An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations
Annual Report 2019

Information Notice

Reference: ComReg 20/22

Version: Final

Date: 31/03/2020

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Additional Information

Document No:	20/22
Date:	31 March 2020

Content

Section **Page**

1 Introduction

1. ComReg's Network Operations Unit ("NOU") is a specialised unit and is a centre of expertise on technical network issues. The NOU sits within the Market Framework Division but its remit entails supporting the activities of ComReg across all of its functions.

2. NOU has recruited specialist staff with relevant expertise and experience. The NOU also has the full support of ComReg's Corporate Services Division, and IT and Facilities sections, in facilitating the required resources.

Figure 1: ComReg Monitoring Room at Dockland Central

3. This annual report is structured as follows:

- Chapter 2: covers the background to the report;
- Chapter 3: covers Resilience and Incidents that affect networks;
- Chapter 4: reviews network incidents for 2019;
- Chapter 5: reviews programmatic work for 2019;
- Chapter 6: deals with the effects of cybersecurity on Network Resilience; and
- Chapter 7: presents an overview of future work for the NOU.

2 Background

4. ComReg was established under the Communications Regulation Act 2002 ("2002 Act") and is the designated national regulatory authority ("NRA") for the purposes of the EU-wide harmonised framework for the regulation of electronic communications networks ("ECN") and electronic communications services ("ECS"), which includes management of the national radio spectrum and numbering resources.

5. Any undertaking that intends to provide an electronic communications network and/or service in the State must be authorised to do so, by ComReg and in accordance with the Authorisation Regulations[1]. Upon becoming authorised, all such undertakings are subject to the 2002 Act and to the provisions of the Authorisation Regulations, Framework Regulations[2], Access Regulations[3], and Universal Service Regulations.[4]

6. ComReg's overall objectives in the exercise of its functions are to promote and protect competition and the interests of consumers, to promote the development of the internal market, and to ensure the efficient and effective use of the national radio spectrum and numbering resources. ComReg must also apply objective, transparent, transparent, non-discriminatory and proportionate regulatory principles.[5]

7. The NOU's core deliverable is to provide technical support and information to the ComReg organisation, as and when required and in order to best enable it to perform effectively, including effective oversight of undertakings' compliance with legislative provisions and with regulatory conditions and obligations imposed by it. NOU is also responsible for overseeing reporting on network incidents by providers of public electronic communications networks and services[6] made pursuant to regulation 23(4) of the Framework Regulations.

[1] European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2011 (S.I. 335/2011)
[2] European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011)
[3] European Communities (Electronic Communications Networks and Services) (Access) Regulations 2011 (S.I. 334/2011)
[4] European Communities (Electronic Communications Networks and Services) (Universal Service and Users' Rights) Regulations 2011 (S.I. 337/2011)
[5] Section 12 of the 2002 Act and Regulation 16 of the Framework Regulations
[6] ComReg Document 14/02 on Reporting & Guidance on Incident Reporting & Minimum Security Standards Regulations 23 and 24 of The European Communities (Electronic Communications Networks

Obligations on Authorised Operators

8. Of particular relevance to NOU are Regulations 23 and 24 of the Framework Regulations. Under Regulation 23, a provider of a “public communications network” or “publicly available electronic communications service” must take appropriate technical and organisational measures to appropriately manage risks to the security of such network or service, having regard to the state of the art and ensuring a level of security appropriate to the risk. In addition, any provider of a public communications network must also take appropriate steps to guarantee the integrity of that network.

9. In the event of a significant breach of security or integrity, the undertaking concerned must notify ComReg, who in turn must inform the Minister. With the agreement of the Minister and where appropriate, ComReg must also inform national regulatory authorities in other EU Member States and the European Union Agency for Cybersecurity (“ENISA”). Where it is in the public interest, and again with the agreement of the Minister, ComReg may inform the public of a breach or require the undertaking concerned to do so.

ComReg’s Powers

10. Regulation 24 sets out the powers available to ComReg and provides that, for the purposes of Regulation 23, ComReg can issue a direction to an undertaking requiring it to:

    a. provide information needed to assess the security or integrity of its network / services; and/or
    b. submit to a security audit by a qualified independent body and to make the results available to ComReg.

11. These directions can also specify time limits for implementation and failure to comply with a direction is an offence.

12. A useful diagram from ENISA, below, relates undertakings’ obligations under Regulation 23 to risk assessments made under Regulation 24. This is a good methodology for undertakings to adopt in reporting incidents. Following an incident, a risk could be lessened by adopting suitable mitigation measures.

and Services) (Framework) Regulationshttps://www.comreg.ie/media/dlm_uploads/2015/12/ComReg1402.pdf

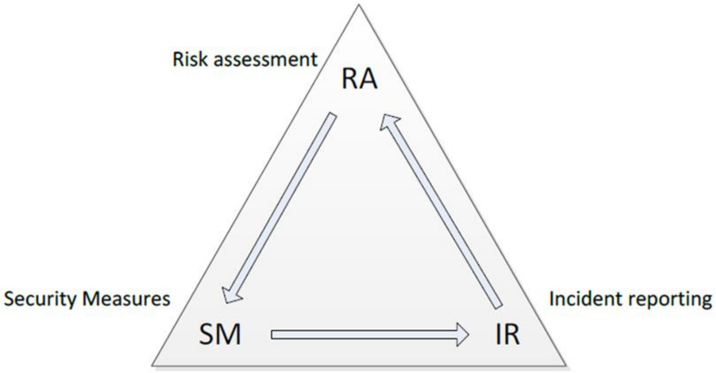


Figure 2: Relationships between Security measures, incident reporting and Risk assessment under Regulation 23 and 24 of the Framework Regulations.

3 Resilience and Network Incidents

Resilience

13. Resilience, as the term relates to electronic communications, describes the ability of a network or service to return to its normal state following a disruptive incident. Resilience is typically a function of number of users supported by a network or service coupled with the availability of that network or service, including any inherent redundancy.

14. The 2016 Directive on Security of Network and Information Systems ("NIS Directive")[7] concerns a high common EU-wide level of security of network and information systems. *Article 4 therein defines the* security of such systems as their ability *"to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*'. This definition is broadly analogous to the concept of resilience as it relates to ECN and ECS.

15. The resilience of an electronic communications network can be affected 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 electronic communications networks and/or services who rely on wholesale access or interconnection to provide same. Furthermore, a large incident that affects a network's resilience, at the core or distribution level, can have effects that propagate outside of Ireland such as international switching issues or damaged international fibre network.

Network Resilience Project

16. Since late 2019, NOU has been engaged in an assessment of the risk management practices of undertakings including Public Telecommunications Network Operators and Service Providers. Where appropriate, the NOU performs an assessment of the risk management practices of the network operators and service providers, based on information provided.

17. It is noted that this is a complex multi-year project and as such entails eight phases, the first of which dealt with the fixed voice and data core. NOU provided

[7] Directive 2016/1148 concerning for a high common level of security of network and information systems across the Union - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

a detailed questionnaire to all the undertakings that it considered operated a fixed core and would like to thank those undertakings that responded positively to this request.

18. The eight phases of the Network Resilience Project are:

- Phase 1 Fixed core, Voice and data, Interconnection;
- Phase 2 Mobile and Radio Core;
- Phase 3 International Access;
- Phase 4 Fibre and copper Access Network;
- Phase 5 Mobile Access Networks;
- Phase 6 Data Centres;
- Phase 7 Operator Provided CPE; and
- Phase 8 ECAS.

What are Network Incidents?

19. If there is a significant breach in the security or integrity of a public communications network or publicly available electronic communications service, the undertaking concerned must notify ComReg. As to what constitutes such a breach, for reference Article 4 of the NIS Directive defines an “incident” as ‘any event having an actual adverse effect on the security of network and information systems’. Typical incidents include:

- Weather and natural phenomena: storms, wind, high temperatures, fog, snow and ice, and solar storms.
- Third party damage: cable cuts, submarine or trawler cable damage.
- Vehicular impact.
- Malicious acts: theft, Telephony Denial of Service (“TDoS”) Distributed Denial of Service (“DDoS”) incidents, vandalism, espionage and sabotage.
- Power outages due to weather, insufficient protection of main supply, no or insufficient back-up power, and poor maintenance of back-up power.
- System failures: hardware and software failure, insufficient redundancy, poor procedures and poor supervision of outsourced staff.

Figure 3: Typical causes of Incidents that affect Network Resilience

Incident Reporting and Thresholds

20. As earlier outlined, Regulation 23(4)b of the Framework Regulations provides that when ComReg has been notified of a breach of security or loss of integrity that has a significant impact on the operation of electronic communications networks or services, ComReg must in turn inform the Minister for Communications Climate Action and Environment (the “Minister”) of the notification and, with the agreement of the Minister and where appropriate, ComReg shall also inform the NRAs in other Member States and ENISA.

21. ComReg must also submit annually a summary report to the Minister, the European Commission and ENISA on incidents notified to it. The last such report was lodged with ENISA on 28 February 2020 and the summary statistics are presented in Chapter 4 below.

22. Under ENISA Guidelines, the threshold for annual summary reporting is based on the duration and number of user connections affected for a particular service (as a percentage of the national user base of that service). The ENISA Guidelines require NRAs to include in their annual summary reports incidents that:

- Exceed 1 hour with more than 15% of users affected;

- Exceed 2 hours with more than 10% of users affected;
- Exceed 4 hours with more than 5% of users affected;
- Exceed 6 hours with more than 2% of users affected; or
- Exceed 8 hours with more than 1% of users affected.

4 Network Incidents in 2019

General Commentary on 2019 ENISA Report for Ireland

23. All incidents reported to ENISA are drawn from notifications made to ComReg using ComReg reporting form 14/02[8] and sent to ComReg at incident@comreg.ie or since October 2019, via the new incident reporting portal accessible via ComReg's e-licensing[9] platform. When an incident report is submitted, NOU may revert to the undertaking concerned for further information regarding the incident and any actions taken to prevent or reduce the risk of a recurrence and / or to mitigate the effects. Once NOU is satisfied that an incident has been appropriately dealt with, the report is anonymised and uploaded to the ENISA portal. A summary of the major incidents is presented at figure 4 below.

24. Many of the reported incidents relate to power outages, mostly caused by weather events, such as storms. Additionally, mobile and radio networks tend to be more prone to the effects of adverse weather, (wind damage, ice, and heavy rain) while fixed underground plants tend generally to be more vulnerable to flooding, caused by storm surges and heavy rain.

25. Other causes of incidents included: software bugs and poorly implemented software updates, resulting from policy and procedural flaws. This latter category often arose from inadequate, or in some instances a lack of, Standard Operating Procedures ("SOPs"). These incidents typically arose during network changes (including both hardware and software). Poor supervision and training of staff and contractors were also notable factors.

Storms and Other Natural Phenomena

26. In 2019, NOU monitored 12 separate weather events, from Storm Erik in February 2019 through to Storm Atiyah in December 2019. NOU monitors warnings from Met Éireann and uses other tools which rely upon data from the European Centre for Medium-Range Weather Forecasts ("ECMWF") model and from the US National Oceanic and Atmospheric Administration ("NOAA"). This includes Atlantic

[8] See Annex 1 of ComReg Document 14/02 for an example of the Incident Reporting Form.

[9] https://www.elicensing.comreg.ie/

storms originating as Atlantic Hurricanes which could pass over Ireland, an example of this would be Storm Lorenzo at the beginning of October 2019.

Named Storms[10] [11]in 2019:

• Erik	08 February	2019;
• Freya	02-03 March	2019;
• Gareth	12-13 March	2019;
• Hannah	26-27 April	2019; and
• Atiyah	08 December	2019;

Storms named by other Agencies;

• Storm Lorenzo	03-04 October	2019; and
• Storm Elsa	18-19 December	2019.

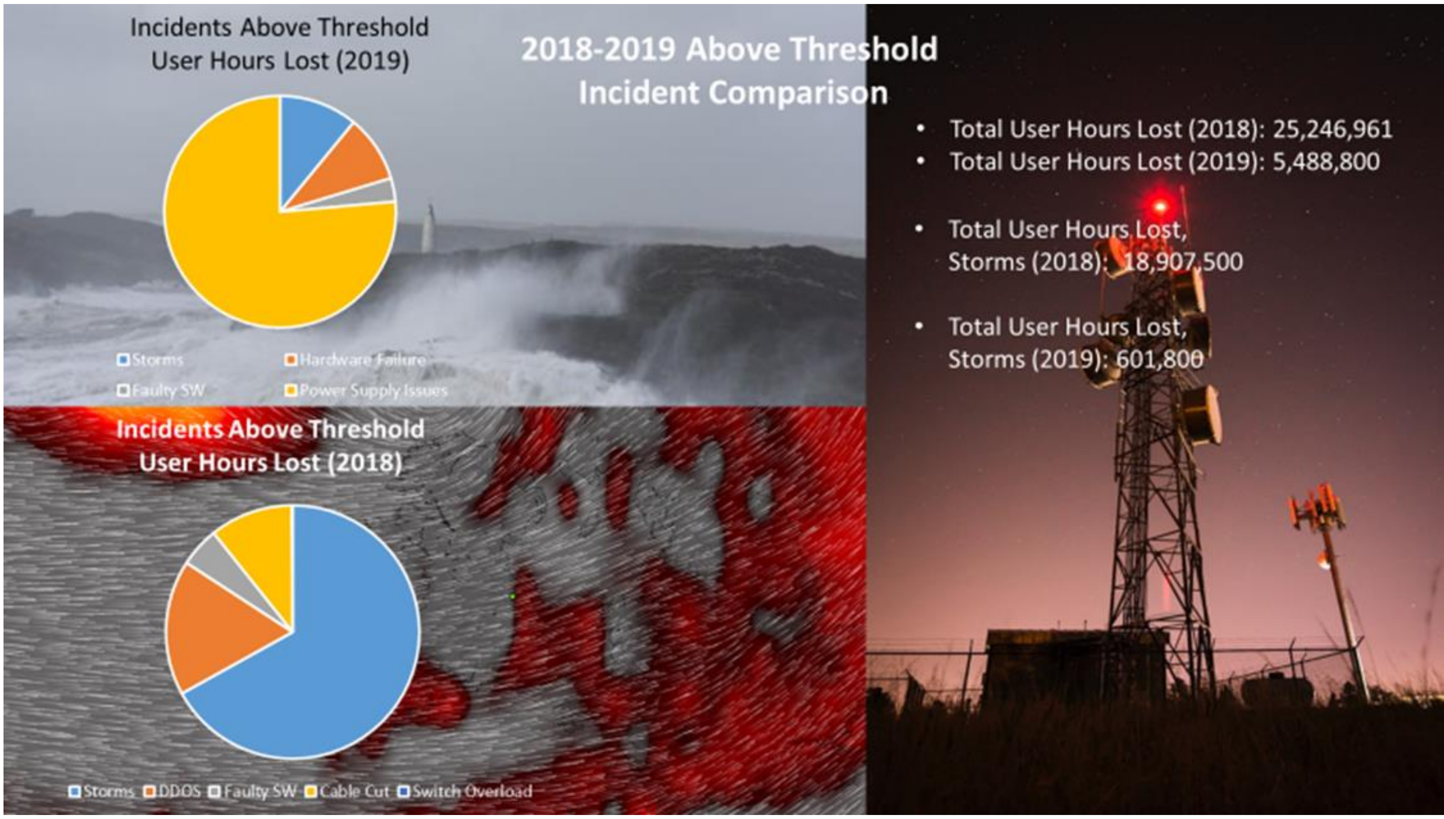
27. If an orange-level[12] warning or named Storm is announced by Met Éireann, then NOU can monitor it as it develops and can communicate with operators of national networks, with NOU receiving twice daily reports from these operators. This information is then passed on to the National Emergency Coordination Group ("NECG") and/or the Department of Communications Climate Action and Environment ("DCCAE"), as necessary.

28. Requests for assistance from network operators can be passed via the NECG to appropriate State agencies, in order to achieve a quicker resolution of any outage than the operator could achieve without such assistance.

[10] Named by Met Éireann and the UK Met Office.

[11] Storms in the 2019-2020 Storm season are named by Met Éireann, the UK Met Office and the Dutch National Weather Service ("KNMI").

[12] See Met Éireann https://www.met.ie/weather-warnings , for an explanation of the warning scheme, and https://www.met.ie/cms/assets/uploads/2019/10/Severe-weather-chartNDFEM.pdf



2018-2019 Above Threshold Incident Comparison

- Total User Hours Lost (2018): 25,246,961
- Total User Hours Lost (2019): 5,488,800
- Total User Hours Lost, Storms (2018): 18,907,500
- Total User Hours Lost, Storms (2019): 601,800

Figure 4: Comparison of above threshold Incidents 2018 vs. 2019.

5 Review of Programmatic Work for 2019

Special Events

29. During 2019, NOU acted as a central coordination point between ComReg and undertakings in monitoring network resilience for special events, such as international sporting events, State visits with high media interest, for example the 2019 visits of the President and Vice President of the United States of America on the 5 – 7 June and 6 – 7 September 2019, respectively.

NOU also works in close cooperation with ComReg's Projects & Licensing and Spectrum Intelligence and Investigations ("SII") units, to ensure that appropriate special events are afforded apposite attention.

Incident Reporting Portal

30. As outlined in the NOU Annual Report for 2018, ComReg has developed a new portal to streamline the notification of incidents. The format for the information required remains as set out in ComReg Form 14/02 but the form is now submitted to ComReg through the incident reporting portal[13]. The guide to the new portal was published by ComReg in 2019[14].

31. The new portal uses two-factor authentication, with only registered undertakings able to use it and it enables the modification and of submitted information while an incident is still in progress. If an incident has ended and if the cause analysis has been satisfactorily completed, then the incident report can be closed by ComReg.

32. The portal usefully facilitates NOU in actively monitoring trends, including but not limited to the type and occurrence of incidents. This allows for the further investigation of events if deemed necessary by ComReg.

Network Monitoring

33. The NOU has responsibility for ComReg's bi-annual drive testing programme which was most recently conducted during Winter 2019 by Advanced Wireless

[13] https://www.elicensing.comreg.ie/login.aspx

[14] See ComReg Document 19/98

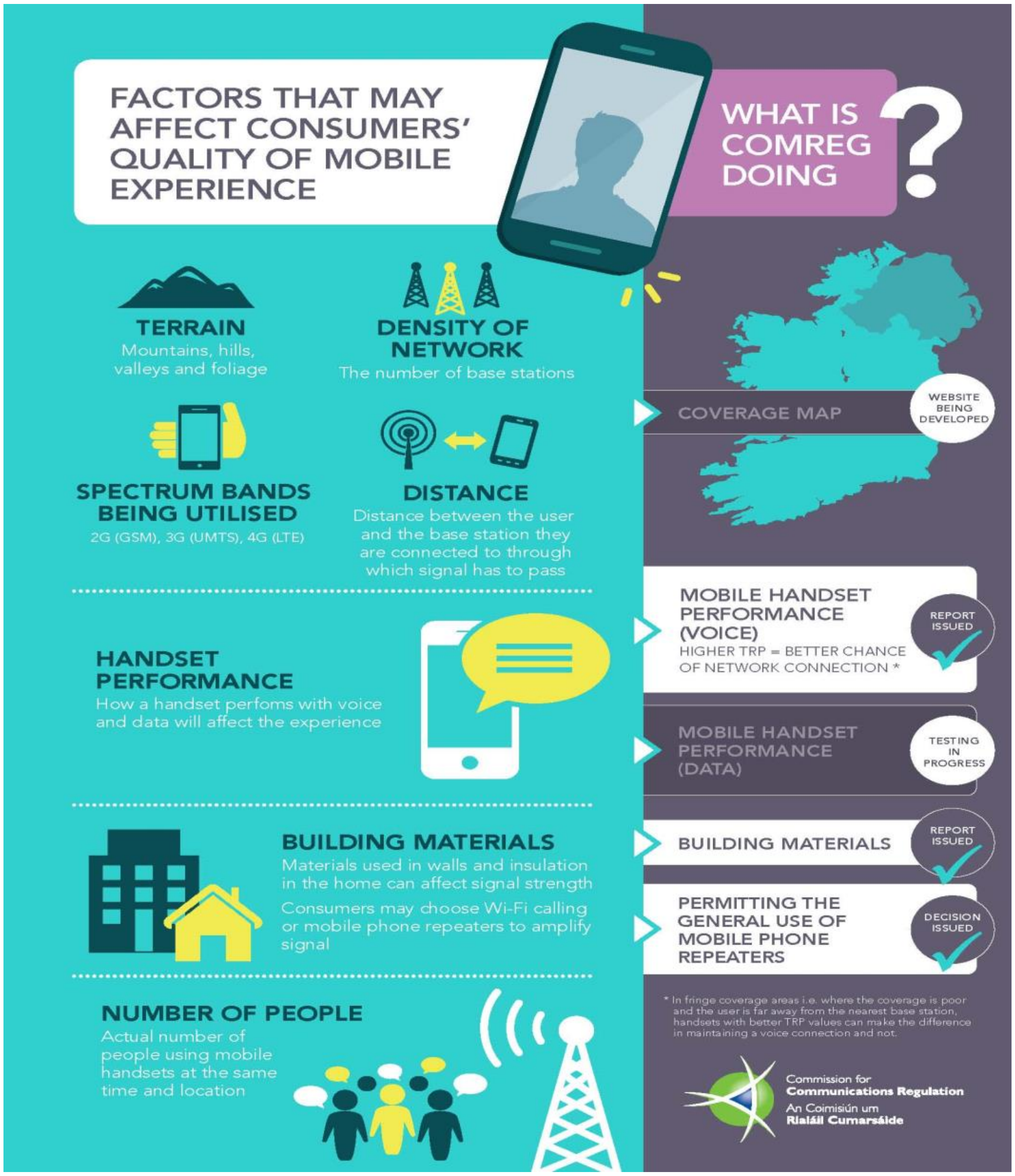
Technologies Group Limited ("AWTG") and during 2019, NOU issued two reports[15].

34. During 2020, NOU plans to advance ComReg's remote radio frequency spectrum monitoring capabilities. In relation to the monitoring of ECN and ECS more generally, NOU is actively involved in enhancing ComReg's capabilities.

Handset Testing

35. A number of factors affect the quality of the mobile service that a user experiences at any given location, see Figure 5 below. While most of these factors vary over time and by location, and this can be seen from the results of the drive testing programme; the one factor that is relatively constant, from the mobile user's perspective, is the mobile handset.

[15] ComReg Documents 19/26 and 19/87; https://www.comreg.ie/publication/assessment-of-mobile-network-operators-compliance-with-licence-obligations-coverage-winter-2018; and https://www.comreg.ie/publication/assessment-of-mobile-network-operators-compliance-with-licence-obligations-coverage-summer-2019 respectively



FACTORS THAT MAY AFFECT CONSUMERS' QUALITY OF MOBILE EXPERIENCE

TERRAIN
Mountains, hills, valleys and foliage

DENSITY OF NETWORK
The number of base stations

SPECTRUM BANDS BEING UTILISED
2G (GSM), 3G (UMTS), 4G (LTE)

DISTANCE
Distance between the user and the base station they are connected to through which signal has to pass

HANDSET PERFORMANCE
How a handset perfoms with voice and data will affect the experience

BUILDING MATERIALS
Materials used in walls and insulation in the home can affect signal strength
Consumers may choose Wi-Fi calling or mobile phone repeaters to amplify signal

NUMBER OF PEOPLE
Actual number of people using mobile handsets at the same time and location

WHAT IS COMREG DOING?

COVERAGE MAP — WEBSITE BEING DEVELOPED

MOBILE HANDSET PERFORMANCE (VOICE)
HIGHER TRP = BETTER CHANCE OF NETWORK CONNECTION * — REPORT ISSUED ✓

MOBILE HANDSET PERFORMANCE (DATA) — TESTING IN PROGRESS

BUILDING MATERIALS — REPORT ISSUED ✓

PERMITTING THE GENERAL USE OF MOBILE PHONE REPEATERS — DECISION ISSUED ✓

* In fringe coverage areas i.e. where the coverage is poor and the user is far away from the nearest base station, handsets with better TRP values can make the difference in maintaining a voice connection and not.

Commission for **Communications Regulation**
An Coimisiún um **Rialáil Cumarsáide**

Figure 5: Some factors that affect end-user experience of mobile networks

36. In 2019, NOU assumed responsibility for ComReg's Mobile Handset Performance measurement programme, which includes publishing reports on the measurement of antenna performance of mobile handsets, when making both voice calls; and receiving or streaming data.

37. Through this work, ComReg's aims to gain a greater understanding of factors that affect the experience of users of mobile services, in making voice calls or in streaming data.

38. NOU has independently acquired mobile handsets available on the Irish market from various sources and has measured their antenna performances in a manner that replicates mobile user experience. Furthermore, it should be noted that the antenna performance of each mobile handset is measured as a complete device and no modifications were made to any device, or to test the antenna in isolation.

39. ComReg published two Handset Testing Reports during 2019:

    a. ComReg Document No 19/110[16]; and

    b. ComReg Document 19/67[17].

40. As set out in its Radio Spectrum Management Strategy Statement[18], ComReg will continue to measure the performance of all new models of mobile handsets that become available on the Irish market, for voice and data, and will publish future reports containing the results of these measurements as appropriate.

[16] https://www.comreg.ie/?dlm_download=mobile-handset-performance-voice-2

[17] https://www.comreg.ie/?dlm_download=mobile-handset-performance-data-2

[18] See footnote 1 above.

6 Cyber Security of Networks and Resilience

General

41. Regulation 23 of the Framework Regulations places obligations on operators providing public communications networks or publicly available electronic communications services in respect of the management of the integrity and security of networks and services. The obligations on operators include that they shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

42. One of the threats to the resilience of ECN and ECS includes cyber-attacks. As a consequence of the threat of cyber-attacks on an ECN and/or an ECS, ComReg collaborates with Ireland's National Cyber Security Centre ("NCSC"), part of DCCAE, which is the lead agency for Ireland within the Cyber domain.

Cybersecurity of networks

43. On 26 March 2019, the European Union published the Commission Recommendation on Cybersecurity of 5G networks C(2019) 2335 final ("Rec. 2335")[19]. Since then, NOU has been working in close collaboration with the NCSC to assist with the deliverables from this Recommendation. During 2019, this included assisting with an NCSC-led risk assessment of 5G networks in Ireland.

44. Further to this, NOU provided input into the relevant EU, ENISA and BEREC working groups and subsequent output documents. This has culminated in the publication of the report on the EU coordinated risk assessment on cybersecurity in Fifth Generation ("5G") networks[20] and the European Toolbox on the security of 5G networks[21] ("the Toolbox") on 29 January 2020. The NOU will continue to collaborate with the NCSC to assist with the implementation of the Toolbox in the coming year.

[19] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks
[20] https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049
[21] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

45. NCSC published its National Cyber Security Strategy 2019 – 2024 (“NCSS 2019 – 2024”) in December 2019[22]. The NCSS 2019 – 2024 lists ComReg as a stakeholder in two of its measures relating to the cybersecurity of telecommunications networks:

- Measure 4: The NCSC, with the assistance of the Defence Forces and An Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber-attack.

- Measure 7: Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the State.

46. NOU will work with the NCSC to assist them in the delivery of these measures over the coming year.

[22] The National Cyber Security Strategy, 2019 – 2024: https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

7 Future Work

Adaptation

47. Given the prevalence of storms and weather events as outlined earlier, ComReg intends to consult on the matter of network incidents and meteorological events during the next reporting period.

Cybersecurity of telecommunications networks

48. NOU will collaborate with the NCSC with regard to the delivery of the measures outlined by NCSS in its NCSS 2019 – 2024 Strategy.

ENISA Report 2020 and NOU Annual Report 2020

49. Through the work of the NOU, ComReg will fulfil its obligation under Regulation 23 of the Framework regulations and once again will summarise the incident types in the NOU Annual Report 2020.

European Electronic Communications Code (“EECC”)

50. NOU has been supporting ComReg’s Operational Divisions with technical advice on any relevant factors under consideration during the transposition of the EECC into Irish law by DCCAE.

Mobile User Experience – Outdoor Mobile Coverage Mapping

51. NOU is responsible for the provision of technical support to the broader project team. NOU staff develop, evaluate and calibrate the model based on inputs received from both the Mobile Network Operators (“MNO”s) and Mobile Virtual Network Operators (“MVNO”)s.

52. The outdoor mobile coverage map[23] allows consumers to assess the level of mobile coverage they might expect to experience in their own localities. Among, other things, this information can also help inform consumers when making purchase choices with regard to mobile operator.

53. The outdoor mobile coverage map allows consumers to search and zoom in, to 10 x 10 metres, to a particular area or address and is designed for use with an eircode, locality or address.

[23] https://www.comreg.ie/outdoor-mobile-coverage-map/

Strategic Technical Support

54. NOU has implemented a Strategic Technical Support function to support multiple technical programs within ComReg.

55. The Strategic Technical Support function also provides centralised expertise in emerging technologies and technical advice, to assist policy and compliance decisions in ComReg. This function will interact with industry, research bodies and other expert bodies as part of its core objectives.