acjrd

NINETEENTH ANNUAL CONFERENCE

CYBERCRIME

Spencer Hotel, IFSC Dublin.

7th October 2016

Mission Statement

ACJRD informs the development of policy and practice in justice

Vision Statement

Innovation in justice

The Association for Criminal Justice Research and Development (ACJRD) seeks to promote reform, development and effective operation of the criminal justice system.

It does so mainly by providing a forum where experienced personnel can discuss ways of working in an informal setting, by promoting study and research in the field of criminal justice and by promoting the highest standards of practice by professionals associated with criminal justice.

Its activities are designed to lead to increased mutual understanding and provide insights into the problems with which all are confronted. In opening unofficial channels of communication, it improves co-operation between the different parts of the criminal justice system. The ACJRD celebrated 20 years of Innovation in Justice in 2016.

For more information on the ACJRD, please see our website www.acjrd.ie.

ACJRD Council

The ACJRD is governed by the ACJRD Council:

- Chairperson: Maura Butler, Solicitor, Education Department, The Law Society of Ireland
- Vice Chair: Professor Shane Kilcommins, Head of the School of Law, University of Limerick (alternate Dr Susan Leahy)
- Co. Secretary: Pádraig Mawe, Solicitor, Office of the DPP
- Treasurer: Eugene Corcoran, Assistant Commissioner, An Garda Síochána
- Dr Yvonne Daly, School of Law & Government, Dublin City University, (alternate Dr Vicky Conway)
- Patricia Flynn, Psychologist, retired Director, Oberstown Girls Detention School
- Gerry McNally, Assistant Director, Corporate Affairs, The Probation Service
- Jim Mitchell, Head of Legal & Professional Services, Irish Prison Service
- Robert Olson, Chief Inspector, An Garda Síochána Inspectorate
- Catherine Pierse, Head of Legal & Governance, The Policing Authority
- Ben Ryan, Crime Division, Department of Justice and Equality
- Michelle Shannon, Director, Youth Justice, Adoption & Legal Division, Department of Children and Youth Affairs

In addition to our Council and membership (www.acjrd.ie/membership) the ACJRD has a number of member Working Groups. For more information on these groups please see www.acjrd.ie/workinggroups.

"CYBERCRIME" REPORT CONTENTS

WORKSHOP SUMMARIES

Foreword from the Chairperson

Maura Butler

The 2016 Annual ACJRD Conference "Cybercrime" convened on Friday, 7th October, 2016.

This one day conference featured distinguished speakers from Ireland, joined by speakers from England and Northern Ireland.

The conference structure facilitated the presentation of plenary sessions supported by break-out groups, where delegates from the public and private sector shared their views, experiences and expertise.

The Conference Plenary speakers included:

- Robert Hayes, Microsoft Executive Cybersecurity Advisor, Europe, Middle East and Africa
- Det. Sergeant Michael Moran, Assistant Director, Vulnerable Communities, INTERPOL
- Professor Clare McGlynn, Durham Law School, Durham University
- Professor Anne-Marie McAlinden, School of Law, Queen's University Belfast
- Professor Dr. Geoffrey Shannon, Special Rapporteur on Child Protection
- Pauline Walley, SC

The conference programme also featured a number of workshops presentations delivered by: Dr. Orla Lynch, Lecturer in Criminology, University College Cork; Rebecca Dennehy, SPHeRE PhD Scholar, University College Cork; Dr. T.J. McIntyre, Chair, Digital Rights Ireland, and University College Dublin Sutherland School of Law; Margaret Martin, Director, Women's Aid; Dr. James O'Higgins Norman, Director, ABC - National Anti-Bullying Research and Resource Centre, and Senior Lecturer and Researcher, Dublin City University Institute of Education; Det. Superintendent Michael Gubbins, Garda Cyber Crime Bureau; Professor Maura Conway, School of Law and Government, Dublin City University and VOX-Pol; and Andy Harbison, Director - Head of IT Forensics, Grant Thornton Ireland.

The Chatham House Rule was invoked as necessary, to facilitate free discussion.

ACJRD sincerely thanks the expert presenters and all who contributed during discussions to this year's conference and subsequently wrote a paper for this publication.

The ACJRD Council is confident that the papers in this publication will benefit all practitioners, policy makers and all who now take the time to peruse them.

Launch of Conference

Maura Butler, Chairperson, ACJRD

Due to matters beyond our control, the person who we wished to launch today's conference is unavailable. Therefore, I will endeavour to set the context for the 19th Annual ACJRD Conference. Having formally welcomed our distinguished panel of speakers I wish to acknowledge how grateful we are for their participation in what promises to be a very informative and stimulating conference.

It behoves those of us who inhabit the Criminal Justice landscape, to become skilled in Cybercrime and its criminological characteristics. But we must remember that we are largely dealing with crimes that we are already familiar with - the means of *committing* the crime has changed.

The Council of the ACJRD agreed that in circumstances where Cybercrime has become a 'hot topic' across many disciplines, criminologists, lawyers, policy makers, practitioners and citizens needed to 'take pause' to better understand and learn about this new 'criminal wrongs' landscape.

It is indeed prescient that the 2016 annual conference aims to meet that challenge in anticipation of the publication of the Criminal Law (Sexual Offences) Bill and the recently published Law Reform Commission Report on Harmful Communications and Digital Safety http://www.lawreform.ie/news/report-on-harmful-communications-and-digital-safety.683.html. The Report on the Internet Content Governance Advisory Group (Department of Communications, Climate Action and Environment) should be consulted when researching this aspect of criminal wrongdoing http://arrow.dit.ie/cgi/viewcontent.cgi?article=1052&context=cserrep.

Cybercrime is a creature of a new world, where some are digital natives, others are digital immigrants and then a sizeable portion are Luddites! But we should remember that IT is just a new pencil and not be fazed by it!

Cybercrime is as varied as crime is itself. One definition States: "*Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, hate crimes)*" www.techopedia.com.

Interpol outlines that "*Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and*

pose very real threats to victims worldwide. Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:

- ***Advanced cybercrime*** *(or high-tech crime) - sophisticated attacks against computer hardware and software;*
- ***Cyber-enabled crime*** *- many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism."*

Interpol give advice on online safety and go on to discuss the changing nature of crime stating:
"New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new - such as theft, fraud, illegal gambling, sale of fake medicines - but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging." https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

The Law Reform Commission Report on Harmful Communications and Digital Safety is a 'must read' for all. We are all very pleased that the primary researcher of this expansive piece of work, Dr. Fiona O'Regan, has chosen to be with us today and we compliment her and all her Law Reform Commission colleagues for their work. I know that many of today's speakers have endeavoured since its publication a mere twelve days ago, to incorporate aspects of the report in this conference's presentations - for which endeavour we are most grateful!

LRC Report 116-2016 recommends the drafting of a Harmful Communications and Digital Safety Bill. It refers to an innovative two-day workshop with children facilitated by the Department of Children and Youth Affairs, the outcome of which is in the appendix of the report. Its proposals include the establishment of an Office of the Digital Safety Commissioner - overseeing/monitoring effective 'take down' systems and the publication of a statutory code of practice - referencing increasing international regulation in this area. Ireland's sphere of influence in that regard and the regulation emanating from various European institutions is referenced. The report also focuses on the necessity to legislate for the extra-territorial nature of wrongdoing in the digital world. Guiding principles championed in the LRC report include education, empowerment, balancing rights of freedom of expression and rights to privacy and the need to regulate actions and behaviour, rather than the means by which the wrong was perpetrated. Stakeholders should also take cognisance of The Report on the Internet Content Governance Advisory Group (Department of Communications, Climate Action and Environment) 2014.

A three level hierarchy response is recommended by researchers and policy makers who will consider cybercrime in the following disciplines: (a) Education (b) Civil Law and Regulatory Oversight and (c) Criminal Law.

The 2016 Annual ACJRD Conference will hear from fourteen experts across the spectrum where the commission of offences is facilitated by an expansive array of IT tools and communication possibilities. Topics discussed will include detection, responses - including enforcement of protocols and legislation and the gendered nature of some of those targeted, where women are exploited. The targeting by wrongdoers of the most vulnerable in our society, our children, will occupy our discussions to a considerable degree. Protection of employees from cyber wrongdoers will be addressed by an expert in that field in law, demonstrating the necessity to look outside our standard conceptions of what crime is.

In the context of the Victims' Rights Directive 2012/29/EU and its transposition into Irish legislation in this area, there will be a distinct victims' focus during this year's conference presentations and discussions, in particular, the effect of cyberbullying on children, how extremism and terrorism use technology to create victims and how the dark net inhabits our world, creating victims in its wake.

Other learning will explore how one should take preventative measures within the context of the positive civil liberties aspects of information technology, the challenges presented to our policing authorities and how to minimise risks - both commercially and in our personal space - as parents, employees, users and especially as young people.

The typically multi-disciplined nature of ACJRD's Annual Conferences, as demonstrated in this 2016 conference programme, ensures that a confluence of expertise from diverse stakeholders will be pooled and become transferable to the practice and policy-making of conference delegates. The conference will also facilitate fruitful networking between conference speakers and delegates, towards meeting the challenges presented when crime is committed through an ever-increasing array of technological tools.

The outcomes from this conference will be very valuable for all of us.

Preventing, Detecting and Responding to Cyberattacks - A Question of Trust

Robert Hayes, Microsoft Executive Cybersecurity Advisor, Europe, Middle East and Africa

A transcript from Robert's presentation is preceded by his summary, below.

"A recent Cybersecurity Ventures report predicts global annual cybercrime costs will grow to $6 trillion by 2021, this includes direct costs such as theft and damage, and indirect costs such as recovery, reparation, and reputational damage.

Headlines such as this, combined with the exponential increase in scale, scope, and complexity of cyberattacks have made cybersecurity a primary issue for CEOs and Boards of both private and public sector organisations.

US CERT estimated in May 2015 that over 85% of targeted attacks can be prevented, yet in my experience very few organisations have an effective plan to protect against, detect, and respond to cyberattack. Why is this?

Advice is not hard to find, and there are a multitude of information sources and standards; the in-house CIO will have a view, and of course there are a myriad of vendors, each with a solution that promises to be the answer to all security problems.

Trust is at the heart of a successful security strategy, yet knowing who and what can be trusted, and whether that trust should be absolute or conditional, is extremely difficult.

In my conversations with CEOs I often ask them their degree of trust in five key security related areas:

- *The people who work in their organisation*
- *The organisations in their supply chain*
- *The integrity, resilience and security of their existing infrastructure*
- *The integrity, resilience and security of cloud based infrastructures*
- *The advice they receive, both internal and external*

Unsurprisingly, the answer to each question is always varying degree of conditional, but not absolute trust.

Where the conversation becomes interesting, is where the CEO and I then jointly explore whether the infrastructure, processes, and policies of their organisation reflect their intent to avoid absolute trust in these five key areas. Invariably, the answer is no.

Recurring examples of this inconsistency, each carrying significant organisational risk, are:

- *IT administrators having unfettered and unaudited access to all corporate systems without effective security*

mitigations such as multi-factor authentication, and privileged access workstations in place

- *HR departments not instructing the IT department to cancel user access privileges for days, often weeks, after an employee is sacked*
- *Supply chain contracts drawn up with no security provisions, standards, or audit clauses*
- *No due diligence or impartial advice at Board level on the assurances and assertions made by both in-house IT teams and vendors on integrity, resilience and security*

A common closing theme of these conversations is the need for CEOs and Boards to have impartial advice and support to help them robustly challenge and undertake effective due diligence in this critical area, and the difficulty achieving this.

In the US proposed SEC regulation will mean that companies, in particular publicly listed firms, must have a cyber-expert on their Board, yet there are currently very few executive or non-executive directors with this skill set, and who are comfortable operating at Board level.

An alternative, but expensive position is to buy in the skill set from a third party, and there are many consultancies who will be delighted to have this conversation. However, some consultancies also have a vested interest in system integration, and their advice may not be as impartial as it seems.

Finally, there exists the challenging option of changing the relationship with key suppliers away from the classic customer – vendor, to one closer to trusted strategic partner, supported by a robust due-diligence process. Many organisations are seeking to move closer to this type of relationship, whilst still maintaining sufficient distance to satisfy probity and procurement rules.

Whilst each of these options has challenges, the reality remains that without a trusted cybersecurity advisor, CEOs and Boards will continue to make decisions without effective challenge or scrutiny that leave their organisation vulnerable to cyberattack."

Robert Hayes' presentation transcript

I'm really grateful for the invitation to be here and I looked before I started at the types of organisations that are represented in the group. One thing struck me is that just about every organisation represented here holds data on people that is pretty sensitive. So this is actually a big issue for you because, for the reputation of all of your organisations, for your ability to function, you need to learn something that we've learnt about trust. I'm going to talk far more about trust than anything that relates to technology or security. I'm going to explain what trust means for us and perhaps leave you with some questions about trust. So those of you who thought you were getting a technology based presentation, I apologise, and I also apologise for not trying to sell you Microsoft stuff, that's not part of what I'm here for either.

So let me just give a little bit of context first, like every other organisation we have a mission statement in Microsoft. ACJRD has theirs on the front of the notepad here today. What we've learned over the last few years is that to achieve that, we have to have trust in a range of people. We have to have the trust of the people who are our customers, we have to have the trust of the people who are our regulators, and who

are our stakeholders. That trust, some of it is made of four components and I would contend that those four components apply equally to all of your organisations too. You've got to be able to say to the people who are important to your organisation, that you understand what privacy means, and that you keep the data that you have had shared with you in a way that justifies the privacy expectations of the people who have given it to you, or the law. To do that there's a piece about transparency, so, if you have my data, do I understand what you're going to do with it?

That became a big issue for us after the Edward Snowdon disclosures, when basically, things that we had shared with governments, some of which was under gagging orders so we couldn't talk about them, became public. There was nothing that we were particularly ashamed of in terms of what we had done, it was all legal, but I can tell you that in places like Germany and Brazil particularly, that caused us a huge problem in terms of how we manage data, we've had to change the way we operate our infrastructure because of that.

So transparency is hugely important. With that part comes the compliance piece. We're a global company, we do business pretty well everywhere, but we have to comply with a network of firstly national and then sector regulations, legislation and policy about the data that we hold. We hold health data so we have to worry about HIPAA which is the US health regulations, we hold financial data, we hold data of all types, and we have an enormous spreadsheet that basically tabulates all our services and everything we do against the regulations both national, regional and sector based.

The last piece is security, and I'm thinking you're probably expecting me to talk a little bit about security. Let me start by first asking you a question, a show of hands please, how many of your organisations have actually got an effective security strategy? (Several hands shown). So why is there a fundamental problem here? The fundamental problem is actually that this has not been a good time, I'm not here to scare you about cyber-security but I do just want to put a bit of context in. I'm only going to highlight one figure, and it's the figure that's in red on this chart (see Fig 1) so let me explain what that means.

So, if on day one an attacker gets into your infrastructure of your network, and usually, almost always that is through a

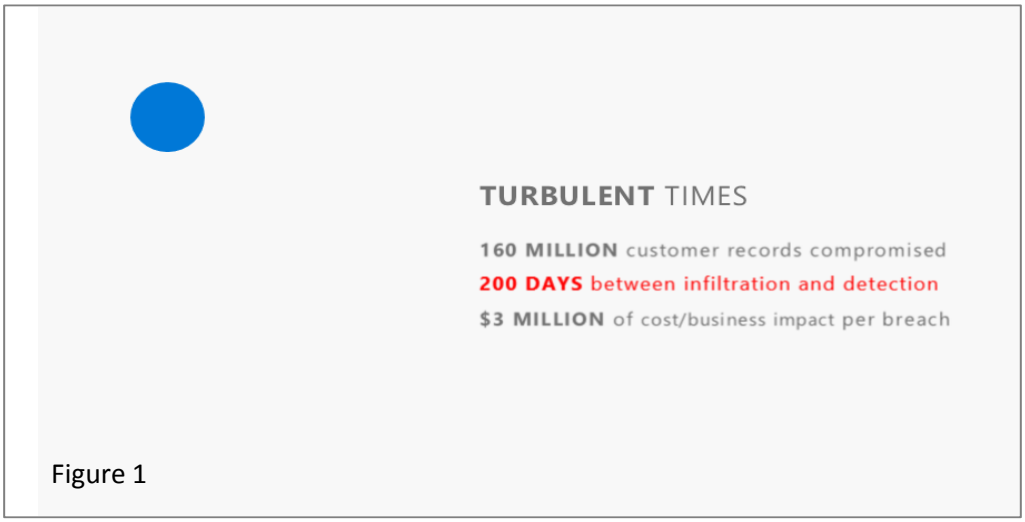


Figure 1

phishing email, someone clicking on a link that they shouldn't, or picking up a USB and putting it into a computer that they shouldn't, that's pretty well how all attacks start. So that's day one. The average that we see, and we do a lot of incident response with government organisations, big enterprises, banks, down to small organisations, is that it's day 200 when that organisation finds that attacker. So that's 200 days an attacker has been in a network before they're discovered, on average. It gets worse, because the time it takes the attacker to compromise the credentials of an organisation to the point where they effectively own it, is about four days. We have plenty of evidence for that. On average, when we go to see an organisation that's found an attacker, we find that that attacker has pretty well unrestricted access across the whole of the organisation for well over 190 days without the organisation realising it. So, that is actually why this is a big deal.

So why is there a fundamental problem? The fundamental problem is that every organisation, big and small, started off with an IT environment that was designed to meet the needs of that organisation. But the world changes, whether you're a public sector organisation, whether you're in the police, part of government, or a commercial organisation, everyone wants to do things suddenly differently. If you're a government, you want to engage with your citizens better, you want to be able to get your citizens to engage through smart phones and apps and on the internet, and you probably have connectivity into other organisations, and possibly a vehicle fleet, you may get telemetry back, you want people to work from home, and actually you have just changed fundamentally the environment of your organisation. The problem with that is, that every time you do that, you create a new attack vector.

My next question to you: How many of you know how many applications and how many cloud applications your employees use when they're on your network at work? Ok that's what I was expecting - no hands. We have a tool, we call it, unsurprisingly, the Cloud App Discovery Tool, which we will help organisations run, which basically says this is what's happening on your network. I always ask people before we do it, what do you think the answer is going to be? And if they say it's probably 30, it's 300. If you then think about it, if your organisation has employees who are running insecure cloud applications that you don't know about, they're one of those red blobs on Figure 2.

Figure 2

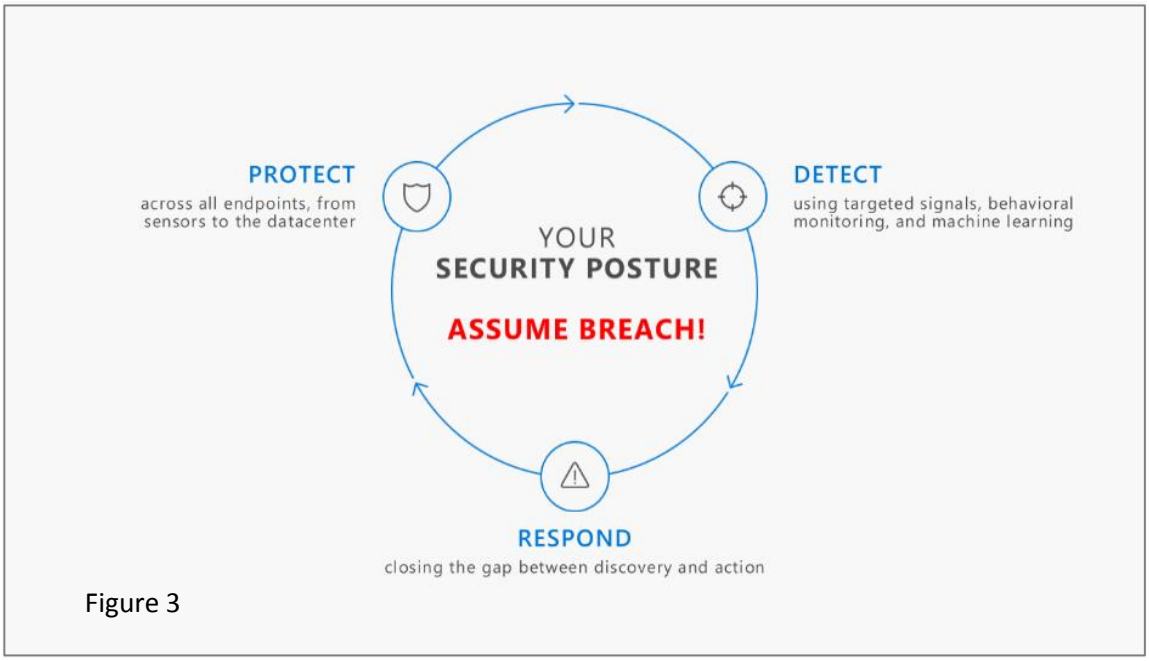


Figure 3

So, this is actually really difficult, now I'm going to be really brief on this, although I can talk for an hour just on this topic. There are effectively three parts to a security strategy, and a culture. The culture is almost the most important, the culture is the bit in red on here, Assume Breach (see Figure 3), and it's the way we operate.

The principle of Assume Breach is that you don't wait to find you've been attacked before you start to worry about it. You actually assume the attackers are in there, you just haven't found them yet. If you adopt that approach and it's not a technology approach, it changes the whole way you think about security.

So my next question, which I hope will give some evidence to this is that: In your organisations, if you sack someone today, because they've been dishonest or whatever, how long does it take for your HR department to tell the IT department to cancel that person's credentials on your IT system? The answer is in most organisations it's a policy thing, and it probably isn't a high priority within the HR department to do that. The problem is that if you don't cancel people's credentials, they can still remote into your organisation for as long as they want to, and probably with access. The best example is an Australian water company, someone was sacked for gross misconduct, three weeks later they remoted into the organisation, because they had remote access, and cross changed the fresh water and the sewage pipes within a pumping station. Perfectly preventable. I use that because it's an example that security isn't always about technology, you can have the best tech in the world but if your users aren't educated, if you don't have support with it across the organisation, you're not secure.

The Protect, Detect, Respond piece, you've seen that if you look at any security advice from any government, it's that you have to have Protect, Detect, Respond.

So what does that mean? The Protect bit most people sort of understand, that is you need to have something that protects the edges of your infrastructure. So if you have a laptop, that you actually have hard disk

encryption on that laptop. To be honest if you're using our stuff, our stuff has hard disk encryption built into it, yet I'm amazed how many organisations, organisations like yours, that have high risk data, don't turn that on. So what it means is, if I accidently leave my laptop in the pub after too many pints of Guinness tonight, I can rest assured, I'll get a bollocking from Microsoft for losing the laptop, but they won't get any data from that because it's got bit locker encryption on it. If you use our stuff, you will have that too - if you turn it on. It's really good, trust me.

The detection is the bit that most organisations fall down on, the detection piece is based on the fact that actually most attacks get through your preventative measures. So if I compromise one of your employees by sending them the email and they click on the link, it doesn't matter how strong your firewall is because I've just gone through it. Most attacks use that type of credential attack. So the problem is, if you don't have something that tells you that somethings going on in your network that isn't usual, that's not what is normally seen, that's why attackers are in networks for 200 days on average before they're discovered.

We can do it, and there are plenty of other people who will sell you detection technologies to sit on networks. I'd argue that for small places we're probably as good as anyone because we do a lot of the analytics for you, but you just need to have something on your networks to tell you what's going on, whether it's us or it's somebody else.

The Respond piece is important too, you are going to be attacked, you just will be. At the moment ransomware is a huge thing, and you don't have to be targeted for ransomware, you can just be unlucky. If you get ransomware on your system, it will encrypt all the data on your system and you have to pay a criminal gang in bitcoins to get access to that data, unless you've got a good backup strategy. So, who's got a good backup strategy in their organisations? How many of you could put your hand on your heart and say you know what it is and it's good enough? I think there's a 'take away' here don't you.

The backup strategy can be really simple. If you're a small organisation you'll spend £50 in Dixons and buy a removable hard disc, and just back your crown jewel data up once a week and then unplug it when you've done it. If you do that and you then get ransomware and you pay the bitcoins and they still don't give you the recovery key, because they quite often don't, then life can still go on.

I've sat on a panel at the International Association of Chiefs of Police Conference, with a Police Chief from America who had ransomware on his system, who lost access to all his police data, who paid a criminal gang in Eastern Europe in bitcoins. He was not happy about it, but to his credit, he was prepared to talk about the lessons learned from it.

So if it can happen to a law enforcement agency, it can happen to you. Be ready, and when you are ready, think about who you need to talk to, so think about what I said about the data you hold, if you were compromised you're going to need to tell the people whose data that you hold, you're going to need to tell the regulator really quickly, and actually having something as a bit of a plan for that day, will make it go so much smoother if that day comes. So Protect, Detect, Respond and Assume Breach, in the security sense is really what I want to leave you with.

I want to go on to talk a little bit about intelligence, because this is important to everyone in the room. I want to talk a little about what that means for us and then I want to show you something that you can take away and use yourselves.

I want to talk about intelligence, now remember everything I said about the way that your networks now operate, that you have connectivity with people at home, it means that you have a lot of intelligence. For us, the numbers that we harvest from our network are pretty big, we have 300 billion user authentications every month to our network, we have four billion emails every day sent through, one-and-a-half billion photographs uploaded onto our network every month. They are big numbers. We take that data in a way that we can harvest that intelligence, and I'm not going to go into great detail, but we have our own cyber defence operation centre.

We work very closely with law enforcement agencies such as Interpol and Europol, on botnet take downs and things like that. The idea of this is that we take the data from all of our areas, things we harvest from our network, from our partners, such as law enforcement, so government certs, our anti-virus partners etc. We have red and blue teams that operate within our network, testing our own defences. The idea of this is to defend our infrastructure and our users almost dynamically.

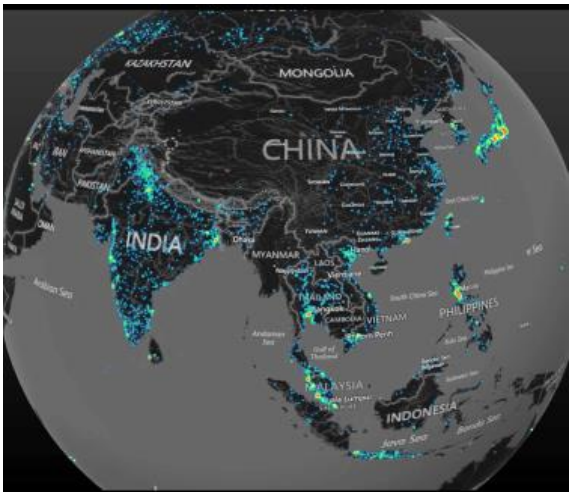
An example of this, before I move on to the piece I really want to show you, we were attacked by a nation state last year, we get attacked by everybody, we're the second most attacked, or the first depending on which figure you read, organisation in the world, either us or the White House. We were able to prevent that attack against our infrastructure, look at what was attacking us, and then we were able to change not only the processes that we had but the defences of all our customers who we hold data of within twelve hours. Effectively we were able to defend over a billion customers from an attack from a nation state within twelve hours, because of the intelligence that we collect, analyse and use. It's big data, we're talking trillions of events here, the reason I highlight this is not to say how wonderful we are, it's to say you need to think about how you do this, because you've got to have someone who does this for you. It may be that you go to a vendor, or it may be that you're really good and you have a great team that can do it in house. You can't make decisions about security without this type of knowledge from somewhere and someone.

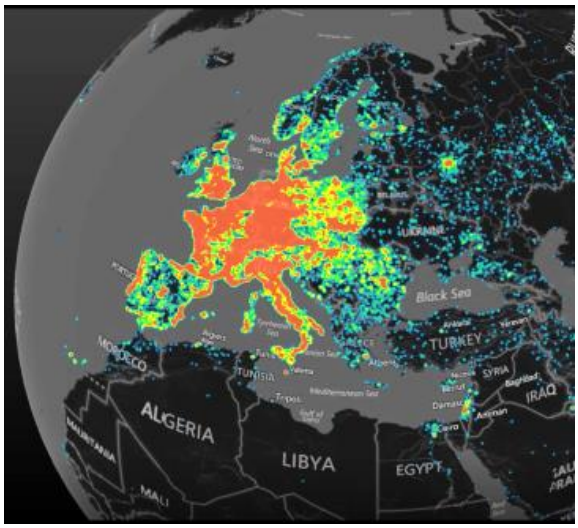
When we go to Interpol and to Europol we take down botnets. Botnets work as follows: I'm a criminal, I decide I'm going to compromise 12 million machines by sending out spam and malware, get people to click on the link, it downloads a bit of software into people's machines and I can then control those machines remotely.

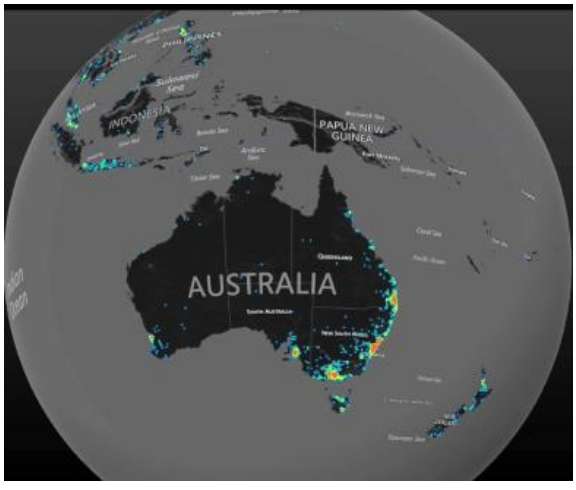
The botnet I'm going to talk about is called Citadel. Last year, there were 12 million machines compromised, and it was banking password stealing malware, so it waited until those users went onto a banking website, and when it realised you were a banking website what it did was it capture all the screen movements, it sometimes turned on the webcam, effectively captured key logging, to the point it would send that data off to a gang in Eastern Europe, they would eventually compromise that account, money would be withdrawn through a network of mules, through ATM machines all over the world.

It made a lot of money, about half a billion pounds profit to that gang, none of whom have been prosecuted. It's why Cybercrime is always going to be a big deal, because it's really difficult.

So when we take down a botnet, we effectively repurpose the command and control networks so instead of talking to the bad folks they talk to us. The following figures illustrate the spread of the Botnet.







It's a heat map so you'll see red is obviously where there is a greater proportion of attacks and it sort of follows the population.

The exception is, there's rather a different fine line between Western Europe and Eastern Europe.

That peaked our attention, we were quite interested because it wasn't obvious, what you're looking at here is about 1.4 million lines of data in an excel spreadsheet, but what we've done is we've put it onto a map. What we actually found, just out of interest, is that the reason there was a demarcation between Eastern and Western Europe was because the malware was specifically engineered not to compromise machines that were running Cyrillic languages, anything effectively Russian or Eastern European. The reason is, the people we know who developed

that malware didn't want the local authorities on their back because they were targeting local people, it sort of validated what we knew.

The reason I show that is, we often go to conferences where groups of people like this think, I wish we had investigative tools, and I wish we had something that would do that, you have! That's Excel, if you use Microsoft Excel, there's a plug in on Microsoft Excel that's called Power BI that will map one and a half million lines of data on big maps like that, and it's a tool you've got already. It's just that people never seem to be aware that they've got it, so I often show it in this type of context to show if there's one thing you've got, you've got a freebie from Microsoft, and that's something that you don't get very often.

So, I want to talk very quickly about trust before I finish and hand over. You will remember I began by speaking about trust, transparency, compliance, privacy and security. I want to refocus that a little bit and I want to ask you to start thinking, and I always say at this point, look at the person sitting on your left, ok, my question is, how much do you trust that person, and what is it that forms your thinking about that? Because when I go and talk to people at senior levels in organisations and government, I always ask them the question, how much for example do you trust your people who work for you; do you trust them absolutely with everything? No one ever says 'yes' to that. But when I look at the organisations, how the environment and the infrastructure is put together, often it does trust them absolutely, particularly if they have IT Administrator in their job title. In most organisations IT Administrators have the keys to the kingdom. All the bad people target IT Administrators, they increasingly now target them at home, through social media, through looking on LinkedIn. If you can compromise someone's machine at home, and they use that machine for doing work stuff, you've just gained the keys to the kingdom. Understanding who you trust . . . do you trust your supply chain, do you even know who your supply chain are? For us when we buy a laptop from Dell like my laptop here, it's got Microsoft Windows on it, we make Microsoft Windows - but the first thing we do is we take it off, we take everything off that machine and we put a gold standard build on it because we don't sort-of trust our supply chain . . . in a nice way. There have been good examples; we've had copies of Windows sold in China that have had malware put on them somewhere in the supply chain. Right now if you buy something from us you don't get a disk, you download it, because we can control a download far better than we can control the production of CDs and DVDs because there's too many bits in the supply chain. And also hardware, we worry a lot about whether some of the hardware we import has come with some added value that nobody told us about, and there are some good examples of that as well.

From Trust to Strategy (Figure 4), the reason I show this particularly is, this is not easy, and anyone who tells you this is easy, hasn't been well briefed. So within your organisations the key one here is the advisor. Who is advising the people at the top of your organisation how you make sense of this world? Because there are some huge opportunities that you can get if you actually get into the ideas of big data analysis, thinking about being more secure. If you're more secure you can innovate more, if you're more secure and you're a private organisation you can win markets. If you're more secure and you're a public organisation, particularly an organisation holding people's data, you'll sleep better at

Figure 4

night, because you're not going to worry about that phone call at five o'clock in the morning when someone says we got a problem, they've stolen the data.

So having an advisor is key, what I want to say to each of you, is within your organisations, ask yourself the question, who advises us? There is actually a number of places you can go for that advice, and probably your own in-house IT department are not that person, because they have a vested interest, I have a vested interest, and I'm a really nice guy, you can *really* trust me, but Microsoft pay my wages so you should be conditional about that level of trust with me, because I might have a vested interest in this as well.

The other part of it is around due diligence. Going finally from that idea of trust strategy, if you're serious about this as an organisation you'll recognise that this is a business decision, it's not a techie thing, it's not for the IT department to do. If you don't deal with this at board level you're probably missing the way there's strategy around this. You need to use due diligence, on your vendors, on your people, on your infrastructure. You need to have trusted advisors, and the final two of course, you need to assume breach and you need to protect, detect and respond to your infrastructure.

Now I always like to finish on a positive, because there are too many security presentations I go to where you can see people's heads go down, and by the end everyone's going, whatever I do they're just going to get me, so I might as well not do anything, and that's not the answer.

Figure 5

This is a figure (See Figure 5) from last year, but it's still valid. This is from US CERT which is their Computer Emergency

Response Team, and they say that as many as 85% of targeted attacks (this is when people are out to get you and your organisation) are preventable, if you do the basics, basic computer hygiene. I would support that and I would say it's probably even higher, because most organisations in my experience just aren't doing the basics.

International Prevention and Enforcement Online

Det. Sergeant Michael Moran, Assistant Director Vulnerable Communities, INTERPOL

INTERPOL is the International Criminal Police organisation based in Lyon, France (IPSG). It is made up of 190 member countries each of which has a National Central Bureau. These bureaus are connected to each other, INTERPOL HQ and the Regional Bureaus (RB) via a secure communications platform. INTERPOL has regional bureaus in Abidjan, Yaoundé, Harare and Nairobi in Africa, Buenos Aires and San Salvador in Latin America and in Bangkok in South East Asia. We also have a Global Complex for Innovation (IGCI) in Singapore.

The vision of INTERPOL is "*Connecting police for a safer world*" while the mission is "*Preventing and fighting crime through enhanced international police co-operation"*. This mission is fulfilled through the application of four core functions. These are:

- Secure Communications - I-24/7 secure platform connecting all members
- Databases - INTERPOL house a number of key international databases such as nominal, International Child Sexual Exploitation database and a suite of border tools.
- Operational Support - INTERPOL supports its member countries through subject matter expertise, project management and investigative support.
- Capacity Building - Training, guidance and best practice are made available through mentorship, operations and e-learning.

In the area of Operational Support INTERPOL works in the online environment in a number of areas from classic cybercrime investigation, open source monitoring and child exploitation. The reality is that no crime area is immune from cyber facilitated crime and so all sections of INTERPOL have some cyber functionality to a greater or lesser extent.

The main section at INTERPOL with responsibility for cybercrime is the Cybercrime centre based at the IGCI in Singapore. This centre is broken down into two main sections dedicated to supporting member countries. These are Digital Crime Investigative support (DIS) and the Cyber Fusion Centre (CFC). The DIS section is dedicated to coordinating and facilitating transnational cybercrime investigations and operations. It focuses on criminality through the use of Botnets, Malware and enablers such as bullet proof hosting or organised crime gangs. Support can be either remote or onsite and can include intelligence development or forensic computing support. The CFC is a multi-stakeholder environment where law enforcement specialists and industry experts come together to develop actionable intelligence using many sources. It can also act as an operational

control centre for multi-jurisdictional operations.

Other sections that have a "cyber" role include Vulnerable Communities. In this section they work tirelessly in the child exploitation space online and indeed are a good example of all the core functions being utilised to assist member countries. They use the secure platform to run the International Child Sexual Exploitation Database (ICSE) which has 50 countries plus Europol connected and is instrumental in the safe guarding of approximately six children per day around the world. They work in a proactive way to source intelligence online, on offenders who distribute and possess Child Abuse Material (CAM)[1] but more importantly they gather the material, analyse it with a view to identifying the location of the abuse and log it in the database.

The cyber strategy currently deployed at INTERPOL is made up of five elements (see Figure 1) with a goal of attributing real world identities to online offenders. Once enough evidence, intelligence and information are in place, an intelligence pack is presented to the member country or countries and an investigation can begin. Of course, where requested, the team can coordinate an operation and bring together actors from different disciplines to tackle a particular investigation. INTERPOL also works very closely with other Law Enforcement agencies, especially those with highly developed skills in this area and especially in that regard with Europol. At Europol the team at EC3 work closely with EU member countries, third countries and INTERPOL to develop their operational actions from the SOCTA and strategic goals of their member countries. Strong review and debriefing ensures that lessons learned strengthen outcomes and improve future actions.

Cyber Crime is a complex issue not least because the definition is not universal. The only international instrument that comes close to an agreed definition and legislative framework is the Council of

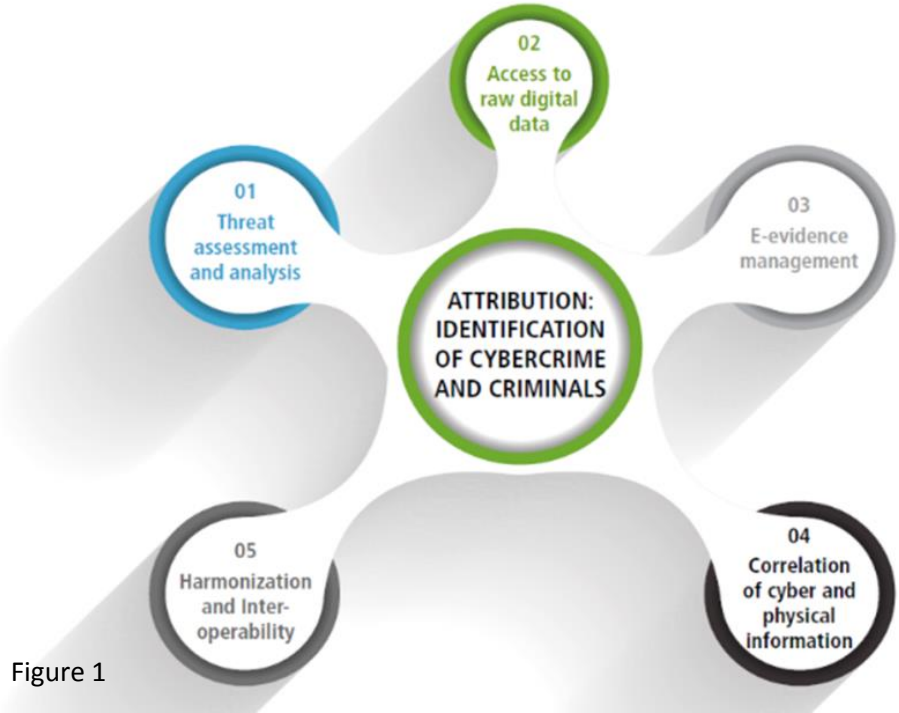


Figure 1

Europe - Convention on Cybercrime 2001, also known as the Budapest Convention, and ratification is reasonable given the limitations especially along geo-political lines. Significant efforts are ongoing at EU level on a specific directive while the UN is also active.

The challenges posed by cybercrime to law enforcement are also reflected in how all institutions of state and society in general are challenged. The global nature of the internet, coupled with the mobile nature of ICT in a globalised world, along with the slow and arduous pace of legislative change, creates a perfect storm for criminality. Fast paced technological innovation such as processing power and storage capability and cloud infrastructure combine to create an environment which is ideal for business but also ideal for the criminal. The next big leaps of virtual and augmented reality will also be the next big leaps in crime, allowing for vast ill-gotten gains to be spirited away by organised crime groups for use in other areas such as drugs, money laundering, corruption and terrorism. All of this will take place in the presence of the perennial distrust between Law Enforcement and industry, engendered by an immature data protection legislative framework and the need for balance in privacy. The result is the use of hopelessly outdated systems for data sharing that is more often than not, too little; too late.

One key area where Law Enforcement and their partners must get better is in prevention. A stitch in time saves nine is a wonderful saying that is one of many espousing the notion. Crime prevention is nothing new in real life (IRL) and the same principles must now be applied in the online world. While everyone must play their part, and indeed industry is stepping up to the plate, law enforcement also needs to contribute. There are already good examples of prevention efforts available, with warning fact sheets about sexual extortion (INTERPOL.int) or with the ransomware (ransomeware.org) portal put in place by Europol, Dutch Police, Kaspersky and Intel Security. There are

Figure 2.

also some tools available such as the BASELINE[2] system from INTERPOL or the ransomware decryption tools being grouped together on the aforementioned ransomware website. This is not however enough. Collaboration is needed in a sustained global way to ensure that the principles of situational crime prevention, strong risk management in the development and business cycles, and designed awareness campaigns, are coupled with robust enforcement of law to reduce offending to somewhat manageable levels. A step in the right direction was recently taken by the publication of "Youth Pathways into Cybercrime".[3] This type of research is essential and should inform strategies to reduce offending in the future.

There is also a need for strong embedding of cybercrime prevention into the training regimes of law enforcement globally, along with coders, managers and policy makers. The whole area needs to be "demystified" to the point where it is normalised and easily spotted and dealt with. We must always remember that people are often the weakest link in a cybersecurity chain and so strong messaging is also needed within our national education curricula from the earliest possible age.

Finally I would like to raise the spectre of regulation. There is no doubt that cybercrime is a rising phenomenon and is already having an effect on the development of nations. Identifying gaps and regulating to close them will eventually seem like the only option and there will come a point where we will have to discuss this in a mature manner. Clumsy and unrealistic efforts are already being tried with disturbing regularity and it's only by working together in a knowledgeable way that we can ensure regulation will be scaled to suit everyone.

1 Child Abuse Material is the agreed terminology to describe files that depict children being abused. It was formally known as "Child Pornography". Further information is available at luxembourgguidelines.org

2 BASELINE is a system that allows file hashes to be compared to a database of known CAM files. It is available from INTERPOL or from national police entities in INTERPOL member countries.

3 Youth pathways into cybercrime. Aiken, Davidson, Amman 2016 https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Pathways-White-Paper.pdf

More than a Breach of Privacy: Image-based Sexual Abuse and the Irish Law Reform Commission on Harmful Communications

Professor Clare McGlynn, Durham Law School, Durham University

Introduction

In September 2016, the Irish Law Commission published its long-awaited report on 'Harmful Communications and Digital Safety'.[1] This compelling document puts forward a comprehensive package of law reforms to tackle the growing problems of online harassment and abuse perpetrated using modern technologies and social media. In addition, and a vital aspect of the Report, is the recommendation to establish a Digital Safety Commission which will promote education and digital safety, and be responsible for take-down processes. Implementation of this aspect of the Report will be essential so that attempts can be made to remove harmful material from the internet, and not just rely on punishing those who have perpetrated abuses in order to challenge behaviour and culture. If the Report is followed through into legislation, Ireland will be introducing one of the more comprehensive and effective approaches to tackling online abuse. The Report has learnt from the inadequacies of the English approach, recognised the benefits of the Scottish legislation, and has taken the best of the international mechanisms focusing on civil sanctions and actions.[2]

Amongst its many provisions, the Report recommends new laws to tackle the phenomenon colloquially known as 'revenge porn' which is rightly identified as a significant harm deserving of legislative intervention. I will examine these proposals. In particular, I want to step back from the detailed technical provisions, to focus on the more conceptual issue of the nature of these online harms, why they are being perpetrated and what are the implications of this. In essence, I want to name and conceptualise harmful communications as 'image-based sexual abuse'.[3] My aim is to emphasise: that these are gendered and sexual harms that are forms of sexual offending; that this is how victim-survivors understand the harm perpetrated against them; and that the victim-survivors are mainly women and girls. I also hope to explain why this conceptualisation matters. I suggest that how we understand these harms will shape legislative responses, educational approaches and our broader awareness of the phenomenon.

Beyond 'revenge porn'

But before we get to the substance of the proposals, let us first outline the activities we are examining. The classic case of 'revenge porn' is where a malicious ex-partner shares private, sexual images without consent - often distributed

through social media.[4] These private, sexual images often end up on commercial pornography websites, on websites specifically dedicated to 'revenge porn' of which there are thousands and all across social media. The consequences, as you may be aware, can be devastating. When we discuss 'revenge porn', we are talking about sharing private, sexual images. It is because the images are sexual that they are shared widely across the internet and it is because they are sexual images that the harm is so great. When distributed across 'revenge porn' and other websites, the images generally attract comment most of which is extremely abusive and the abuse is sexualised. In one recent Irish example, a video was uploaded to a website and it had 10,000 views before the victim-survivor even found out about it.[5] Often personal info is posted about the individual - her name, social media details and sometimes a home address. The effects are felt as shame, humiliation, abuse and harassment - as well as a fear for personal and physical safety. And the harm is on-going: taking down these images is extremely difficult, meaning that victim-survivor's online and personal lives are often scarred for years. This is the classic 'revenge porn' scenario, but this is just one form - one motivation - of this type of abuse. There is more to this than just 'revenge'.

Here are just two more examples. Jennifer Lawrence, the Hunger Games actor, was one of many celebrities whose iCloud accounts were hacked and naked images distributed without consent a few years ago.[6] This was not done for 'revenge' - but for notoriety and financial gain. As well as the distribution of intimate images without consent, there are serious harms perpetrated by the non-consensual *creation* of private sexual images. For example, images are sometimes surreptitiously taken up a woman's skirt - 'upskirting' - and then distributed without consent.[7] Again, this is undertaken for a variety of reasons, sometimes for sexual gratification, but also for financial gain, or notoriety.

These are just a few examples of what my colleague Erika Rackley and I have termed and conceptualised as 'image-based sexual abuse'. We have developed this term to cover all forms of non-consensual creation and/or distribution of private sexual images. Our term includes the classic 'revenge porn' cases and this is often where the legislative focus begins, and ends. But image-based sexual abuse encompasses all forms of non-consensual distribution, focusing on the harm to the victim-survivors, not the motives of the perpetrators. It therefore also includes the non-consensual *creation* of images, for example 'upskirting', but also 'sexual extortion' where victim-survivors are coerced into creating/sending private sexual images, and then blackmailed.[8] It includes images of sexual assaults, often taken and distributed as a 'trophy' and/or to coerce women to not report the assault to the police. Voyeurism, the 'peeping tom' who surreptitiously spies on someone in private, for example in a toilet or changing room, is also covered. All of these forms of abuse, and more, are labelled harmful communications. But I argue that they are better conceptualised as forms of image-based sexual abuse. Criminal laws are proposed to tackle these crimes. Why, therefore, does the label matter?

Terminology matters: image-based sexual abuse

The terminology used, the label applied to describe these harms, matters because it influences our actions. My particular concern is that the Irish Law Commission in

its report suggested that these harms are not sexual offences. The report states that the primary purpose of the new offences is to '*protect against harmful interferences with privacy*' and that '*these offences are not sexual offences as such*'.[9] The UK Government has taken a similar approach in resisting the label sexual offences.[10] It is this conceptualisation that I would like to challenge.

First of all, the images involved are sexual. Countries across the world, including Ireland and the UK, are taking action against these harmful practices because the images are sexual. It is because they are sexual that they go viral across the internet. It is a plain fact that non-sexual images simply do not have the same potency to cause harm and abuse, nor would thousands more people distribute the images unless they were sexualised. There are thousands of websites dedicated specifically to 'revenge porn', 'upskirting' and such like and this is because it is sexual material. Therefore, while the language of 'intimate' is often used to describe the material under discussion, it is because images are *sexual* that there is such a problem.

Further, the abuse and harassment meted out to women and girls - and it is mainly women and girls who are victim-survivors - is sexualised. The language used and threats made are sexualised. In essence, this is because the sexual double standard is alive and well. Women are castigated for exercising sexual agency (taking or 'allowing' to have taken sexual images). They are harassed and abused for transgressing expected norms of women's sexuality. The language of the abuse is sexualised and brutal, as are the threats, including rape threats, which are experienced as real threats, especially when images are often accompanied by women's names, addresses and other contact details.

The sexualised nature of the abuse and harassment further identifies the harms suffered as breaches of women's rights (and the victim-survivors are predominantly women) to sexual freedom and sexual autonomy. The impact of image-based sexual abuse is that all women are made to feel constrained in their sexual choices - criticised and then often blamed for expressing themselves sexually through imagery. Victim-blaming is rife, with police and media often telling women to simply prevent the abuse by refusing to take or share pictures of themselves. But everyone should be free to express their sexuality as they choose - without harming others - including if they wish to take and share private, sexual images, and without fear of these being distributed without their consent. Online intimacy is now commonplace; we need to adapt our laws, policies and practices to reflect this, not to blame women. The impact of these offences on women generally is to inhibit their sexual expression. Women are being silenced.

Finally, women who have spoken out about their experiences of image-based sexual abuse characterise what happened to them as a form of sexual offending and abuse. YouTuber Chrissy Chambers has described her experiences of images being distributed worldwide as a form of 'sexual assault'.[11] Jennifer Lawrence, the Hunger Games actor, described the hacking and distribution of naked images of her as a 'sex crime'.[12] Other jurisdictions are beginning to recognise this. Israel prosecutes 'revenge porn' as a form of sexual offence[13] and recently an Australian Senate inquiry described the phenomenon as a 'sex crime'.[14]

Further, many organisations supporting women who have survived image-based sexual abuse characterise these harms as a form of violence against women. Irish Women's Aid has been doing excellent work in this area, raising awareness and rightly seeking legislative action. Image-based sexual abuse is used as a measure of control and abuse in abusive relationships - especially the threats to distribute images which are part and parcel of some methods of coercive control in intimate relationships.[15] This is where the work of Women's Aid organisations across the UK and Ireland has been so effective and necessary.

The work of Women's Aid is germane not just to the general argument about the need for legislative and policy action, but also because it recognises and emphasises the gendered nature of these harms. I have so far been suggesting that we treat 'harmful communications' as forms of sexual abuse. I also want to emphasise that these are gendered harms; and therefore in some cases, gendered crimes. Data from the UK and the US has found that the vast majority of victim-survivors are women and girls.[16] For example, the Revenge Porn Helpline in the UK takes calls predominantly from women victim-survivors[17], and police data show the complaints are most commonly made by women and prosecutions for offences against women.[18] Snapshot data of a 'revenge porn' website over a 28 day period found that 95% of posts were images of women, and that it is women's images that receive the most commentary from users and the wider online community.[19]

Image-based sexual abuse is just part and parcel of the broader phenomena of online abuse and harassment. This abuse is mostly perpetrated against women and girls. Not exclusively, and those men who do not conform to masculine norms or stereotypes are similarly at risk of abuse and being harassed. But, it is clear that online abuse is mostly gendered and misogynistic.

Vital expressive role of the criminal law

Having explained the nature and context of image-based sexual abuse, I return to the question of why it matters what we call this abuse. A major purpose of the criminal law is to express societal condemnation of specific practices with the hope of changing people's behaviour. The law can only achieve these purposes if the label applied to a crime is the right one. And 'revenge pornography' is the wrong one. But so are terms which do not name the harms and label them for what they are. Few legislators or policy makers, or Law Commissions, use the term 'revenge porn'. All recognise it is problematic. However, even when other terms are used, they fail to recognise the harms as sexual, or that they are a form of sexual offending. This is vital in terms of identifying the harm and then taking action.

I argue that terminology is important as it frames our debates. If we recognise these harms as a form of sexual offence, it shapes our legal and policy responses. For example, using the most appropriate terminology and concepts may enable us to more easily recognise the harms as serious - that they are a form of abuse, with potentially serious long-term consequences. It may mean we more readily recognise that support services are required for victim-survivors - to encourage them to report to the police, to help them recover, to support legal action - just as these support services and structures are required for victim-survivors of sexual offences. Specifically, if we recognise the harms as sexual and

gendered, we should then recognise the need for specialist support services such as Women's Aid and Rape Crisis. If we recognise the gendered nature of image-based sexual abuse, we might also realise the seriousness of threats; specifically that they are often used as part of control and abuse in intimate relationships. Without that context, we might not see the seriousness of criminalising threats to distribute private, sexual images without consent.

Further, we may treat victims of image-based sexual abuse in the legal system the same as other victim-survivors of sexual offences. In England, this would have the important ramification of ensuring that victim-survivors have automatic anonymity when reporting to the police. In this specific regard, I welcome the recommendation from the Irish Law Commission that anonymity is granted to complainants.[20]

Beyond law reform: education and public awareness

Finally, how we describe these harms, how we frame them, will influence our education and prevention campaigns. While image-based sexual abuse - or 'revenge porn' - is indeed an egregious breach of privacy, it is not education and prevention campaigns focused on privacy per se that are needed.

It is compulsory, age-appropriate and effective education on sexual ethics and respectful relationships that is vital. Education needs to be about how we navigate intimate relationships and the use of technology; on valuing women's sexual expression and autonomy; on sexual consent and coercion, especially within sexual relationships of young people. Education and public awareness is also important as this is what matters when the law runs out; when we might not be able to catch abusive actions as criminal.

And this is what takes me to a final example of harassment and abuse. At the beginning of the year, reports came out of images of young Irish women being taken from Facebook and posted on various pornography websites.[21] Many of the images did not involve nudity - and so would not be covered by laws relating to private, sexual images. This was not 'revenge porn'. But it is certainly abusive and it is highly sexualised. As well as the images being posted, they were accompanied by harassing comments and abuse. The language used in many of the comments accompanying these images cannot be included here due to their nature - highly sexual, pejorative and abusive. Some of the images were of what are known as 'cum shots', where someone has ejaculated over the image and then posted it. This is a form of abuse and attempt to exercise power over the person in the image. But, again, is unlikely to fall foul of criminal laws in this area.

I highlight this example to make two final points. Even the broadest law on image-based sexual abuse may not cover the myriad of ways in which women and girls - and it is predominantly, even if not exclusively, women and girls - are subject to abuse online. Therefore, education and prevention measures are vital. But, they will only work and be effective if we recognise the real nature of these harms as gendered and sexualised.

Conclusion

The harms of the non-consensual distribution and/or creation of private sexual images, including but not limited to 'revenge porn', are best conceptualised as image-based sexual abuse. These are gendered harms that are forms of sexual

abuse. I urge policy-makers, Parliamentarians, and all of us working in this field, to take this on board and let this knowledge - and the experience of victim-survivors - shape our legal and policy responses.

1 Law Reform Commission, *Harmful Communications and Digital Safety* (Law Commission, 2016).
2 For a full discussion of these international perspectives, see Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) *Oxford Journal of Legal Studies* forthcoming.
3 See further: Clare McGlynn & Erika Rackley, 'Not 'revenge porn' but abuse: let's call it image-based sexual abuse' *EverydayVictimBlaming.com* (9 March 2016) http://everydayvictim-survivor-survivorblaming.com/news/not-revenge-porn-but-abuse-lets-call-it-image-based-sexual-abuse-by-%E2%80%8Fmcglynnclare-erikarackley/
4 Clare McGlynn & Erika Rackley, 'The new law on 'revenge porn' is welcome but no guarantee of success' *The Conversation* 16 February 2016, available at: https://theconversation.com/the-new-law-against-revenge-porn-is-welcome-but-no-guarantee-of-success-37598
5 James Ward, 'Irish girl reveals revenge porn attack horror after ex-boyfriend uploaded intimate video and images' Irish Mirror 21 June 2016, available at: http://www.irishmirror.ie/news/irish-news/crime/irish-girl-reveals-revenge-porn-8244939
6 Paul Farrell, 'Nude photos of Jennifer Lawrence and others posted online by alleged hacker' *The Guardian* 1 September 2014.
7 Clare McGlynn and Julia Downes, 'Why we need a new law to combat upskirting and downblousing' *Inherently Human* 15 April 2015: https://inherentlyhuman.wordpress.com/2015/04/15/we-need-a-new-law-to-combat-upskirting-and-downblousing/.
8 See the recent report by the Brookings Institute into 'sextortion', available at: http://www.brookings.edu/research/reports2/2016/05/sextortion-wittes-poplin-jurecic-spera.
9 Law Reform Commission, *Harmful Communications and Digital Safety* (Law Commission, 2016), para 1.07.
10 As discussed in the research briefing 'Anonymity for Complainants of Image-Based Sexual Abuse', 11 July 2016, available at: https://claremcglynn.com/2016/07/18/new-briefing-on-anonymity-for-complainants-of-image-based-sexual-abuse/
11 Jenny Kleeman, 'US woman pursues ex-boyfriend in landmark UK revenge-porn action' *The Guardian* 3 June 2015.
12 Vanity Fair, 'Jennifer Lawrence calls 'photo hacking' a sex crime', 7 October 2014, available at: http://www.vanityfair.com/hollywood/2014/10/jennifer-lawrence-cover
13 Yifa Yaakov, 'Israeli law makes revenge porn a sex crime' *The Times of Israel* 6 January 2014.
14 Legal and Constitutional Affairs Committee, *Phenomenon Colloquially Referred to as 'Revenge Porn'* (Commonwealth of Australia, 2016), para 5.37.
15 See, for example: https://www.womensaid.ie/about/newsevents/pastevents/2015/11/25/digital-abuse-of-women-international-day-opposing/
16 Amanda Lenhart et al, *Online Harassment, Digital Abuse and Cyberstalking in America* (Data Society, 2016), available at: http://datasociety.net/pubs/res/Online_Harassment...Oct-2016.pdf
17 UK Government Equalities Office Press Release, 'Hundreds of victim-survivors of revenge porn seek support from helpline', 20 August 2015.
18 Josh Halliday, 'Revenge porn: 175 cases reported to police in six months' *The Guardian* 11 October 2015.
19 Abby Whitmarsh, 'Analysis of 28 Days of Data Scraped From a 'revenge pornography' Website' *everlastingstudent.wordpress.com* 13 April 2015.
20 Law Reform Commission, *Harmful Communications and Digital Safety* (Law Commission, 2016), para 2.212.
21 Stephen Rogers, 'Facebook images of young cork girls posted on porn site' *Irish Examiner*, 14 January 2016, available at: http://www.irishexaminer.com/ireland/facebook-images-of-young-cork-girls-posted-on-porn-site-376096.html

On-Line Child Sexual Exploitation: Grooming, Sexting and Cyberbullying

Professor Anne-Marie McAlinden, School of Law, Queen's University Belfast

The following paper draws on two research projects based on original primary research - one of them completed, the other ongoing: (1) *'Grooming' and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions*, which was funded by the British Academy (Grant Ref: SG10187) (McAlinden, 2012) and published as a monograph by Oxford University Press in 2012; and (2) *Children as 'Risk': Child Sexual Exploitation and Abuse by Children and Young People*, which was funded by the National Organisation for the Treatment of Abusers (NOTA) and is to be published as a monograph by Cambridge University Press in 2017 (McAlinden, 2017). The first project entailed fifty-one in-depth semi-structured interviews with professionals who risk assess, treat or manage sex offenders and those engaged in victim services and support across the three jurisdictions of the United Kingdom as well as the Republic of Ireland. The second involves thirty-two interviews with professionals who work with young people displaying harmful sexual behaviour and with victims of such behaviour. Taken as a whole, these projects encompass children as both 'victims' as well as potential 'perpetrators' of harmful sexual behaviour in both on-line as well as off-line contexts.

'Grooming' is a term which has almost become synonymous with sexual offending, at least within public discourses. The term is generally taken to refer to the process which helps the offender 'set up' opportunities to abuse and subsequently avoid discovery or disclosure (McAlinden, 2006). As other writers have put it, it is about accessing a victim, creating opportunities to abuse and sustaining or maintaining the child in an abusive situation (Craven et al, 2006). It is traditionally said to be a staged, sequential process, beginning with befriending the child, creating an 'exclusive' relationship, introducing sexual themes, culminating in sexual harm (Elliott et al, 1995). One of the most publicly prominent forms is on-line grooming but it also encompasses grooming within a range of intra-familial and extra-familial contexts, such as within institutions (institutional grooming), and within families and also among peers (McAlinden, 2012). As discussed further below, there may also be a cross-over between on-line and off-line forms of grooming. Indeed, grooming can operate with respect not just to the child, but also with respect to the surrounding environment and protective significant others (Craven et al, 2006). The difficulty with grooming behaviour, however, is that it can be very difficult to identify potential grooming and pinpoint harmful intent prior to the occurrence of harm. My own definition is as follows:

'(1) the use of a variety of manipulative and controlling techniques (2) with a vulnerable

subject (3) in a range of inter-personal and social settings (4) in order to establish trust or normalise sexually harmful behaviour (5) with the overall aim of facilitating exploitation and/or prohibiting exposure' (McAlinden, 2012: 11).

This underlines the fact that grooming can operate in a range of contexts, both on-line and off-line, and that the overall essence of the process can be distilled to one of 'normalisation' to the extent that the victim may not even realise that they have been 'groomed' or harmed.

In relation to on-line grooming specifically, it is useful to compare grooming in virtual and real world contexts. While both on-line and off-line grooming may follow a staged process, as broadly outlined above, grooming on the internet is often much more expedient, where the introduction of sexual language, themes and behaviours can take minutes, as opposed to months or years. This is generally because the often faceless nature of on-line interactions is facilitative of anonymity which in turn has dual implications for both would-be perpetrators and potential victims - it may simultaneously offer enhanced opportunity for perpetrators and increased vulnerability for victims. In this respect, the internet may also be said to promote risk-taking behaviour by both offenders and victims - perpetrators may be more ready to approach victims in the relative safety of the on-line setting, while victims may also perceive themselves to be safer than within the context of face-to-face interactions.

On one level, it is easier to police on-line grooming because of the digital chain of evidence which is generated by chat and service provider logs. There are, however, unique challenges of preventing, targeting and criminalising grooming and abuse on-line. In particular, there are problems with advancing technology; the ubiquitous use of mobile phones and social media among children and young people especially; and the cross-jurisdictional element to potential offences where the offender lives in one jurisdiction and the victim in another. A further complexity underlies the fact that not all on-line sex offenders set out to groom surreptitiously by concealing their identity and intention. In fact, as Webster and colleagues (2012) have noted, there are 'hyper cautious' groomers, for example, an adult man posing as a 17-year old boy in order to target and groom a 14-year old girl. There are also, however, what they term 'hyper confident' groomers who are open about their sexual intentions as an adult man towards a teenage girl under the age of consent. While there is a potential cross-over between on-line and off-line grooming and abuse, not all virtual contacts progress to contact sexual offences in the real world. Indeed, there are a range of purposes for which sex offenders seek to use the internet in order to sexually abuse or exploit children (Durkin, 1997). Some sex offenders will seek to groom children on-line for the purposes of engaging in inappropriate sexualised communications with children or producing child pornography and others will seek to groom children on-line for the purposes of arranging a meeting in order to commit a contact sexual offence off-line. The salient point is that the non-contact sexual offences against children committed on-line are no less harmful than contact sexual offences committed off-line. As discussed below, while the majority of offenders against children on-line are adult males, a growing number are under 18.

There are also difficulties, in on-line as well as off-line contexts, surrounding the

complexity of the victim-offender relationship. By way of example, the victim, via grooming and the normalisation of abusive behaviour, may not see themselves as a victim and may even perceive themselves to be in a relationship with their abuser. This is arguably augmented within the cyber setting due to the range of factors highlighted above. In this respect, there are manifold difficulties for professionals in dealing with 'statutory' or 'compliant' victims within the context of justice or welfare interventions (Wolak et al, 2004). Victims may be initially unwilling to disclose the abuse or engage with police or other professionals providing therapeutic or support services. Having made a complaint, this may subsequently be withdrawn as the victim often finds themselves in a 'push-pull scenario' - they may, for example, welcome the attention or gifts associated with grooming and the process of entrapment but, at the same time, not want the abusive acts that accompany this. In this vein, the complexities of grooming and how it may impact on victims, also has potential consequences for their credibility as witnesses and thus for prosecution.

One of the fastest growing forms of grooming and abuse is that between peers, particularly within on-line settings. While figures vary between studies, it is generally thought that between one quarter and one half of all child sexual abuse or exploitation is committed by children and young people themselves. This may relate to a range of contexts such as institutional abuse, street or localised grooming, and on-line forms of abuse including new forms such as 'sexting' or 'cyber bullying' (McAlinden, 2017). Indeed, there is some evidence to suggest that the figure may be higher for peer-based abuse in on-line settings. In Finkelhor et al's (2000) American study, for example, 48% of perpetrators of on-line forms of sexual offending against children were under eighteen. More recent NSPCC figures for England and Wales highlight that one in six of those reported to the police for indecent images are under eighteen (NSPCC, 2016). As with adult-child abuse discussed above, a complicating factor can be the complexity of the victim-offender relationship which is arguably enhanced between peers in pinpointing harm or risk of harm, due to the potential lesser degree of an age differential and the consequent reduced power imbalance. Indeed, in complex cases the 'victim' may have been groomed and exploited or abused themselves but also 'groomed' or coerced into recruiting other victims for offenders. This has occurred in a range of offending contexts such as on-line (for example, a child or young person being coerced into bringing their friends in front of a web cam to produce naked images for offenders), but also off-line in relation to organisational offending and within the context of street or localised grooming. This points to what I have previously termed 'the victim-offender continuum' (McAlinden, 2014) and the difficulties which professionals and wider society may face in distinctly identifying a child or young person as either a victim or a perpetrator, when in fact they may be technically said to be both.

In this respect, two of the most publicly prominent forms of on-line sexual exploitation involving children and young people are 'sexting' and 'cyber bullying.' 'Sexting', broadly defined and measured, is the act of sending sexually explicit messages and/or photographs primarily between mobile phones (Wolak and Finkelhor, 2011). Rates vary across studies, depending on how the phenomenon is defined. Ringrose et al (2012), for example, found rates of sexting

of between 15-40% among young people in their review of existing studies. 'Sexting' emerges as a highly gendered phenomenon in that girls are more often the subject of the message or image, usually with an element of underlying coercion. Sexting often poses difficulties for law enforcement along a number of fronts: First, in clearly identifying the 'victim' and the 'perpetrator', where for example the initial sending of the image was unsolicited or where the image was initially sent on a consensual basis but then disseminated to third parties without the subject's consent; Second, in classifying the image as harmful or illegal, in terms of the differences between posed or sexually explicit images and where technically those who take and send, receive and distribute such images could be deemed the producers, possessors and distributors of indecent images of children. There is also a discrepancy across the legal frameworks in some jurisdictions, such as Northern Ireland and England and Wales, where the age of consent is sixteen but conversely children who are the subject of potentially indecent images are protected up to the age of eighteen. Due to the fact that sexting may entail an element of latent coercion in the form of blackmail, bullying or emotional harm for victims, it is usually classified as a form of child sexual exploitation where children are exploited for reasons or motivations including money, power, status, attention seeking as well as the infliction of actual harm (Ashurst and McAlinden, 2015).

Similarly, 'cyberbullying' is broadly defined as the use of the internet and other mobile technologies to harass, threaten or harm other people, usually in a deliberate and sustained manner (Kofoed and Ringrose, 2011). While studies in other jurisdictions have reported slightly lower rates, a 2013 NSPCC study reported that 38% of young people had been affected by cyberbullying. Sexting is a form of cyberbullying in that it can often involve the use of social media as well as on-line platforms to harm or harass. Indeed, in a number of high-profile cases, the abuse and harm suffered by victims of cyberbullying has led to suicide and self-harm. Cyberbullying may also pose challenges for professionals and organisations in that it bridges the public-private divide - for instance, if the bullying occurs within the context of a school setting between two pupils which then continues on-line, this has potential implications for the school, parents/carers as well as police.

Peer-to-peer grooming and child sexual exploitation pose a number of challenges for society and professionals. In the main, there are difficulties in separating out 'normal', problematic and harmful sexual behaviour, particularly that which occurs within the context of peer-based relationships. Indeed, even at the serious end of the spectrum there may be related difficulties for assessment professionals in determining whether the behaviour amounts to innocent exploration or an experimental, transitory phase, or the early indication of the onset of something more sinister. Peer-based sexual behaviours present as particularly challenging for society because they challenge accepted societal and cultural norms about children and young people relating to the sexual innocence of children and their accepted identity as 'victims' rather than 'perpetrators' of abuse. There are also challenges stemming from the emergence of new and rapidly changing technologies and modes of communication between adolescents in particular (Ashurst and McAlinden, 2015) and in determining what is the 'new normal' which may vary across time and place, between adults and children, and between children

themselves. Perhaps the biggest challenges, however, relate to the subversion of a highly sexualised popular culture which stem in particular from the music, fashion and gaming industries (McAlinden, 2017). Similarly, given the prevalence of sexting and the proliferation of a sexualised popular culture, there are related difficulties in engaging children and young people around discussion of behaviours that they do not regard as particularly unwelcome or harmful (McAlinden, 2012). Phippen (2012), for example, highlights that many young people regard sexting as 'flirting' and as much safer than off-line forms of sexual interaction.

Finally, in relation to criminal justice responses to peer-based abuse, the prevalence of sexting against a backdrop of the widespread use of social media and mobile phones and the diffusion of cultural messages about sex, means that criminalisation is not a viable solution for all on-line forms of child sexual exploitation by children and young people. This points towards the need to develop a more nuanced approach to 'risk' which differentiates between 'aggravated' motivations (e.g. gang status, revenge, intentional infliction of harm) and 'experimentation' (Wolak and Finkelhor, 2011). At the same time, for those children and young people who do warrant a criminal justice response, there is the need to avoid labelling and stigma as 'offenders' because of the potential life-long social and personal consequences of being branded a 'sexual abuser' or 'offender.' Ultimately, it underlines the need to develop public health and educative responses to sexual health and healthy relationships, beginning in primary schools and involving parents. This should encompass messages around e-safety as well as broader life skills in relation to relationships off-line. This would have the aim of equipping children with the personal tools and skills to build self-esteem and reduce vulnerability to both on-line and off-line forms of sexual abuse and exploitation.

References

Ashurst, L. and McAlinden, A. (2015), 'Young People, Peer-to-Peer Grooming and Sexual Offending: Understanding and Responding to Harmful Sexual Behaviour within a Social Media Society', *Probation Journal* 62(4): 374-388.

Craven, S., Brown, S. and Gilchrist, E. (2006), 'Sexual Grooming of Children: Review of Literature and Theoretical Considerations', *Journal of Sexual Aggression* 12(3): 287-299.

Durkin, K. (1997), 'Misuse of the Internet by Paedophiles: Implications for Law Enforcement and Probation Practice', *Federal Probation* 61(3): 14-18.

Elliott, M., Browne, K. and Kilcoyne, J. (1995), 'Child Sexual Abuse Prevention: What Offenders Tell Us' *Child Abuse & Neglect* 19(5): 579-594.

Finkelhor, D., Mitchell, K.J. and Wolak, J. (2000), *Online Vicimization: A Report on the Nation's Youth* (Alexandria, VA: National Center for Missing and Exploited Children), at http://www.missingkids.com/en_US/publications/NC62.pdf.

Kofoed, J. and Ringrose, J. (2012), 'Travelling and Sticky Affects: Exploring Teens and Sexualized Cyberbullying through a Butlerian-Deleuzian-Guattarian Lens', *Discourse: Studies in the Cultural Politics of Education* 33(1): 5-20.

McAlinden, A. (2006), '"Setting 'Em Up": Personal, Familial and Institutional Grooming in the Sexual Abuse of Children', *Social & Legal Studies* 15(3): 339-262

McAlinden, A. (2012), '*Grooming' and the Sexual Abuse of Children: Internet, Institutional and Familial Dimensions* (Oxford: Oxford University Press), Clarendon Studies in Criminology.

McAlinden, A. (2014), 'Deconstructing Victim and Offender Identities in Discourses on Child Sexual Abuse: Hierarchies, Blame and the Good/Evil Dialetic', *British Journal of Criminology*, 54(2): 180-198.

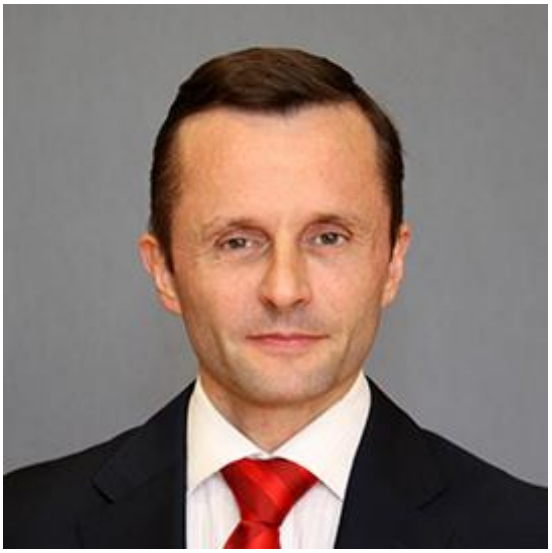
McAlinden, A. (2017), 'Children as "Risk": Child Sexual Exploitation and Abuse by Children and Young People' (Cambridge: Cambridge University Press), forthcoming.

NSPCC (2016), '1 in 6 reported to police for indecent images are under 18', 1 September 2016, at

https://www.nspcc.org.uk/fighting-for-childhood/news-opinion/1-6-reported-police-child-sexual-images-under-18/
Phippen, A. (2012), *Sexting: An Exploration of Practices, Attitudes and Influences* (London: NSPCC).
Ringrose, J., Gill. R., Livingstone, S. and Harvey, L. (2012), *A Qualitative Study of Children, Young People and 'Sexting'*, A Report Prepared for the NSPCC at http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research_wda89260.html.
Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A. and Craparo, G. (2012), European Online Grooming Project: *Final Report* (March 2012), at http://www.europeanonlinegroomingproject.com/wp-content/file-uploads/European-Online-Grooming-Project-Final-Report.pdf
Wolak, J., Finkelhor, D. and Mitchell, K.J. (2004), 'Internet-initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings From a National Study', *Journal of Adolescent Health* 35(5): 424-433.
Wolak, J. and Finklehor,D. (2011) *Sexting: A Typology* (University of New Hampshire, USA: Crimes Against Children Research Centre).

Recommended Legislative Reforms on Child Protection

Professor Dr. Geoffrey Shannon, Special Rapporteur on Child Protection



Sincere thanks are extended to Professor Dr. Geoffrey Shannon, Special Rapporteur on Child Protection, who dedicated further time to bring added value to his paper by incorporating updates in the law between the conference date and March 2017, in particular the publication of the Criminal Law (Sexual Offences) Act 2017.

The child protection concerns that our society faces continue to evolve and develop. It is of the utmost importance that our criminal justice system also evolves and develops in order to keep apace with real threats to the safety and protection of children in our society. Our child protection ethos needs to be proactive and not reactive.

The digital world brings many positives for children but unfortunately it also brings new tools through which children can be abused and exploited. Advances in technology have created a new child protection frontier. For example, in the area of child pornography, the growth of Information and Communications Technology (ICT) has made what was once regarded as a somewhat remote crime more accessible. Technology has allowed child pornography to be disseminated in a way that allows much of the offending behaviour to be hidden, and the offender to remain anonymous. In addition, children and in particular adolescents may be impacted by cyber harassment, the consequences of which may be life changing and indeed in some cases lead to the suicide of the victim. The requirement for legislation to be introduced to protect children online is a crucial and pressing concern.

Children are active users of ICT. At a global level, children represent almost a third of internet users.[1] Indeed, internet usage amongst children in Ireland exceeds the European average. In Ireland, 86 per cent of nine year olds have a computer in the home.[2] Social networking is a 'near universal' feature in the lives of Irish children, in particular adolescents: three in five children have a social networking profile.[3]

Technological advances, in particular the internet, have created certain dangers for children and to protect children the law must keep apace of these developments. On balance, Ireland has been slow to take action in response to the new threats to child protection posed by ICT. To date, Irish legislation has been limited in its reach and has failed to deal with sexual exploitation carried out through social media, the internet and other such technology. There has been some welcome legislative progress made with the enactment of the Criminal Law (Sexual Offences) Act 2017. However, further legislative reform and other measures are needed to ensure Ireland has a robust

framework to tackle issues including cyber bullying and harassment.

As a signatory to the UN Convention on the Rights of the Child, Ireland has a duty to take measures to protect children from abuse, neglect and sexual exploitation.[4] To develop the right further, the Committee on the Rights of the Child issued General Comment 13 on the right of children to be free from all forms of violence. The General Comment recognises that while advances have been made towards the prevention of violence against children, "*existing initiatives are in general insufficient. Legal frameworks in a majority of States still fail to prohibit all forms of violence against children, and where laws are in place, their enforcement is often inadequate*".[5] In particular, the General Comment recognised that common understandings of violence are often under-inclusive, and so it attempted to provide a more comprehensive outline of the behaviours captured by the term "*violence against children*". For present purposes, it is important that this includes "*psychological bullying and hazing by adults or other children, including via information and communication technologies (ICTs) such as mobile phones and the Internet*,"[6] sexual abuse and exploitation outside of commercial settings,[7] and specifically violence committed through the use of ICT. This final category includes various aspects of child pornography as well as bullying, harassment or stalking of children and/or coercing, tricking or persuading children into meeting strangers off-line, and being groomed for involvement in sexual activities and/or providing personal information.[8] State parties must, therefore, ensure that relevant legislation provides adequate protection of children in relation to ICT.[9]

These developments recognise the various ways in which violence can be perpetrated against children through ICT. However, these statements operate at a significant level of generality. More specific instruments are found within Europe, as both the Council of Europe and the European Union have taken measures to address the problem.[10] There are two Council of Europe conventions which are relevant - the Convention on Cybercrime (the Budapest Convention)[11] and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention).[12] Ireland has signed both Conventions, but has ratified neither. In order to ensure the highest standards of protection for children, and the highest level of international co-operation in this area, it is imperative that both Conventions are ratified without reservation.

The Budapest Convention, although focused on the issue of cybercrime, provides in Article 9 for a range of offences relating to child pornography. It was felt that "*specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children*."[13] Member States must, under Article 9(1), criminalise the following offences, if committed intentionally and without right:

(a) producing child pornography for the purpose of its distribution through a computer system;
(b) offering or making available child pornography through a computer system;
(c) distributing or transmitting child pornography through a computer system;
(d) procuring child pornography through a computer system for oneself or for another person;

(e) possessing child pornography in a computer system or on a computer-data storage medium.

In order to give child pornography the widest possible meaning, Article 9(2) stipulates that the term includes images of a minor engaged in sexually explicit conduct, images of a person appearing to be a minor engaged in sexually explicit conduct, and realistic images representing a minor engaged in sexually explicit conduct. The term "child" is understood to be a person under the age of 18, although States Parties may adopt a lower age limit which may not in any event be lower than 16 years.[14] The age provisions were adopted so as to provide a uniform approach to the treatment of children as sexual objects, and so may differ significantly from the age of consent in national laws.[15] The inclusion of the phrase "*without right*" is included in the Convention so that legal defences and other relevant principles can be taken into account in specific circumstances, such as the possession of material which may otherwise be considered pornographic for *bona fide* artistic, medical, scientific, or similar merit.[16]

While the Budapest Convention moves beyond the emphasis on the commercial exploitation of children to cover individual actions of production, possession, distribution and solicitation of child abuse images, the Convention's focus on cybercrime inherently limited its ability to deal comprehensively with the broader problems of abuse and exploitation. It did not deal with the issue of grooming or soliciting a child to engage in activity that could facilitate the production of pornographic material. The language of Article 9 makes clear that the measures to be adopted at national level are effectively content related offences - they focus on the material produced from child abuse rather than the abuse itself or actions leading to that abuse.

This latter concern was, however, the subject of the Lanzarote Convention.[17] The genesis of this Convention is outlined in its Explanatory Report, which recalls the advances made by the CRC, the Optional Protocol on the sale of children and the Budapest Convention as well as a variety of other international legal instruments and political declarations.[18] The resulting Convention therefore provides a comprehensive set of obligations for Member States in respect of sexual exploitation and abuse, including a variety of preventative measures such as vetting and information sharing, consciousness raising and participation measures, intervention programmes for offenders, child-friendly investigation procedures and international co-operation measures. This paper will, however, focus on Chapter VI relating to substantive criminal law.[19] The measures contained within Chapter VI are designed to facilitate the harmonisation of national laws so as to in turn facilitate the enforcement of laws due to the decreased ability of perpetrators to select jurisdictions with more lenient penal codes.[20]

Articles 18 to 24 provide for a variety of substantive criminal law offences which Member States are obliged to enact, while the remainder of the chapter deals with jurisdictional matters, sentencing and corporate liability. Article 18 provides that Member States shall enact legislation against the sexual abuse of children, Article 19 deals with child prostitution, Articles 20 and 21 deal with child pornography while Article 22 seeks to criminalise the corruption of children. Importantly, the provisions relating to child pornography are not, unlike the Budapest Convention,

limited to offences involving computer systems. In a further development of the Budapest Convention, Article 20(1)(f) stipulates that Member States must criminalise the intentional act of "*knowingly obtaining access, through information and communication technologies, to child pornography*." As the Explanatory Report clarifies, this is "*intended to catch those who view child images online by accessing child pornography sites but without down-loading and who cannot therefore be caught under the offence of procuring or possession in some jurisdictions*,"[21] while at the same time ensuring that persons who inadvertently access websites containing child pornography are not sanctioned.

The remainder of this paper explores significant gaps in Irish law which need to be addressed to ensure we are fully protecting, promoting and fulfilling children's rights to be protected from all forms of abuse. It begins with an exploration of the offence of cyber harassment and then moves on to examine recent legislation on sexual offences and proposed legislation on protecting the rights of victims.

Cyber Harassment

A challenge that is not yet fully addressed in Irish law is that of cyber harassment. Online harassment has become a problem in societies such as ours where people communicate regularly by e-mail and where social media platforms such as Facebook, Twitter and Instagram are often used. Given technological advances, computers are not required to carry out a campaign of cyber harassment as mobile devices are now equipped with the same internet options. This means that cyber harassment can take place more frequently and with ease when perpetrated with the use of mobile phones. It enables perpetrators to communicate with others and disseminate content online instantly, with little effort. Cyber harassment may take three different forms. Firstly, it could take place through the non-consensual publication of images online of an intimate nature, whether consensually generated or gained through covert recording. This type of publication often takes place out of spite or revenge, colloquially termed "*revenge porn*". Secondly, cyber harassment may also involve the use of a fake Facebook profile to terrorise a victim through the publication of abusive material, images or videos about him or her which may be foul, fabricated, racist and/or defamatory. Thirdly, the internet can be used to bully a particular person by the repetitive sending of malicious messages to the intended victim, often anonymously. The effects of these types of online behaviour are immediate, they have the capacity to go viral and they can be extremely invasive.

Teenagers and young adults can be and often are the targets of cyber harassment. An Garda Síochána has recognised this problem with the publication of its Crime Prevention Information Sheet on Online Harassment (2012), directed towards both children and their parents.

The capacity for damage from cyber harassment is enormous. Aside from the impact of such behaviour on a victim's emotional wellbeing, including embarrassment, hurt and fear, there can be other more drastic consequences of cyber harassment, such as depression and suicide. Harassment or online abuse can equally have an impact on a young person's reputation and could potentially damage his or her future job opportunities.

Irish law is currently inadequate to deal with cyber harassment. The law only deals

with harassment to a limited extent. It has not been updated to take into account the potential for online abuse or to provide for an effective "*takedown procedures*" remedy. The key provision in force at present is section 10 of the Non-Fatal Offences Against the Person Act 1997. It creates the offence of harassment in criminal law, by providing that:

"(1) Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence.

(2) For the purposes of this section a person harasses another where -

(a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and

(b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other."

Section 10 is wide enough to include digital or online harassment. It specifies that a person who "*by any means*" harasses another shall be guilty of an offence. While the telephone is specified as one particular instrument that may be utilised to carry out a campaign of harassment, the provision is broad enough to allow a prosecution to be taken for harassment through the use of online communication such as by e-mail or social media.

A key weakness of section 10 is that it requires the conduct in question to be committed persistently. The Law Reform Commission's Report on Harmful Communications and Digital Safety (2016)[22] recommends the amendment of section 10 to include specific reference to harassment *by digital or online means, including through social media sites or other internet medium*.

Criminal Law (Sexual Offences) Act 2017

In a very positive development the Criminal Law (Sexual Offences) Act 2017 was passed by the Oireachtas in February 2017, demonstrating Ireland's commitment to better protecting its children from online predators. The 2017 Act creates a wide range of new criminal offences in relation to child pornography and the grooming of children for sexual exploitation and in particular, it addresses the role of ICT in committing such offences.

<u>Increased powers of An Garda Síochána</u>

A number of new offences concerning the solicitation and grooming of children have been introduced in sections 3 to 8 of the 2017 Act. These provisions vastly expand upon existing legislation of this kind, better protecting children from predators. In light of these new offences, it is submitted that further powers need to be granted to An Garda Síochána. It cannot be denied that mobile devices are now very powerful computers with the memory capacity to contain many thousands of images, text and video files that constitute child pornography, along with ICT evidence of grooming, solicitation, sexual exploitation and important evidence relating to contact sexual offences (e.g. images and chat/SMS messages discussing the incident). To reflect this modern situation, An Garda Síochána should be provided with a power similar to section 23 of the Misuse of Drugs Acts. The historic position whereby child pornography was often stored on an offender's computer in his or her home does not reflect the reality of modern technology.

Also in this vein, it must be recognised that Facebook, Google, Yahoo, Adobe and

Microsoft are some of the many non-Irish companies with offices in this country. Many of them store their Irish data in Ireland but some of them claim it is stored in the US or elsewhere. For the investigation of child pornography and sexual offences cases against children where ICT is involved, An Garda Síochána should be provided with the power to obtain a production order in respect of data that is either "*held or accessible*" by content providers based in Ireland. This order could then be served on any such provider registered in Ireland requiring production of ICT evidence - photos, chat, account information and IP Addresses. An order similar to that provided for in section 15 of the Criminal Justice Act 2011 for fraud and banking is worthy of consideration. It seems anomalous that powers introduced to deal with the banking crisis should not be available to protect vulnerable children.

Jurisdiction

Part 7 of the Criminal Law (Sexual Offences) Act 2017 vastly extends Ireland's jurisdiction over offences committed outside the State. Previously, the Sexual Offences (Jurisdiction) Act 1996, as amended, provided that the State had jurisdiction over offences committed outside the State if certain criteria were fulfilled, namely that the behaviour constituted an offence in the place in which it was committed and would constitute an offence in Ireland if it had been committed here. Furthermore, the offence had to be one listed in the Schedule to that Act and notably, the production, distribution or possession of child pornography was not included in said Schedule. A number of amendments were made to the 1996 Act by Part 7 of the 2017 Act. Firstly, section 41 of the Act increases the upper age threshold for the purposes of the 1996 Act from 17 to 18 years of age, ensuring that Irish legislation conforms to the general international standard of protecting persons under 18 against exploitative sexual acts. In addition, the offences listed in the Schedule to the Act are expanded to include offences updated and created by the 2017 Act, such as possession of child pornography and the offences contained in sections 5, 6, 7 and 8 of the Criminal Law (Sexual Offences) Act 2017. It is therefore an offence for a citizen of the State, or person ordinarily resident in the State, to do an act, in a place other than the State, against or involving a child which would constitute an offence under the law of that place, and if done within the State, would constitute an offence under or referred to in an enactment specified in the Schedule to the 1996 Act.

Pursuant to section 42 of the 2017 Act, for certain child sexual offences, the dual criminality rule, applicable under section 41, will not apply. Where a person who is an Irish citizen or ordinary resident in the State does an act against a child abroad that if done in Ireland would constitute rape, sexual assault or any of the child prostitution offences, he or she is guilty of an offence. This behaviour no longer has to constitute an offence in the place in which it is committed - thereby signalling a relaxation of the dual-criminality rule. The 2017 Act therefore ensures that Ireland will permit the exercise of jurisdiction based both on the territoriality principle and based on nationality or ordinary residence.

Statutory Definition of Consent

Section 48 of the 2017 Act inserts a new section 9 into the Criminal Law (Rape) (Amendment) Act 1990. The definition of consent set out below which has been introduced into Irish law for the first time is a welcome development. It provides:

"(1) A person consents to a sexual act if he or she freely and voluntarily agrees to engage in that act.

(2) A person does not consent to a sexual act if -

- *(a) he or she permits the act to take place or submits to it because of the application of force to him or her or to some other person, or because of the threat of the application of force to him or her or to some other person, or because of a well-founded fear that force may be applied to him or her or to some other person,*
- *(b) he or she is asleep or unconscious,*
- *(c) he or she is incapable of consenting because of the effect of alcohol or some other drug,*
- *(d) he or she is suffering from a physical disability which prevents him or her from communicating whether he or she agrees to the act,*
- *(e) he or she is mistaken as to the nature and purpose of the act,*
- *(f) he or she is mistaken as to the identity of any other person involved in the act,*
- *(g) he or she is being unlawfully detained at the time at which the act takes place,*
- *(h) the only expression or indication of consent or agreement to the act comes from somebody other than the person himself or herself.*

(3) This section does not limit the circumstances in which it may be established that a person did not consent to a sexual act.

(4) Consent to a sexual act may be withdrawn at any time before the act begins, or in the case of a continuing act, while the act is taking place.

(5) Any failure or omission on the part of a person to offer resistance to an act does not of itself constitute consent to that act."

Child Prostitution and Trafficking

The sexual exploitation of children is one of the main purposes of child trafficking and stringent legislation has been called for to attempt to eliminate the demand for this. In particular, my Fourth Report on Child Protection specifically recommended that consideration be given to the position in Sweden and Norway, in which the purchase of sexual services has been penalised, with a view to introducing a similar system in this country.[23] The Criminal Law (Sexual Offences) Act 2017 does just this - creating new offences regarding the purchase of sexual services and addressing recommendations of the Joint Committee on Justice, Defence and Equality in its Report on the Review of Legislation on Prostitution (June 2013). These new offences target the persons who are purchasing rather than those who are selling the sexual services and are described by Minister Fitzgerald as sending "*a clear message that purchasing sexual services contributes to exploitation*".

Section 25 of the 2017 Act introduces a new section 7A into the Criminal Law (Sexual Offences) Act 1993, criminalising paying for sexual activity with a prostitute. This provides that it shall be an offence where, in the context of prostitution, a person pays money or any other form of remuneration or consideration for the purpose of engaging in a sexual activity with a prostitute. It also is an offence to promise payment for sexual activity with a prostitute. This section expands the law whereby it is only an offence to solicit or importune another person for the purposes of prostitution in a street or public place.[24] Section 26 amends section 5 of the Criminal Law (Human Trafficking) Act 2008, making it an offence to pay money or any other form of remuneration or consideration in exchange for sexual activity with a person, for the purpose of

prostitution, where it is known that person was trafficked. These provisions are to be welcomed as a positive development.

For a person to be found guilty of an offence under section 5 of the 2008 Act (as amended by section 26 of the 2017 Act) that person must knowingly purchase a sexual service from a trafficked person for the purposes of prostitution. It is a defence for the defendant to prove that he or she did not know and had no reasonable grounds for believing, that the person in respect of whom the offence was committed was a trafficked person. This provision provides for tougher sentences for those who purchase these services from trafficked persons as opposed to non-trafficked persons. Users are threatened with terms of imprisonment, compared with section 25 of the Act where fines are proposed as the penalty. This is designed to address the trafficking and exploitation associated with prostitution, reducing demand.

Grooming

Soliciting a child for sexual exploitation is an offence under Part 2 of the Criminal Law (Sexual Offences) Act 2017. Previous definitions of '*sexual exploitation'* were insufficient in capturing all possible forms of sexual exploitation of a child and loopholes in the legislation were apparent. The revised definition closes off those loopholes thereby rendering the offence more robust. In general terms the 2017 Act addresses previous concerns I highlighted in that it now prohibits the sexual exploitation of children taking place entirely online or through ICT. The 2017 Act also revises the offence of grooming and provides a new definition of this offence which brings it in line with internationally recognised standards thereby providing for greater child protection in Ireland.

Enclosed within sections 3 to 8 of the Criminal Law (Sexual Offences) Act 2017 are a number of new offences designed to tackle the solicitation and grooming of children. With regard to solicitation, section 3 of the Act vastly expands upon existing legislation of this kind. Currently in Ireland, soliciting a child is governed by section 6 of the Criminal Law (Sexual Offences) Act 1993, as amended. This provision states that a person who solicits or importunes a child, being a person under 17, for the purpose of committing a sexual assault (namely sexual intercourse, buggery, section 4 rape and aggravated sexual assault) is guilty of an offence, punishable by a maximum sentence of 5 years' imprisonment following conviction on indictment.

In section 3, not only is it a crime to solicit or importune a child, it is also an offence to pay, give, offer or promise to pay or give, a child or another person money or any other form of remuneration or consideration; to provide, offer or promise to provide, a child to another person; or to obtain a child for oneself or for another person, for the purpose of the sexual exploitation of a child by that person or any other person. This, therefore, greatly increases the circumstances that may come under the offence of solicitation and deals with situations where a child is given rewards or presents by the exploiting adult. Furthermore, it provides that the offender does not have to carry out one of the aforementioned acts for the purpose of sexually assaulting the child. If he or she does so for the purpose of the *sexual exploitation* of a child, he shall be criminally liable. Given the broad definition of "*sexual exploitation*" under Part 1 of the Act,[25] which encompasses and expands upon those offences named above and includes a range of acts such as

"*inviting, inducing or coercing the child to engage in prostitution or the production of child pornography*", the new Act will serve to cover more eventualities, thereby better protecting children. With this proposal, a loophole that has been long since recognised will be addressed. Gillespie noted that where an offender's intention is for the child to touch him or herself, then this would be outside the scope of the soliciting offence as provided for in section 6 of the 1993 Act.[26] Such behaviour would not come under sexual assault, as a child cannot assault itself. With the development of the solicitation offence in the 2017 Act, however, encouraging a child to touch him or herself would presumably come within part (d) of the definition of sexual exploitation, namely "*inducing or coercing the child to engage or participate in any sexual, indecent or obscene act*" and thus will be within the scope of the soliciting offence.[27] Further appropriate amendments to the existing offence include raising the age limit of a child for the purposes of this offence from 17 to 18, as set out in section 3(6), and increasing the maximum penalty that can be imposed on conviction on indictment to 10 years.

Entirely new offences are created in sections 4, 5 and 6 of the 2017 Act. They criminalise the invitation of a child to sexual touching, sexual activity in the presence of a child and causing a child to watch sexual activity. These offences closely follow those contained in sections 10, 11 and 12 of the UK Sexual Offences Act 2003 respectively and serve to criminalise behaviour that has previously gone unpunished in Ireland. Section 4, for instance, similarly closes the loophole discussed above whereby a person cannot be convicted of sexual assault where he/she causes the child to touch him/her, specifically making it an offence to invite a child to sexually touch the offender, themselves or a third party. It is worth noting, however, that a child for the purpose of section 4 of the Act is defined as a person under the age of 15 years. While under the corresponding Head 3 of the General Scheme of the Bill, an offence could be committed under this provision against a child under 18, the Explanatory Memorandum of the Bill states that a child is defined for the purposes of this section as being under 15 years of ages as this offence is effectively a passive form of sexual assault, to which a child under the age of 15 years cannot consent.

At present, the two offences created by the Criminal Law (Sexual Offences) (Amendment) Act 2007 which ostensibly deal with "grooming" remain far removed from the international standards outlined in the Conventions and the Directive. The 2007 Act makes it an offence for any person to intentionally meet or travel with the intention of meeting a child, within the State, having met or communicated with that child on two or more previous occasions, and does so for the purpose of sexually exploiting that child. It also criminalises the same behaviour taking place outside the State, by a citizen or someone who is ordinarily resident in the State. As recognised previously, these provisions do not adhere to international requirements.[28] Both the Lanzarote Convention and the Directive demand that Member States criminalise a proposal to meet a child, made through ICT, where that proposal was followed by material acts leading to such a meeting, for example arranging a place to meet.[29] This essentially prohibits the act of grooming itself, once preparatory acts are taken following initial communication with a child. The criminal conduct is not dependent on the offender actually meeting or travelling to meet the child, as is currently the case in this jurisdiction.

Existing legislation in Ireland fails to adequately protect children as only the effects of grooming are criminalised and not the act of grooming itself. In addition, there is no requirement under international standards for at least two separate contacts as are mandated by the 2007 Act. Indeed no minimum is set in the Convention or Directive.

Section 7 of the 2017 Act ameliorates the existing situation in Ireland, repealing the offences introduced by the 2007 Act. It provides that any person who "*intentionally meets, or travels with the intention of meeting, a child, or makes arrangements with the intention of meeting a child or for a child to travel … having communicated by any means with that child on at least one previous occasion and does so for the purpose of doing anything that would constitute sexual exploitation of the child*" shall be guilty of an offence. First, by providing that the communication with the child may have taken place "*by any means*" explicitly allows for such communication to have been made through the internet, mobile phones and social media. This amendment is beneficial for the purposes of child protection as it can be understood as including offline contact as well as contact through ICT, thereby covering both eventualities. Secondly, the section provides that it is not solely the offender who must travel to meet the child or make such arrangements. If the offender makes arrangements for the child to travel, for example sending the child money for a taxi, the offence is satisfied – strengthening a weakness of the current legislation. Thirdly, the addition of the phrase "*makes arrangements with the intention of meeting a child*" can be seen as incorporating the requirements of the Directive. No longer is the commission of the offence only complete upon the person actually meeting the child or travelling to do so, making arrangements to meet is sufficient. This does not have to be predicated on two previous contacts, as is presently the case. If the offender has communicated with the child by any means once prior to meeting, travelling to meet or making arrangements to meet, he falls within the offence. Again, therefore this development is to be welcomed as it strengthens the existing offence in Irish law.

A notable gap in existing Irish legislation has been rectified by section 8 of the 2017 Act. At present, sexual exploitation that takes place entirely online is not prohibited in criminal legislation. As discussed above, an offline meeting is required for an offence to take place under section 3(2A) and 3(2B) of the 1998 Act, as inserted by the 2007 Act. A situation where a child is encouraged by a predator to send pornographic images of themselves online or through their mobile phones is not explicitly dealt with in current statutes and Irish law has until now been silent with regard to a situation where an offender exposes themselves through ICT to a child without attempting to solicit reciprocal behaviour from the child. Specific offences addressing the sexual exploitation of children carried out solely through the use of information and communication technology were not provided for in Ireland and are greatly needed. Section 8(1) of the Act addresses this lacuna in the law and provides that it is an offence for a person to communicate with another person, including a child, through ICT where the purpose of the communication is to facilitate the sexual exploitation of a child by that person or another person. In addition, section 8(2) provides that sending sexually explicit material to a child under 17 by means of ICT is criminalised. Given the real danger of online sexual

exploitation, the developments that seek to be implemented by section 8 of the 2017 Act demonstrate a practical and stringent approach to criminalising predatory behaviour using the internet and other communication technologies.

Criminal Justice (Victims of Crime) Bill 2016

In December 2016, the Criminal Justice (Victims of Crime) Bill 2016 was published. Hailed as a landmark new Bill, Minister Frances Fitzgerald stated that it has been introduced to "*strengthen the rights of victims of crime and their families, to ensure that victims and their needs are at the heart of the justice process and that rights to information, advice and other appropriate assistance are met effectively and efficiently*." For the first time in Ireland, the Bill seeks to put the rights of victims of crime on a statutory footing and the place of victims in the criminal justice system is being explicitly recognised. This welcome development follows a definite movement on the part of the State in recent years towards greater acknowledgement of the victim within the criminal process and mirrors significant developments in this regard at EU level.

In criminal prosecutions, it is the State that assumes the role of the victim - crimes being viewed as wrongs against the State. The effect of this is that the person against whom the crime is perpetrated is often reduced to being a mere witness in the case. While this long-standing position remains in place, the Victims of Crime Bill aims to assist in promoting the involvement of victims at all stages of the criminal process, thereby preventing the victim from becoming lost through the course of criminal proceedings. At present, victims' rights in Ireland are governed by the Victims Charter. This is not legally binding and it provides no legal entitlements or rights to victims. There are some special provisions for vulnerable witnesses, including victims, in existing criminal legislation which go some way toward protecting victims of crime at a trial, but their remit is currently quite limited. The Criminal Justice (Victims of Crime) Bill 2016 is therefore to be welcomed for its progress in the area of victims' rights.

International Developments

Recent decades have seen increasing developments with regard to victims as a class of persons within the criminal process.[30] In 1985, the *United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power* was adopted by the UN General Assembly. While not a legally binding document, it sets out the basic principles of treatment for crime victims, urging access to judicial and administrative processes and restitution, compensation and assistance for victims. The emphasis on victim's rights continued and in 2001, the Council of the European Union adopted a *Framework Decision on the standing of victims in criminal proceedings.*[31] Designed to give victims the best legal protection and defence of their interests regardless of the EU Member State they are in, this Decision required all Member States to align their legislation to guarantee victims certain defined rights and supports. European developments culminated with Directive 2012/29/EU (Victims' Directive) of the European Parliament and of the Council establishing minimum standards on the rights, support and protection of victims of crime. The Victims' Directive replaces Council Framework Decision 2001/220/JHA and was adopted on 25th October, 2012.

Victims' Directive

Directive 2012/29/EU provides extensive rights for crime victims within the criminal process, seeking to ensure that all victims benefit from minimum standards, support and protection throughout the EU. A "*victim*" is defined as a natural person who has suffered harm, including physical or mental injury, emotional suffering or economic loss directly caused by a criminal offence. Family members of a person whose death has been caused by a criminal offence also come within the definition of a victim. It is worth noting that Article 1 of the Directive makes specific reference to children as a special category of victims. It states as follows; "*Member States shall ensure that in the application of this Directive, where the victim is a child, the child's best interests shall be a primary consideration and shall be assessed on an individual basis. A child-sensitive approach, taking due account of the child's age, maturity, views, needs and concerns, shall prevail. The child and the holder of parental responsibility or other legal representative, if any, shall be informed of any measures or rights specifically focused on the child*."

Chapter 2 of the Directive governs the provision of information and support to victims. In relation to the provision of information, certain rights of victims are set out, including the right to understand and be understood (Article 3), the right to receive information from the first contact with a competent authority (Article 4), the right to receive written acknowledgment of their complaint (Article 5) and the right to receive information about their case (Article 6). The purpose of these Articles is to ensure that victims obtain sufficient information in a form which is easy for them to understand and enables them to fully access their rights. Member States are to ensure that communications with victims are given in simple and accessible language and such communications should take into account the personal characteristics of the victim, including any disability which may affect the ability to understand or be understood. Articles 8 and 9 require Member States to ensure that victims have access to support services, including specialist support services, free of charge, acting in the interests of victims before, during and for an appropriate time after criminal proceedings.

These victim support services must provide information, advice and support relevant to the rights of victims. This includes information and advice on accessing national compensation schemes for criminal injuries and on the role of victims in criminal proceedings including preparation for a trial.

In relation to the participation of victims in criminal proceedings, Chapter 3 of the Directive identifies a number of important rights for victims. These include the right to be heard during criminal proceedings (Article 10), rights in the event that a decision is taken not to prosecute (Article 11) and rights directed towards safeguarding the victim in the context of restorative justice services (Article 12). Chapter 4 of the Directive concerns the protection of victims and recognises that certain victims have specific protection needs. Article 18 requires Member States to endeavour to ensure that measures are available to protect victims and their family members from secondary and repeat victimisation and on a practical level, Article 19 requires necessary conditions to be established to enable the avoidance of contact between victims and the offender. In particular, new court premises are required to have separate waiting areas for victims.

During the course of criminal investigations, victims must be protected. In this regard, Article 20 requires interviews with victims to be conducted without unjustified delay after the complaint has been made and it mandates that the number of interviews with victims be kept to a minimum. To identify the specific protection needs of persons, Article 22 denotes that Member States ensure that victims receive a timely and individual assessment, in accordance with national procedures. This assessment is to determine whether they would benefit from special measures in the course of criminal proceedings, as provided for under Articles 23 and 24 of the Directive, due to their particular vulnerability to further victimisation or intimidation. The Directive presumes that child victims have specific protection needs, but still requires children to be subject to an assessment to determine whether and to what extent they would benefit from the special measures in Articles 23 and 24.

In Article 23, pre-trial special measures require interviews with victims to be carried out in premises designed for that purpose, by or through professionals trained for that purpose. All victim interviews should be conducted by the same person, where possible, and all interviews with victims of sexual violence, gender-based violence or violence in close relationships must be conducted by a person of the same sex of the victim, where the victim so wishes. During court proceedings, measures must be taken to avoid visual contact between victims and offenders by appropriate means and measures are to be taken to ensure that the victim may be heard in the courtroom without being present. Other means of protecting victims required by the Directive include measures to avoid unnecessary questioning concerning the victim's private life not related to the criminal offence and measures to allow a hearing to take place without the presence of the public. While Article 23 is general in nature, Article 24 deals specifically with child victims. In addition to the aforementioned measures provided for in Article 23, it states that where the victim is a child, in criminal investigations all interviews with the child victim may be audio visually recorded and such recorded interviews may be used as evidence in criminal proceedings. Furthermore, it provides that a special representative may be appointed for a child victim where the holders of parental responsibility are precluded from representing the child victim or where the child victim is unaccompanied or separated from his or her family.

Finally, Chapter 5 of the Directive concerns the training of practitioners. Its purpose is to ensure that public officials who are likely to come into contact with victims receive both general and specialist training to a level appropriate to their contact with victims. This training aims to increase their awareness of the needs of victims and to enable them to deal with victims in an impartial, respectful and professional manner. The detailed content of the Victims' Directive with its specific recognition of the vulnerability of child victims is to be welcomed. It provides a clear means of addressing the justice needs of child victims, rather than simply increasing the range of criminal offences and the severity of penalties. Overall, it represents an important move toward the emphasis on victims as opposed to conventional legal responses which have often focused solely on "symbolic justice" by way of increased convictions.[32]

While the Directive is directly effective in Irish law as of 16th November, 2015, its implementation is to be carried out through the Criminal Justice (Victims of Crime) Bill 2016.

As previously stated, at present, victims' rights in Ireland are governed by the Victims Charter. This is not legally binding and it provides no legal entitlements or rights to victims. It is thus recommended that the Criminal Justice (Victims of Crime) Bill 2016 be expedited and treated with priority as it moves through the Oireachtas to ensure that the existing uncertain status of victims be ameliorated as soon as possible. This is particularly important in light of Ireland's obligation to transpose Directive 2012/29/EU. In accordance with Article 27 of the Directive, Member States were to have brought into force the laws, regulations and administrative provisions necessary to comply with the Directive by 16th November, 2015. The deadline has therefore passed some time ago and Ireland must begin to rectify this unacceptable delay.

1 Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights', Innocenti Discussion Paper No. 2016-01, UNICEF Office of Research, Florence, 2016.

2 Brian O'Neill, Simon Greha, Kjartan Ólafsson, 'Risks and safety for children on the internet: the Ireland report', (LSE, 2011) <http://arrow.dit.ie/cserrep/22/> accessed 27 October 2016, 7.

3 *Ibid.*

4 Articles 19 and 34 .

5 United Nations Committee on the Rights of the Child, *General Comment 13: The Right of the Child to be Free from All Forms of Violence* (2011, CRC/C/GC13) at para. 12.

6 *Ibid*., at para. 21(g).

7 *Ibid*., at para. 25.

8 *Ibid*., at para. 31.

9 *Ibid*., at para. 41.

10 At EU level, see generally, Verónica Donoso, *Assessment of the implementation of the Safer Social Networking Principles for the EU on 9 services: Summary Report* (European Commission, Safer Internet Programme 2011).

11 Opened for signature November 23, 2001, CETS 185, entered into force 1 July 2004.

12 Opened for signature October 25, 2007, CETS 201, entered into force 1 July 2010.

13 Council of Europe, Convention on Cybercrime Explanatory Report (Council of Europe 2001) at para. 93. The pending legislation will address this issue.

14 Article 9(3).

15 Council of Europe, *supra* note 13, at para. 104.

16 *Ibid.,* at para. 103.

17 See generally, Susan H Bitensky, 'Introductory Note to Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse' (2010) 49(6) *International Legal Materials* 1663.

18 *Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse Explanatory Report (Council of Europe 2007)* at paras. 4-24.

19 Bitensky, *supra* note 17.

20 *Ibid*., and Council of Europe, *supra* note 18, at para. 112.

21 Council of Europe, *supra* note 18, at para. 140.

22 LRC 116-2016 Report on Harmful Communications and Digital Safety.

23 Dr. Geoffrey Shannon, *Fourth Report of the Special Rapporteur on Child Protection* (2010) at p. 114.

24 Criminal Law (Sexual Offences) Act 2017, section 7.

25 The definition of "sexual exploitation" contained in the Act is broadly the same as the existing definition of "sexual exploitation" contained in section 3(5) of the Child Trafficking and Pornography Act 1998 Act, as amended, with minor amendments. Indeed, section 10 of the Act amends section 3(5) of the 1998 Act to bring it in line with the definition in section 2 of the 2017 Act.

26 Gillespie, *Sexual Exploitation of Children* (2008) at p.121. The Law Reform Commission similarly recognised this loophole in its 1990 Report on Child Abuse.

27 In any event section 4 of the Act explicitly creates a new offence of inviting a child to sexually touch the offender, themselves or a third party.

28 See Dr. Geoffrey Shannon, Seventh Report of the Special Rapporteur on Child Protection (2014) at p.137.

29 This provision is contained in Article 23 of the Lanzarote Convention and Article 6(1) of the Directive.

30 See Dr. Geoffrey Shannon, *Fifth Report of the Special Rapporteur on Child Protection* (2012), section 3; and Geoffrey Shannon, *Second Report of the Special Rapporteur on Child Protection* (2008), section 1.4 for discussions in relation to victims' rights internationally and in the EU.

31 2001/220/JHA.

32 See Geoffrey Shannon, *Fifth Report of the Special Rapporteur on Child Protection* (2012), section 3.

Cyberlaw and Offending in Employment Context

Pauline Walley, SC

Pauline Walley SC delivered the above named presentation. ACJRD is grateful for her contribution to the conference.

CONFERENCE WORKSHOPS

1. Victims, Victimisation and Terrorism: the Myths, Motives and Assumptions

Presenter: Dr. Orla Lynch, Lecturer in Criminology, University of Cork
Chairperson: Jim Mitchell
Rapporteur: Megan Coughlan

Firstly, given the theme of the talk, one of the most important issues to clarify is the concept of terrorism. In order to better understand the concept of terrorism, it is helpful to draw from lessons in the study of crime. One major lesson in the study of crime is the fact that victims of crime may also be perpetrators of crime. While this lesson is not evident to the same extent in terrorism, it is helpful to look at the study of victimisation to gain a better understanding of terrorism. In Spain, for example, legislation recognises victims of terrorism and this clearly separates victims from perpetrators. However, in Northern Ireland this distinction is less clear cut. These examples emphasise the highly politicised nature of terrorism and given this, terrorism as a concept is extremely difficult to clarify given its inherent association with politics; it is extremely difficult to strip away political associations. A more beneficial approach to understanding terrorism may be to look at the individual terrorist rather than overall terrorism, as we can learn about an individual, and understand terrorist acts at that level. What is evident is that terrorism reflects the shared beliefs of a large population, for example Al Qaeda focuses on the treatment of Muslims internationally. What is difficult to ascertain is when these beliefs turn into violence.

Terrorist groups tap into shared beliefs or understanding or identity. Overall, terrorism is a communicative act whereby violence is used to send a message. There are no theories of terrorism but looking at the individual terrorist, a number of steps can be identified which are involved in the process of becoming a terrorist. Firstly, there has to be an opportunity to get people involved. Secondly, terrorism needs a supportive community and therefore people through their social, peer or family networks become involved in terrorism - this includes online activity. Thirdly, the idea of culture and history is very important as they can create a narrative of victimhood/grievance which then can be used to frame terrorism. However, this idea of ideology is problematic as radicalisation can exist with or without ideology, in some cases violence comes first, then an ideology is developed, in other cases ideology is secondary and people become involved in terrorism for its oppositional stance. Fourthly, there is a link to petty crime and involvement in terrorist causes, the terrorist is most likely to be 99% criminal and 1% violent extremist.

Having established an individual as a terrorist (and all of the issues inherent in this process), a key question is, how does that individual become radicalised? Radicalisation seems to be a key part of terrorism and can be described as a two part process of the cognitive (i.e. being willing to carry out violence) and the behavioural (i.e. actually doing violence) which leads an individual from non-violent to violent extremism. Radicalisation is often understood using the notion of grievance or victimisation which can be

seen in some cases as the root causes of terrorism. However despite this understanding there are still difficulties with the idea of radicalisation as well as the root causes. For terrorists therefore, there appears to be no straightforward pathway towards radicalisation. What is important to recognise however is that terrorism is often made up of a small fringe group and it is wrong to associate that fringe group with the main group, for example the danger of associating all Muslims with Al Qaeda. Furthermore, publically there is a fear that radicalised thoughts lead to behaviour and people have stopped differentiating between the two which is also a dangerous myth for people to believe.

Given limited knowledge about the processes which are involved in becoming a terrorist and becoming radicalised, learning from other fields is essential to try and further understanding of terrorism and to prevent it. Risk assessment tools have been produced to predict terrorism. However, terrorism, like other complex human behaviours cannot be predicted, as they likely lead to a significant degree of false positives. One of the recent ways in which reacting to terrorism is necessary is online, due to online supportive communities which can be implicated in radicalising people. However, the likelihood of radicalisation in isolation in very low, approximately, 3-6% of individuals are reported to have been radicalised online. However, the internet can create opportunity which is a significant step towards terrorism. It also can create online networks, relationships which are initially normal and non-radicalised but which become criminalised and this is the second step towards terrorism. Governments are reacting to these online supportive networks by creating online counter narratives to prevent radicalisation and show that they care about groups but really, these initiatives cannot compete with radicalised networks.

Overall, people appear to undergo four steps to become a terrorist: opportunity, social networks, culture or history, and crime. Understanding how radicalisation occurs is more complex as we do not yet understand how an individual moves from being non-violent to being willing to carry out violence and then to actually committing violence. What is really important to stress is that main groups should not be associated with small fringe terrorist elements. It is crucial to distinguish between the two groups. Moving forward, terrorism cannot be predicted. Therefore, in order to prevent it, strategies need to be proactive and focusing on online activity and its interactivity with other elements in an individual's life may be appropriate.

2. Cyberbullying in Young People: Behaviour, Experiences, Resolutions

Presenter: Rebecca Dennehy
Chairperson: Aisling Kelly
Rapporteur: Eret Haava

Over 80% of young people own at least one form of media technology. In most cases, information and communication technology offers them many positive social and learning opportunities, such as connection with their peers, friends and family. Technology, unfortunately, also has a dark side. It has been used in a negative way to cause harm, bullying, intimidation and to harass. This new technology orientated phenomenon, cyberbullying, has become a social problem, which is associated with

emotional stress, anxiety, low self-esteem, substance abuse, suicidal ideation and suicidal behaviour. On average 20-40% of young people report being a victim of cyberbullying. Therefore it is very important to address this problem because of the negative impact on young people.

There is no consistent definition for cyberbullying. So the question is, how can we move forward if we don't know what it is or what are we dealing with? Current definitions of cyberbullying are based on our understanding of traditional bullying, which is characterized as *"…when a person or group engage in any negative action intended to inflict harm or discomfort on another"* and where three necessary components - intention, repetition and power imbalance - are required to take place. Cyberbullying, which is also called online harassment, online aggression, internet bullying and online bullying, is characterized as *"…wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices"*. There are three unique features which separate cyberbullying from traditional bullying - it is far more pervasive (traditional bullying stays at the school gate but cyberbullying follows you home from school, there is no escape for victims, there is no getting away, they are accessible anytime of the day through different media), it affords anonymity (some people who usually don't engage in bullying will get involved with this type of aggression because of the anonymity, behind the screen people might do things they usually don't do because they can't see the result or the damage they do) and it is poorly regulated.

Cyberbullying is usually carried out by using two media sources - phones and internet. It is disseminated by phone calls, text messages, pictures and videos, emails, chat rooms, instant messages, websites, online gaming, blogs and social networks, where Facebook, Twitter, Instagram and Snapchat are the most popular mediums. There are seven categories of behaviour in cyberbullying

- flaming (sending hurtful, vulgar, aggressive messages)
- harassment (which is ongoing, repeated over time)
- impersonation (pretending to be someone else online to cause harm and discomfort, setting up fake account with someone else's picture)
- outing and trickery (putting someone else's personal/sensitive information out, tricking people into giving that information and then posting that by themselves to cause harm)
- exclusion (purposely excluding someone from an online group/network)
- denigration (putting out false or cruel statements online)
- cyberstalking (repeated threats, repeated aggressive acts online)

The contents of aggressive messages involve threats towards home and family including death threats, abusive or hate related speech, name-calling, sexual acts, demands/instructions (blackmailing), and menacing chain messages.

A recent study, which was conducted by Vodafone and which involved 5000 young people between the ages 13-18 from eleven different countries, revealed that one in four teenagers have been victims of cyberbullying in Ireland compared to one in five elsewhere. Because of its potential negative impact of the mental and physical health of young people and the link between depressive symptoms, self-harm and suicidal thoughts, which is much higher among victims of cyberbullying than traditional bullying, it has become a key

issue among parents, teachers, researchers and legislation makers.

In academic literature there are many guidelines to follow while working with young people. In schools there are programmes to deal with cyberbullying, its causes and different methods of how to avoid/stop it. However most of the research, which led to the resolution how to avoid/stop it, has been done by using quantitative methods. Therefore Rebecca Dennehy's currently in-progress, qualitative research (CY:BER Study) on young people's experiences and perspectives on cyberbullying might offer a fresh and more successful approach how to tackle the problem from a young person's perspective.

"We think that we know what is going on but the reality is as soon as we, adults, leave school, as soon we move on, we are out of touch with the reality of young people. Involving young people in research, gives us contemporary insight into what is going on and gives us access. It is the right for young people to be involved in matters which affect them anyway."

There are four schools (an all-girls school, an all-boys school, a mixed DEIS school, a mixed private school) in East Cork who are taking part in the CY:BER Study. Because the role of age and gender in cyberbullying is not clear, the selection gives a mix of different backgrounds, age and gender, and gives a better chance to look at the problem from different viewpoints. The Youth Advisory Group to the CY:BER Project, which is called #Soci@lSesh, consists of 16 participants from those four schools and a local youth worker. There will be five sessions held in a local youth centre over the course of the school year. Because "knowledge is power", the Youth Advisory Group was provided training on public health, basic research methods and different methods of data collection. In the first session when they were asked about their first thoughts on cyberbullying, the answers varied - depression, anonymous, abusive comments, not being safe, laughed at, social media, hurtful, being trapped in your own home, damages people mentally. At the moment their opinion is that cyberbullying is not going to stop and rather than trying to prevent it, the focus should be on helping to cope with it and how to better manage it.

Discussion

- Are the numbers in cyberbullying higher in Ireland because of the Irish *"sense of community, social engagement and sense of humour"*? It was acknowledged that this might be the case, but because most of the research has been done using quantitative methods, looking at prevalence and different behaviours, the appropriate questions have not been asked, so there is no data to support this.
- Should we keep focusing on coping mechanisms rather than changing behaviour? It was emphasised that the purpose of CY:BER Study was to establish what young people think and want in relation to cyberbullying. If they identify that they need to learn how to cope better and how to manage better, then that's what the study will recommend to be focused on.
- Should it be the responsibility of providers on devices and software to control cyberbullying? Technology isn't going away, so even reporting by providers and software giants would be a great success.
- A question was raised about criminalising cyberbullying. It was highlighted that current legislation is

not really up to date to address this problem. The legislation which is used at the moment - Postal and Telecommunications Services Act, 1983 (sending offensive messages) - is more than 30 years old. Because cyberbullying is ongoing, emerging and constantly developing, the legislation should be brought up to date. We have to identify the problem, label it, and indicate its seriousness. But we have to bear in mind - do we want to criminalise every single offence? There should be interventions put in place before criminalisation. Therefore, we should engage in restorative justice, get young people involved, so they can understand the harm they are doing and the consequences of cyberbullying behaviour.

The majority of those present at the workshop acknowledged that cyberbullying is a serious problem and harmful to the physical and mental health of young people. Previous researchers have shown that if we involve young people in things which directly impact them, the results will be more successful and outcomes will be more positive. We should learn from these findings and include the voice of young people, because without their perspectives these issues will never be properly understood by stakeholders such as law enforcement, health and caring agencies, counselling services etc.

3. Cybercrime and Civil Liberties

Presenter: Dr. T.J. McIntyre, Chair, Digital Rights Ireland, and University College Dublin Sutherland School of Law
Chairperson: Supt. Tony O'Donnell
Rapporteur: Kaleb Honer

Outline
The fight against cybercrime presents novel civil liberties issues which the law has been slow to address. It strains the ability of the legal system to adapt. The relevance of this issue is heightened in Ireland due to the presence of many EMEA (Europe, Middle East and Asia) headquarters of internet firms, such as Facebook, Google, Microsoft, Twitter and Apple. As a result, the scope of Irish Law is extended to millions of users worldwide.

Effective protection against cybercrime is itself a civil liberties issue
The case of KU v Finland (Application no. 2872/02) is highly relevant as it highlights the conflict between cybercrime enforcement and civil liberties protection. The primary point of the case addressed a concern relating to an infringement of the applicants ECHR Article 8 right. The court found that national law was not effective to allow the identification of users.

Increased use of self-regulation undermines constitutional constraints
Self-regulation of online intermediaries is a common response to cybercrime. Intermediaries are primary actors in the field. Additionally, automated systems are in place, which seek to remove infringing content from platforms. A prime example of this is YouTube's Content ID system. The question then arises - where does the rule of law stand in this self-regulatory environment? Should intermediaries' policies reflect fundamental legal principles such as transparency and the ability to appeal a decision?

Internet blocking as a case-study
Internet blocking is an ideal case study for the issue of civil liberties in the fight against cybercrime as it brings together key developments in the field; automated

enforcement, intermediary regulation, self-regulation and mass surveillance.

This method of enforcement is already in wide use in Ireland in a statutory (i.e. the blocking of file sharing sites) and non-statutory capacity (i.e. child protection filters). Mobile phone industry blocking of child abuse images is the most prominent example of the non-statutory use of internet filtering. The then Minister for Justice and Equality, Alan Shatter, summarised this agreement as:

"*All mobile phone operators in Ireland, under a voluntary agreement brokered by the European Commission with GSM Alliance Europe, an association which represents European mobile phone operators, implement a form of filtering on their mobile Internet services which prevents access to websites identified as containing illegal child pornography*." (Alan Shatter TD, 13/4/2011)

What issues does internet blocking present? In essence, the issue can be summed in three distinct categories; fundamental rights, transparency/ accountability, and more general concerns. In relation to fundamental rights, the most evident issues related to the legal basis of internet blocking, whether such actions would satisfy a proportionality test, are fair procedures implemented, and does such an approach have an impact on vulnerable groups of individuals? Regarding transparency, there are issues relating to whether users are notified of blocking, if there are remedies available for users and the potential for function creep. Lastly, this method of enforcement demands an increase in surveillance of users' activities and requires draconian anti-circumvention.

How is web blocking implemented?

Web blocking is generally implemented in one of three ways:

- Blocking by Internet Protocol (IP) address e.g. 129.22.8.51. This blocks all sites, legitimate and criminal, hosted on a particular server.
- Domain Name System blacklisting ("DNS poisoning"). This blocks all content hosted on a particular domain name, even content which is unrelated to the material targeted. It often also impacts on unrelated services such as email. This has been used in, for example, Finland and Pennsylvania.
- Uniform Resource Locator (URL) blocking. This blocking occurs at full URL level. It is more expensive and therefore has historically been less commonly used. This has been pioneered in the UK in the so-called Cleanfeed system. This is sometimes termed hybrid blocking in that its implementations usually combine DNS blocking or IP blocking with some form of deep packet inspection.

The impact and proportionality of blocking varies hugely between these technologies, but policymakers appear to have little awareness of the issues which these technical choices present. In each case blocking systems are relatively easily evaded - again, however, there is relatively little understanding of their limitations or the fact that *web* blocking systems are ineffective to block other protocols (such as file sharing).

Fundamental rights standards

The European Convention on Human Rights is highly relevant when addressing the filtering of content online. The following rights in particular must be taken into account:

- Art. 6/Art. 13 ECHR: Notice, reasoned decision, appeal, redress against wrongful blocking
- Art. 8 ECHR: Privacy in communications, especially re email
- Art. 10 ECHR: Freedom of expression/ access to information

Who has standing to assert these rights? The ECtHR has identified Art. 10 as a tripartite right which can be invoked by the speaker, intermediary, and recipient of speech online.

The rights of those seeking blocking are also relevant and Art. 1 Protocol 1 (copyright) and Art. 8 (as elaborated in *KU v. Finland*) have both been invoked to support claims that blocking systems should be used in particular circumstances.

Yildirim v. Turkey (2012)

The case of Yildirim v. Turkey is highly important in relation to online filtering. The pivotal issue of the case was the blanket blocking of access to sites.google.com. The court held that:

"*In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion and the manner of its exercise.*"

As a result, it was found that even where internet blocking was authorised by law, blanket blocking was not proportionate as the ban was not solely targeted at the content in question.

What should we be doing on blocking?

After examining the above case, it is difficult to see a situation where network level blocking is the best option for tackling cybercrime. The civil rights issues presented by such blocking, combined with its ease of evasion, make it difficult to see how such blocking could be necessary and proportionate in a democratic society. However, if such an approach is to be taken the following would need to be accounted for:

- Legitimacy, transparency and accountability
- A legislative basis for any state blocking
- Ensuring that state blocking is brought within ECHR norms
- Work on (civil society) transparency tools
- Tackling problematic private blocking
- Facilitating decentralised and voluntary blocking
- Resisting anti-circumvention measures (bans on VPNs, open Wi-Fi, etc.)

In addition to this, alternatives may be taken, for example removal of the content at the source, and better parental control on mobile devices.

Discussion

- Given the volume of illicit content online, what alternatives are there to an automated process? It depends on the content in question. Judicial determination is possible in cases of child abuse images and the growth of hash value databases provides a model for how this could be done.
- What is the difference between virus scanning and content scanning? End point scanning and scanning with user consent are very different from mandatory network scanning or blocking.
- What if An Post wanted to open all parcels to look for illicit content, would there be a public concern about privacy? Suspicionless searches by state actors are illegal in the offline

context, and it is important to preserve that norm online.

- The Law Reform Commission has proposed a state takedown system for social media content with no input from the author of the content - is there a need for an individual right to appeal takedown determinations? An individual remedy is important, particularly in the context of what is often a subjective assessment.
- What is needed in order to validate these blocking/takedown procedures? Oversight and definitions are needed. Notice and a right to appeal are central, particularly when seeking compatibility with the ECHR.

4. Online Abuse, Harassment and Dating Abuse

Presenter: Margaret Martin, Director, Women's Aid
Chairperson: Vicky Conway
Rapporteur: Kate Moloney

As a victim-centred organisation, Women's Aid works to make women and children safer with one to one services and a court accompaniment service.

Anonymised data collected by Women's Aid highlights that the barriers to seeking help intensify the longer a couple have been together, with 40% of women contacting Women's Aid having been abused for a number of decades. Preventative work with younger women is essential to narrow the gap between initial abuse and contact with support services.

The Impact of Myths and Stereotypes
Myths about domestic violence victims fail to acknowledge that it occurs across every ethnicity, socio economic group and class. Faced with these myths, many women don't identify as victims and may not see Women's Aid as a support for them.

While we need to tackle these victim stereotypes, we also need to tackle the stereotypes of abusers. Often, an abuser is seen as charismatic, interesting or fair, and many people would be shocked to learn that such a person could ever be abusive. Where abusers are considered to be pillars of the community, it can be much harder for women to get help.

2in2u
As a response to queries about how to decide what is healthy in a relationship, Women's Aid built the 2in2u website for young women. It is in a magazine-style "relationship health check", aiming to increase understanding of the signs of an abusive relationship. The focus is "trust your instincts". The website includes case histories based on composites of real women who have come in contact with Women's Aid.

Since www.2in2u.ie went live in February 2011 there have been over 70,000 visits. This is despite funding restrictions which sees the 2in2u campaign advertised around Valentine's Day each year. Paid advertising in bars, restaurants, universities and online is key to bringing the campaign to young women's attention. However, traffic to the website is declining after a 100% cut to the public awareness funding to Women's Aid by the State. Women's Aid is committed to keeping the 2in2u website available and is using other (free) ways to highlight this vital resource. For example, in June 2016, SHEmazing! (www.Shemazing.net) released the results of their dating abuse survey, which highlighted the 2in2u website and resulted in an increase in views.

SHEmazing! surveyed 1000 women between the ages of 18 and 35, showing that one in three women were affected by dating abuse, with 24% experiencing digital abuse.

We have seen an increase in younger women engaging with our services and we have also seen where parents of young women who are being abused often contact the organisation looking for guidance. Another interesting and unanticipated trend of the 2in2u campaign was young women putting their mothers in contact with Women's Aid.

Digital Abuse and Image Based Sexual Abuse

In focusing on younger women, the focus was naturally brought to digital abuse. Often, lies, rumours and images are spread online with the intention of damaging women's reputations. Uploading of videos is often without consent, or even knowledge.

The phrase "image based sexual abuse" which had been discussed throughout the conference was cited here with approval. The phrase accurately depicts what happens and highlights the intermeshing of different forms of abuse online.

One particular case was discussed involving a young woman whose ex-boyfriend had uploaded videos from his webcam to a pornography website. He had also been impersonating her on the website and encouraging sexualised commentary on the video. She went to the Gardaí, but there was no legislation or legal sanction that could protect her. Eventually he was shamed into taking it down, but a huge gap in legislation was highlighted. This woman spoke out and said that she was pleased to see the recent Law Reform Commission recommendations.

Image based sexual abuse often occurs where women are at the beginning of their careers. It causes grave concern that the images will be discovered in a background check. Once something has been uploaded on the internet, it is essentially beyond reach and this level of uncertainty causes an impact that cannot be underestimated. SHEmazing!'s survey showed the long term effects of this kind of abuse, with 93% of women turning to self-harm, with drugs, excessive dieting, exercising and drinking being big issues.

EU Survey

A 2014 EU survey set out wider prevalence levels on cyber abuse for Ireland:

- 12% of women experienced stalking since age 15, and 3% in the 12 months before the survey
- 5% experienced cyber-stalking since age 15, and 2% in the 12 months before the survey, with young women being particularly vulnerable.

Cyber stalking was measured by

- Emails, text messages or instant messages that were offensive or threatening
- Posting offensive comments about them on the internet
- Sharing intimate photos or videos on the internet or by mobile phone

In 50% of the cases the woman's partner (current or ex) was the perpetrator of stalking.

The survey also examined how long the stalking had been going on for:

- 26% had been stalked for over a year
- 35% had been stalked for up to a month
- 37% had been stalked for between a month and a year

STIR (Safeguarding Teenage Intimate Relationships)

This five country study looked at Bulgaria, Cyprus, England, Italy and Norway. It examined the incidence and impact of interpersonal violence in the intimate relationships of young people between fourteen and seventeen years of age, particularly in relation to sending and receiving sexual images.

The study found that 50-66% of young women and 33-66% of young men had experienced interpersonal violence and abuse. The findings on the impact were striking, with 81-96% of young women experiencing negative impact only, but 60-70% of young men experiencing positive or no impact.

- A seventeen year old Italian boy said that *"If a naked picture of mine goes around the web, no problem… for a girl it is different… Her reputation would be in trouble…"*
- A seventeen year old Norwegian girl said that her abuser walks around with her 'whole life' in his mobile phone, ready to share it with anyone at any time.

In all five countries, young people experienced control and surveillance. A major trend was duality of abuse, with control and surveillance occurring both online and offline.

Online control included being instructed on who they could chat to, being forced to share passwords, having text conversations monitored or receiving constant phone calls.

Offline control included limiting contact with friends, telling partners what to wear, turning up uninvited and getting angry or upset if partners wanted to go somewhere without them.

The Need for Education and Awareness

The education system has yet to catch up to concerns about online abuse and "sexting", with no embedded support systems in SPHE curriculum, for example. It is vital that victim-blaming is avoided, while focusing on increasing consciousness of the harms involved. There had been a programme running in boys' schools which was having very good results and was raising issues about consent, but unfortunately was not sustained. The real issue is the lack of understanding among young people about what is normal sexual behaviour. The internet merely provides a forum for abuse that also occurs offline. Age appropriate programmes are needed so that "our children of today are not our perpetrators of tomorrow".

Current campaigns provide grounds for optimism. SpunOut's work on internet safety was discussed as being very effective, and Women's Aid is now partnering with Facebook on launching a guide to using Facebook more safely.

To raise awareness, we must open up conversations. Louise O'Neill's recent book, "Asking for It" about a schoolgirl who was raped at a party, has been extremely effective in that regard. It has been a massive conversation starter and a real vehicle for raising awareness.

Conclusion

Abusive behaviours were prevalent long before the internet. The internet simply provides new tools to carry out and amplify abuse and we need to come to grips with this. It also facilitates abusive behaviours starting much earlier in relationships.

A strong point of concern is the unescapable nature of digital abuse and the psychological impact that this can have on a victim.

Awareness is key to prevention. It will reduce the likelihood of offending, help women to protect themselves online and increase awareness of the support services available so that women will come forward and ask for help much sooner.

5. Towards preventing cyberbullying: Can Irish parents' online facility and perceptions help inform practice? A quantitative study

Presenter: Dr. James O'Higgins Norman, Director, ABC, National Anti-Bullying Research and Resource Centre, and Senior Lecturer and Researcher, DCU Institute of Education
Chairperson: Ursula Fernée
Rapporteur: Jane Mulcahy

This workshop used information from a recent publication by Dr. James O'Higgins Norman and Lian McGuire, MEd, MScPsych "*Cyberbullying in Ireland A Survey of Parents Internet Use and Knowledge*" (2016) Dublin City University

Irish children's use of the internet at home and on mobile devices is well above the European average - 87% v 62%, and 20% v 9% respectively. (O'Neill *et al*, 2011). Although this means that Irish children are more exposed to the risk of cyberbullying, they actually report lower levels of the phenomenon (4% v 6%), according to the EU Kids Online findings.

Cyber-bullying moves beyond the traditional "one to one" sphere of traditional bullying where bully and victim directly interact. Technology provides another avenue of attack where home and personal spaces are no longer safe. The physical space in which young people exist is no longer within the four walls. While a once-off nasty event would not constitute bullying in the real world, in the online environment a once-off upload can frequently take on a life of its own.

Bullying is not an isolated, dyadic affair. It has multiple levels of influence, including:

- Individuals
- Peers
- Bystanders
- Parents
- School and the wider community
- Society

These factors converge to provide the environment for bullying behaviour to thrive, or be prevented. Multi-layered approaches to bullying prevention are more successful than individual interventions alone.

Bronfenbrenner's bio-ecological theory of human development is relevant in this context. Since the internet is present in all areas of a child's life, as well as the lives and structures around them, it also exerts influence at the:

- Mesosystemic level - at both home and school,
- Exosystemic level - as an influence on parents, peers and teachers that may impact on the individual
- Macrosystemic level - as reflector and influencer of societal values and ideologies
- Chronosystem - altering the practices over time of how we work, when we work.

In terms of the importance of parents in preventing and addressing cyberbullying, at the most basic level they provide the technological hardware (computers,

tablets and phones) for children to use and they pay for the internet access. Parents, therefore, have a greater degree of control over their children's internet usage than any other external influence. They also retain the right to monitor and restrict usage as they see fit. Conversely, parents bear more responsibility for monitoring their children's internet usage. When cyberbullying invades the home, there is more of an onus on parents to discover whether a child is being bullied, or doing the bullying, than in traditional offline bullying situations. Parents often opt to notify schools about bullying, or alternatively may decide to deal with it entirely themselves.

Existing research on parents and cyberbullying has involved parent-child pairs (Byrne et al, 2014; Dehue et al, 2008, Mesch, 2009) and tends to approach parents only as adjunct to the child's interaction with the net. It is also fragmented as regards the information garnered from parents, may possibly have been influenced by the parents' awareness that their child is also being surveyed, leading to a more socially acceptable style of answering, and neglects adult supervision and coping (Livingstone & Haddon, 2009, Pg. 28).

The purpose of the ABC study was to analyse a more direct and holistic approach to the experience of Irish parents of using the internet to see what it can reveal about what they think and do about cyberbullying and online risks, and what that might tell us for future work with parents. The research questions included:

- How familiar are parents with the internet and social networks?
- How much do parents interact with their children with regard to bullying and other internet risks?
- What is the nature of parents' knowledge of their children's internet use?
- How confident are parents in protecting their children from cyberbullying and other online risks?
- How familiar/confident are parents with the use of procedures for online safety?

908 parents, of which 89% were female and 11% were male, and whose children were aged between 9 and 16 years, participated in the research. All participants were associated with Parents' Associations across Ireland and undertook a 23 item, segmented, self-report online questionnaire. Since internet access was required, participants were people who were comfortable using the internet themselves. The questionnaire was designed initially as part of an ongoing E.U. Erasmus+ Life Long Learning Project "ParentNets" to be distributed online to parents in Spain, Ireland, Portugal, Romania and Belgium.

Among the key findings of the research, it emerged that the highest level of daily social network usage by parents was on Facebook (55%) and via Texting (61%). The Facebook finding was particularly interesting because this is not where children go to engage online. Children preferred Twitter and Instagram at the time.

As regards bullying, 65% of respondents said they often/always spoke with their children about bullying on the internet, while 16.5% never or hardly ever had such conversations. Parents showed a high reliance on what their children told them regarding their internet activities, with only 18% of parents continuously monitoring their children's behaviour online. Such heavy reliance on the

statements of children about what they're doing online is interesting, because children are not always going to tell their parents the truth. Less than a quarter of parents required permissions for networks, websites or downloads or engaged in blocking.

As an analogy for the lack of parental awareness as to what their children were doing online and their abdication of responsibility for playing a more active role in their offspring's online safety, Dr. O'Higgins Norman likened it to the situation where parents of a small child left him or her unattended in a playground for several hours, while they went off to the pub to enjoy their own fun only to return later to say "*Were you happy? Were you safe? That's ok.*" In Dr. O'Higgins Norman's view, parental abandonment of their children in cyberspace is essentially the same thing.
As regards the risk of cyberbullying, 53% of parents reported that they knew of the risk and were happy their children were safe. 47% of parents were either worried their child was exposed, or weren't sure what the risk involved. 56% of parents forbade the use of the internet with the door closed, but as Dr. O'Higgins Norman observed "*the door is actually on the phone now*". In general, social network filters seemed to provide the most difficulty for parents in keeping tabs on their children.

Discussion
During the discussion about ways of dealing with the complexities of cyberbullying and parents' over-reliance on what children tell them about their internet usage, Dr. O'Higgins Norman cautioned that as a parent or teacher one should never threaten to take away the device: "*taking away the device is the equivalent of locking me in a room back in my day*." The reticence of young people to reveal they are being bullied online often comes down to the fact that their number one fear is that their parent will (a) take away the hand-held device and (b) make the situation worse.

The point was made that parents will worry about their child being bullied but must also remember that their child may also be engaging in the bullying behaviour for a multiplicity of reasons including peer pressure. The importance of teaching young people to be good cyber citizens was highlighted and some information was shared about education initiatives taking place in youth projects.

6. Policing Challenges in Tackling Cybercrime in Ireland

Presenter: Detective Superintendent Michael Gubbins, Garda Cyber Crime Bureau
Chairperson: Doncha O'Sullivan
Rapporteur: Veronica Downey

Introduction
For many years, responsibility for investigating online criminal activity rested with the Computer Crime Investigation Unit, a division of the Garda Bureau of Fraud Investigation. In 2015, the Department of Communications, Climate Action and Environment developed the National Cyber Strategy. It states -
'In recognition of its responsibilities for providing policing and security services to the State, it is envisaged that An Garda Síochána will be in a position to offer appropriate advice and guidance concerning preventative and investigative strategies. It will also be in a position to draw on its liaison relationships with other

security services in identifying emerging threats, vulnerabilities and best practice preventative measures.' (National Cyber Security Strategy 2015-2017)

In addition to the National Cyber Strategy An Garda Síochána developed its own Cyber Strategy document. Resulting from the development of this the Commissioners Modernisation and Renewal Programme established the Garda Cyber Crime Bureau in September 2016. It is a dedicated national unit operating from the Garda Harcourt Street premises and is headed up by Detective Superintendent Michael Gubbins. The unit has responsibility for:

- Forensic Examinations
- Cybercrime Investigation
- International Liaison

The scale of cybercrime

The present scale of online activity is vast. For example, worldwide there are more than 3 billion users, more than 100 billion sent emails daily, more than 7 billion mobile devices and billions of social media users across various platforms. The scale of online criminal activity is likewise vast. For instance, there are more than 300 new cyber threats every minute and the cost in financial terms is estimated at roughly 1% of global income. It is within this busy environment that evidence of criminal activity must be sought.

Types of current cybercrime activity

- **CEO Fraud, Business E-Mail Compromise & Invoice re-direction** Such attacks occur where a criminal impersonates a legitimate business user or hacks a user's email. If successful, a criminal can use this attack to extract valuable information (such as banking details) from other unsuspecting users. People can be reluctant to query activity like this, particularly if the individual being impersonated is in a more senior position to them. Scams such as this can be lucrative, even if the criminal is successful only a small percentage of the time.
- **Distributed Denial of Service Attacks (DDoS)** These attacks operate by flooding a target system (such as an online banking system) with traffic, thus disrupting or preventing legitimate use of the service. Such attacks may be carried out in an effort to extort money from the target or merely to cause disruption to the service. The recent high profile extortion racket masterminded by the group calling itself DD4BC prompted an international response and took two years and significant international co-operation before the perpetrators were apprehended.
- **PABX/International Revenue Share Fraud (IRSF)** A typical example of IRSF might start with a criminal striking a revenue sharing deal with a local carrier in a high-cost destination. The fraudster will then criminally access a VoIP Service provider's network, sending large volumes of traffic through the compromised network to the high-cost destination. The criminal will collect a share of the profit and the innocent party will be left with a large bill. However, if this activity is detected in time, funds can be prevented from going 'down-stream' into the hands of criminals.
- **Ransomware** is malware that is installed on an individual's/ organisation's system for the sole purpose of extracting payment from the victim(s). It acts by preventing or limiting the users' access to their files or computer until the 'ransom' is paid, generally in the form of Bitcoins.

- **Phishing** scams have become more sophisticated. Det. Supt. Gubbins showed samples ranging from the most basic scam to more authentic-looking examples which incorporate drop-down menus or which request answers to security questions.

Future cyber threats

Det. Supt. Gubbins highlighted what he foresees to be the future developments in cybercrime. These include:

- Online extortion
- Exploitation of next generation mobile payment apps
- Ransomware attacks
- Destructive data breach attacks

New attack targets will include ATMs, NFC cards and the Swift Payment System. The increase in the breadth, complexity and volume of threats means that the roles of Data Protection Officers, Chief Risk Officer and Chief Information Security Officer will become more mission critical in business.

Challenges to detection and prosecution

Offences against minors tend to occur on P2P networks and forums on the Darknet, which make them difficult to police. Phishing attacks and DDoS will continue to present a problem due to the victims' reluctance to report, as they prioritise their need to avoid business interruption. Cryptocurrencies such as Bitcoin present a particular challenge for investigators. While the currency has legitimate uses, it is the currency of choice for many criminals and is used in the payment for criminal services, such as receiving payments from extortion victims. Investigation is also hampered by a difficulty in distinguishing between legitimate anonymity and encryption usage, and use for illegal purposes. Det. Supt. Gubbins anticipates that the threat from ransomware will eventually overtake that posed by banking trojans.

Awareness and prevention of cybercrime

Businesses can be more cognisant of their e-commerce/security requirements. Det. Supt. Gubbins highlighted issues such as a lack of digital hygiene (e.g. careless 'dumping' of digital information online), the absence of security by design (in order to make life easy for the customer) and the lack of user awareness. He also drew attention to the work of www.nomoreransom.org, an initiative of Europol and several leading IT companies to disrupt the work of ransomware criminals. Finally, Det. Supt. Gubbins discussed the role which younger people play in committing cyber-crime. He noted that we need to think about how we prevent young people from making the transition from 'curious teenagers' to actual criminals.

Discussion

Participants were curious about the profile of cyber criminals; they recognised that they are not the so-called 'traditional criminal.' It was made clear that cyber criminals can come from any background and merely need access to a computer - hence the need for preventative strategies.

It was suggested that the lack of reporting may be a breach of the Criminal Justice Act 2011 but it was recognised that enforcement could be problematic. Organisations tended to be more willing to report if the crime resulted in an insurance claim that required a PULSE number.

There was also a discussion on how best to distinguish legitimate transactions from potentially criminal ones. Some participants suggested that an online forum to discuss the challenges facing organisations, along with a platform for reporting cybercrime, might be useful. In this regard, it was highlighted that An

Garda Síochána plans to engage with the public through a public awareness campaign in October 2016 that will focus on malware. In addition, it was concluded that companies and organisations need to bring the same mentality to their online security as they currently do to other areas of their business e.g. stock security and recruitment.

7. Online Extremism: Then and Now

Presenter: Professor Maura Conway, School of Law and Government, Dublin City University & VOX-Pol
Chairperson: Supt. Tony O'Donnell
Rapporteur: Clare Cresswell

Violent online political extremism has at least two major aspects. On the one hand, there has been a lot of press about so-called 'Islamic State' (hereafter IS), and the way in which they have used the internet to ramp-up their propaganda activity since establishment of their so-called 'caliphate' in 2014. IS are not the only violent jihadi organisation to maintain an online presence however; every violent jihadist organisation now operating has some online presence. On the other hand, there are a range of other prominent online extremists, besides violent jihadis, also currently active. The extreme right has a longstanding and growing online presence. A variety of online extremisms are therefore the subject of research in our VOX-Pol project (see www.voxpol.eu). Due to time constraints, this presentation is however focused on IS online activity.

Terminology

- *Violent Extremism/Extremists* - use this term to describe extremisms/extremists of whatever type that advocate the use of violence as the way to re-order government, politics, and/or society
- *Violent Jihadism* - An ideology whose adherents aim to reorder government and society through the implementation by violence of Islamic law (i.e. Sharia)
- *Violent Online Radicalisation* - violent online radicalisation is a process whereby individuals, through online interactions and exposure to certain types of internet content, come to see violence as a legitimate method of solving social and political conflicts.

What's the Problem?

Relatively large numbers of Europeans have travelled to Syria and Iraq to join IS. Belgium is a European country particularly affected by this; France also has a high incidence of especially young women leaving to become so-called 'Jihadi brides'. Children (under 18 and mainly male) are also departing from European countries and being used as fighters, suicide bombers, and executioners.

A concern for EU policymakers is that while individuals were originally encouraged to travel to the 'caliphate' and fight with IS there, the main obligation as advocated online now, is for these individuals to carry out attacks in in their European home countries.

History and Background

In the late 1990s, English language websites and forums were used by terrorist groups (e.g. ETA, Tamil Tigers, etc.). This involved a top-down process whereby the groups were in control of what was said on their websites. However, a shift took place from the late 1990s into the 2000s, with a greater emphasis, first, on the use of online forums and, later, social media. These shifts greatly changed

access to information and the ways in which people interacted online.

Web 2.0 (the social web) – is characterised by:

- Social networking (interactivity/ sociality)
- User-generated content
- Digital video - YouTube, Vimeo, etc.

Content is 'king' on the social web and groups such as Al Qaeda established jihadi media production outlets (e.g. As-Sahab and Global Islamic Media Front (GIMF)) to build upon this. These outlets began to produce content in a variety of formats for wide and easy circulation across a variety of platforms and devices. Content included text (e.g. books and magazines), still images (e.g. adverts and screensavers), and videos. Different genres of video emerged: statements, 'sermons', attack footage, beheading videos (e.g. Berg, 2004).

Positive aspects of the social web for extremists

A reliance on social media had both positive and negative aspects for extremists. The positives were that content was easier to locate. No high literacy or language skills (for example, Arabic) were needed and social media is known and attractive, especially to young people. Free 'fan' labour supplied, such as translation, subtitling, etc. Copying and dissemination were easy and direct access to the internet was not required, as content could be distributed via email links and copying of content to VHS, DVD, and mobile phones. Most big releases came in different formats (e.g. for PCs, different types of mobile phones, etc.) and social media platforms cannot generally be shut down in entirety, like online forums could. Whereas forums came under attack from governments and hackers, social media platforms are very difficult for governments to take down and are therefore protected, with a built-in redundancy via the networked structuring of communities.

Negative aspects of the social web for extremists

There were also some negative aspects to this shift to social media for extremists however. This included a loss of the 'top-down' control that extremists had originally wielded through websites. Social media use also enabled the showcasing of internal disputes and disagreements (e.g. al-Shabab; AQ vs. IS - an ongoing public spat between jihadi outfits in Syria). Additionally, there has been increased disruption recently by social media companies of jihad's social media networks (e.g. by Twitter).

IS/ISIS/ISIL

What this organisation has developed is a 'slick' online strategy, which at its height produced a very high volume of output of circa 800-1100 items per month, including photos, videos, audio and text, across a wide variety of over seventy different social media platforms: Soundcloud, Tumblr, Twitter, Ask.fm, Facebook, Flickr, Instagram, JustPaste it, PasteBin, YouTube. Their output is professional in appearance and carefully structured. Examples are the use of aerial drone footage in a number of videos, the high quality graphics displayed in the al-Kasasbeh video, the Cantlie series, and *Dabiq* magazine (Iss. 15 July 2016).

IS/ISIS/ISIL tapped into youth and internet culture, resulting in direct contacts from 'fighters in the field,' the use of pop culture 'hacks' (e.g. selfies, cat pics), hashtag hijacking e.g. #YODO ('You only die once'), development of the *Dawn of Glad Tidings* app, and use of catchy jingles (i.e. *nashid* in their videos). The content is definitely not all gruesome, and pictures showing moody

nature scenes, 'heroic fighters,' and scenes from 'everyday life' are aimed at showing that IS have a functioning state.

What this extremist group has been setting out to do over time is to 'crowd-source' Jihad. They have done this through contents which glamorise the Syrian conflict, especially suicide attacks, and exalts the virtues of the Islamic State. They use content which makes direct exhortations to travel to Syria to become 'foreign fighters', but also encourages committing acts of terrorism in home or third countries and provides practical instructions on how to achieve this. Interaction takes place around the content, with other 'fans' and with 'fighters'. The success of all this is due not only to the technological context but also to the conflict context, with the two contexts combining to produce an immersive online experience for 'fans.'

However, as previously mentioned, Twitter currently has a very serious disruption campaign underway against IS. Forty thousand IS-related accounts were suspended or deleted per month from mid-February to mid-July 2016 and they are also targeting IS hashtags. This means some dislocation to other platforms, but these are less readily accessible. An example is Telegram, a more private communication medium, which is much less trafficked and is less easy for people to find. Whereas law enforcement agencies generally approve of such disruption, intelligence agencies are less so, due to the loss of valuable information.

Conclusion

The intersections of media, information communication technologies (ICTs), and terrorism have a long history and, while IS's success is partially as a result of social media, it is also partially a result of the Syrian conflict. However, significant disruption is now underway particularly from Twitter.

Discussion

Is there any research on why people become involved?

Yes, a lot of research has been done on this. Different motivations are involved. There is a difference, for example, between a local joining Islamic State in Iraq or Syria and somebody deciding to travel to join them as a 'foreign fighter'. Such 'foreign fighters' are not new; people left Ireland to fight in the Spanish Civil War, for example. There is also emerging work now about people leaving the EU to go to fight with the Kurds against IS.

Why is IS encouraging more attacks in Europe rather than encouraging people to travel to them?

IS are under pressure now in Iraq and Syria, so they prefer to see attacks in EU states stepped-up. This is to create

(a) Fear amongst targeted populations, and

(b) Targeting of Muslims to produce more disenchantment on their part and hopefully, from IS's viewpoint, more recruits to their cause.

Are anti-IS groups also on social media?

Yes, many individuals and groups cause disruption by interference through trolling (see e.g. ISIS-chan) and mocking IS hashtags or inserting rubber ducks and other humorous items into IS content. There was also a US campaign 'Think again, turn away' and a series of counter terroristic cartoons called 'Average Mohammed'.

What motivated the Twitter disruption?
Jihadis love to use Twitter so the US government started to put pressure on Twitter. Most academic research is done on Twitter because it is so open.

8. Computer Fraud: How it Happens, and How to Minimise the Risk

Presenter: Andy Harbison, Director - Head of IT Forensics, Grant Thornton Ireland
Chairperson: Pádraig Mawe
Rapporteur: Eoin Guilfoyle

The speaker began by highlighting the extent of the problem that exists today. Using a power point slide he showed the number of records stolen in some of the world's biggest data breaches. He argued that despite huge spending in this area the problem is getting worse. The 'bad guys' have changed. It is no longer young people sitting at home doing some hacking in their spare time. It is now a business. It is a transnational crime. As a result there is now a huge problem with jurisdiction when it comes to investigating and prosecuting this type of crime.

The general process of a hack begins with an external reconnaissance. This involves identifying security vulnerabilities, finding a target to open vulnerabilities and planning the initial attack vector. The next step is the exploitation of the vulnerabilities. The attackers gain access to the system and then protect and cover entry tracks. Then there is the internal reconnaissance. The attackers access further security weaknesses within the system and gather information on the company. The next phase of the process is to execute the attack, using stolen passwords or vulnerabilities in the system. In some instances the final phase involves the selling of the acquired assets. Stolen credit cards, for example, can be "fenced" using sites such as Rescator.cc. The speaker then showed the audience real examples of hacks that have taken place in recent years.

The hiring of hackers or hacking groups was also discussed. These groups can be hired to attack a company or organisation. The hacking of the Microsoft Xbox and Sony PlayStation networks during Christmas 2015 was given as an example of a group demonstrating their power and abilities – essentially advertising their services. The Christmas 2015 hack was carried out by a group calling themselves "the Lizard Squad". These were specialist hackers referred to as "Booters" or "Stressers" who carry out denial of service attacks for hire.

When discussing solutions the speaker emphasised the need to trust, but verify; to have a clear and detailed acceptable use policy; to have privileges and access restricted to only those who need it and to check leavers. It was also stressed to never let any electronic device connect to your network that you do not own. This is because it is very difficult to investigate data theft carried out using equipment to which you do not have legal access. The speaker also highlighted the importance of regular and sufficient training for staff. He argued that an organisation could have the best IT security but if staff are not properly trained (for example not to open emails from unknown sources) then it will do little to prevent attacks. Examples of phishing emails were shown to the audience. They can appear to come from someone within

the organisation or someone closely related to it. The email addresses can look very similar to the real email address of the person it is pretending to be from, but with very slight variations. Another solution which was highlighted was the need to have proper procedures in place, for example, to always phone the person directly if you receive an email asking to have their bank details changed and to ensure there are proper controls in place.

The presentation then moved on to cyber extortion and ransomware. This can occur when an infected email is opened or when an advert is clicked on. The company's files are then encrypted and money is demanded in order to decrypt the files. The solutions given to protect against this type of attack were to back up files offline regularly, to have up to date antivirus, to have file integrity software, to have restricted web-access, and proper awareness and training for staff.

It was suggested that to a large extent we are protecting against the wrong things. Most of the focus is on network attacks while little attention is given to the protection of user devices (workstations, mobile devices etc.). It was also suggested that we are not detecting breaches as we should. Why? Because we do not know what is on our networks. How can you protect what you do not know? It was said that if one does not know what is important then one cannot know what to protect. You end up trying to protect everything equally, valuable or not, which is usually impractical and always wasteful – '*He who defends everything defends nothing*' (Frederick the Great). So, therefore, document management is important. Pick your key assets and protect them. What is easy to defend may not be what needs to be protected and what is easy to justify may not be worthwhile.

The speaker concluded by giving an equation for risk. 'Risk = Severity of Vulnerability multiplied by the Risk of the Vulnerability Arising multiplied by the Countermeasures in Place'. He therefore argued that incident response now matters (incident response planning, incident response training, proper network design and awareness).

Once the presentation concluded a discussion took place between members of the audience and the speaker. Members of the audience shared stories of attacks/attempted attack of their organisations and gave their opinion about what they believe needs to be done to address some of the issues raised. There was a widely held belief amongst many members of the audience that senior management within organisations and companies need to become more aware/involved in these issues and take the necessary steps to ensure that all staff are properly trained.

CONFERENCE ATTENDEES

NAME	ORGANISATION
Taghreed Al Mashari	
Paul Bolger	Ossory Youth
Bridget Buckley	An Garda Síochána
Maura Butler	ACJRD Chairperson
Rebecca Carbery	Ossory Youth
Marion Cerisuela	
Joan Cherry	NIAP
Maggie Clune	PACE
Professor Maura Conway	Dublin City University
Dr. Vicky Conway	ACJRD Council
John Corr	PACE
Megan Coughlan	ACJRD Volunteer
Caroline Counihan	Rape Crisis Network Ireland
Angela Coyne	University of Huddersfield
Clare Cresswell	ACJRD Volunteer
Ms Karyn Cronin	Youth Work Ireland Galway
Siobhán Cullen	Letterkenny I.T
Cliona Curley	Cybersafeireland
Dr Lisa Cuthbert	PACE
Lucile Daidie	
Rebecca Dennehy	University College Cork
Paul Doran	Probation Board of Northern Ireland
Veronica Downey	ACJRD Volunteer
Isolde Doyle	Office of the DPP
Ursula Fernée	The Probation Service
Eileen Finnegan	One in Four
Éimear Fisher	Garda Síochána Inspectorate
Yvonne Furey	Department of Justice and Equality
Sylwia Gryczuk	Youth Work Ireland Galway
Det. Supt. Michael Gubbins	An Garda Síochána
Eoin Guilfoyle	ACJRD Volunteer
Eret Haava	ACJRD Volunteer
Andy Harbison	Grant Thornton Ireland
Robert Hayes	Microsoft Corporation
Dermot Hearne	Irish Prison Service
Valerie Hearns	Roscrea Youth Service
Greg Heylin	COSC Victims of Crime Office
Kaleb Honer	ACJRD Volunteer
Dr Maria Ioannou	University of Huddersfield
Aisling Kelly	
Deirdre Kenny	One in Four
Edmund Lynch	
Dr. Orla Lynch	University College Cork

Garda Susan Malone	An Garda Síochána
Shauna Markey	SAFE Ireland
Margaret Martin	Women's Aid
Pádraig Mawe	ACJRD Council
Professor Anne-Marie McAlinden	Queen's University Belfast
Jenny McGeever	KOD Lyons
Professor Clare McGlynn	University of Durham
Dr. TJ McIntyre	Digital Rights Ireland
Jim Mitchell	ACJRD Council
Kate Moloney	ACJRD Volunteer
Det. Sgt. Michael Moran	INTERPOL
Jane Mulcahy	ACJRD Volunteer
Denis Murray	HSE Adolescent Addiction Service
Eithne Ní Mhurchadha	Etherapy
Superintendent Tony O'Donnell	An Garda Síochána
Tony O'Donovan	Irish Youth Justice Service
Geraldine O'Dwyer	The Probation Service
Dr. James O'Higgins Norman, PC	ABC - National Anti-Bullying Research and Resource Centre
Chief Inspector Robert Olson	ACJRD Council
Dr. Fiona O'Regan	Law Reform Commission
Dr. Catherine O'Sullivan	University College Cork
Doncha O'Sullivan	ACJRD Council
Finbarr Philpott	National University of Ireland Galway
Catherine Pierse	ACJRD Council
Dalila Pinto	Ombudsman for Children's Office
Superintendent Colette Quinn	Garda Office for Children and Youth Affairs
Sgt. Robert P. Reilly	An Garda Síochána
Brian Rowntree	Business Improvement Services
Shirley Scott	Dublin Rape Crisis Centre
Professor Dr. Geoffrey Shannon	Special Rapporteur on Child Protection
Michelle Shannon	ACJRD Council
Dr. John Synnott	University of Huddersfield
Maighréad Tobin	National University of Ireland Maynooth
Lisa Underwood	Houses of the Oireachtas Service
Pauline Walley SC	
Rachel Woods	Department of Justice and Equality

www.acjrd.ie

acjrd

ACJRD would like to thank the staff and offenders of the Irish Prison Service and Arbour Hill prison for their assistance in the printing and design of the report.