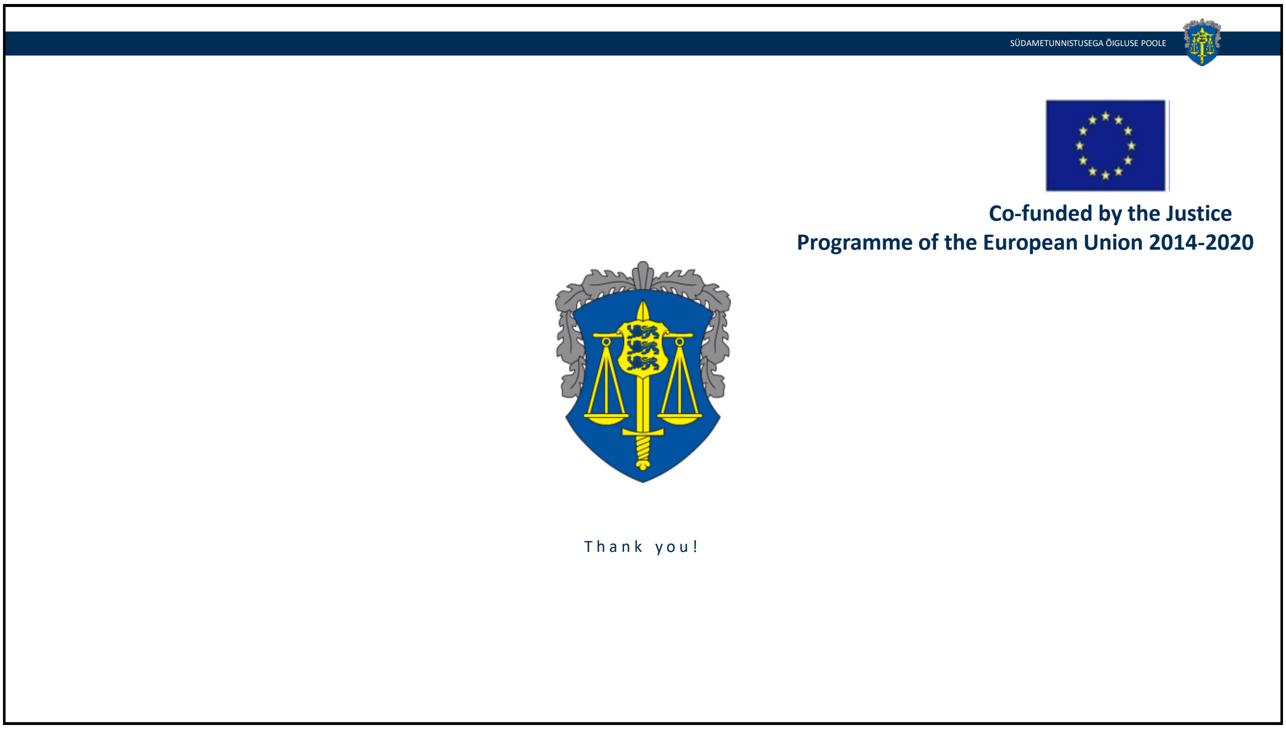


SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Concluding thoughts

- When it comes to combating child sexual abuse material, there is a strong emphasis on identifying the victims. This is the case also in Estonia.
- A strong emphasis is be placed on comprehensive training of bodies conducting the proceedings.
- We entrust most of the file viewing to “machines” in order to save people.
- Court case law is fairly stable in this area and there are no “surprises”.

11



SÜDAMETUNNISTUSEGA ÕIGLUSE POOLE

Co-funded by the Justice
Programme of the European Union 2014-2020

Thank you!

12

ERA
Académie de Droit Européen

UCD
DUBLIN

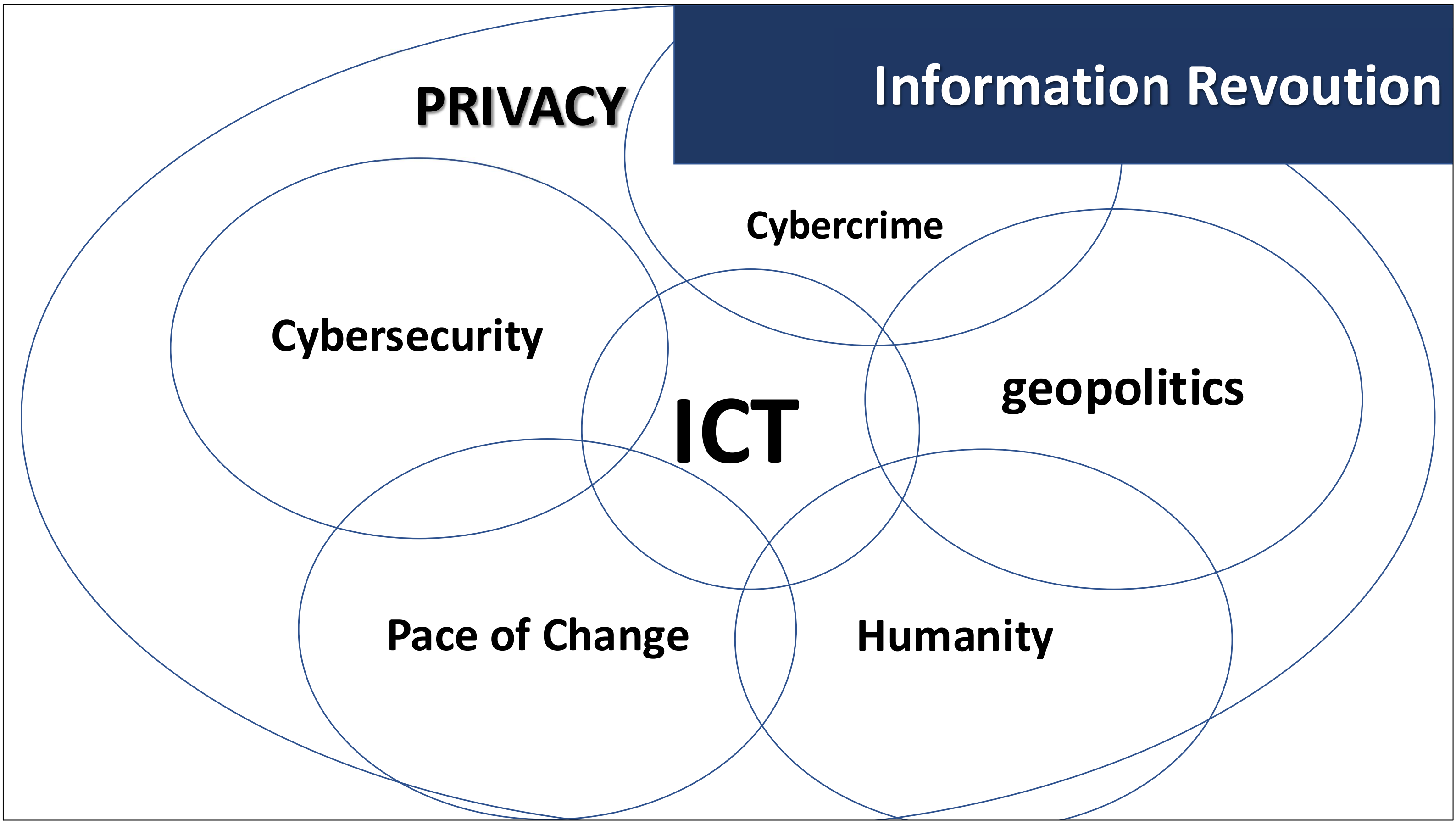
Cooperation between

Law enforcement authorities and the internet industry

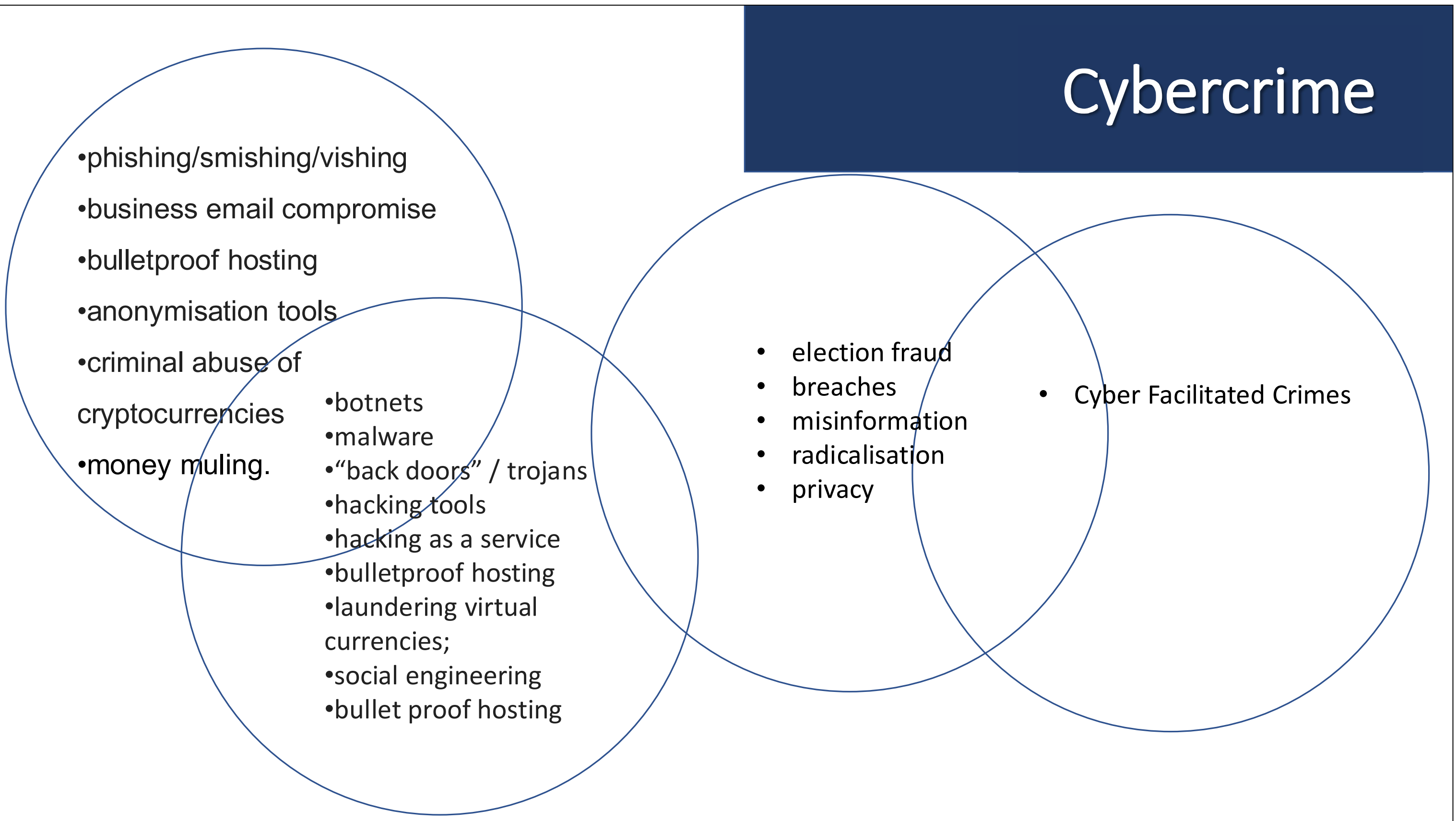
to fight child sexual abuse

With the support of the Internal Security Fund – Police
Programme 2014-2020 of the European Union

Information Revoution



Cybercrime



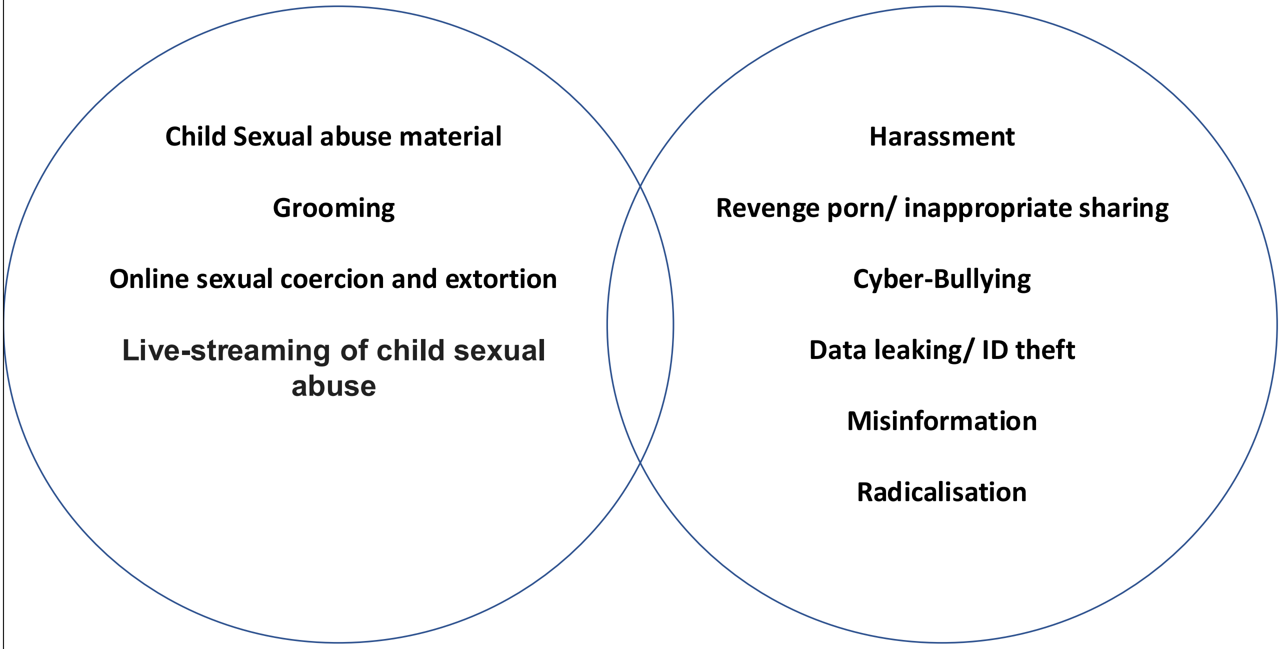
- •phishing/smishing/vishing
- •business email compromise
- •bulletproof hosting
- •anonymisation tools
- •criminal abuse of cryptocurrencies
- •money muling.

- •botnets
- •malware
- •“back doors” / trojans
- •hacking tools
- •hacking as a service
- •bulletproof hosting
- •laundering virtual currencies;
- •social engineering
- •bullet proof hosting

- election fraud
- breaches
- misinformation
- radicalisation
- privacy

- Cyber Facilitated Crimes

Online Child Exploitation



Child Sexual abuse material

Grooming

Online sexual coercion and extortion

Live-streaming of child sexual abuse

Harassment

Revenge porn/ inappropriate sharing

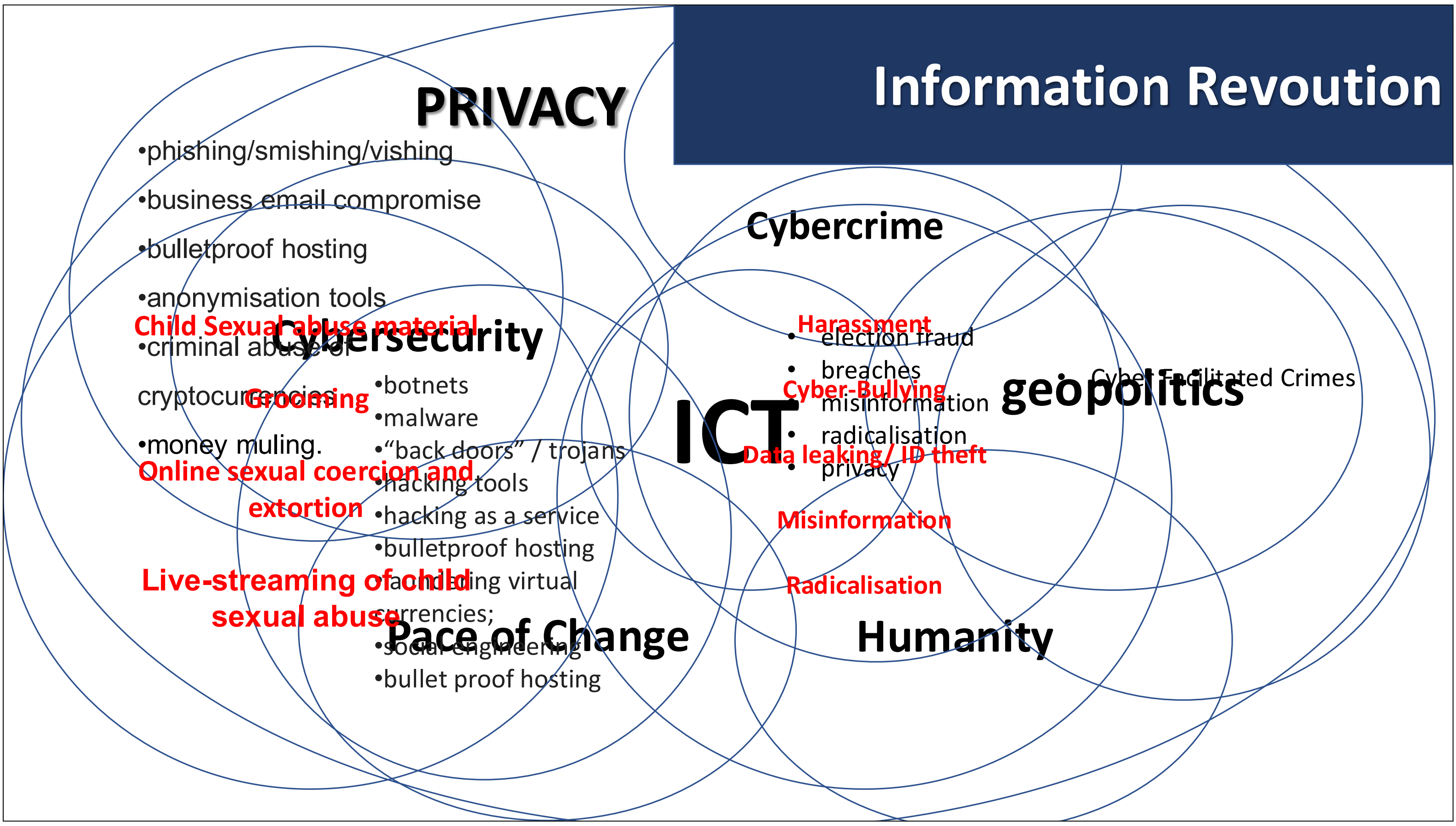
Cyber-Bullying

Data leaking/ ID theft

Misinformation

Radicalisation

Information Revoution



PRIVACY

- phishing/smishing/vishing
- business email compromise
- bulletproof hosting
- anonymisation tools
- criminal abuse of cryptocurrencies
- money muling.

Child Sexual abuse material

Grooming

Online sexual coercion and extortion

Live-streaming of child sexual abuse

Cybersecurity

- botnets
- malware
- "back doors" / trojans
- hacking tools
- hacking as a service
- bulletproof hosting
- laundering virtual currencies;
- social engineering
- bullet proof hosting

Pace of Change

Cybercrime

Harassment

Cyber-Bullying

Data leaking/ ID theft

Misinformation

Radicalisation

ICT

- election fraud
- breaches
- misinformation
- radicalisation
- privacy

geopolitics

- Cyber Facilitated Crimes

Humanity

Industry

BACKBONE – UNDERSEA CABLES

TERRESTRIAL ISP

HOSTING

DNS

HARDWARE/ ROUTING

ONLINE SERVICE PROVIDERS

SOCIAL MEDIA PROVIDERS

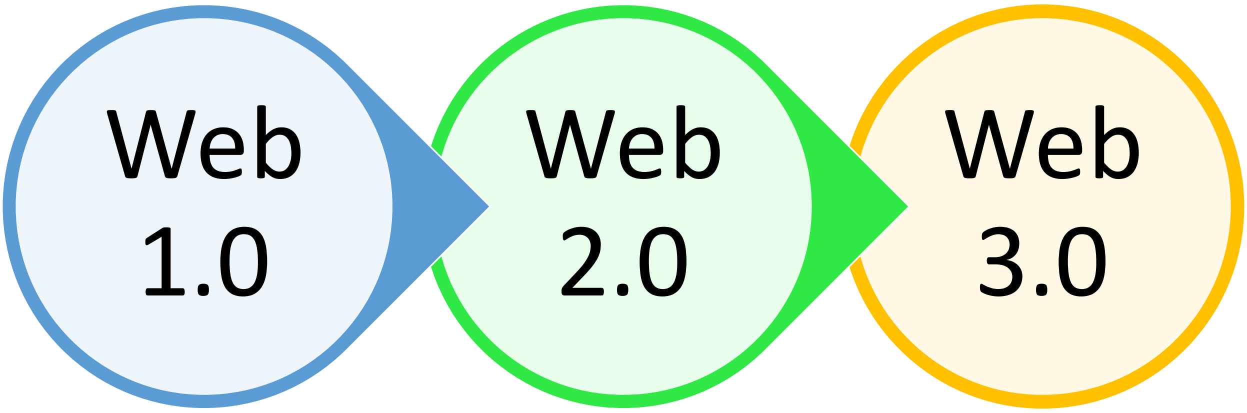
ONLINE COMMERCE

CYBER SECURITY

FINTECH

OTT SERVICES

Online Content Providers



Web 1.0

Web 2.0

Web 3.0

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Cooperation between law enforcement and Internet service providers

- common guidelines for both law enforcement and service providers
- specific guidelines for each of them
- are not to substitute legislation or other formal regulations
- supplement and help regulations work in practice
- based on good practices already available
- malleable to specific circumstances in each country.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Dialogue between law enforcement and Internet service providers INDUSTRY

- More dialogue welcome
- Tackling crime is difficult because lack of harmonization across borders
- Increasing pressure on companies over human rights and working with Govts can be seen as negative
- No back doors!
- Better education of judges

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Dialogue between
law enforcement and Internet service providers
LAW ENFORCEMENT

- more regular dialogue with Internet companies is welcomed
- guidance is needed to interpret partnerships undertaken, in particular their added value, scope, rules of procedure, and tangible outcomes envisaged
- roadmaps are necessary to help measure progress in the implementation of partnerships undertaken, this should include a "rendez-vous clause" for their periodic review".

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Dialogue between
law enforcement and Internet service providers
CyberCrime@EAP III project - MSP

- Low level of understanding of business model by law enforcement
- No understanding of range of services resulting in bad applications and frustration for investigators
- Mature cooperation model with efforts at building relationships will improve understanding and therefore applications.
- Requests from countries with low human rights records will get higher scrutiny.
- Management in MSP might not necessarily prioritise LEA requests and capability might not be present *
- Bad quality of requests creates even further problems – training should be considered.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Dialogue between
law enforcement and Internet service providers
CyberCrime@EAP III project - LEA

- Varying policies in each MSP
- Uncertainty and lack of communication from MSPs – Lucky Dip!
- Many MSPs do not reply to some countries at all
- No feedback as to why an application is rejected
- Disclosure policies of MSPs can be concerning

Online service providers and LEA

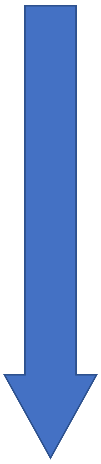
- Fiduciary duty to their shareholders
- The scale is enormous
- Damned If They Do, Damned If They Don't
- Technology Positive – cyberutopians
- Skewed understanding of people – eyeballs
- Underpinned by Barlow's Declaration of the Independence of Cyberspace

Law Enforcement Portals - LEAP

- Most of the big companies have law enforcement portals.
- A request to freeze information is followed by an MLAT
- Some companies will accept local orders or processes
- Some companies have law enforcement liaison officers

Online Content Providers

- **Subscriber information** ★
- **Content** ★★
- **Live Tap** ★★★



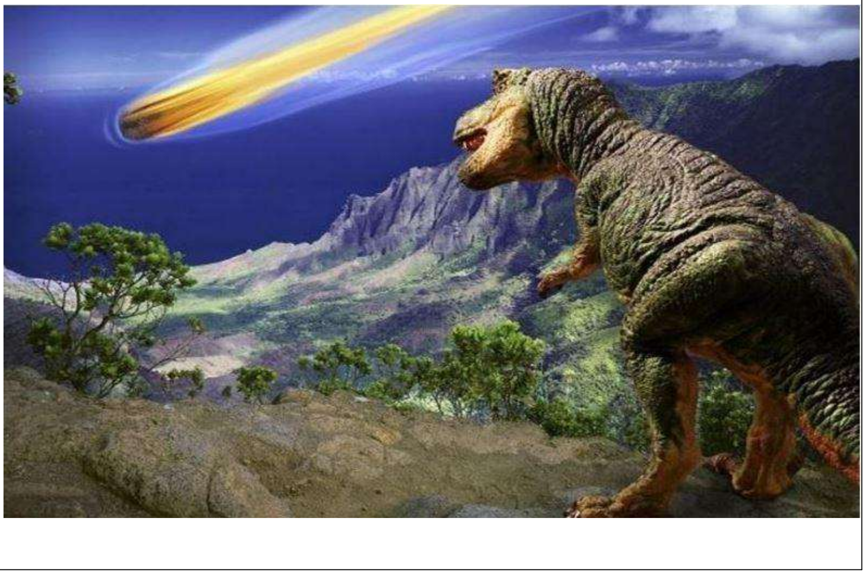
Level of difficulty

Level of intrusiveness

Emergency procedures

Legal Process:

- MLAT is default
- Some countries have their own processes + agreements
- Telecoms data retention



Legal Process:

GDPR

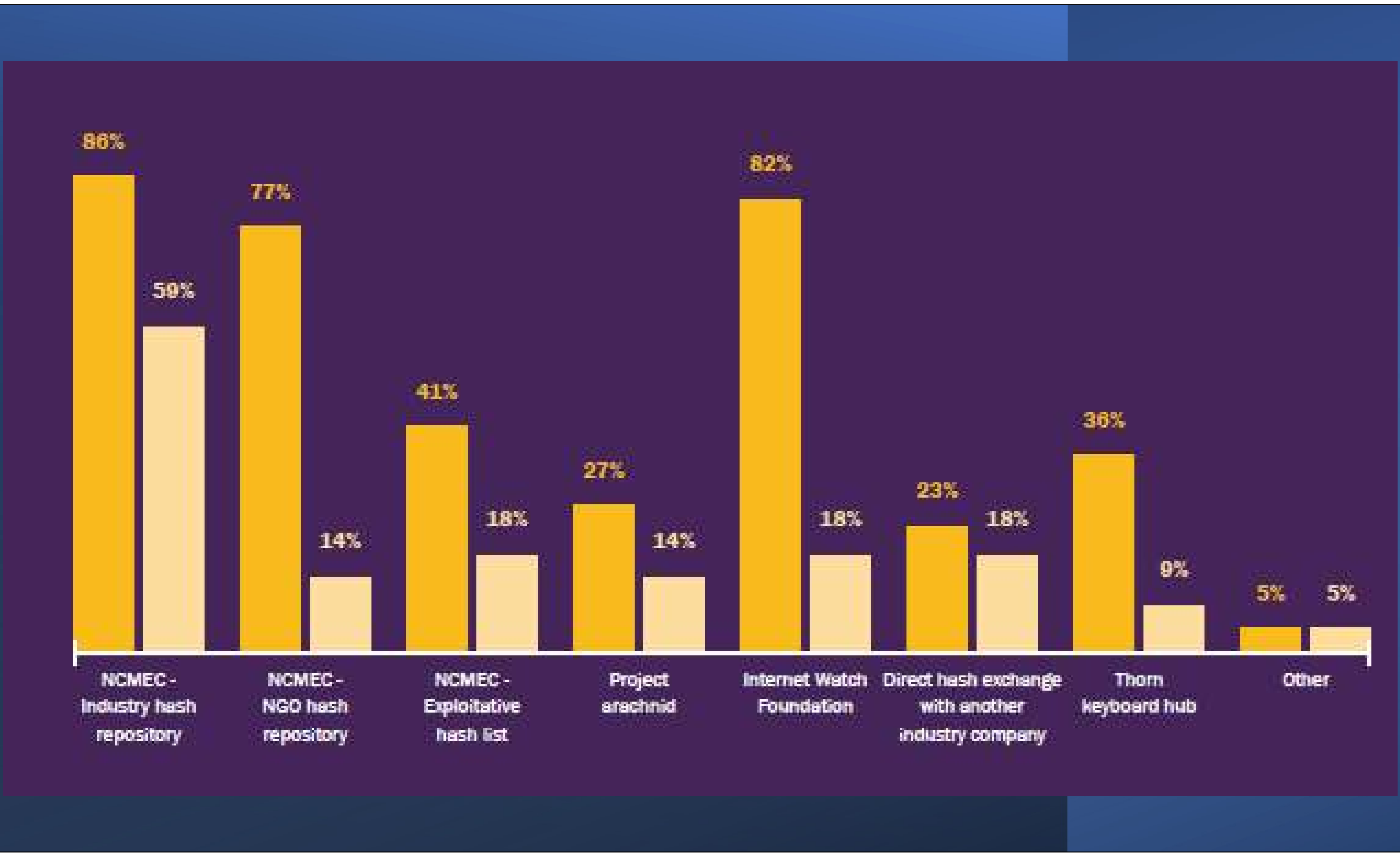
ePrivacy

Data Retention

E-evidence directive

US 4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

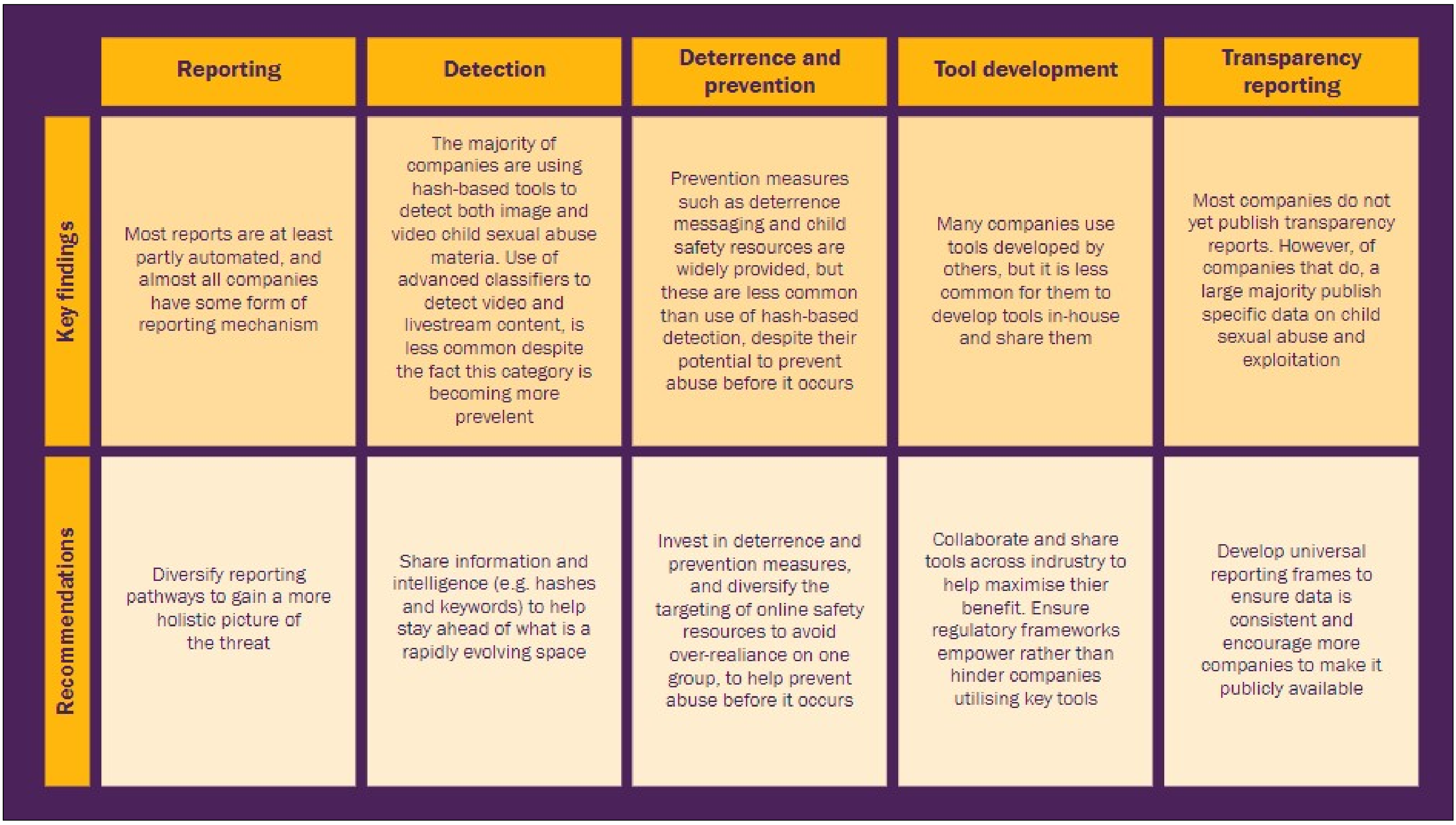


Organisations

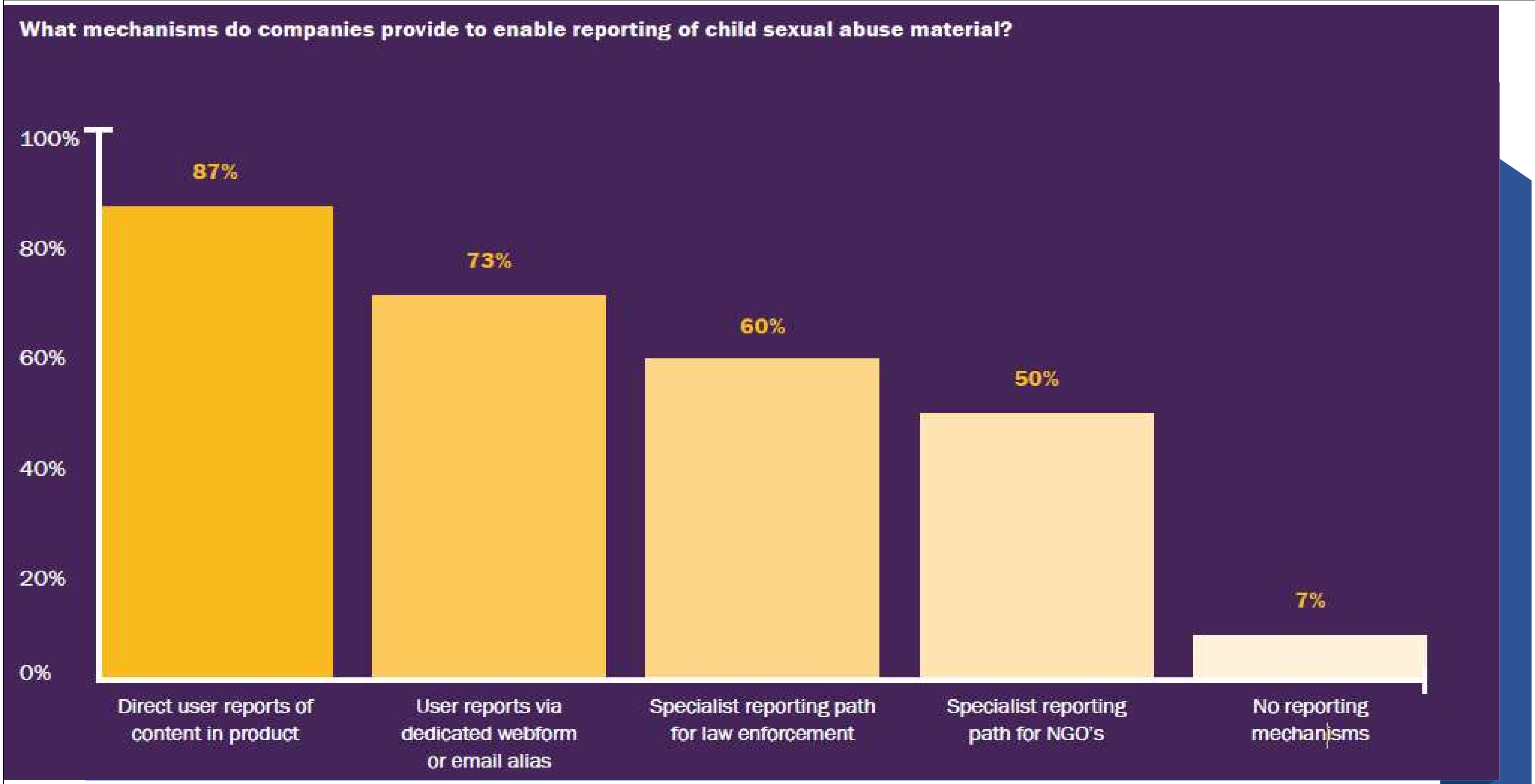
- Two Organisations very active in this field:

WeProtect
GLOBAL ALLIANCE

TECHNOLOGY
COALITION
FIGHTING CHILD SEXUAL ABUSE



	Reporting	Detection	Deterrence and prevention	Tool development	Transparency reporting
Key findings	Most reports are at least partly automated, and almost all companies have some form of reporting mechanism	The majority of companies are using hash-based tools to detect both image and video child sexual abuse materia. Use of advanced classifiers to detect video and livestream content, is less common despite the fact this category is becoming more prevelent	Prevention measures such as deterrence messaging and child safety resources are widely provided, but these are less common than use of hash-based detection, despite their potential to prevent abuse before it occurs	Many companies use tools developed by others, but it is less common for them to develop tools in-house and share them	Most companies do not yet publish transparency reports. However, of companies that do, a large majority publish specific data on child sexual abuse and exploitation
Recommendations	Diversify reporting pathways to gain a more holistic picture of the threat	Share information and intelligence (e.g. hashes and keywords) to help stay ahead of what is a rapidly evolving space	Invest in deterrence and prevention measures, and diversify the targeting of online safety resources to avoid over-realiance on one group, to help prevent abuse before it occurs	Collaborate and share tools across indrustry to help maximise thier benefit. Ensure regulatory frameworks empower rather than hinder companies utilising key tools	Develop universal reporting frames to ensure data is consistent and encourage more companies to make it publicly available



What mechanisms do companies provide to enable reporting of child sexual abuse material?

Prevention

- Most companies scan for CSAM and some for Grooming
  - Find, Remove, Report
  - Privacy difficulties
- Most companies take reports and moderate
  - Moderation team difficulties
- Start-ups are a particular concern
  - Rush to market

Prevention

- Most online platforms do provide prevention messaging
- However, the majority of this is towards parents
- Not enough towards other actors such as children themselves, teachers, offenders
- Prevention messaging can take various forms

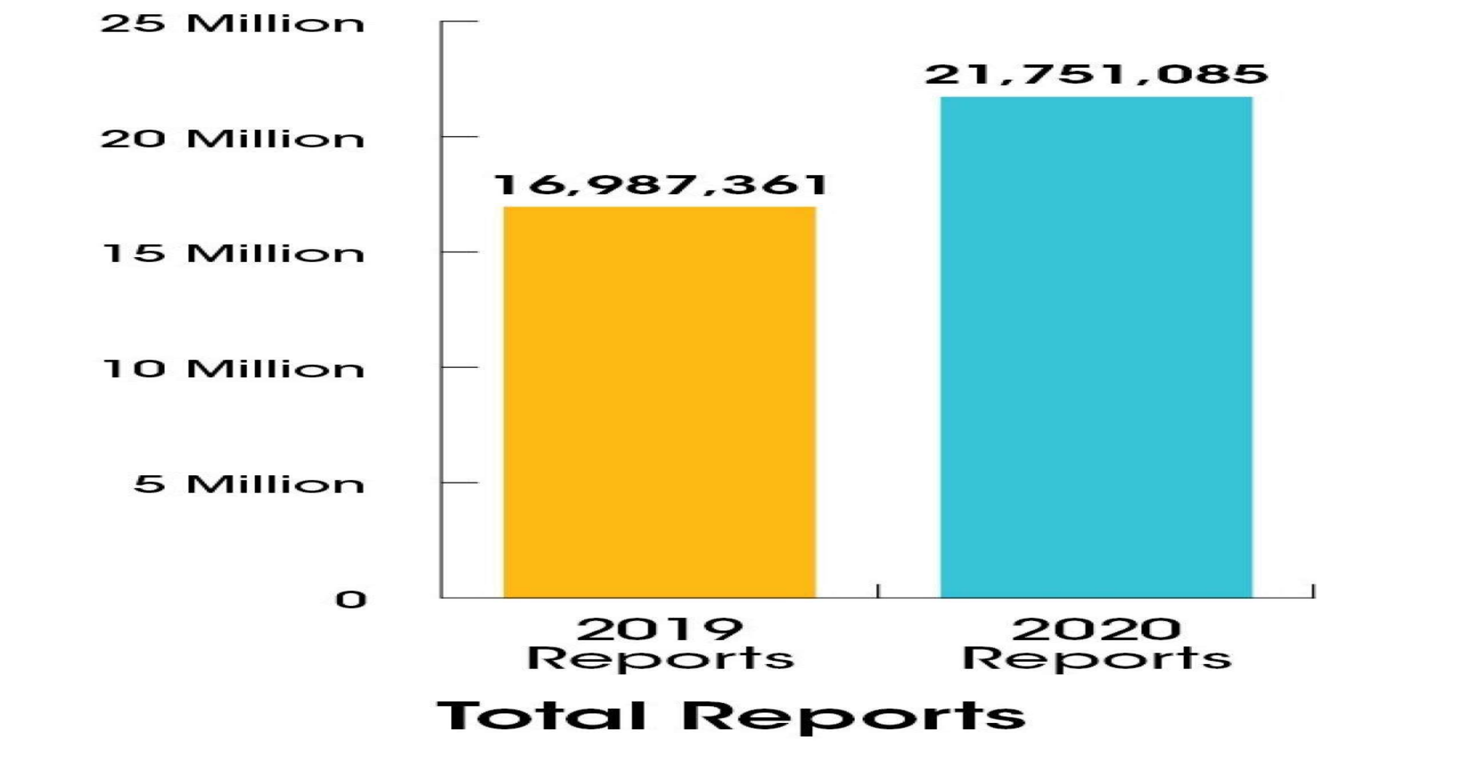
Prevention

- Brings safety to the fore especially in brand awareness and funding applications
- Strong Safety advisory board – experts in different fields
- Age gates, mute words, banned hashtags, real users, device banning, age verification,
- Strong live moderation, developing AI solutions,
- Engagement with law enforcement including proactive reporting

Prevention

Cybertips

- US based companies are obliged to report CSAM or Grooming activity on their systems
- They report it to NCMEC –National Centre Missing and Exploited Children
- These reports are processed and distributed to law enforcement
- Cybertips are essentially intel
- Police use these to commence investigations



Prevention

Cybertips

2019 : 16,987,361

2020 : 21,751,085

San Marino	7	12
Saudi Arabia	514,832	510,240
United States	521,658	494,388
Italy	57,113	62,399
Denmark	6,148	6,504
Portugal	30,369	26,982
Estonia	1,951	4,695
Israel	28,691	23,597
Finland	4,850	4,419
France	71,422	89,871
Ireland	6,653	6,959
United Arab Emirates	330,268	216,874
Philippines	801,272	1,339,597

Final Message

- Understand the regulatory and politically sensitive environment in which they operate.
- Build a relationship with local people from the company – even if they are not associated with the service side of the business
- Consider joint training days or seminars – suggest your pan-European agencies to do this.
- Put a SPOC in place. All queries from your country flow to and from this office
- Feedback to them on results
  - They have moderators and staff who work full time on these issues. Feedback makes them feel proud and encourages them which is great for their motivation and mental well-being.

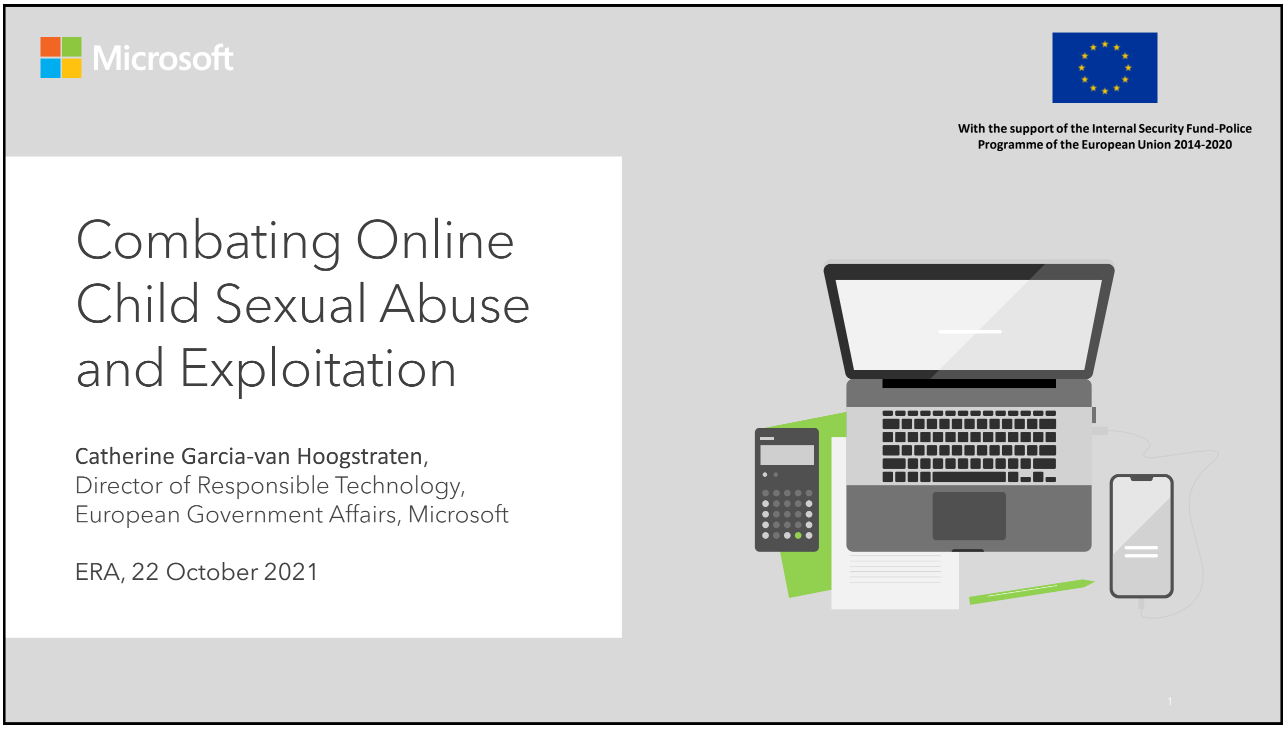
Europol IOCTA

COE Cooperation between MSP and LEA

COE Human rights and scanning

NCMEC Figures

We Protect and Tech Coalition survey



Microsoft

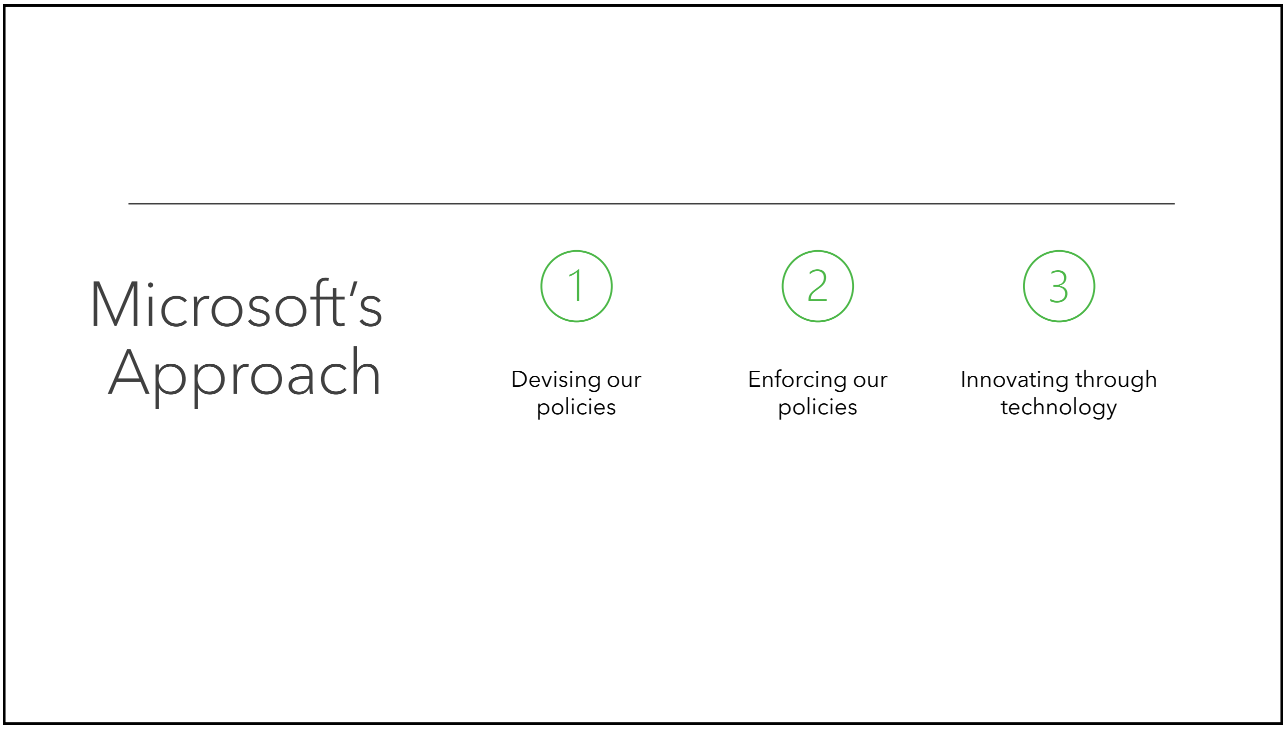
With the support of the Internal Security Fund-Police Programme of the European Union 2014-2020

Combating Online Child Sexual Abuse and Exploitation

Catherine Garcia-van Hoogstraten,
Director of Responsible Technology,
European Government Affairs, Microsoft

ERA, 22 October 2021

1



Microsoft's Approach

1 Devising our policies

2 Enforcing our policies

3 Innovating through technology

2

Devising and enforcing our policies

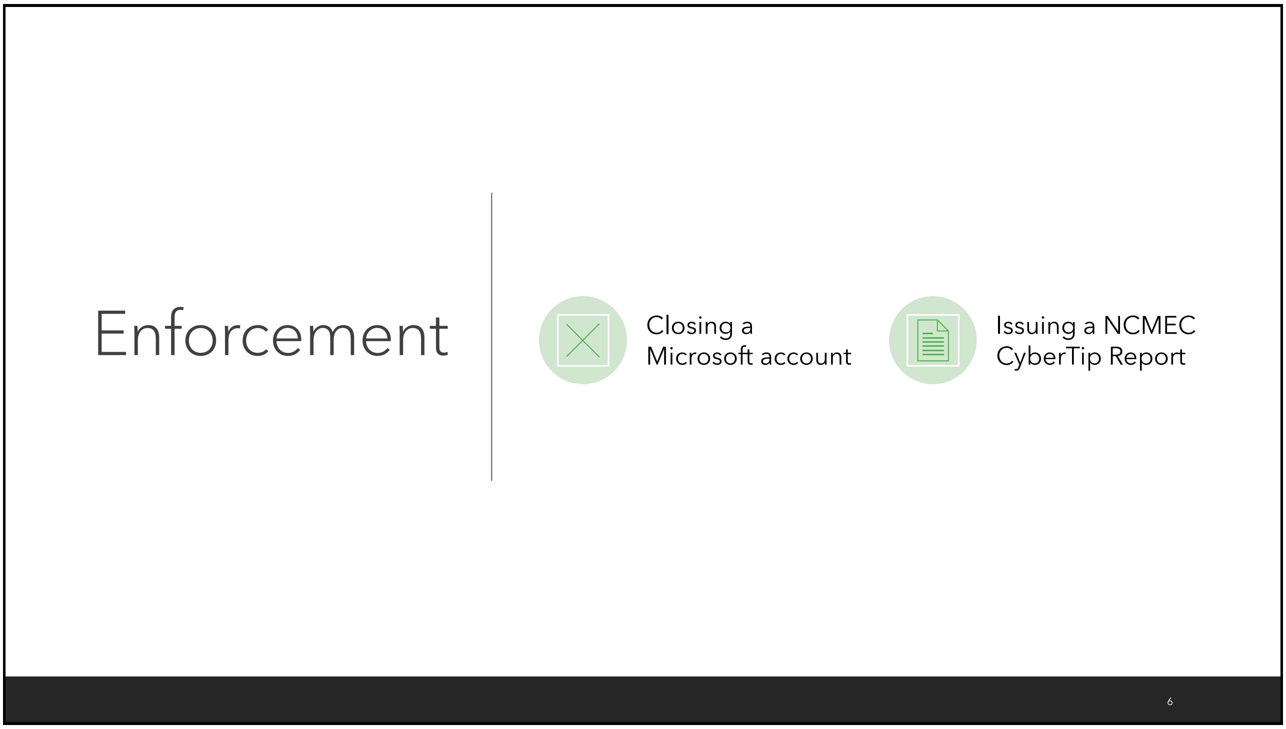
4

Microsoft Services Agreement

By agreeing to these Terms, you're agreeing that, when using the Services, you will follow these rules:

i. Don't do anything illegal.
ii. Don't engage in any activity that exploits, harms, or threatens to harm children.
iii. Don't send spam or engage in phishing. Spam is unwanted or unsolicited bulk email, postings, contact requests, SMS (text messages), instant messages, or similar electronic communications. Phishing is sending emails or other electronic communications to fraudulently or unlawfully induce recipients to reveal personal or sensitive information, such as passwords, dates of birth, Social Security numbers, passport numbers, credit card information, financial information, or other sensitive information, or to gain access to accounts or records, exfiltration of documents or other sensitive information, payment and/or financial benefit.
iv. Don't publicly display or use the Services to share inappropriate content or material (involving, for example, nudity, bestiality, pornography, offensive language, graphic violence, or criminal activity).
v. Don't engage in activity that is fraudulent, false or misleading (e.g., asking for money under false pretenses, impersonating someone else, manipulating the Services to increase play count, or affect rankings, ratings, or comments).
vi. Don't circumvent any restrictions on access to or availability of the Services.
vii. Don't engage in activity that is harmful to you, the Services or others (e.g., transmitting viruses, stalking, posting terrorist or violent extremist content, communicating hate speech, or advocating violence against others).
viii. Don't infringe upon the rights of others (e.g., unauthorized sharing of copyrighted music or other copyrighted material, resale or other distribution of Bing maps, or photographs).
ix. Don't engage in activity that violates the privacy of others.
x. Don't help others break these rules.

5



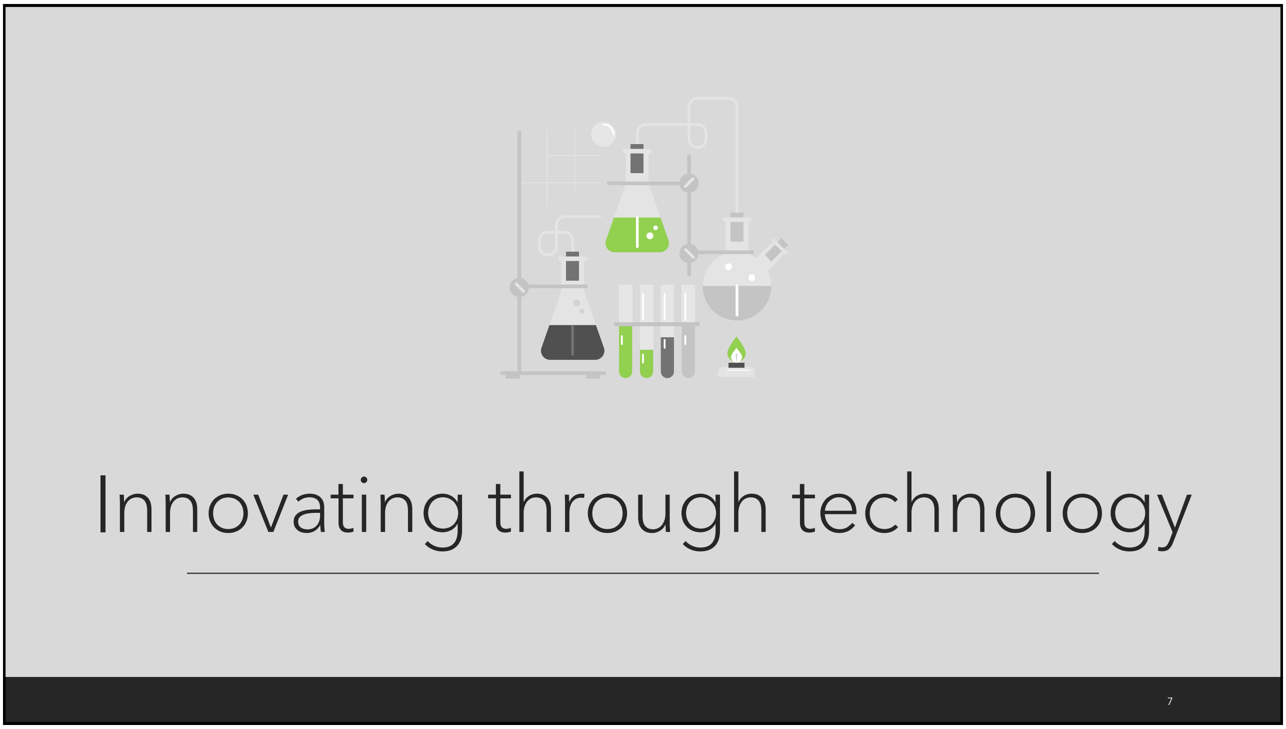
Enforcement

Closing a Microsoft account

Issuing a NCMEC CyberTip Report

6

6



Innovating through technology

7

7

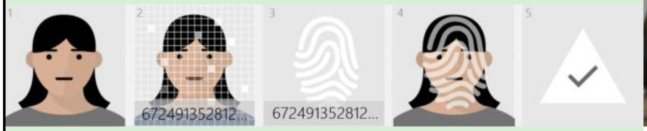
PhotoDNA

… creates a unique digital signature (“hash”) of an image, which is then compared against digital signatures (hashes) of other photos to find copies of the same image.

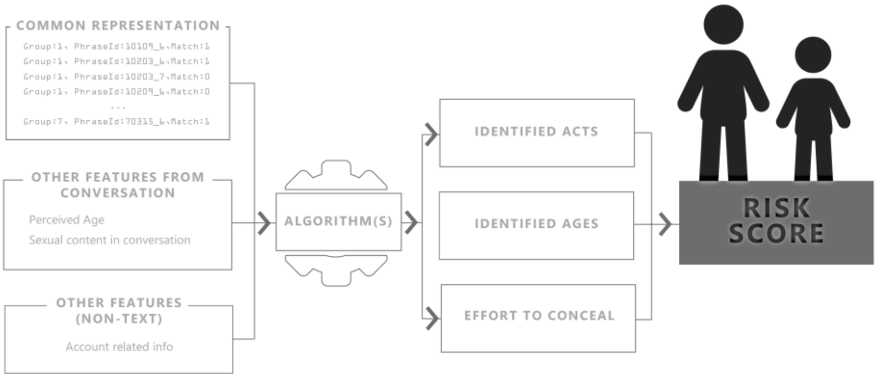
When matched with a database containing hashes of **previously identified** illegal child sexual abuse images, PhotoDNA helps detect, disrupt, and report the distribution of known child sexual abuse material.

… is not facial recognition software and cannot be used to identify any person or object in an image.

A PhotoDNA hash is not reversible, meaning it cannot be used to recreate an image.



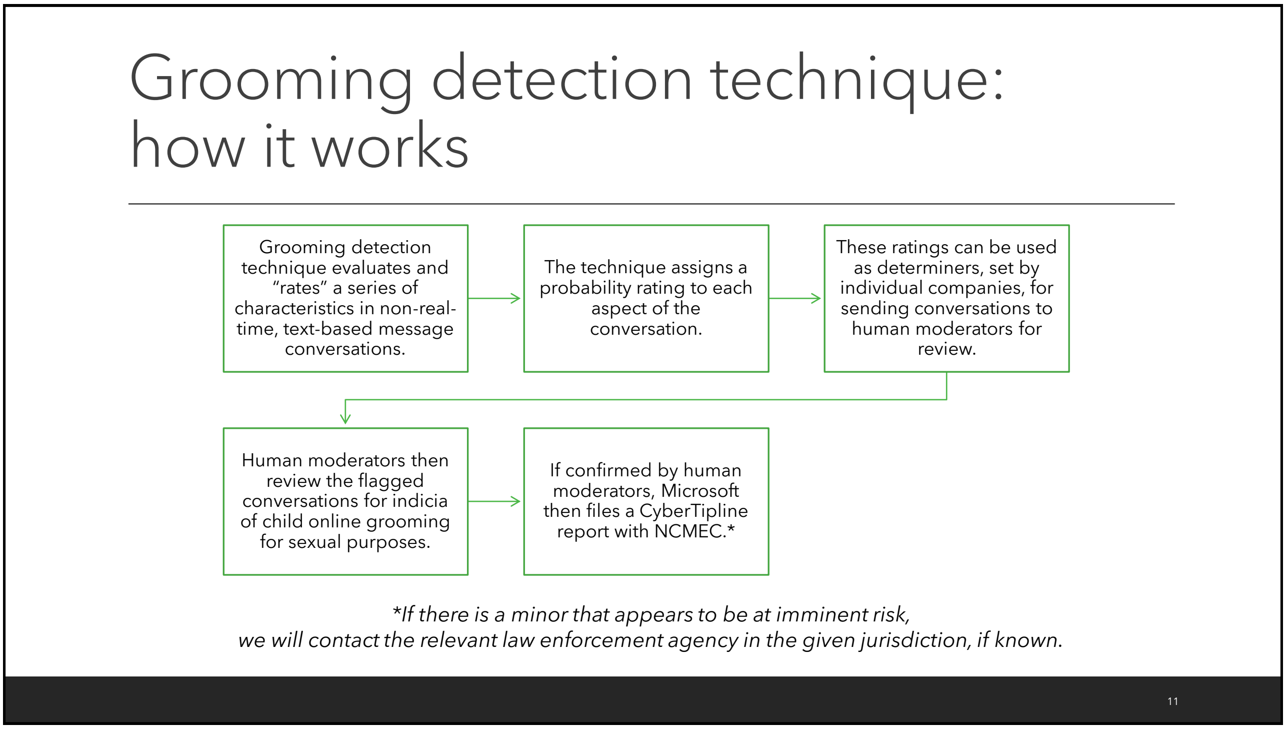
8



```
Group:1, PhraseId:10109_6,Match:1
Group:1, PhraseId:10203_6,Match:1
Group:1, PhraseId:10203_7,Match:0
Group:1, PhraseId:10209_6,Match:0
...
Group:7, PhraseId:70315_6,Match:1
```

Grooming-detection technique

10



Grooming detection technique: how it works

Grooming detection technique evaluates and "rates" a series of characteristics in non-real-time, text-based message conversations.

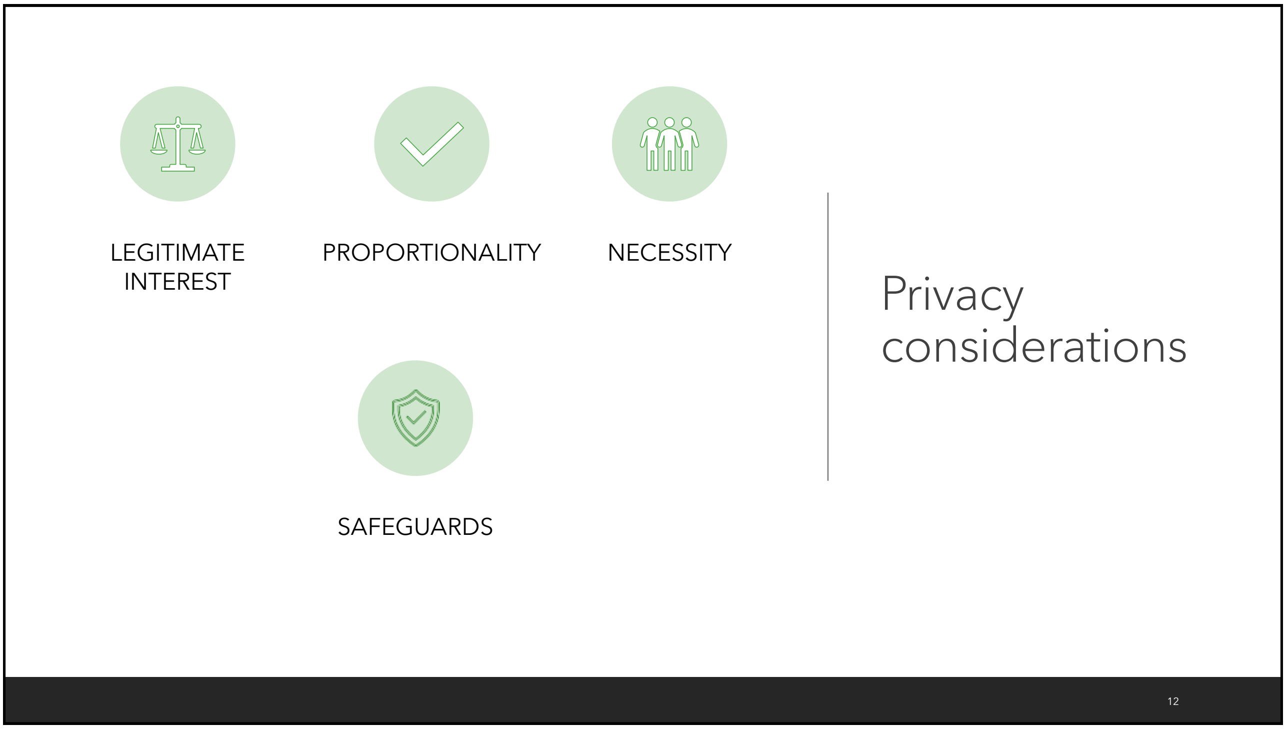
The technique assigns a probability rating to each aspect of the conversation.

These ratings can be used as determiners, set by individual companies, for sending conversations to human moderators for review.

Human moderators then review the flagged conversations for indicia of child online grooming for sexual purposes.

If confirmed by human moderators, Microsoft then files a CyberTipline report with NCMEC.*

**If there is a minor that appears to be at imminent risk,*
we will contact the relevant law enforcement agency in the given jurisdiction, if known.



LEGITIMATE INTEREST

PROPORTIONALITY

NECESSITY

SAFEGUARDS

Privacy considerations

Microsoft

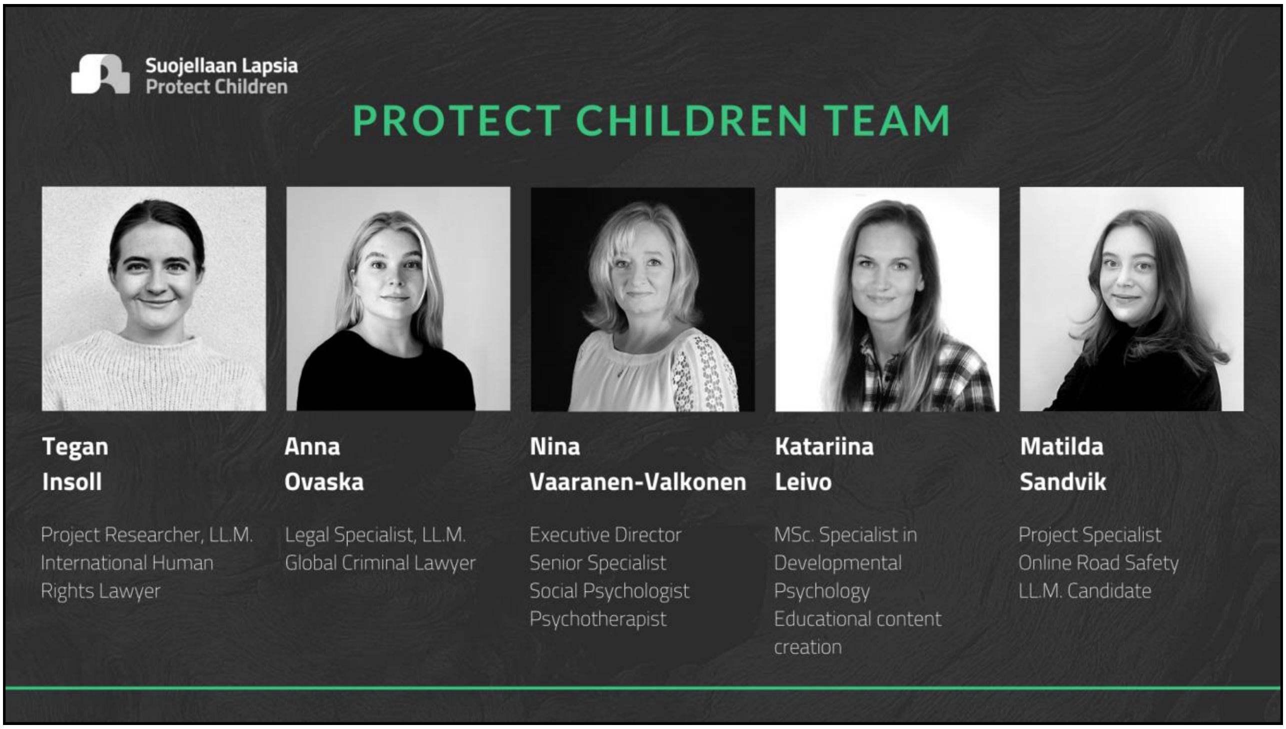
13

Suojellaan Lapsia
Protect Children

Children have the right to protection.

With the support of the Internal Security Fund-Police Programme of the European Union 2014-2020

1



Suojellaan Lapsia
Protect Children

PROTECT CHILDREN TEAM

Tegan Insoll
Project Researcher, LL.M.
International Human Rights Lawyer

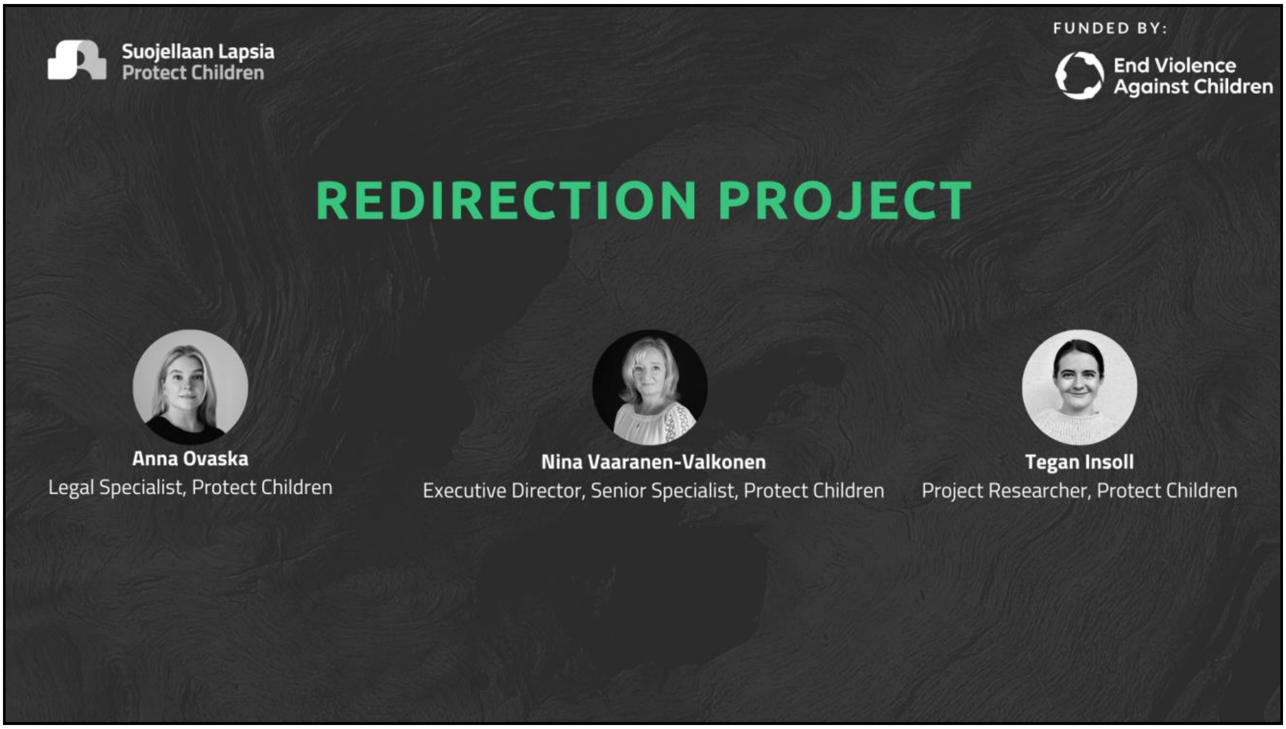
Anna Ovaska
Legal Specialist, LL.M.
Global Criminal Lawyer

Nina Vaaranen-Valkonen
Executive Director
Senior Specialist
Social Psychologist
Psychotherapist

Katariina Leivo
MSc. Specialist in Developmental Psychology
Educational content creation

Matilda Sandvik
Project Specialist
Online Road Safety
LL.M. Candidate

2



Suojellaan Lapsia
Protect Children

FUNDED BY:
End Violence Against Children

REDIRECTION PROJECT

Anna Ovaska
Legal Specialist, Protect Children

Nina Vaaranen-Valkonen
Executive Director, Senior Specialist, Protect Children

Tegan Insoll
Project Researcher, Protect Children

3

Suojellaan Lapsia
Protect Children

4

End Violence Against Children

CSAM USERS IN THE DARK WEB

PROTECTING CHILDREN THROUGH PREVENTION

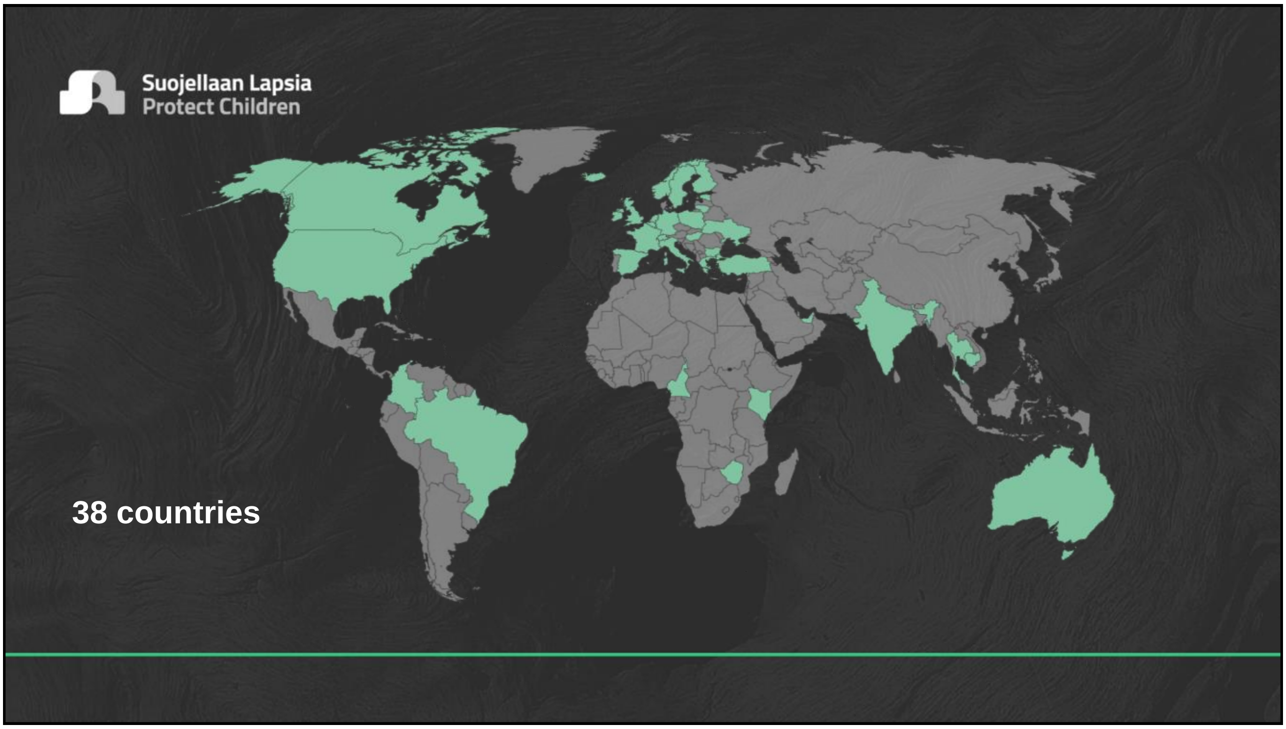
REDIRECTION SURVEY REPORT

Suojellaan Lapsia
Protect Children

Tegan Insoll, Anna Ovaska & Nina Vaaranen-Valkonen
Suojellaan Lapsia ry. / Protect Children

SEPTEMBER 2021

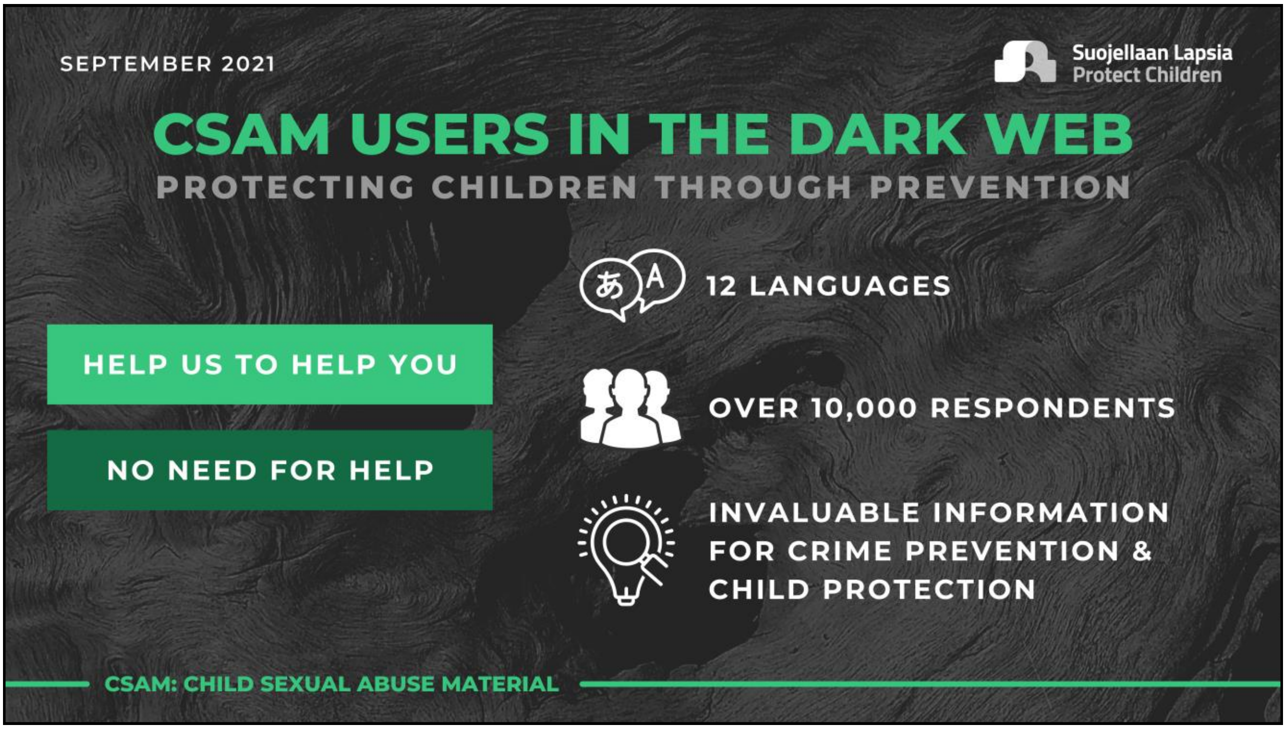
5



Suojellaan Lapsia
Protect Children

38 countries

6



SEPTEMBER 2021

Suojellaan Lapsia
Protect Children

CSAM USERS IN THE DARK WEB

PROTECTING CHILDREN THROUGH PREVENTION

HELP US TO HELP YOU

NO NEED FOR HELP

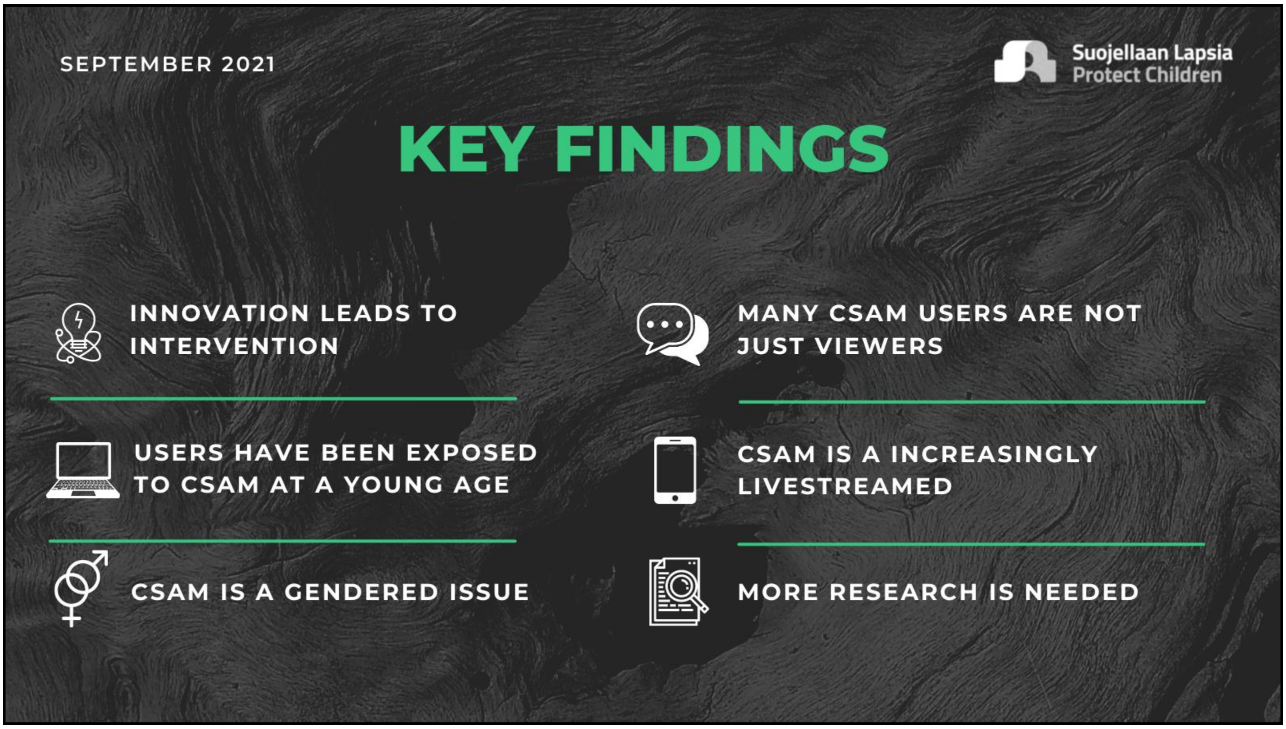
12 LANGUAGES

OVER 10,000 RESPONDENTS

INVALUABLE INFORMATION FOR CRIME PREVENTION & CHILD PROTECTION

CSAM: CHILD SEXUAL ABUSE MATERIAL

7



SEPTEMBER 2021

Suojellaan Lapsia
Protect Children

KEY FINDINGS

INNOVATION LEADS TO INTERVENTION

MANY CSAM USERS ARE NOT JUST VIEWERS

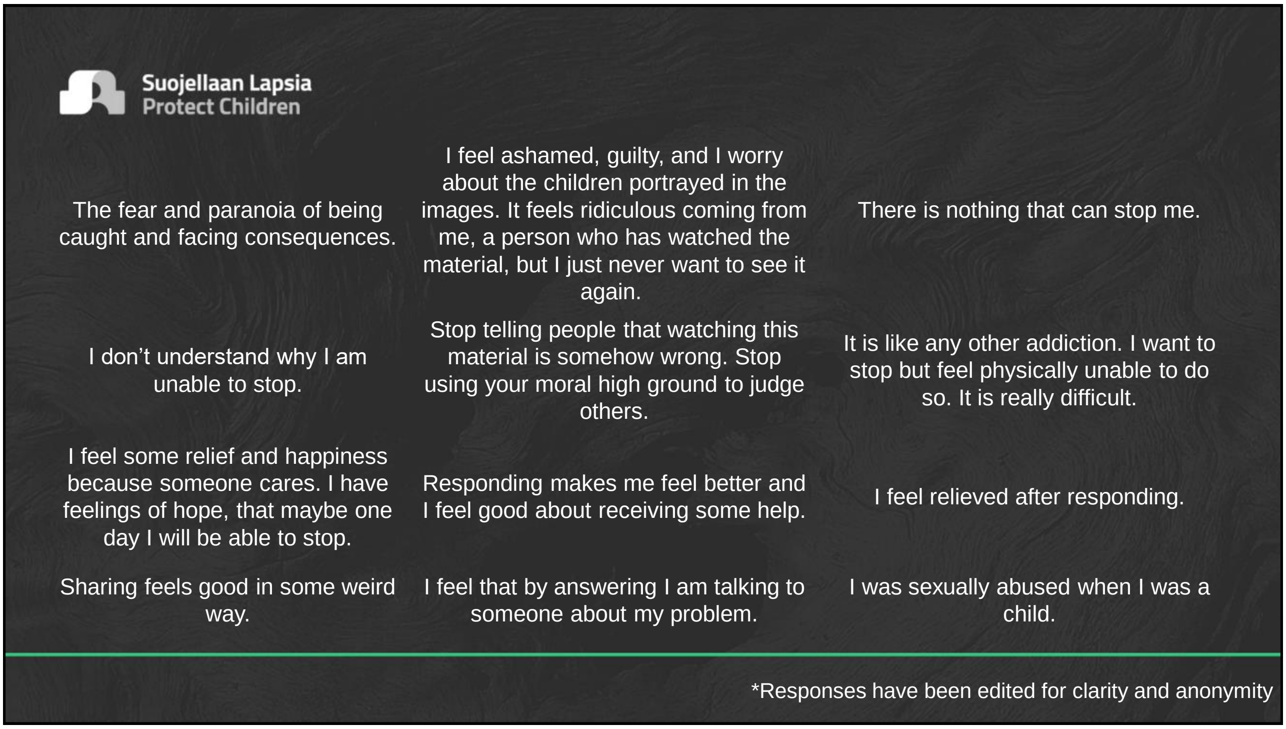
USERS HAVE BEEN EXPOSED TO CSAM AT A YOUNG AGE

CSAM IS A INCREASINGLY LIVESTREAMED

CSAM IS A GENDERED ISSUE

MORE RESEARCH IS NEEDED

8



Suojellaan Lapsia
Protect Children

The fear and paranoia of being caught and facing consequences.

I feel ashamed, guilty, and I worry about the children portrayed in the images. It feels ridiculous coming from me, a person who has watched the material, but I just never want to see it again.

There is nothing that can stop me.

I don’t understand why I am unable to stop.

Stop telling people that watching this material is somehow wrong. Stop using your moral high ground to judge others.

It is like any other addiction. I want to stop but feel physically unable to do so. It is really difficult.

I feel some relief and happiness because someone cares. I have feelings of hope, that maybe one day I will be able to stop.

Responding makes me feel better and I feel good about receiving some help.

I feel relieved after responding.

Sharing feels good in some weird way.

I feel that by answering I am talking to someone about my problem.

I was sexually abused when I was a child.

*Responses have been edited for clarity and anonymity

9

Suojellaan Lapsia
Protect Children

REDIRECTION SELF-HELP PROGRAM

FOR INDIVIDUALS WHO VIEW CHILD SEXUAL ABUSE MATERIAL

ANONYMOUS

REHABILITATIVE

COGNITIVE BEHAVIOURAL THERAPY

10

Suojellaan Lapsia
Protect Children

ReDirection Self-Help Program

27 September – 5 October 2021

Surface web (Helsinki University Hospital website)

- English: 888
- Spanish: 293

300+ people a day have accessed the ReDirection Self-Help Program on the dark web

11

12

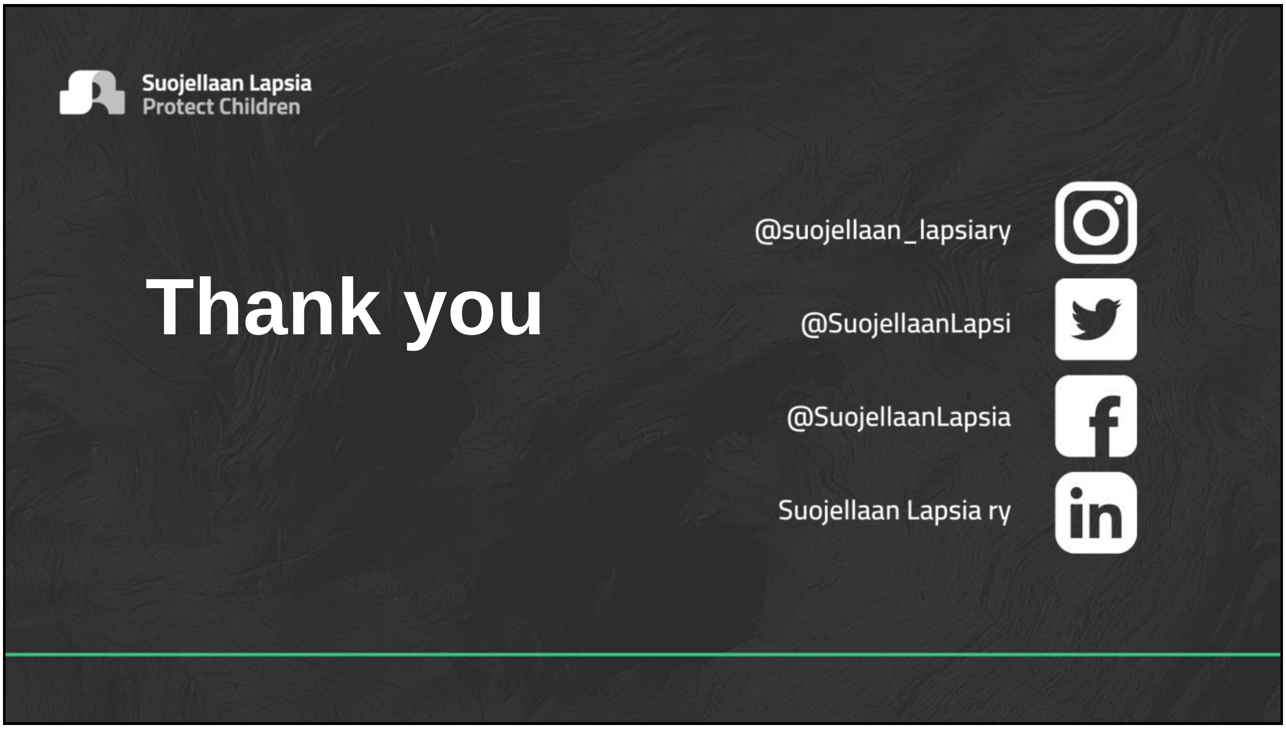
Suojellaan Lapsia
Protect Children

#REDIRECTION

FUNDED BY

End Violence
Against Children

13



Suojellaan Lapsia
Protect Children

Thank you

@suojellaan_lapsiary

@SuojellaanLapsi

@SuojellaanLapsia

Suojellaan Lapsia ry

14

Viljandi Haigla

mõistuse ja südamega

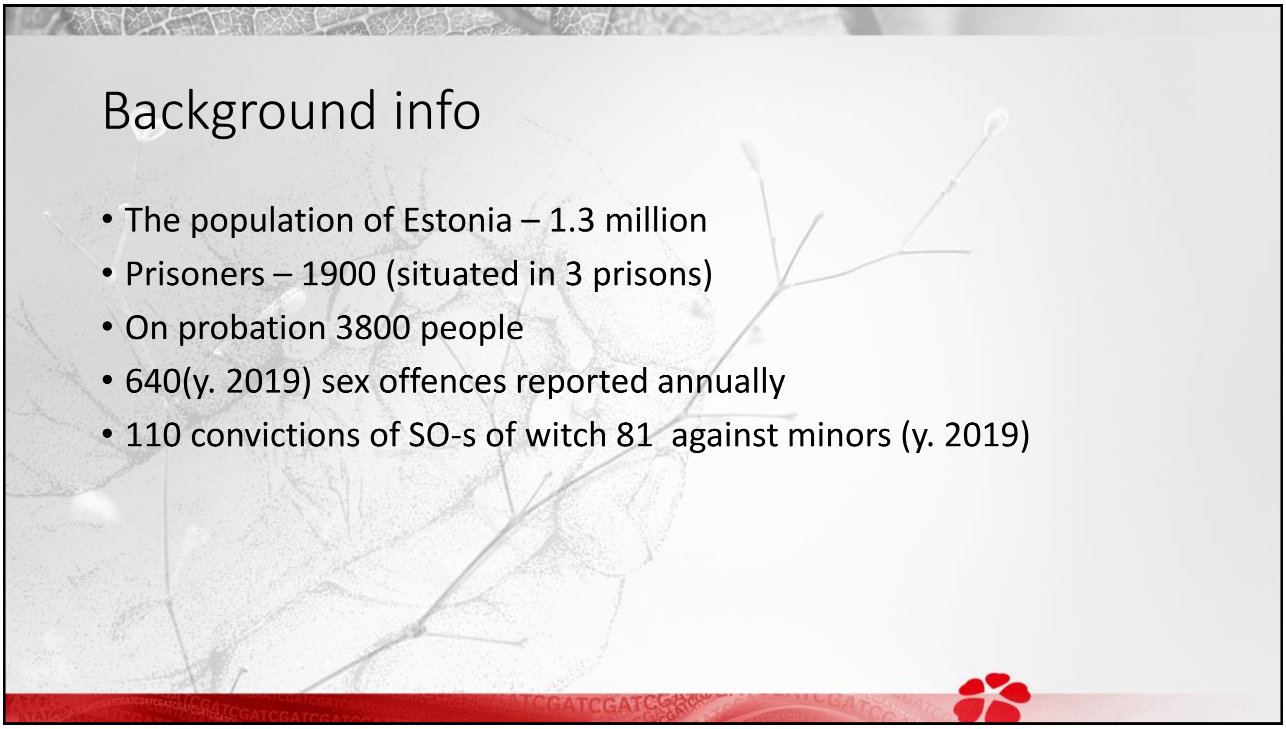
With the support of the Internal Security Fund-Police Programme of the European Union 2014-2020

1

Preventing and minimizing the risks of repeated offences of a sexual nature against children: experiences to share

Margus Veem
Psychologist
Viljandi Hospital

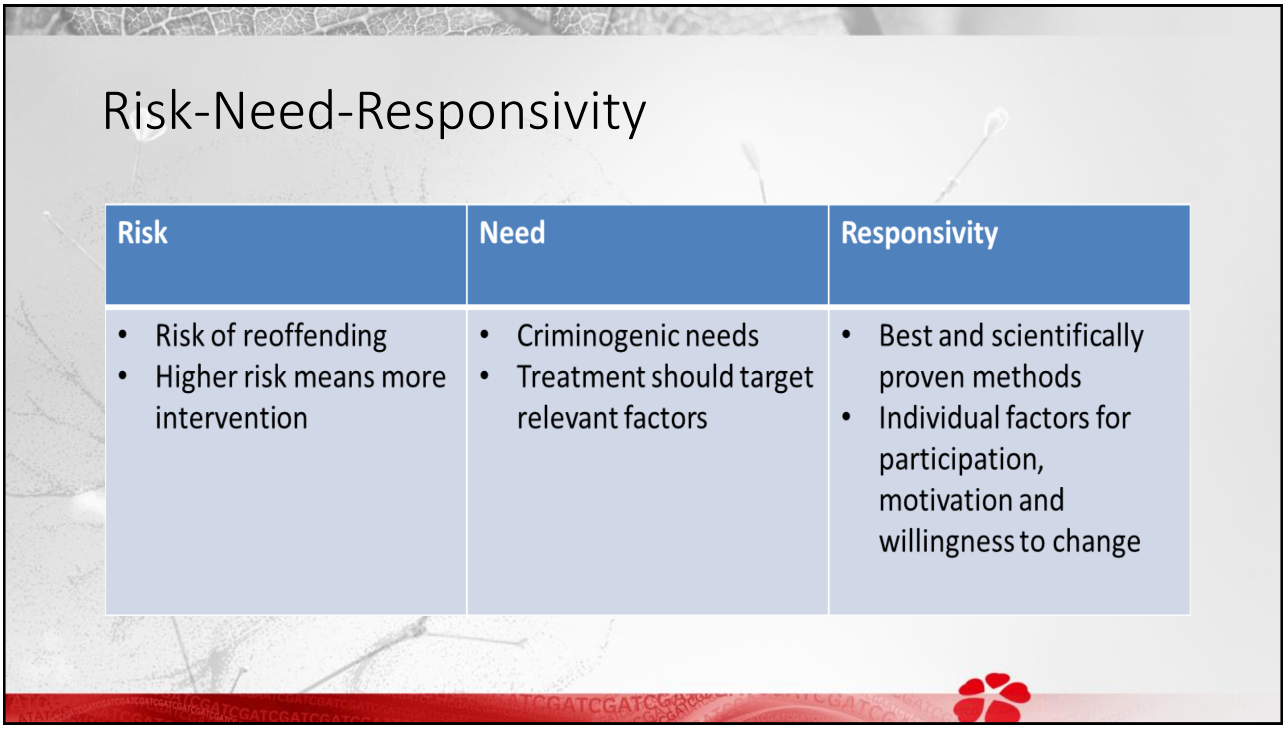
2



Background info

- The population of Estonia – 1.3 million
- Prisoners – 1900 (situated in 3 prisons)
- On probation 3800 people
- 640(y. 2019) sex offences reported annually
- 110 convictions of SO-s of witch 81 against minors (y. 2019)

3

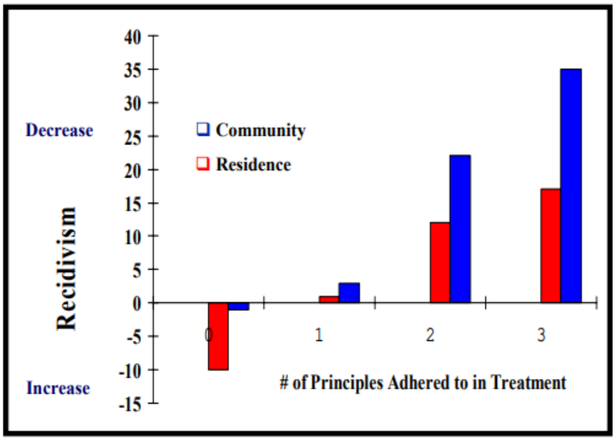


Risk-Need-Responsivity

Risk	Need	Responsivity
• Risk of reoffending • Higher risk means more intervention	• Criminogenic needs • Treatment should target relevant factors	• Best and scientifically proven methods • Individual factors for participation, motivation and willingness to change

4

RNR principles in action.



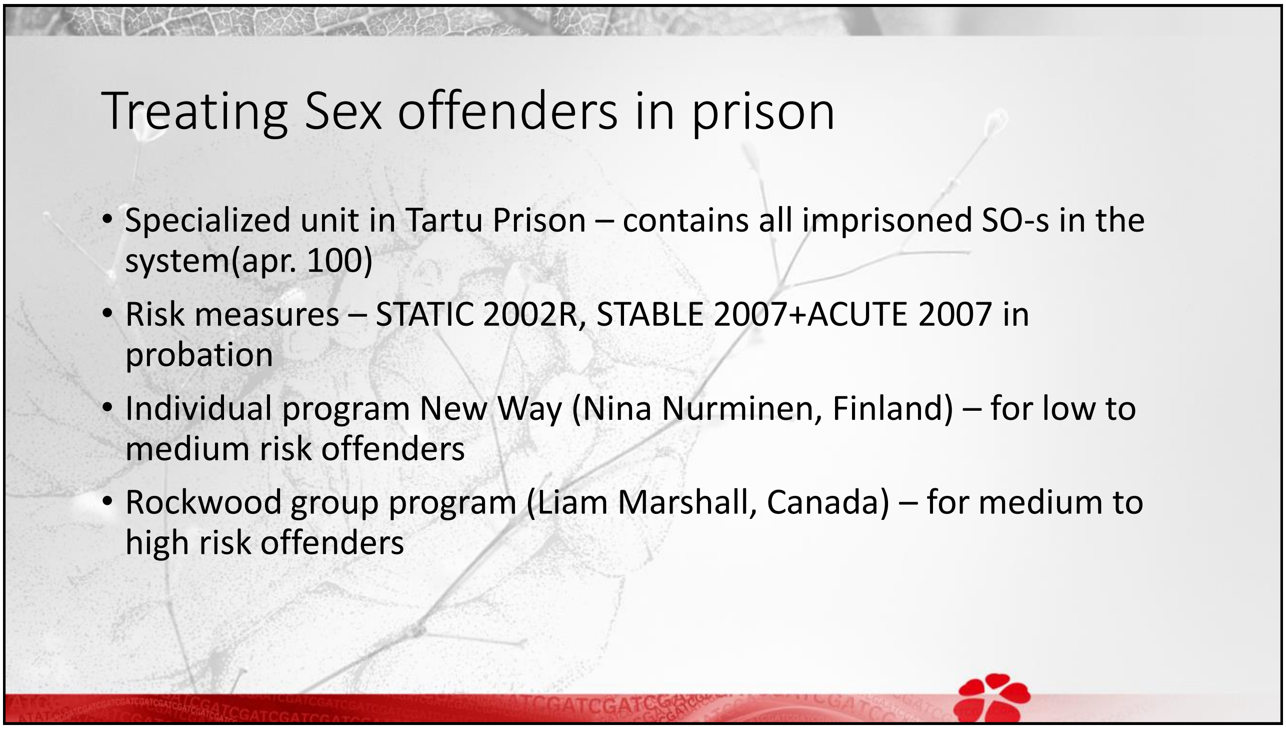
(Adapted from Andrews & Bonta, 2006)

5

Is treatment effective?

- Meta-analysis found that Interventions that utilized R-N-R principles reduced reoffending rates (Hanson et al. 2009) (treatment group 10.9%, comparison group 19.2%)
- In Finland reoffending rate differed almost twofold (10.5% vs. 5.6% but small group of offenders, n. 143)(Laaksonen et al. 2015)
- In Estonia – no effectiveness studies conducted as off yet, but using scientifically proven methods should make it as good as it gets.

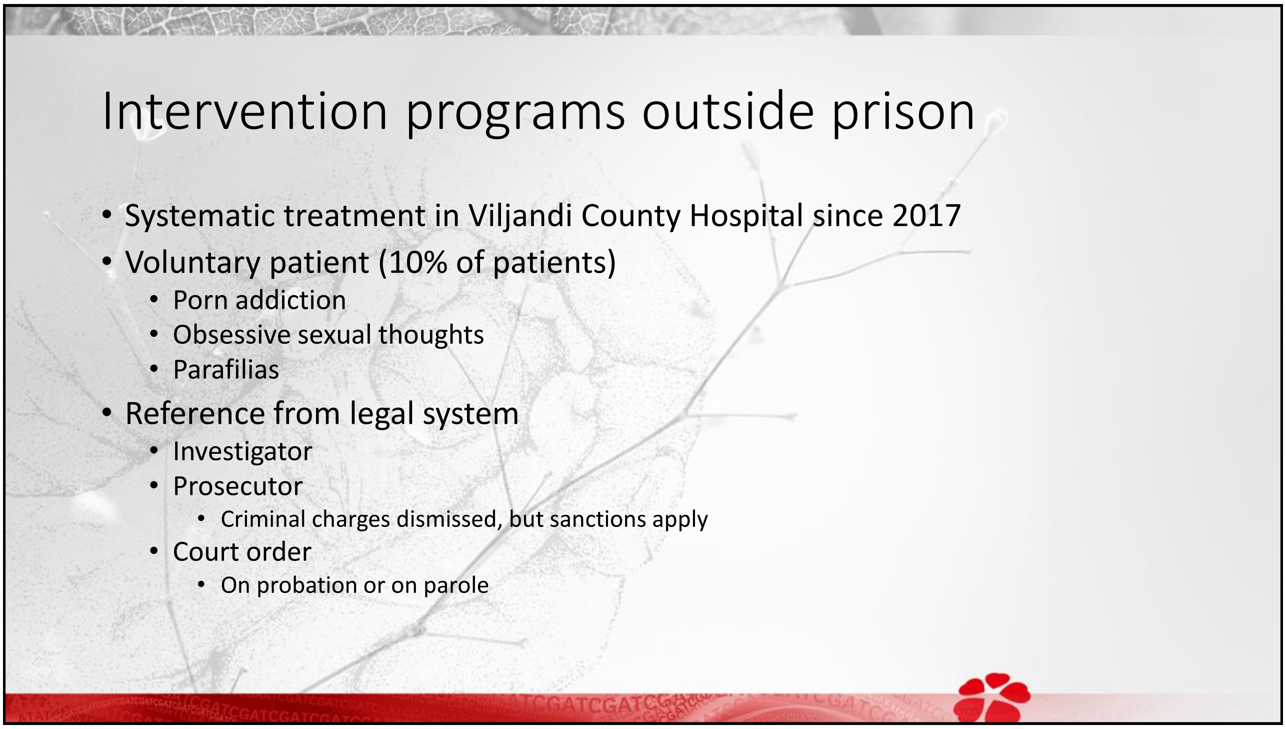
6



Treating Sex offenders in prison

- Specialized unit in Tartu Prison – contains all imprisoned SO-s in the system(apr. 100)
- Risk measures – STATIC 2002R, STABLE 2007+ACUTE 2007 in probation
- Individual program New Way (Nina Nurminen, Finland) – for low to medium risk offenders
- Rockwood group program (Liam Marshall, Canada) – for medium to high risk offenders

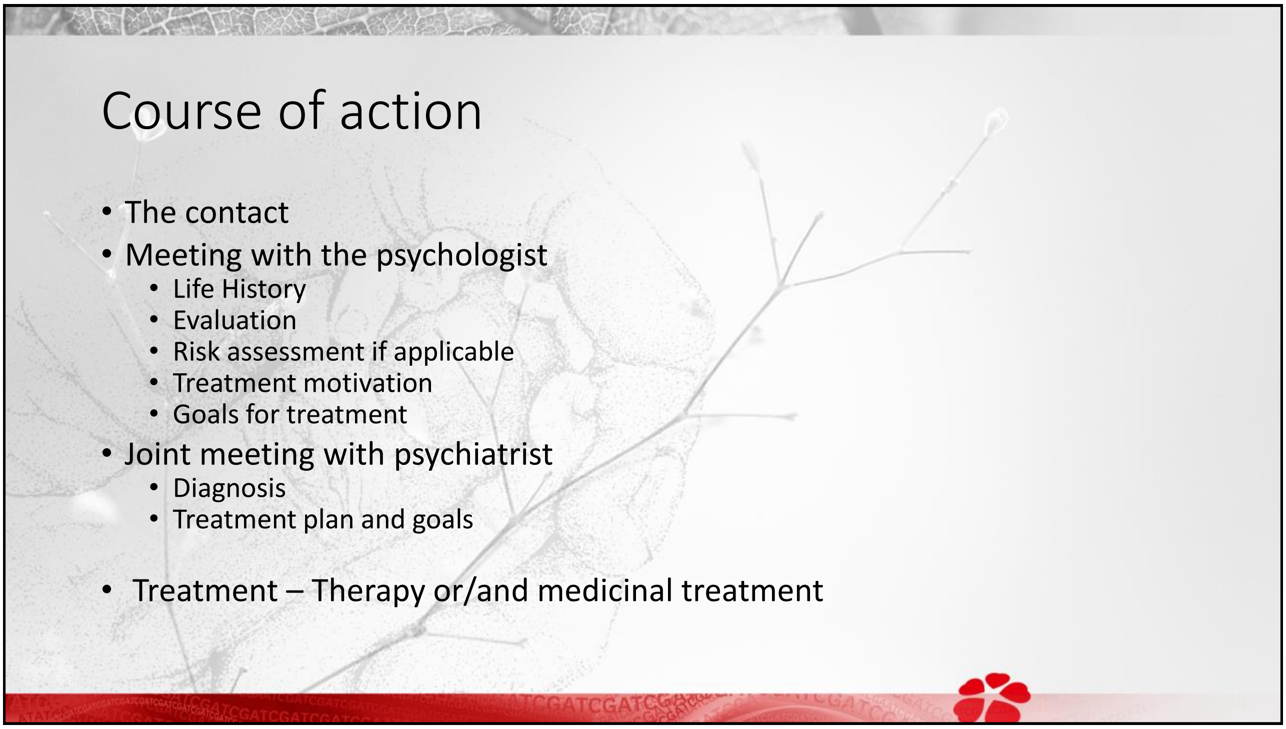
7



Intervention programs outside prison

- Systematic treatment in Viljandi County Hospital since 2017
- Voluntary patient (10% of patients)
  - Porn addiction
  - Obsessive sexual thoughts
  - Parafilias
- Reference from legal system
  - Investigator
  - Prosecutor
    - Criminal charges dismissed, but sanctions apply
  - Court order
    - On probation or on parole

8

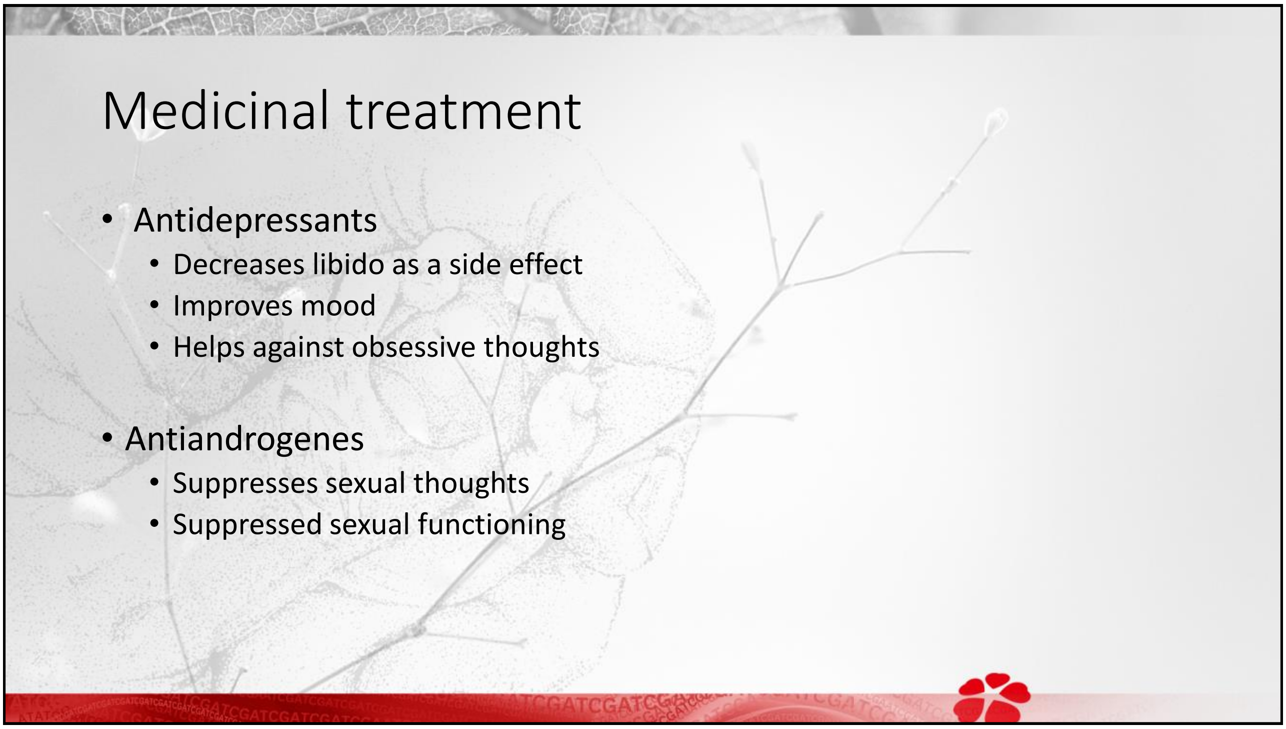


Course of action

- The contact
- Meeting with the psychologist
  - Life History
  - Evaluation
  - Risk assessment if applicable
  - Treatment motivation
  - Goals for treatment
- Joint meeting with psychiatrist
  - Diagnosis
  - Treatment plan and goals

- Treatment – Therapy or/and medicinal treatment

9

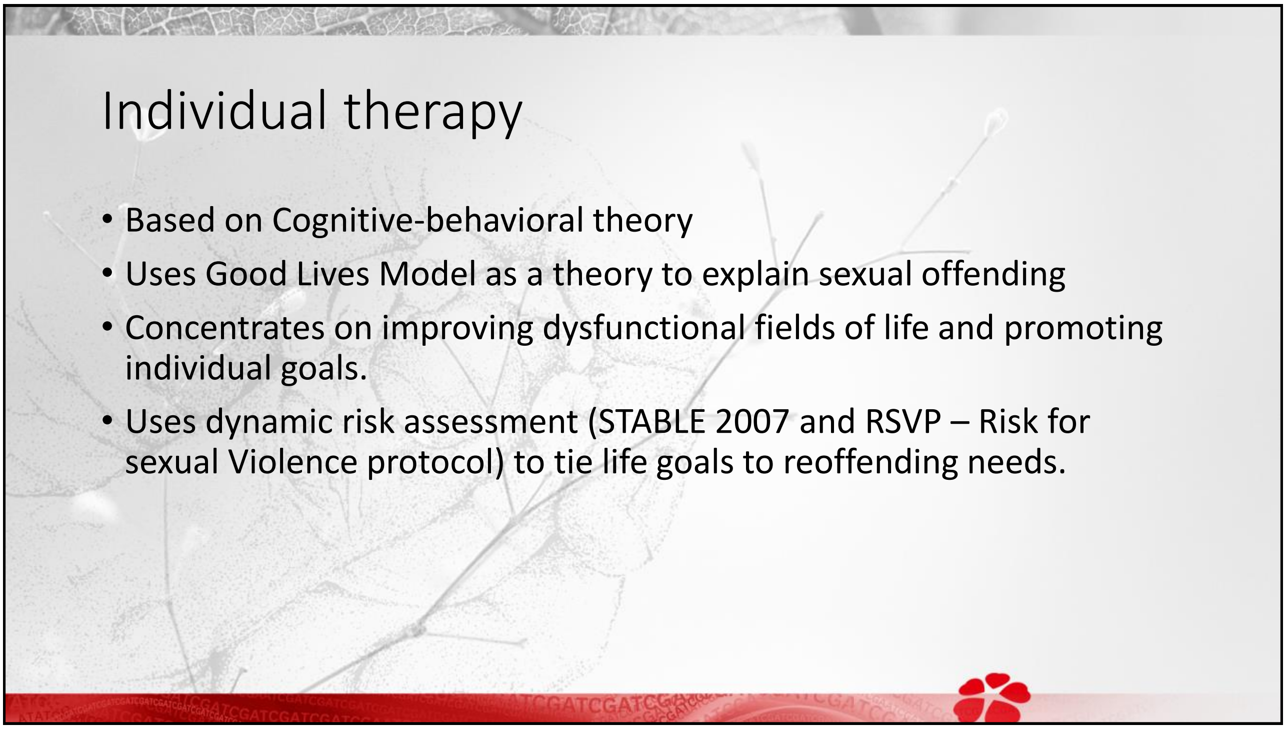


Medicinal treatment

- Antidepressants
  - Decreases libido as a side effect
  - Improves mood
  - Helps against obsessive thoughts

- Antiandrogenes
  - Suppresses sexual thoughts
  - Suppressed sexual functioning

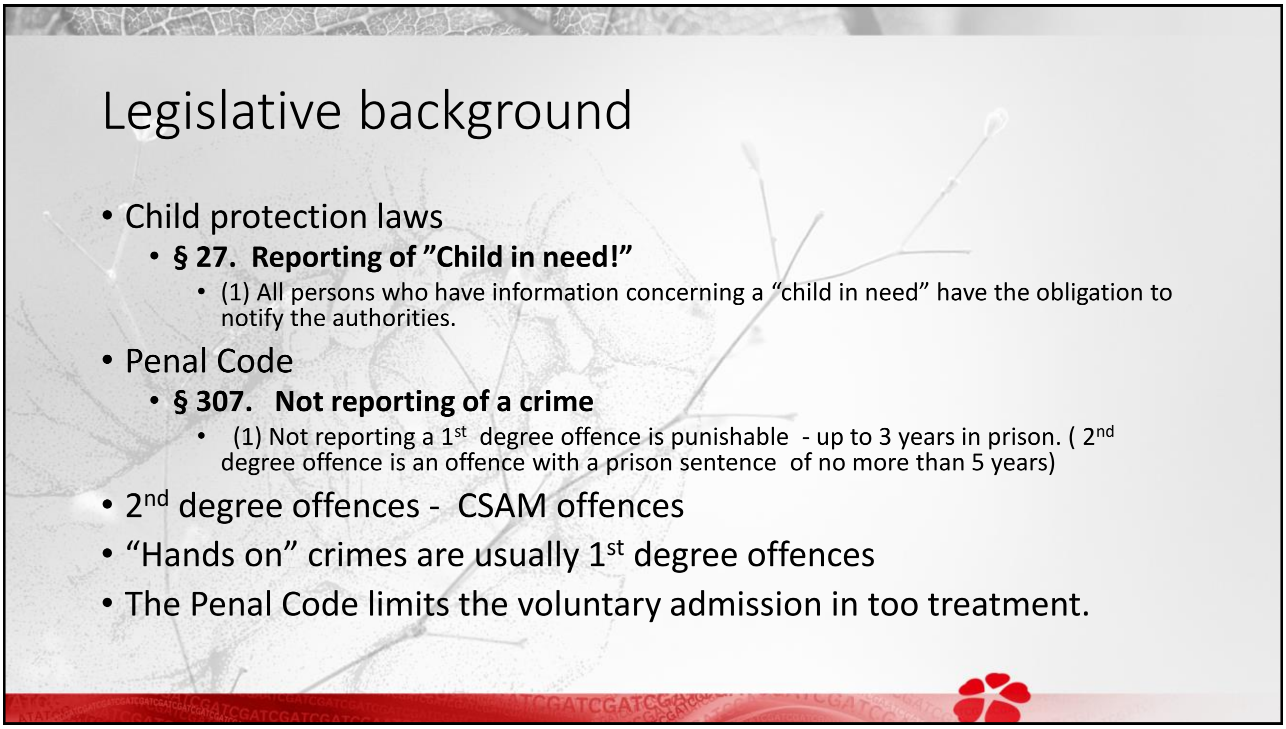
10



Individual therapy

- Based on Cognitive-behavioral theory
- Uses Good Lives Model as a theory to explain sexual offending
- Concentrates on improving dysfunctional fields of life and promoting individual goals.
- Uses dynamic risk assessment (STABLE 2007 and RSVP – Risk for sexual Violence protocol) to tie life goals to reoffending needs.

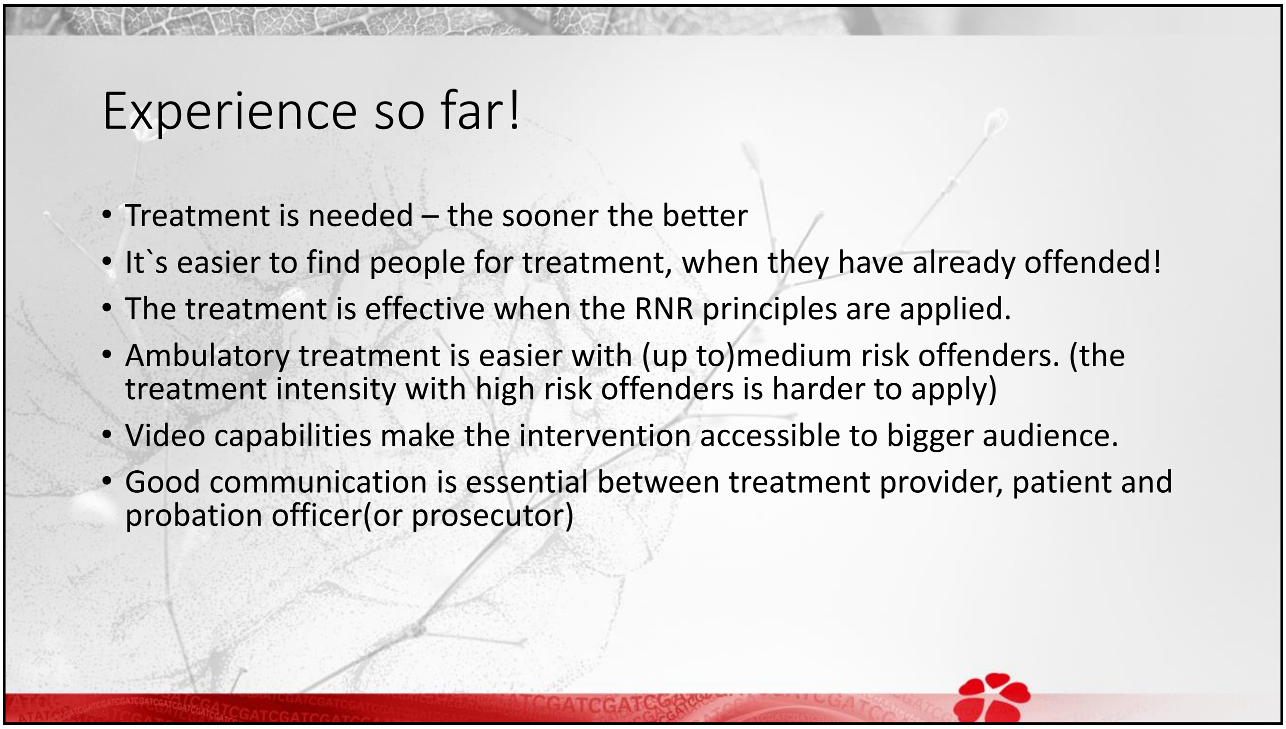
11



Legislative background

- Child protection laws
  - **§ 27. Reporting of ”Child in need!”**
    - (1) All persons who have information concerning a “child in need” have the obligation to notify the authorities.
- Penal Code
  - **§ 307. Not reporting of a crime**
    - (1) Not reporting a 1st degree offence is punishable - up to 3 years in prison. (2nd degree offence is an offence with a prison sentence of no more than 5 years)
- 2nd degree offences - CSAM offences
- “Hands on” crimes are usually 1st degree offences
- The Penal Code limits the voluntary admission in too treatment.

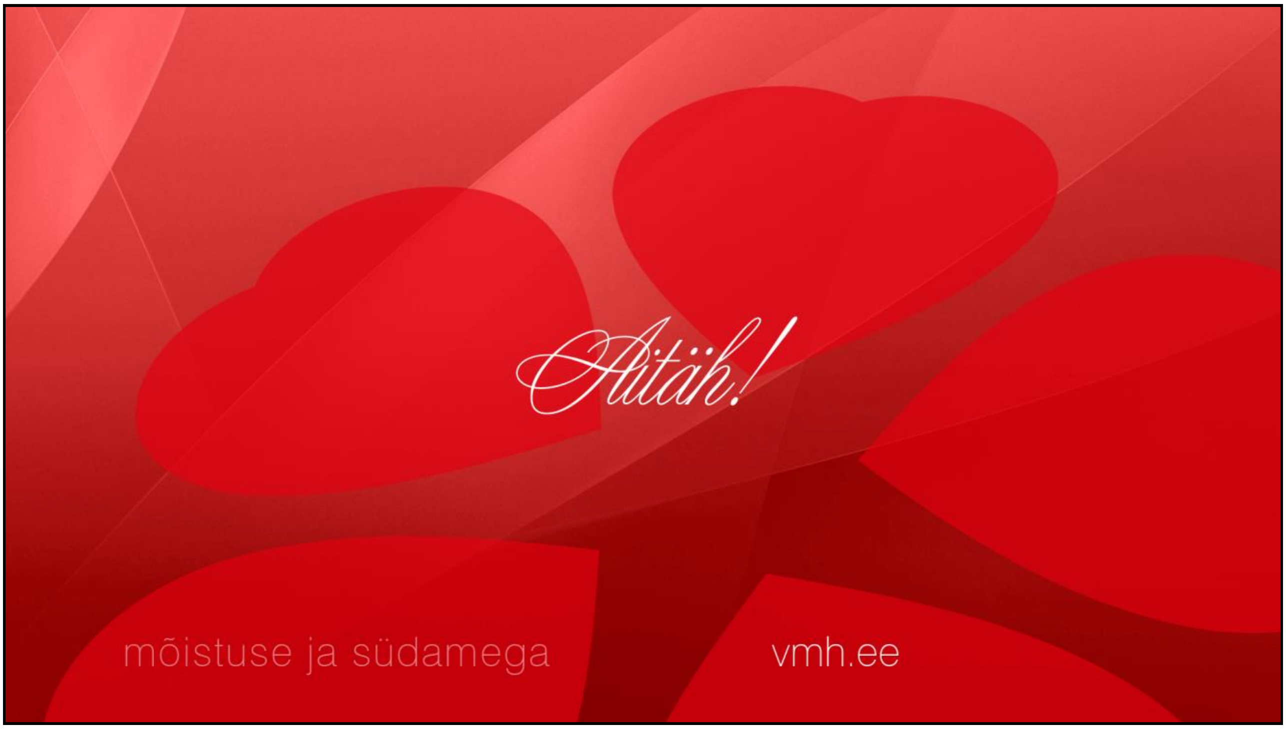
12



Experience so far!

- Treatment is needed – the sooner the better
- It`s easier to find people for treatment, when they have already offended!
- The treatment is effective when the RNR principles are applied.
- Ambulatory treatment is easier with (up to)medium risk offenders. (the treatment intensity with high risk offenders is harder to apply)
- Video capabilities make the intervention accessible to bigger audience.
- Good communication is essential between treatment provider, patient and probation officer(or prosecutor)

13



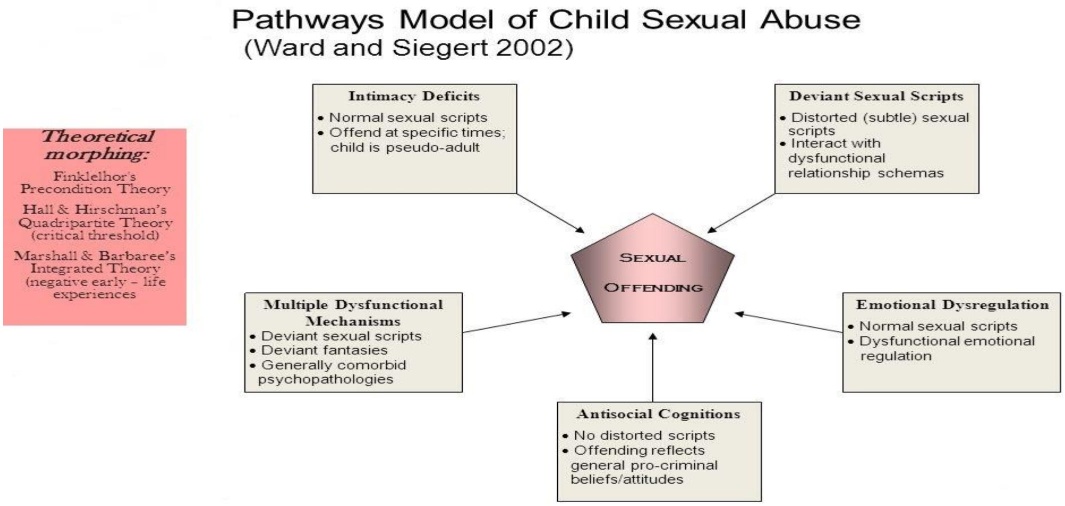
Aitäh!

mõistuse ja südamega

vmh.ee

14

Bonus material



Pathways Model of Child Sexual Abuse
(Ward and Siegert 2002)

Theoretical morphing:

Finklelhor's Precondition Theory

Hall & Hirschman's Quadripartite Theory (critical threshold)

Marshall & Barbaree's Integrated Theory (negative early – life experiences

Intimacy Deficits
- Normal sexual scripts
- Offend at specific times; child is pseudo-adult

Deviant Sexual Scripts
- Distorted (subtle) sexual scripts
- Interact with dysfunctional relationship schemas

SEXUAL OFFENDING

Multiple Dysfunctional Mechanisms
- Deviant sexual scripts
- Deviant fantasies
- Generally comorbid psychopathologies

Emotional Dysregulation
- Normal sexual scripts
- Dysfunctional emotional regulation

Antisocial Cognitions
- No distorted scripts
- Offending reflects general pro-criminal beliefs/attitudes

15