Crime prevention policy	
EU- priority	Cybercrime; • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	
Year	

1. Overview of the field

Definition of cybercrime

Cybercrime comprises traditional offences (e.g. fraud, forgery and identity theft); content related offences (e.g. online distribution of child sexual abuse material, hate speech or incitement to commit acts of terrorism); and offences unique to computers and information systems (e.g. attacks against such systems, spread of malware, hacking to steal sensitive, personal or industry data and denial of service attacks to cause financial and/or reputational damage). Electronic devices are also used to sell or transfer all sorts of illicit goods and services, from illicit drugs to online child sexual abuse and exploitation materials to lists of stolen credit card numbers.

Please note that this descriptor is not enshrined in Irish law.

Assessment of trends and developments

Europol's Internet Organised Crime Threat Assessment 2018 outlines the current trends and developments in this area in Europe, including the persistence of ransomware, distributed denial of service attacks, child sexual exploitation and card-not-present fraud.

Similar trends and developments would anecdotally be present in Ireland.

Recent overview of statistics and research

Necessary action has been taken, following enactment of the Criminal Justice (Offences Relating to Information Systems) Act 2017, to ensure that PULSE, the IT system utilised by An Garda Síochána, Ireland's national police force, for the recording of crime, has the capacity to facilitate the recording of data relating to cybercrime. Thus, since September 2018, the capacity of An Garda Síochána to ensure that cybercrime related data is recorded and available for analysis, has been significantly enhanced.

The Law Reform Commission (LRC) undertook a review of the law on cybercrime affecting personal safety, privacy and reputation and in September 2016 published a report on 'Harmful Communications and Digital Safety'. The report made a total of thirty-two

recommendations, including the creation of a number of new criminal offences that relate to harassment online; stalking and the distribution of intimate images without consent. The Harassment, Harmful Communications and Related Offences Bill 2017, a Private Members Bill, addresses these criminal offences.
The LRC also recommended the establishment of a Digital Safety Commissioner for Ireland. The report envisages an Office of the Digital Safety Commissioner for Ireland being established on a statutory basis and having functions related to

- the promotion of online safety
- having legal powers to compel the take down of online material
- publishing a statutory Code of Practice on Digital Safety

The proposed legislation in relation to the appointment of a Digital Safety Commissioner is being dealt with by the Department of Communications, Climate Action and Environment (DCCAE).

The Net Children Go Mobile project investigated access and use, risks and opportunities of mobile internet for children in the European context. The latest survey, conducted in November 2014, shows an increase in both opportunity and risk for children accessing the internet. It also showed that 48% of 11-16 year olds in Ireland had encountered one or more risks on the internet.

The Department of Communications, Climate Action and Environment (DCCAE) have been collecting figures relating to cybersecurity incidents since mid-2017 and intend to publish statistics in 2019.

Other national priorities besides child sexual exploitation, payment card fraud and cyber-dependent crimes?

A General Agreement on the proposed EU Regulation to prevent the dissemination of terrorist content online was reached at the JHA Council in December 2018 and it is now before the EU Parliament. Once adopted, Member States will only have a 12-month period to implement the provisions of the Regulation. The Department of Justice and Equality is currently considering how best to implement the Regulation and if similar arrangements to those set out in the Regulation could be adapted to apply to other forms of illegal content.

The area of cyber security is also important and an updated cyber security strategy is currently being developed, details below.

2. Crime strategy and coordination

Objectives of the crime strategy

An Garda Síochána has a crime strategy, as set out in An Garda Síochána Strategy Statement July 2016 – 2018. An Garda Síochána Policing Plan 2018 commits to developing cybercrime and cyber security strategies in order to enhance ability to prevent and respond to cybercrime and cyber security incidents.

In addition, a new Cybercrime area of responsibility was established within the Crime and

Security Directorate of the Department of Justice and Equality in September 2018.

The National Cyber Security Strategy 2015-2017 was implemented in full. A new strategy is being developed, overseen by a high level interdepartmental steering group. A public consultation document is expected to be published in Q1 2019.

Role of prevention in the crime strategy on state/regional/local level

Ireland has a single national police force and An Garda Síochána Strategy Statement states that "crime prevention is now our number one policing priority with a focus on high visibility patrolling, targeting criminals and preventing crime from happening".

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)

An Garda Síochána has established a dedicated cybercrime bureau, to ensure that An Garda Síochána has the capacity and capability to deal with cybercrime and cybersecurity.

The Garda National Cyber Crime Bureau (GNCCB), under the direction of Detective Chief Superintendent, Garda National Economic Crime Bureau and Assistant Commissioner, Special Crime Operations, has responsibility for the forensic examination of all seized computer media, international liaison with regard to cyber matters and the investigation of cybercrime matters.

Cases examined by the GNCCB include all crime-types, in particular banking and financial crime matters, as well as the examination of equipment and media to assess images in the context of offences relating to child pornography and exploitation.

The continued roll out, on a phased basis, of Regional Triage units, is ongoing; units have been established in the Southern and South-Eastern regions, at Ballincollig and New Ross Garda stations. The triage model provides a tiered response and capability for computer forensic services on a regional basis, utilising locally-based and trained first-responders and cyber triage specialists. The triage model also reduces demands on the central Bureau, while remaining under the supervision of that Bureau. The triage units currently in place are subject to review to inform and establish best practices and processes for the establishment of further such units in other regions.

Implementation of An Garda Síochána Strategy Statement is an operational matter for An Garda Síochána.

Stakeholders (working groups, specialised agencies, partners, etc)

An Garda Síochána recently hosted a first stakeholder meeting in relation to cybercrime, with representatives from government departments and private companies in attendance. An open discussion took place regarding initiatives to combat cybercrime and it is intended these meetings will take place on a regular basis.

The National Advisory Council for Online Safety is a forum for non-governmental, industry,

and academic stakeholders to discuss online safety issues and provide advice to Government on online safety issues.

Ireland is part of the EU Safer Internet Programme, which aims to combat illegal, harmful and predatory use of the internet. As part of the programme, Ireland provides awareness raising, helplines and a hotline. These services are provided by partner organisations, with the Cybercrime area in the Crime and Security Directorate of the Department of Justice and Equality providing coordination.

The awareness raising function is carried out by Webwise.ie, part of the PDST (Professional Development Service for Teachers) Technology in Education in the Department of Education and Skills. It deals with awareness raising, develops materials and programmes for schools and runs the annual event for Safer Internet Day in Ireland.

Hotline.ie is operated by the Internet Service Providers Association of Ireland (ISPAI) and allows members of the public to report suspected illegal content or activities found on the internet.

The Irish Society for the Prevention of Cruelty to Children (ISPCC) runs a helpline (Childline), which provides a 24/7 service where children affected by issues encountered on the internet may turn for advice and guidance.

The National Parents Council (NPC) Primary operates a helpline for parents/adults to deal with issues relating to internet safety. The NPC also provides parents with training courses, both online and face to face.

The above activities combine to help prevent individuals from falling victim to crime, through awareness raising, advice and guidance, and the reporting of illegal content or activities on the internet.

Participation in European/ international networks, working groups, etc.

Webwise are members of the INSAFE network and Hotline are members of the INHOPE network. Webwise contributes information and best practice examples to the EU online platform, Better Internet for Kids. Hotline.ie participates in the dedicated closed platform for hotlines.

The Cybercrime area of the Department of Justice and Equality represents Ireland at all relevant EU and international networks and working groups.

3. Good practices

Overview of recent good practices, prevention programs, etc.

As part of European Cyber Security Month in October 2018, the Department of Justice and Equality and An Garda Síochána coordinated their efforts in order to raise awareness of cyber security. A series of awareness-raising material (supplied by Europol) was posted on DJE's Twitter account, promoting cyber security and highlighting simple steps that can be taken to protect personal, financial and professional data. Topics covered included CEO fraud, invoice fraud, phishing/smishing/vishing, spoofed bank, romance scams, personal data theft and investment scams.

Online safety is being tackled in a coordinated manner by the Government's first Action Plan for Online Safety, which was launched in July 2018. The Action Plan reflects a whole of Government approach and contains twenty-five actions under five main goals. The actions are assigned to six different Government Departments for implementation.

The key objective of the Plan is to set out and implement actions over an 18 month period that are achievable and will have the greatest impact on online safety for everyone in Ireland. Such actions include equipping teachers to embed digital awareness in their practice, supporting student participation in safer internet day activities, promoting best practice standards for quality content for children and strengthening links and processes with industry for removing illegal and harmful material.

Specific examples of good practice are also placed on the Better Internet for Kids portal by the relevant EU Safer Internet partner bodies in relation to awareness raising and helplines.