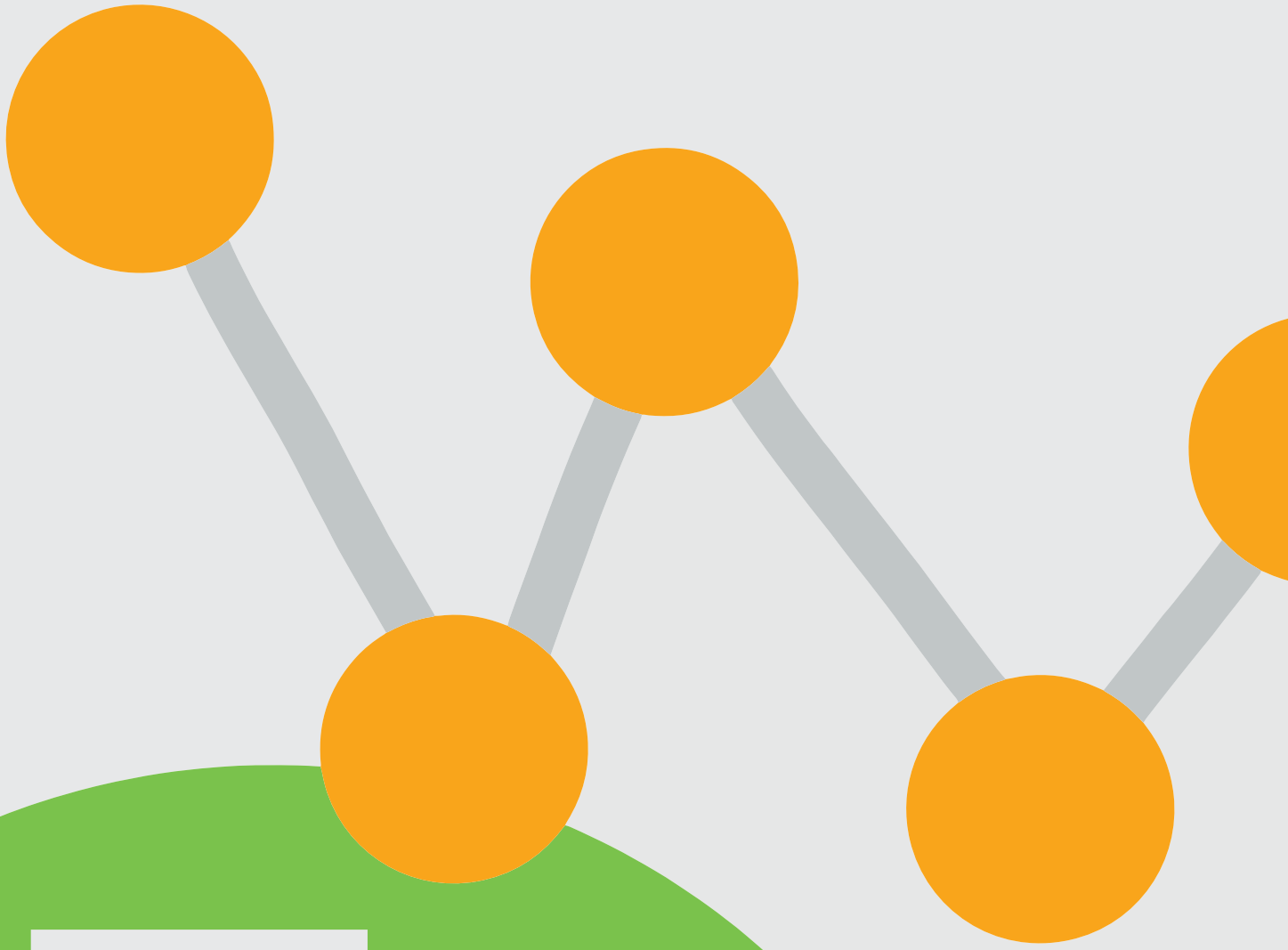


5

Connectivity & Network Resilience

5. Connectivity & Network Resilience

Introduction

5.1 ComReg's strategic intent regarding connectivity is to **ensure that end-users have widespread access to high-quality and secure communications networks, services, and applications**. By 'connectivity' ComReg means having access to the necessary ECN to allow for the use of various services and applications in a secure manner. For ComReg, the connectivity of end-users is not about pitting one network technology against another, but rather the widespread, continuous, secure and high-quality connectivity of end-users.

5.2 The EECC includes a new objective that ComReg, Government and BEREC shall pursue: promote connectivity and access to, and take-up of, very high-capacity networks, including fixed, mobile, and wireless networks, by all citizens and businesses of the Union. In pursuit of this objective, the EECC also restates the need for a balance between providing adequate incentives to invest in VHCN and the need for regulation.

5.3 Today, the connectivity of end-users has become essential to ensuring social and digital inclusion. It is ComReg's view that end-users can only fully participate in society and the wider economy when their connectivity needs are met.

Strategic Intent 3:

End-Users have widespread access to high-quality and secure communications networks, services, and applications.

What does this look like?

- Widespread availability of ECS and ECNs allows for digital inclusion by all consumers
- Connectivity challenges are addressed, and indoor mobile voice services (via mobile connections or Wi-Fi calling) are available to all.
- Networks are secure and resilient.
- EU Objectives for 'Connectivity' of end-users are met.

5.4 There are often a variety of networks, technologies, and solutions available to people to help fulfil their connectivity needs. For ComReg, it is the quality and reliability of ECS/ECN that matters, rather than the means of delivery.

5.5 However, some end-users are poorly served by ECN. Some of these poorly served end-users may not benefit from the presence of multiple different reliable networks. Other end-users may experience poorer services intermittently, due to a range of factors beyond their control.

5.6 Ensuring everyone can access online and digital services, regardless of where they live or how they connect to these services, will be key to driving participation in the digital economy and society. Use cases that require reliable high-quality connectivity such as remote working, education and e-health have become more important for organisations and individuals in the wake of the Covid-19 pandemic.

5.7 There are a number of risks facing Ireland's ECN that could result in service disruption for end users. These issues include equipment malfunction, human error, malicious and cyber-attacks, severe weather events and external incidents (e.g. electricity outages). Accordingly, network resilience, reliability, and security is an area that is becoming more important. ComReg's role in this area is to have a holistic understanding of the nature of the various connectivity risks facing the country. This includes network security, which has now become a key part of the Government's national digital strategy 'Harnessing Digital - The Digital Ireland Framework'.

5.8 While ComReg will continue to use its regulatory powers to address network issues, in some cases, where the appropriate regulatory powers are held by other authorities, a multi-agency approach will be required. ComReg will continue to support other responsible authorities (e.g. DECC) and act as a knowledgeable regulator by making informed contributions to policy discussions and debate.

Network Coverage

5.9 There are still areas of Ireland that are unserved by high-quality and reliable ECS / ECN. These areas are almost all rural areas with a low population density. As population density decreases, the distance between premises generally increases, thus increasing the cost of deploying ECN. Therefore, it is not always economical for commercial ECN operators to deploy high quality, reliable networks in these areas without additional incentives.

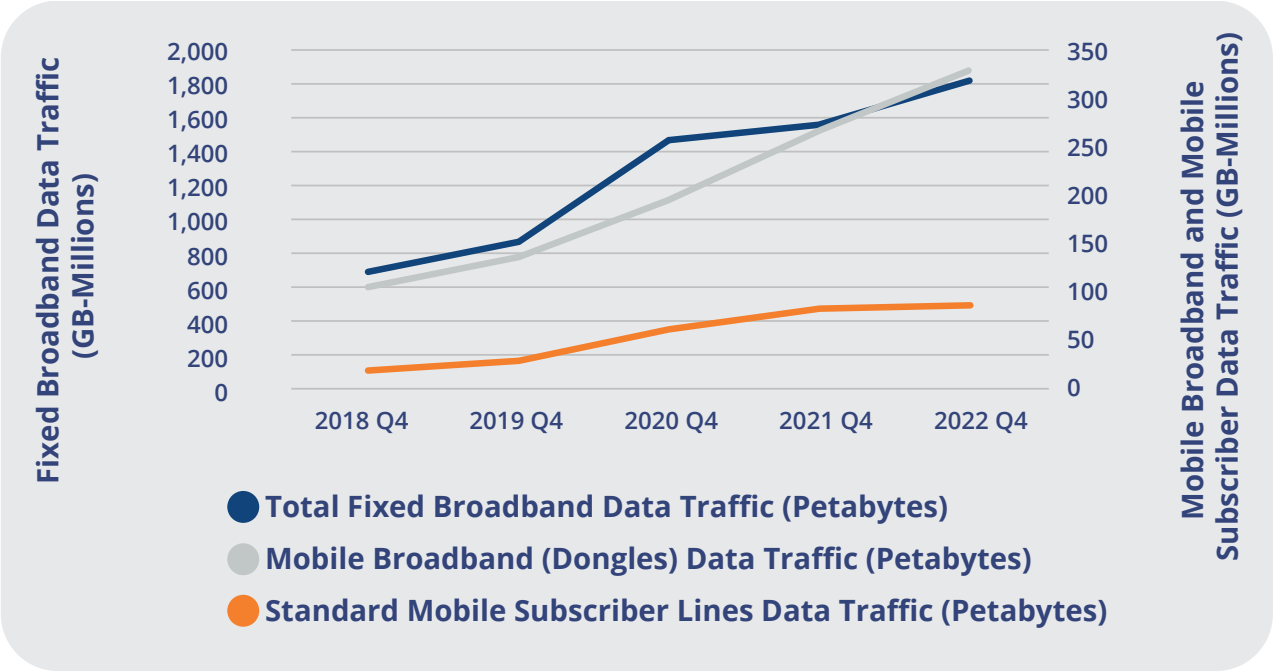
5.10 By the end of the decade ComReg expects that fixed VHCN will have been rolled out to almost all premises (households and businesses) in the country through a combination of commercial deployments and public investment through the NBP.

5.11 Meeting the growing demands of Irish consumers in the future will likely require not only improved mobile coverage and increased network density, but also for mobile devices and services to be able to seamlessly migrate between mobile and fixed (e.g., Wi-Fi) networks when in use. In this regard key enablers to meet this challenge are the rollout of fixed networks and the availability of additional spectrum.

5.12 The use of ECN/ECS has increased over the last three years with fixed and mobile data traffic volumes having increased since 2019. As set out in Figure 9 below, data use has remained high and continues to increase, more than doubling in the period from Q4 2019 to Q4 2022.[61].

61 QKDR Q4 2023

Figure 9: Data Traffic on Fixed and Mobile Networks



Supporting Digital Infrastructure

5.13 ComReg's goal regarding digital infrastructure is that **telecommunications networks, technologies, and solutions allow end-users to fully participate in all aspects of society**. Thus, the focus of ComReg's strategy is ensuring the widespread availability of high-quality and reliable services.

5.14 Over the coming period ComReg will continue to work towards this through the following actions:

- **Digital Divide**: ComReg will continue to monitor the emergence of digital divides in various ECS and ECS adjacent markets. These insights will help give us a holistic understanding of the connectivity challenges facing end-users and help inform various policy and regulatory decisions made by ComReg.
- **Geographic Mapping of Networks**: In accordance with Article 22 of the EECC, ComReg is continuing to work towards compiling and publishing a map of broadband networks in Ireland, including forecast coverage. Maps such as these can be useful to consumers, industry, government and ComReg. This is in addition to ComReg's Outdoor Mobile Coverage map, as discussed in Chapter 4.
- **Monitoring network and technology developments**: ComReg will continue to monitor developments and innovations[62] in network technologies and to facilitate their use where appropriate.

Goal 3.1

Telecommunications networks, technologies and solutions allow end-users to fully participate in all aspects of society.

62 Such developments and innovations are likely to include the rollout of 5G, Low Earth Orbiting satellite broadband, ViLTE (Video over LTE), DOCSIS 4.0 and Small Cells

5.15 The Broadband Cost Reduction Regulations[63] ('**BCRR**') came into effect in 2016 with the aim of facilitating and reducing the cost of deploying high-speed public ECN. However, the BCRR have not been used to any great extent by Irish operators. ComReg has three functions under the BCRR:

- Ensuring compliance with the BCRR;
- Acting as national dispute settlement body in relation to the BCRR[64]; and
- The provision of a Single Information Point ('**SIP**')[65] to facilitate access to information regarding permits for civil works.

5.16 ComReg notes the EC has recently reviewed the BCRR and proposed the Gigabit Infrastructure Act[66] as part of its February 2023 Connectivity Package to speed up the deployment of 5G and fibre networks.

5.17 The proposed Gigabit Infrastructure Act aims to overcome the challenge of slow and costly deployment of the underlying physical infrastructure sustaining advanced Gigabit networks. It aims to reduce 'red tape' and the costs and administrative burden associated with the deployment of Gigabit networks. The proposed regulation will also enhance the coordination of civil works between network operators to deploy the underlying physical infrastructure, such as ducts and masts, and ensure that the relevant actors obtain access to it.

5.18 Articles 76 and 79 of the EECC set out arrangements for co-investment agreements between an SMP operator and another operator to build a VHCN or mobile base station, exempting such investments from SMP-type access remedies. The EECC sets down further conditions to be considered by ComReg (e.g. risk sharing and continued access for access seekers) before allowing such co-investment arrangements. Article 79 sets out new powers for the NRA to make access and co-investment offers made by an SMP provider binding, in-lieu of imposing SMP obligations. ComReg will consider any such proposals from industry regarding such co-investment should they arise.

Supporting Connectivity and Network Resilience

5.19 ComReg and Government have a range of regulatory tools available to incentivise infrastructure deployment into areas currently unserved by commercial networks. In this context, it is ComReg's goal that **by utilising the regulatory toolkit, ComReg's activities will promote connectivity and/or incentivise infrastructure rollout**.

5.20 Competitive forces, if left to their own devices, will deliver ECS/ECN to a certain level and quality. However, achieving high-quality connectivity beyond this level is unlikely to be provided due to the uncommercial nature of network rollout in some geographic areas.

Goal 3.2

Utilising the regulatory toolkit, ComReg's activities promote connectivity and/or incentivise infrastructure rollout.

5.21 ComReg also recognises that while useful, its regulatory toolkit does have limitations in addressing the connectivity problems facing some end-users. Where other public bodies have policy or legislative roles relating to the

63 The European Union (Reduction of Cost of Deploying High-Speed Public Communications Networks) Regulations 2016 (S.I. No. 391/2016)
64 ComReg's Disputes Handling Process is available on its website – ComReg Doc 16/77r
65 See https://ec.europa.eu/eurostat/databrowser/view/tps00003/default/table?lang=en
66 Gigabit Infrastructure Act Proposal and Impact Assessment - https://digital-strategy.ec.europa.eu/en/library/gigabit-infrastructure-act-proposal-and-impact-assessment

ECS sector and adjacent markets, ComReg seeks to engage positively with such bodies and contribute to the wider policy setting with DECC and other Government departments.

5.22 Licenses awarded as part of ComReg's recent **MBSA2** included coverage obligations to ensure that outdoor mobile voice coverage exceeds 99% of the population and outdoor mobile data coverage at speeds greater than 30 Mbps eventually exceeds 95% of the population.

5.23 As set out in Chapter 4, ComReg maintains outdoor mobile coverage maps that allow the public to check coverage details by operator. ComReg expects to continue enhancing these maps with new features. In 2022 ComReg added 5G outdoor mobile coverage to its mobile coverage maps.

5.24 Meeting the future needs of Irish consumers accessing data hungry applications from mobile devices will likely require not only the improved coverage of mobile networks, but also the ability of consumers and services to move seamlessly between mobile and fixed broadband networks when making a call or using data services. The rollout of fixed networks by commercial operators and NBI and the availability of additional spectrum through future spectrum awards are key enablers to meet this challenge.

5.25 ComReg had previously indicated there may be a case for more interventionist measures to provide coverage in locations where it would not be commercially viable. However, there are significant policy issues to be addressed, including whether such measures are value for money, how target locations might be chosen, and how any initiative would comply with EU State Aid rules. While it would not be appropriate for ComReg to make policy choices, it can provide expert input to inform consideration of possible mechanisms to secure coverage outcomes beyond market-driven levels.

5.26 Over the coming period ComReg will also continue to engage with the Mobile Phone and Broadband Taskforce to provide solutions to the broadband/phone coverage deficit, and to investigate how to provide better services for consumers.

State Aid and Universal Service

5.27 Where the commercial and regulatory levers are insufficient to deploy networks, public funding is bridging the gap to serve remote areas. The EU State Aid Guidelines ensure that such funding does not distort competition in the market. Over the last 15 years the Irish Government has invested in ECN through various schemes[67], including the awarding of the NBP to National Broadband Ireland.

5.28 While not responsible for the NBP, ComReg does provide technical advice to DECC on the NBP and has seconded staff to DECC to provide such assistance. ComReg recognises that the NBI rollout, over time, may have implications for regulation. At all times ComReg will consider the impact of the NBI rollout on the state of competition in the relevant retail and wholesale markets.

5.29 As discussed in Chapter 4, the purpose of Universal Service is to ensure consumers have access at an affordable price to both adequate broadband and to a voice communications service, including the underlying connection, at a fixed location.

Network Security

5.30 The security of networks and services relates to the ability of ECN or ECS to resist at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted data or processed data, or of the related services offered by, or accessible via, those ECN or ECS.

67 Including through the Metropolitan area networks, National Broadband Scheme and National Broadband Plan

5.31 Ireland's modern digitally connected society and economy is highly dependent on reliable and secure ECN and ECS. They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisational security measures.

5.32 As part of measures to enhance the security of electronic communications networks and services in Ireland announced by the Government in late November 2021, DECC published its consultation on the Electronic Communications Security Measures ("**ECSMs**"). The ECSMs are a detailed set of technical and organisational measures that providers of public ECN and publicly available ECS will be required to implement. DECC has recently issued its response to consultation.

5.33 The Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 gives ComReg compliance and enforcement powers in respect of the implementation of the ECSMs by these providers. These new statutory obligations and functions for ComReg will act as a minimum-security baseline for providers of ECN and ECS. This requirement will further enhance and secure the electronic communications infrastructure within the State.

5.34 Whilst many of the security measures outlined in the ECSMs reflect policies, process and procedures already in place for many operators of ECN and ECS, others will require significant changes to daily operations. Implementation of the ECSMs will be a programme that will in some cases require significant investments in time, financial and human resources. However, the costs of recovering from an attack can often dwarf the cost of preventive security measures both directly and indirectly having regard to the reputational risks and damage such attacks can cause to operators, customers and consumers.

5.35 Given the dynamic nature of electronic communications services, the ECSMs must be considered as "living documents" and will require regular revision. Additional ECSMs will also need to be developed to reflect further innovations, for example, the use of eSIM.

5.36 One of the threats to the security and resilience of ECS and ECN is a cyber-attack. Because of the threat of a malicious security breach resulting in cyber-attacks in Ireland, ComReg collaborates with Ireland's National Cyber Security Centre ('**NCSC**'), part of DECC, which is the lead agency for Ireland within the Cyber domain.

5.37 Operators are required to notify ComReg in the event of a breach of security threshold or loss of integrity that has a significant impact on the operation of their networks or services[68]. Where such reports are received, ComReg notifies when required the NCSC, DECC, the European Network and Information Security Agency ('**ENISA**') and the public.

5.38 ComReg interacts with the operator to ensure services are restored and actions are put in place to mitigate against future similar breaches in Network Security.

5.39 There are many aspects to network security which do not fall within ComReg's remit, including for example, data privacy. Several other public bodies also have a role in network security and resilience, including DECC, ENISA, the Data Protection Commission ('DPC') Gardaí and the Defence Forces. The relevant agencies vary according to the issue at hand and its potential impact. Effective engagement with these stakeholders is necessary to ensure appropriate oversight and consistency and

68 See ComReg Document 14/02a and ComReg Document 19/98

to avoid the duplication of activities. In this context, it is ComReg's goal that operators have **appropriate risk-based procedures in place to manage network security and resilience**.

Goal 3.3

Operators have appropriate risk-based procedures in place to manage network security and resilience.

5.40 Over the coming period, ComReg intends to undertake the following:

- **Implementation of Electronic Communication Security Measures**: ComReg will develop the framework to enable the proportionate, transparent and non-discriminate implementation of the ECSMs by providers of ECN or ECS. Furthermore, ComReg will be responsible for the assessment, compliance, audit and enforcement of operator ECSM obligations on an on-going basis. ComReg will maintain the ECSMs relevance by updating on a regular basis as required and develop additional ECSMs which are focussed on other areas of security relevance as the networks and technology on which they are based evolves.

Network Resilience

5.41 The resilience of an ECS or ECN[69] relates to the ability of that ECN to return to its normal state following a disruptive incident. The resilience of a network can be compromised in its core and in its distribution and access sections, all of which can then impact the network operator, its customers, and other providers of ECS and/or ECN who rely on wholesale access or interconnection. Network and service outages can cause significant disruption to end-users resulting in economic, financial, and societal losses. While ComReg recognises that 'force majeure' events can and will happen, resulting in an unavoidable temporary loss of service, it is essential that all reasonable precautions and processes are in place to ensure continuity of supply. It is therefore essential that adequate precautions and investments are made to ensure continuity and availability of networks and the services provided over these networks.

5.42 The interconnectivity and interoperability of networks has become increasingly important, particularly regarding the resilience of networks and assurances around the continuity of services. Resilience is an issue, not just for individual networks and services but also because of the increased potential for problems arising from the interdependence of networks and services. This includes, for example, the interrelationship between mobile and fixed networks.

5.43 ComReg considers whether there is a risk of market failure which could cause operators to underinvest in the security and resilience of networks and services. There is a potential market failure with respect to systemic risks – risks that could affect the whole industry. Investments in mitigating systemic risk would benefit all end-users, not just the customers of the operator making the investment. On the other hand, if all operators are exposed to the same systemic risk, then there will be no competitive disadvantage if the risk crystallises – so there is a reduced commercial incentive to mitigate it.

69 ComReg's activities in respect of the resilience of ECS and ECN is limited to Reg 23 & 24 of the Framework Regulations and Article 40 & 41 of the EECC

5.44 Providers of publicly available ECN/ECS are required to manage the integrity and security of their networks and services[70]. They are also required to take appropriate technical and organisational measures to manage risks to the security of such networks and services. Such a risk-based approach should lead operators to prevent, resist, mitigate and recover from threats to security and resilience of networks and services they provide.

5.45 To ensure that network resilience is effectively managed, operators should have a comprehensive understanding of all relevant risks to which they are exposed and analyse those risks.

5.46 In the context of ComReg's Goal 3.3 relating to network security and resilience, over the coming period, ComReg intends to undertake the following projects:

- **Collaboration**: ComReg will continue to work with relevant stakeholders where matters of network resilience have an impact. One such matter which ComReg has been and is currently engaging with the operators on, is the risk of power outages due to electricity generation shortfall. ComReg first engaged with operators in October 2021 because of the risk of possible power outages over winter 2021/2022. The purpose of this ongoing engagement is to ensure operators are factoring into their risk assessments the increased risk of power outages across the national grid.
- **Network Resilience**: ComReg continues to engage with the industry in assessing the risk management practices of ECS/ECN providers. The project focuses on risk and resilience in the different aspects of ECS/ECN network functions, for both fixed and mobile networks and services. The focus of this work will be reviewed in line with the obligations and functions set out in the new Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023.
- **Economic and Societal Cost of a Network Incident**: ComReg has commissioned a study to investigate the impact of network incidents and to develop a model which can give an indication of the economic and societal cost of such events. The outcome of this assessment could be used to inform ComReg on future regulatory intervention.
- **Climate Change and its Effect on Network Resilience in Ireland**: ComReg has published a study by Frontier Economics[71] to investigate how climate change has been affecting ECN, and to understand what providers of ECN are doing to mitigate against these affects. ComReg will review the findings from this study and may further explore any of these which could be of added benefit to the resilience of ECN in Ireland.
- **Network Operations Annual Report**: ComReg publishes an annual network operations report relating to its activities.
- **ENISA Annual Incident Report**: ComReg will continue to report incidents to ENISA on an annual basis, in line with its statutory obligations.

Nuisance Communications

5.47 Nuisance communications, means unwanted, unsolicited communications generally directed at large groups of the population. Nuisance communications often have the intent to mislead the receiver, so that they unknowingly provide sensitive personal information. This in turn can enable the criminal to perpetrate fraud.

5.48 Irish society and its economy have become ever more reliant on telecommunications technology. It is deeply integrated into all areas of the economy and society, however, this constant in our lives comes with its own threats and vulnerabilities. Fraud, which is perpetrated by using ECS and ECN, and particularly nuisance communications, has become a low-risk form of crime.

70 Under Regulation 23 of the Framework Regulations and Articles 40 & 41 of the EECC
71 https://www.comreg.ie/publication/climate-change-and-its-effect-on-network-resilience-a-study-by-frontier-economics

5.49 The reduced cost and increased availability of means has seen fraud in the form of nuisance communications rise substantially in Ireland. Our daily use of ECS and ECN is exploited by criminals, who use social engineering type attacks – for example vishing, smishing and CLI spoofing, with the intention of illegally acquiring personal consumer information, ultimately to abet financial fraud.

5.50 At its heart, this fraud is the abuse of telecommunications products (mainly telephones and mobile phones) or services with the intention of illegally acquiring money from a communication service provider or its customers. Criminals prey on our daily use of electronic devices and continuously seek out new ways to exploit vulnerabilities and access information. The reduced cost and increased availability of enabling-equipment means this type of fraud is on the rise.

5.51 As an English-speaking country, Irish residents are targeted disproportionately compared with their EU counterparts. This is because fraudsters can move seamlessly between other English-speaking countries, targeting their resources where scam communications are most likely to have the highest success rate. It is inevitable that fraudsters will continue to target (and commit more fraud in) those countries, and particularly English-speaking ones, that remain vulnerable to telecommunications related fraud. Ireland must therefore proceed with haste in the best interests of our society, businesses, and residents and ComReg is pleased to play its part in that response.

5.52 The latest available Central Statistics Office ("CSO") publication on crime indicates that nuisance communications continue to grow. While the data relates to fraud more broadly, and not solely to fraud conducted via nuisance communications, the CSO notes that the 90% year-on-year increase in 2021 was "*largely driven by unauthorised transactions and attempts to obtain personal or banking information online or by phone*"[72], matching similar experiences abroad.

5.53 Aware of the damaging effects and complexity of nuisance communications, and the pressing need for a cross-industry effort to combat the problem, ComReg, in December 2021, announced the formation of the NCIT[73]. The NCIT held its first meeting under an independent Chair in February 2022. In addition to ComReg itself, there are fifteen industry members[74] who collectively carry the bulk of calls and SMS messages that are delivered to Irish users.

5.54 The NCIT began by bringing together representatives of the telecommunications industry to, amongst other things:

- discuss potential interventions to be applied to networks to minimise/mitigate the volume and effect of nuisance communications;
- develop an implementation roadmap to ensure that the interventions are implemented by the appropriate network and/or service providers as quickly as possible in line with the expected timelines of the deliverable of the taskforce; and
- facilitate an effective means for industry to collaborate and share information over the long term should nuisance communications evolve or should a network/networks come under a sustained nuisance communications attack.

5.55 The focus for ComReg and the NCIT is to restore trust in telecommunications services by putting in place interventions to reduce the prevalence of the damaging effects of nuisance communications and their impact on Irish consumers and society.

72 CSO "Recorded Crime Q1 2022" accessible here https://www.cso.ie/en/releasesandpublications/ep/p-rc/recordedcrimeq12022/
73 ComReg Information Notice 21/129
74 BT Ireland, Blueface, Colt, Eircom, Imagine Communications, Intellicom, Magnet, Sky Ireland, Tesco Mobile, Three, Twilio, Verizon, Viatel, Virgin Media, Vodafone

5.56 NCIT success requires the support and expertise of the entire telecommunications industry, including international gateway providers, and the strong endorsement of its work by the CEO's[75] concerned. ComReg readily accepts that it is these companies who operate and run Ireland's telecommunications networks and therefore have the greatest concentration of know-how and resources needed to tackle this problem.

5.57 The NCIT has now scoped several interventions and agreed high-level technical specifications which, when implemented, should notably lessen the quantity of nuisance communications currently being experienced in the State. ComReg notes:

- The implementation phase of the NCIT is underway, with operators now free to proactively deploy interventions;
- A Do Not Originate ("DNO")[76] trial took place over the month of September 2022 with the assistance of relevant organisations, and was subsequently made available by ComReg to all organisations wishing to avail of the protection it offers from October 2022 onwards[77]; and
- Each intervention design encompasses the gathering of metrics to help evaluate and monitor the effectiveness of the intervention.

5.58 Given the extent of the fraud and the damaging effect it continues to have on trust in Irish telecommunications services, at an NCIT meeting on 4 January 2023, members agreed that the NCIT should continue beyond its initial 12 months. A new Terms of Reference was also agreed[78], with an emphasis on members of the NCIT to be fully focused on rapid implementation and accelerated deployment of these interventions.

5.59 Going forward, further work will be required by the telecommunications industry to address other, more complex vulnerabilities and to help stymie new or evolving types of nuisance communications. Such tasks may include, but are not limited to:

- delivering on agreed member's implementation roadmaps to ensure that the interventions are implemented by the appropriate network and/or service providers as quickly as possible;
- providing metrics as per agreed technical specifications and in line with the expected timelines of the deliverable of the taskforce;
- undertaking a gap analysis to identify further measures that may be taken, including more dynamic interventions;
- proactive monitoring of trends in nuisance communications both in Ireland and abroad;
- formalising inter-operator and cross-sector cooperation and coordination;
- identifying actions for industry and ComReg to raise consumer awareness of scams;
- ultimately, developing an overarching long-term national strategy to combat nuisance communications; and
- contributing to international regulatory initiatives to promote an international approach, as appropriate.

5.60 ComReg looks forward to the continuing work of the NCIT in the months ahead, together with the full and active commitment of all its members and other interested parties.

75 To that end, CEOs of NCIT member organisations have signed a Code of Conduct that commits members to uphold that and the NCIT Terms of Reference.

76 Many organisations use phone numbers for inbound-only calls to provide a wide variety of services to consumers. Fraudsters sometimes originate calls to look like they are coming from these numbers to trick consumers into answering the calls, This is an activity known as spoofing. To address the problem, ComReg has now compiled a Do Not Originate" or "DNO" list, comprising phone numbers that are never used for outbound calls and so can be blocked by operators.

77 See www.comreg.ie/dno and ComReg document 22/86a

78 Nuisance Communications: Agreed revised Terms of Reference for Nuisance Communications Industry Taskforce, 23/12.