Victim Support Europe

With Financial support from the Justice Programme of the European Union

conference
online victimisation
developing a comprehensive response
brussels, 12 december 2018

Minutes of the conference

Welcome and Intros

Welcome note: Barbara Schretter, Director of the Representation of the Free State of Bavaria to the EU

Barbara Schretter welcomed all participants and VSE, and introduced the conference. Internet and technology have brought many advantages for many citizens but where there is online human interaction, there are criminal energy not far away. There are more and more cases of cybercrime. Police feel confident that the real number is even higher as many cases remain unreported. Local police in Bavaria are equipped with specialists and experts about cybercrime. Many cybercrime are related to espionage. Cyber alliance centre is ready to help when attack has occurred for businesses.

Welcome note: Chair of Event, João Lázaro President, Victim Support Europe

JL welcomed all participants and introduced the conference.

Graham Willmott, Head of Unit Cybercrime, DG HOME – Trends in cybercrime and future EU action

Graham Willmott talked about the EC's role in the fight against cybercrime. Cybercrime seriously violates the fundamental rights of victims, ruins competition and businesses, and leads to economic losses. There is a real increase in all forms of cybercrime. By 2021, cybercrime attack could cost 10% of the worldwide GDP.

Cybercrime is a low risk enterprise because the police does not come right away to investigate. There are increasing opportunities for criminals. Everyone relies on internet for their daily life. More than half of online users have already been a victim of cybercrime, which means about 2 billion victims globally. Some groups are more targeted and vulnerable that others: children victim of sexual abuse, the elderly, cyber harassment and bullying.

What is done in the EU:

- Child sexual abuse directive oblige MS to provide help to victims. Additional trauma through court proceeding
- Non cash payment fraud: EC and PE are keen to enhance the protection of victims in the new piece of legislation. SME do not have the means to fight cybercrime.
- Horizontal measure: victims directive, right to access to information, right to support, right to protection

- LEA is an incredible deterrent actor in cross border cases

Implementation? At EU level; EUROPOL and Eurojust help European law enforcement to investigate and apprehend criminal.
Cybercrime is a complex phenomenon and requires cooperation of all different sectors.

A Europe that protects, that delivers on big things, should reflect on the challenges on fighting cybercrime to protect its citizens.

Philip Adlem, Victim of Cyber hate crime – Experience of online harassment as an LGBTI person

Philip Adlem is a Hate Crime Caseworker for GALOP, an LGTBI anti-violence charity based in London. He was previously a police officer in the Metropolitan Police Service's emergency response team. In 2016 he proposed to his partner during the London LGBT Pride Parade, the recording of which has had over 100 million views on various media platforms worldwide. He and his partner received direct messages and indirect comments, including death threats and other hate messages. He left the police and joined GALOP as an advocate for victims of hate crime as a result.

Effects:

- Emotional: fear, anger, self-blame, guilt, feeling constantly under threat, impending disaster
- Social: damaged confidence, social isolation, withdrawal from sources of support
- Health: depression, anxiety, eating disorders, insomnia, stress induced illness
- Economic: problems at work

What was the police response and investigation? Because his name was not mentioned in the comments, tweets and other messages, there was no direct threat. He also did not want to admit to this was affecting him so badly.

Comments from people, police, from support, from friend, family "they are just comments, ignore them" → this minimalizes the event.

Stats:

- UK national LGBT survey 40% in the past 12 months
- See PP for more.

A participant asked him what he would like to see from police, their response? Philip answered that the most important thing is to show trust in the victim. Police officer need to believe the victims and understand that what they are going through is difficult. It is also important not to compare this with other crime, there is no difference because it happened online.

Session 1 - Understanding the criminal approach to improve our safety

Focus on the way that victims are targeted, what make certain groups and people vulnerable.

Cathal Delaney, Team Leader for Combating Child Sexual Abuse Online and Related Crimes at EUROPOL - The criminal's approach to targeting children

Cathal Delaney presented the approach of criminals to children, online and offline, and how they gain their confidence and trust. He also wants to share with the professionals the means they can use in their program, education, training to deal with this.

Europol EC3 was founded in 2013, European cybercrime centre. It focuses on 3 different types of cybercrime: cyberattacks, non-cash payment fraud, sexual child exploitation and abuse. Different approaches to these crime. IOCTA report is produced every year. EC3 also supports the MS into their investigation. It provides support in relation to forensic, support in digital forensic investigation

AP Twins – online child exploitations

- CSAM: child sexual abuse material
- Grooming
- Victim identification
- Transnational child sex offenders

The points of approach, the way the offender approach children, manipulate and exploit them is not different in the virtual and physical world. The online world is very real, it's no longer a separate thing, it is part of our real world and it affects people the same way.

- **Grooming**: predatory pact of manoeuvring another individual into a position that makes them more isolated, dependent, likely to trust and more vulnerable to abuse behaviour
    - Child grooming: deliberate act of establishing an emotional bond with a child, to lower the child' resistance. It can result in the minor falling victim to physical, sexual, and emotional abuse, specifically to manipulate children in to participating in slave labour, positions, and the production of images/videos
    - Can take place on social networking websites, instant messaging apps, phots sharing apps, and sites, chat rooms dating apps, online gaming apps. They are designed for social interaction by consensual people but they can be abused.
    - Predatory process:
        - Survey environment
            - Online platform
            - Open profiles
            - Contact and connections
            - Vulnerabilities
        - Gather data
            - Family/friends
            - Interests
            - Online behaviours: posting, sharing pictures
            - Online comments: interaction with others, responses to posts
        - Engage

                - Compliments
                - Establish common friends, interests, humour, geographical location, personal
                - Make themselves interesting and available
            - Assess vulnerability
                - Amount in common
                - Degree of isolation
                - Factors tending to secrecy/isolation
    - They try to isolate the child
        - Change channel of communication
        - Promote sense of safety/stability/privacy
        - Emphasise uniqueness of relationship
        - Push to reveal more about self, reinforce they need to be private/secret
    - Exploit vulnerability
        - Manipulate child using information gathered
        - Ensure production and sending of material
        - Reinforce isolation through shame, guilt, self-blame
        - Require them to involve others

Other methods used are also coercion and extortion and abuse of trust / position.

The impact on the child has multiple form: emotional, physical and societal.

Case example: Slovenia. Individual has groomed girls for over 10 years under 15 years old.

Direct contact:

- Abuse of trust/position: the major cases it's not a stranger, someone in their circle.
- Vulnerabilities: family/social situation, age. Those who are in poor social and family situation their vulnerability is great and its more difficult for them to resist. Usually below 15 yo.
- Solo abuse:
- Recording of abuse

Use same methods that can be used offline to manipulate the child, and gain their trust. If their record the abuse: relive the experience later and share it online with others.

Matthew Falder – convicted this year. Arrested last year. Active online for about 10 years. Online advertising platform: women and children to be models, send him images of them, tell them he would pay for naked pictures, would not pay and then threat to post online. Appeared to his friend to be a normal and sociable individual. Online he was targeting fathers, mothers and children to create child abuse material and create abusive and degrading materials. He would post these materials online on the dark net. Sentenced to 32 years in the UK, reduced to 25. Many victims are still struggling with the effects. He never met the victims. Everything was online. He never saw one of them until he met them in court.

He used sexual coercion and extortion:

- Motives: financial and additional content
- Means: grooming, threat, extortion and blackmail

- Opportunity: self-generated sexual content: self-circulated, circulated by others, send by deception

Things you may notice as victim support workers: withdrawn, suddenly behaves differently, anxious, clingy, depressed, aggressive, problems sleeping, eating disorders etc

Encourage children to find somebody to talk to, an adult, a friend, somebody else. By giving them our confidence, love, support, time. Do not express any judgement.

Laurens Dauwe, Osborne Clarke International Legal Practice – Responding to online fraud – from investigation to company and individual action

Introduction into cybercrime

Cybercrime is a broad notion 'any criminal activity in which a computer or networked device is targeted and/or used'. Four main categories:

- Finance related-cybercrime: cyber extortion, WannaCry, phishing
- Privacy related cybercrime; identify theft; spam
- Social and politically motivated cybercrime: cyberbullying, hate crime, terrorism
- Cybercrime for illicit activities: illegal pornography, trafficking of illegal substances

Why increase in cybercrime?

In offline world, proximity factor, offender has kind of direct link with the victim. Online crime, this is not the case. You can commit cybercrime from thousands of kilometres away and anonymously.
Common misconception: people always thing that cybercrime affect the vulnerable people, and to a certain degree they are the preferred targets. But major corporation and SME are also targets, but they are reluctant to come out as a victim.

What to do when you are a victim of cybercrime?

The golden rule: always act. The only way for us to fight, investigate and prosecute cybercrime.
When you're victim, different channels to use to report:

- On online platform: notice and take down procedure. Important to report
- Go to police authority: public prosecutor, file a criminal complaint
- Consult a specialised lawyer: they know how to respond. They can consult the criminal case file. They can ask for additional investigation action

How to investigate cybercrime?

Investigation, remediation and, and prosecution of cybercrime is complex due to:

- The complexity of the subject matter. Not the police are effectively skilled and equipped to assist you.
- Cross border nature of most events of cybercrime
- The number of actors involved

How to investigate?

- Engage your own security experts:

    - Very experiences teams, relatively quick root cause analysis and remediations
    - Costly, limited investigative powers
- LEA investigations
    - Very experienced teams, no cost for victim, very broad investigative powers
    - Limited resources, legal hurdles (
        - Lack of jurisdiction to perform investigation
        - Issues as regards
        - See PP

Paradigm shift in compliance obligations?

Case law in Belgium. Yahoo Doctrin ->

- Yahoo was required to provide the name of an individual using a yahoo mail address for online fraud
- Yahoo refused as it was established in the US and BE law enforcement had no jurisdiction. Belgian LEA's need to follow the MLAT procedure
- Supreme Court BE: if you provide services that are available in Belgium, Belgium law applies and you need to comply with requests from Belgian LEA's.

Confirmed in a case against Skype.

Laws on criminal procedure (Belgium and EU)

Terrorist attacks and growing cybercrime -> change in laws

- In BE: Act of 25 Dec 2016 Belgian code on criminal procedure was amended and provided for a significant broadening of investigative measures
    - Confirming Yahoo doctrine in law
    - Hacking by LEA became permitted for the investigation of several crime including informatics fraud
- In EU: new initiatives are underway or have been adopted
    - EIO Directive
    - E-Evidence regulation (proposal)
    - E-Evidence Directive (proposal)

Perception of internet operators: they did not want to interfere. Goals of major companies: maintain their neutrality, not to police the internet, respect freedom of expression. However growing abuse of their technologies, discussion on manipulations of election, discussion on possible regulation forces perpetrators to slowly but surely take action by : engaging teams to review content, cooperate with LEA, increase and improve their relationship with LEA.

Cybercrime is a complex matter; regardless of the complicity you should act. LEA, lawyers, public society get more needs to tackle cybercrime.

Question by Gabor about social media and its effect on the children who are born into it today – Cathal responded that the rules are the same as before – don't talk to strangers

Session 2 - What makes us vulnerable to cybercrime – who are the criminals targets and why

Patricia Le Cocq, Myria, Federal Migration Centre and Independent National Rapporteur on Human Trafficking - What makes a person vulnerable to trafficking?

Myria

Myria – the Federal Migration Centre, an independent public body working on migration and against human trafficking. They publish an annual evaluation report on the fight against trafficking in Belgium; they also initiate criminal proceedings. Each year, the report has a focus, and last year it was on the social media and internet.

THB – Trafficking in Human Beings – international and Belgian definitions

Use of internet and social media in trafficking

By traffickers:

- Recruitment of victims
- Marketing prostitution
- Services management of criminal activities

Most used platforms: Facebook, Viber, Whatsapp, Skype, and chat forums of sex dating sites.

The internet is also used by law enforcement in the fight against trafficking.

It is also used by victims to create a certain image on the Internet, especially migrant victims who try to create an idealized picture of their life for the people back home.

New technologies facilitate human trafficking through:

- Broader public
- Anonymity
- Social networking sites

Examples of sexual exploitation through internet/social media usually are based on promising perspectives/better life and happen through:

- Debt bondage
- Dishonest modelling agencies
- Victims' own ads
- Job offers through fake Facebook profiles

Labour exploitation takes places in agriculture, hotel industry, transport, construction, catering, domestic work, etc. Many of victims are in precarious financial and/or residence situation. Debt bondage also happens here.

Traffickers seek out emotionally vulnerable victims, and they can obtain the relevant information on the social media sites. Many of the targeted victims are girls aged 15-24.

Loverboys

Loverboys' victims are usually isolated young girls with low self-esteem. Emotionally fragile, they have family problems, and often take drugs. Loverboys specifically target young girls in youth institutions, and they also find the relevant information on their victims on their social media. 50% of victims are recruited via social media. Facebook is more often used for starting relationships. Many of the victims have open profiles on Facebook. Loverboys also use Skype to search for vulnerable potential victims through searching for specific sayings showing that they don't feel good about themselves.

In the charming phase, loverboys show a lot of love and attention, but this is designed to develop into an emotional dependency phase. They will isolate the girl, make her emotionally and/or financially dependent, become aggressive one day and nice the next one, etc. The next phase is the exploitation phase when the girl becomes completely dependent; she has to work to "pay back the costs" and is forced into prostitution.

Points of attention

- Training professionals – for instance, in NL, a tool has been developed to identify victims of loverboys (a kind of a checklist)
- Awareness raising
- Avoiding stigmatisation
- Increasing online monitoring – especially on social media, online job agencies, etc. (for law enforcement)
- Strengthening resilience – for instance, through exchanging experiences about websites

Estefanía Sancho Muñoz, Plena Inclusion Aragón – The perspective of people with intellectual disabilities

Estefania introduces herself as part of Plena inclusion Aragón, Cermi, and Los que no se rinden – the first Spanish association created by people with disabilities.
Some of the activities she has been doing include:

- First social forum of women with disabilities
- Protest of people with disabilities rights

Estefania defined cyberbullying and its types (sexting, grooming, indirect cyberbullying, etc.)
We don't know how many people are being bullied; some of them might not realize they are suffering from cyberbullying. Others do not know how to solve the problem or who to ask for help.

Propositions for people with a disability to feel safer and less vulnerable when using the internet:

- Easy reading tutorials for Facebook, Instagram, etc. explaining how to use them safely
- Having a contact person when we do not feel secure
- Easy reading app for social media sites so that we know what we area actually agreeing to
- Recognising other types of disabilities (e.g. adding sign language in videos)
- Information on what we can and cannot do
- Having the option to be supervised by someone
- Having the option to say you have a disability when you create an account

Recommendations for everyone:

- Think before you click
- Don't open messages from people you don't know
- Use complex passwords
- Be careful with personal information
- Cover the webcam
- Think about you post, don't say anything you wouldn't say in real life
- Do not trust strangers – do not send anything to people you don't know

Video screening – a victim of cyberbullying

Question about the notion of consent – do you collaborate with education systems? We need to teach young people not only how to use the internet but also how to say no and that their body belongs to them.
Patricia replies that they don't really work in educational institutions but that they do publish recommendations in which the notion of consent is very important, especially with regard to trafficking. If a victim does not know the conditions they will be working in they will be considered a victim of trafficking
Estefania said about people with a learning disability – if education is not adapted, it is very hard for them to study.

Question about boys as victims of exploitation – Patricia replies that they do not see many boys as victims of sexual exploitation; in labour exploitation there are a lot of men (sometimes minors).

Session 3 - How we can reduce risks online and support victims

Introduction by Helgard van Hullen and Levent Altan – looking at different kinds of support to victims of cybercrime. Introducing Celine and Denton.

Céline Sturm, Weisser Ring German – Supporting victims of cybercrime

Weisser Ring – Germany's largest victim support organization with 18 regional organizations with more than 3 000 volunteers and over 50 000 members.
Definition of cybercrime from the German federal office of criminal investigation – defined as crimes committed by means of information technology.
Statistics: 90.3% of the German population older than 14 are online, while 77% go online on a daily basis. High growth rates for the population over 60. 97% of young people own a smartphone. Every second German internet user (**49%**) in 2017 became a victim of cybercrime.
It is also getting easier for offenders to commit crime as one can 'buy' it as a service on the dark web.

The internet is a popular medium of crime as it is anonymous, fast, and has a worldwide network.
Victims often don't go to the police because they think the offender won't be caught.

T**wo examples of victims helped by Weisser Ring:**

- Victims of Cyber mobbing/cyberbullying
  A girl who posted a photo in a bikini and got a lot of offensive comments
- Victims of identity theft
  A girl whose identity was stolen, including her name and address, and she was receiving packages in her name and address

How Weisser Ring supports victims of cybercrime:

- National hotline
- Online consultation
- Immediate emotional assistance and personal care after the crime
- Accompaniment to appointments at the police, court, etc.
- Assistance in dealing with other authorities
- Connecting to other organisations
- Assistance checks for the victims' fees for a visit to an attorney/lawyer
- Recovery measures for victims & relatives
- Financial support for emergency costs

Cybercrime prevention and sensitization

Press releases, special publications, workshops and presentations, seminars for volunteers.
Knowledge transfer is very important (high schools, teachers, etc; brochures; congresses)

Denton Howard, Executive Director, INHOPE – Removing illegal content on the internet

Hotlines deal with victims immediately after what's happened and are part of one big ecosystem where different actors come in at different stages and are all victim-centric.

Denton Howard is responsible for making hotlines more effective based on previous experience.
Solutions have to be invented in a fast-changing environment. Howard's mission is to remove online CSAM (child sexual abuse material) as soon as possible from the internet. He does not use the term 'child pornography' since pornography can be consensual; children can not give consent → it is always abuse.

A hotline – an organization operating on a national basis that allows anonymous reporting of suspected illegal internet material including CSAM.
Each report is assessed by the hotline in accordance with national legislation and against Baseline classification.
If content is classified as illegal, INHOPE wants the content removed, not deleted, so that police can gather evidence.
The sooner the content is offline, the less time it has to be re-shared and to re-victimize the victim.

Report → hotline classification → exchange to relevant hotline (often in a different country) → law enforcement → internet service provider → removal of content

Why have the INHOPE network?

CSAM is a global issue, hence, it needs a global response. INHOPE has a transnational network in many countries around the world.

ICCAM system (based in the basement of Interpol) allows for instant exchange when hosted in other countries.

INHOPE network helps reduce re-victimization by taking down files referenced by many websites.
For every 100 reports, only a small portion of them (around 10) is illegal → INHOPE reduces the workload for the police

Achievements
In 2017, there were 87 390 actioned CSAM reports routed via ICCAM (many containing multiple images)
259 016 unique CSAM items (real figure much higher)

Questions:
The analysist has to review only the content that has never been reviewed before. A person does not have to see that content again. Hotline analysist are valuable, hard to train.

How does INHOPE interact with someone who report the content on a platform such as Facebook? Facebook has their own platform, they have their own process to remove the content. We are in contact with Facebook.

The phrase child porno is not acceptable to the EP, victims, victim support organization. It's really important.
What happened when there are servers that are in jurisdiction that are not governmental. Sealand – micro nation, there was server which hosted materials which in the UK would have been considered illegal; how INHOPE would go around such a situation?
A: we have issues where countries are in a disarray, not very clear from a technology perspective who is governing what. Important that the info goes to the right person in LEA.

Session 4 - Changing public perception and response to cybercrime

Pia Micallef, Co-founder of the MetooEP campaign – The perception of cybercrime against women and changing reactions

MeTooEP is a movement of workers in the EP. Victims of sexual harassment inside the EP could not get justice because reporting system in the EP was not functioning correctly. They went to the media. The EP reacted by drafting a resolution on combatting sexual abuse in Europe. In the resolution, main thing that needed to change within the EP:

- In the EP, when a person comes forward with allegation of sexual harassment, the committee is made up of 3 MEPs and 2 assistants. There is a psychologic and doctor as observers. There are two committees on harassment:

- One for assistants
- One for rest of the staff: doctor and observer can vote

There is therefore a difference of treatment for assistants.

There is still no implementation of any concrete action to fight sexual harassment in the EP.
Creation a petition, 1000 signatures. Still no action.

Creation of the website www.metooep.com : publish anonymous testimonies of sexual harassment within the EP. The victim comes forward on their own accord. Created the website to raise awareness. EP continues to tell there is no problem of sexual harassment, because victims do not come forward.
Victims do not feel safe in the EP. Victims have the opportunity to share their story and tell the EP that there is a problem with sexual harassment in the EP.

Media portray bullies, they are almost glorified, they are given the perception that to be a bully is to be popular and be cool. Children who watch this are growing up with a key message that is cool to be cruel. Popularity is amplified online with Facebook, Instagram etc. "The untouched bullies of yesterday become the harassers of today."

Online sexual harassment. Differentiation in the way we treat victim and aggressors. Art always portrayed the women as an object of desire. At the same time, women are shamed to be like that. Differentiation we treat male and female is unjust. We need to start teaching children that bullying, physical and emotional, are the same level. If they were adults such behaving would be illegal.

Maria Teresa Giglio, Mother of Tiziana Cantone, Victim of non-consensual image sharing
Maria Terese Giglio is the mother of Tiziana Cantone who committed suicide after videos of her were shared on internet without her consent. The videos are still online and circulating. There has been merchandising campaign, meme, fake facebook pages using the images and words of the videos. The Italian justice system does not support Maria Teresa. She is here today to talk about her story and to make change for mothers and women in the future. She advocates for the adoption of stronger control procedures on social media.

Closing remarks

Helgard van Huellen, Vice President, Victim Support Europe
Helgard highlighted how essential is it that VSE, member organisations, the EU institutions, and other stakeholders all work together, locally, nationally and internationally. Importance of bringing everyone together to find better ways to help victims in a coordinated approach.