COE – Octopus 2011 – Michael Moran (Interpol)

Ten years is a long time but I think that is only in Politics and in the lives of children. As a father I am shocked at how I have gone about my daily business while my beautiful pliant babies have turned into cheeky teenagers busy pushing against every rule, constraint and direction as they develop their own personalities and learn to deal with the world around them. That world includes, for them, the wonderful world of connectivity. Connectivity that is as natural as walking, as "just there" as electricity and fast becoming a basic human right.

In the world of online child exploitation ten years is but the blink of an eye but a lot has been done in that time. Around the time the convention on cybercrime was born Operation Landslide was winging its way to Europe and the rest of the world and waking everyone up to the realities of online child exploitation. In this operation many thousands of people had knowingly paid for access to Child Abuse Material (CAM). In most countries in the world it was not even illegal but this payment facilitation website was taken down in the USA along with the names, addresses, telephone numbers, credit card numbers and email addresses of suspects. A lot of suspects. In some countries it was ignored, in others it was dealt with as some kind of once off Operation but those in the know, knew it was just the start.

It was a symptom of the fact that Child Abuse Material was coming back after it had been driven underground in the USA and Europe in the mid-eighties. Prior to that it had enjoyed almost ten years of unfettered availability in glossy magazines and 8mm movie format. The repeal of laws at the end of the sixties in some European countries allowed Child Abuse Material to become readily available and be exported around the world. In the mid-eighties it was driven underground to the extent that it disappeared from the radar completely and was confined to a few "cottage" collectors and aficionados. Incidentally an incident took place around the same time as legislative change that brought the reality of CAM home to the public. In August 1984 a pornography actress died of a cocaine overdose in a hotel in a premier European Capital. Her name was Thea Puijmbroek; she was six years old.

Not long after this the Internet became popular and a combination of availability, affordability and apparent anonymity[1] produced a resurgence in CAM that is rapidly becoming a societal issue not seen since drugs problem was first identified in the 1960's. The fact that many thousands of white, middle-class, taxpaying voters, who never came to the attention of the police are now committing offenses that carry very stiff custodial sentences should be on the agenda of policy makers. The fact that they offend while showing a sexual interest in children should be very high on the agenda and finally that the children are their own and range in age from zero to twelve in the most part should be very high on the agenda indeed.

Indeed, it seems to be high on the agenda. In the last ten years since the convention was born we have seen the

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (T-ES)
- EU Framework Decision 2004/68/JHA and the more recent Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography
- Many laws in this area in the US including the legislative imperative for Electronic Service Providers to report any instance they find to law enforcement via the National Centre for missing and exploited children
- Legislation in some countries in Asia
- European Commission and G8 support of the ICSE database
- INTERPOL resolutions on blocking and victim centric national centres
- Many other resolutions, statements and advise from organisation like ITU, UN and OECD

All of this has led to strong definitive law in most first world countries and along with significant NGO activity in this area the development of the wherewithal necessary to deal with these issues.

---

1 Cooper (2000)

Strong definitions along with strong penalties show societies aversion to this type of criminality and coupled with prevention and all important awareness a real change is being made and seen.

At the coalface we have also been busy with an operational capacity increasing in a lot of countries. An intuitive started in Norway saw an agreement between the largest ISP and the Police lead to a blocking regime implemented based on a list of websites that contained CAM as defined by national legislation. This quickly spread to other ISPs and subsequently to the rest of Scandinavia. CIRCAMP was born with the assistance of COSPOL and other countries began to see the merit of this action. When a domain on the list is sought by the user they get a STOP page back with an explanation thereby fulfilling the preventative purpose of the initiative as well as stopping the re-victimisation of the children. This coupled with robust investigation resulting in some notable arrests and convictions, the notice and take-down by InHope members, the financial coalitions of US and Europe, the reduction of visible spam plus the changing habits of web users has resulted in web based child exploitation being brought to manageable levels. The INTERPOL “worst of” list of domains has rarely more than 300 on it at any one time. Efforts are continuing amongst the ICANN Governmental Advisory Committee, law enforcement and the European Commission to have registrars, registries and ICANN itself assist in this area by reducing abuse of the domain name system (DNS). All this, combined with increased awareness and zero tolerance among the Electronic Service Providers means that this material is being driven from the web. PhotoDNA, from Microsoft and its deployment by them and Facebook are notable in that they refuse to tolerate CAM on their networks.
None of this changes the fact that the vast majority of child abuse material is exchanged like for like in off-web services of the Internet. Areas such as Peer to Peer (P2P), IRC, Usenet and others continue to be very popular with those that seek to exploit children online.

An increase in privacy movements has created a number of anonymity networks, valuable for activists during the recent Arab spring but abused to a huge degree by people with a sexual interest in children. Unfortunately those involved in these movements are unable to deal with this hijacking of their networks, as to try and deal with the child exploitation issue would cause a loss of confidence in the system as a whole.

Law Enforcement in countries that have operational capacity in this area have increased their understanding of the issues surrounding this offending and are beginning to work smarter. They have realised that Victim Centric Identification measures are a far better use of resources in conjunction with the identification and prosecution of possessors and distributors of material. Apart from the obvious disclosure on behalf of the victim of child sexual abuse, it remains the only way to actually reduce the amount of CAM available online. Analysis of CAM and the location of the child where possible most often results in the identification of the offender as the exclusivity required to sexually abuse is generally not given lightly.

International Operations are also getting better as investigators network more through initiatives such as the INTERPOL specialists group on crimes against children, operational meetings or the Europol Experts meeting or AWF twins. Speedier exchange of intelligence is the result of Law Enforcement leveraging the technologies available to move information quickly. Police to Police exchange remains the fastest and most underutilised method of data exchange available.

Law Enforcement are also increasing the use of technology to identify and locate offenders. Whether by smarter use of existing technologies or by bespoke development the result is prioritisation, where possible, is increasing.

All of the preceding upbeat discussion should not be allowed to hide the challenges that still exist. There continues to be a lack of understanding or acceptance of this global problem among Policy makers, Senior Police and Judiciary that fails to realise that it is a problem that is here to stay. It is my opinion that Moore's law applies to CAM available as much as it applies to storage space or processing power. Progress in dealing with this issue will be slow until it is accepted as a societal issue rather than a law enforcement or criminal justice problem.

Definitions remain a problem. The words “child pornography” put an image produced by a child themselves during the exploration of sexuality in the same category as an image produced during sexual abuse. This makes it difficult to help people understand the gravity of the vast majority of material dealt with by law enforcement on a daily basis. This material is of prepubescent children and pre-speech children are not uncommon. Pornography itself is socially acceptable in some

countries, it implies consent between all parties concerned and at its base level is designed to titillate. Can we accept any of those descriptions for a full length movie of a four year old boy being groomed and eventually raped?

Police continue to struggle with whether online child exploitation is a cybercrime or child crime? The reality of course is that both sides of the house bring different skill set that when combined produce a formidable solution. A form of Hybrid investigation unit drawing on the strengths of both sides.

In this crime type Law Enforcement are being seriously challenged by volume. A terabyte of information can now be stored for less than €100. Forensic capability, investigative capability plus social services, the court system, probation services can all be challenged by this as well. Short cuts are tempting and in some cases inevitable but no amount of justification can make it "OK" to miss an abused child.

Ten years later and the biggest problem facing us is still the movement of information between Law Enforcement and Industry. Certain large multi-national companies do their best with certain countries but the double lock remains. Getting basic subscriber information (BSI) from companies in another country is the starting point in all cybercrime investigation yet officers in some countries wait months to get a response after sending national process by letter or fax requesting the information. Once they get the IP addresses of the suspect they have to make application to local ISP to establish a location for the machine itself or the person responsible for it. Even then an officer must hope that the information is still available or that the ISP will assist with the investigation. This matter is not going to get any better until there is some procedure or recognised instrument that allows the free and easy movement of BSI and ISPs recognise assisting the police as a cost of doing business. The result of this difficulty is that cybercrime is not being investigated as while getting the starting information is technically possible it is practically impossible.

Large gaps still exist in capacity building, Judicial and prosecutor training, forensic capability, law, academic research and many other areas. The Internet is a rapidly changing environment, unfortunately legal systems and investigative techniques are not.

Advocacy for sex with children, access to Child Abuse Material and access to children continue unabated on the Internet. Only by all sectors of society working together can we hope to improve.

Thank You,

Michael Moran, INTERPOL