Online safety.

Opening Statement by the Garda Síochána to Joint Committee on Tourism, Culture, Arts, Sports and Media.

Wednesday, 14th July 2021, from 15.30 to 16.40.

The primary objective of the Garda Síochána in undertaking the many tasks that fall within its remit, is to keep people safe. Throughout its almost one-hundred years in existence, keeping people safe has involved the Garda Síochána devising strategies to prevent people being harmed while traveling on its road networks as pedestrians, on bicycles and within vehicles and through violence that may be inflicted on them in their homes and on our streets, by way of assault, burglary and other such crime that we will all be familiar with.

However as we approach the beginning of our second century in existence, the Garda Síochána is required to be equipped also to keep people safe in the online world where they are connected to others through computer or telecommunications systems, such as the internet, to an ever increasing extent.

Words and phrases now in common usage within law enforcement, such as malicious domain; ransomwar; data-harvesting malware; botnet; cryptojacking, the darknet, were until recently not well known. However, cybercrime is progressing at, what Interpol has described as, "an incredibly fast pace", with new trends constantly emerging. Interpol warns that cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before. The crimes concerned know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

It is essential the Garda Síochána and other law enforcement entities, therefore, keep pace with new technologies, to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime.

The *Commission on the Future of Policing in Ireland* in its report published in 2018, refer to the fact that extortion, fraud, ransomware, child pornography, sexploitation and other cybercrime and internet-enabled crimes are proliferating fast. In this regard, the Commission observed, Ireland is not alone in struggling to deal with the threat.

While we are all vulnerable to being a victim of online related criminal activity, the Garda Síochána recognises that some are more vulnerable than others, including children and old people and this is reflected in the strategies and initiatives it has undertaken to tackle cyber related crime.

The Garda Síochána endeavours to ensure that all personnel throughout the organisation are aware of, and appropriately trained and equipped to participate in an appropriate manner in tackling, online related crime. However, responsibility for ensuring a coordinated approach to tackling the criminality involved is assigned to particular sections and units.

Garda National Protective Services Bureau.

The Garda National Protective Services Bureau (GNPSB) provides advice, guidance and assistance to members of the Garda Síochána investigating sexual crime; online child exploitation; domestic abuse; human trafficking organised prostitution and plays a particular role in supporting victims of Crime. The bureau leads the investigation in more complex cases.

The GNPSB liaises with relevant Government Departments, State Bodies and voluntary groups, embracing the essential multi agency approach to tackling relevant crimes and their causes. The Bureau has provided a wide range of advice for use by adults and children, for the purpose of protecting children from those who target them online and with a view to making relevant contact details available to those who fall victim to such crime.

The Garda National Protective Service Bureau (GNPSB) keep peer-to-peer activity, relating to file sharing of illegal material over private networks, under constant review including through use of particular software tools. In this regard, it has recently undertaken particular investigations targeting relevant criminality, under *Operation Ketch.*

Divisional Protective Services Units (GPSUs) have been rolled out nationwide, by the Garda Síochána. Rollout of these units meets a key commitment in *A Policing Service for our Future*, the four-year implementation plan giving effect to the recommendations of the *Commission on the Future of Policing in Ireland.* The GPSUs participate in protecting people who engage in online activity and in investigating associated criminality.

Ireland's national service for the reporting of suspected online illegal content is Hotline.ie. On receipt of reports, Hotline.ie's Content Analysts examine the content and, if the material is considered illegal, will issue notice and takedown request orders to the appropriate service provider and will notify the Garda Síochána with the relevant information.

Garda National Cyber Crime Bureau

The Garda National Cyber Crime Bureau (GNCCB) was established as the Cyber Crime Investigation Unit in 1991, and re-established as the Garda National Cyber Crime Bureau (GNCCB) in 2017. The Bureau is the national Garda unit tasked with the forensic examination of computer media seized during the course of any criminal investigations. These include murders, cybercrime, online harassment, computer intrusions, child exploitation offences and any criminal investigation in which computers are seized or may contain evidential data. The unit also conducts investigations into cyber dependent crime which are significant or complex in nature network intrusions, data interference and attacks on websites belonging to Government departments, institutions and corporate entities.

The GNCCB is responsible for the prevention, detection, investigation and prosecution of cybercrime incidents in the State. Cybercrime generally involves incidents where the internet, information and communication technology (ICT) systems or digital devices play a significant role in the commission of a criminal offence. The GNCCB works collaboratively with local and national Garda units along with national and international stakeholders to reduce the threat and impact of cybercrime on individuals and organisations.

The GNCCB is staffed by civilian personnel and Garda members of various ranks up to Detective Chief Superintendent. Personnel assigned to the Bureau undergo intensive training in the area of forensic computing and cybercrime investigations, and give expert witness testimony in all types of investigations and prosecutions in court. In addition to its forensic and investigative role, GNCCB acts as a liaison with various partner agencies and law enforcement bodies.

The Garda Síochána has recently increased its dedicated resources in the cyber area and is continuing to grow its capabilities in this area. In recent months, the GNCCB has established regional hubs throughout Ireland, in places including, Cork, Wexford, Galway and Mullingar

Garda National Economic Crime Bureau.

The Garda National Economic Crime Bureau (GNECB) is a specialist bureau that investigates fraud-related crime involving complex issues of criminal law or procedure. The bureau investigates serious and complex cases of commercial fraud, cheque and payment card fraud, counterfeit currency, money laundering and breaches of the Companies Acts and the Competition Act.

The GNECB has been to the forefront in tackling an increase in online related crime experienced during the COVID-19 pandemic, including investment fraud, phishing/vishing/smishing frauds; online shopping fraud; invoice redirect / business email compromise fraud and fraud involving people allowing others to use their bank accounts (money mule). Along with launching criminal investigations relating to the many frauds discovered and reported, the GNECB has engaged in an extensive media campaign designed to alert people to the existence of the frauds, in the hope that they will not engage, online or otherwise, with the criminals involved.

The Garda Síochána interacts with the National Centre for Cyber Security and contributes to ensuring implementation of a number of commitments with regard to cyber security included in the Programme for Government.

In tackling the wide range of online associated criminality, the Garda Síochána enforce provisions within all relevant legislation, including the Criminal Justice (Offences Relating to Information Systems) Act 2017, the Harassment, Harmful Communications and Related offences Act, 2020; the Child Trafficking and Pornography Act 1998, as amended by the Criminal Law (Sexual Offences) Act 2017, the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021 the Prohibition of Incitement to Hatred Act 1989 and Organised crime related legislation within the Criminal Justice Act 2006.

International Cooperation.

European Cybercrime Centre

Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime.

Each year, EC3 publishes the *Internet Organised Crime Threat Assessment* (IOCTA) its flagship strategic report on key findings and emerging threats and developments in cybercrime. The Garda Síochána works closely with the EC 3 unit at Europol in targeting cybercrime impacting on Ireland, that has a European dimension.

Interpol Cybercrime Directorate

The Garda Síochána also utilises the services of Interpol in tackling online related crime. Interpol's cybercrime directorate is working with its almost 200 member countries, private sector partners and cybersecurity communities across the globe in attempting to ensure a robust law enforcement response to cybercrime.