An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations

Annual Report 2020

Information Notice

Reference:	ComReg 21/29
Version:	Final
Date:	29/03/2021

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:	21/29
Date:	29 March 2021

Content

Section **Page**

1 Introduction

1. The Commission for Communications Regulation ("ComReg")'s Network Operations Unit ("NOU") is a specialised unit and is the centre of expertise on technical network issues. The NOU sits within the Market Framework Division and its remit is to support the activities of ComReg, across all of its functions and Divisions.

2. 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 or 2020;
   - Chapter 5: reviews programmatic work for 2020;
   - 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

3. 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.

4. 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]

5. ComReg's overall objectives in the exercise of its functions are to:

   - promote and protect competition and the interests of consumers;
   - promote the development of the internal market; and
   - ensure the efficient and effective use of the national radio spectrum and numbering resources.

6. In meeting its objectives ComReg must also apply, objective, transparent, non-discriminatory and proportionate, regulatory principles.[5]

7. The NOU's core deliverable is to provide technical support and information on public electronic communications networks to ComReg organisationally, as and when required and to inform the compliance and policy function of ComReg. This includes ensuring effective oversight of undertakings' compliance with legislative provisions and with regulatory conditions and obligations imposed on them by ComReg. NOU is also responsible for overseeing reporting on network incidents by providers of public

[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

electronic communications networks and services[6] made pursuant to regulation 23(4) of the Framework Regulations.

Obligations on Authorised Operators

8. Of 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. Such obligations, on authorised undertakings, are expected to be maintained with the transposition of the European Electronic Communications Code[7].

9. In the event of a significant breach of security or integrity, the undertaking concerned are obliged to notify ComReg, who in turn must inform the Minister[8]. With the agreement of the Minister and where appropriate, ComReg must also inform NRAs in other EU Member States (“MS”) 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.

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

[7] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[8] The Minister for the Department of the Environment, Climate and Communications.

12. The current powers, pursuant to this Regulation, are expected to be maintained with the transposition of the European Electronic Communications Code[9].

13. A useful diagram from ENISA in the form of the virtuous triangle 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.

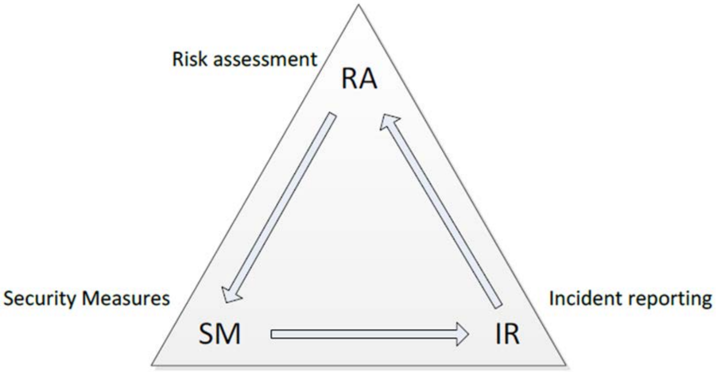


Figure 2: Relationships between Security measures, incident reporting and Risk assessment under Regulation 23 and 24 of the Framework Regulations.

[9] For reference, the security provisions of the European Electronic Communications Code are contained in Articles 40 and 41.

3 Resilience and Network Incidents

Resilience

14. Resilience, as the term relates to electronic communications, describes the ability of a network or service, provided by an undertaking, 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.

15. The 2016 Directive on Security of Network and Information Systems ("NIS Directive")[10] 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.

16. 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 undertaking, 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 an undertaking's 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

17. Since late 2019, NOU has been engaged in an assessment of the risk management practices of undertakings including, operators of publicly available electronic communications networks and services. Where appropriate, the NOU performs an assessment of the risk management practices of the network operators and service providers, based on information provided.

[10] 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

18. It is noted that this is a complex multi-year project and as such, entails eight phases, the first and second of which, were in the main, dealt with in 2020. The first two phases included: the fixed voice and data core; and the Mobile Voice and Packet Data Core.

19. 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 (submarine cables);
- 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.

So far, phase 1 – Fixed core, Voice and data, Interconnection and phase 2 – Mobile and Radio Core, have been in the main completed during the 2020 work programme.

What is a Network Incident?

20. 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'. Examples of some of the causes of typical incidents include:

- Weather and natural phenomena: storms, wind, high temperatures, fog, snow and ice, and solar storms.

Figure 3: Solar storm, wind damage, flooding and snow

- Third party damage: including, vehicular impact, cable theft; cuts, deep diving submarines, anchor, cable plough or trawler related, cable damage.

Figure 4: Marine Hazards: Deep Diving Submarines, Anchor, Cable Plough and Remotely Operated Vehicles

- Malicious acts: theft, Telephony Denial of Service ("TDoS") Distributed Denial of Service ("DDoS") incidents, vandalism, espionage and sabotage.

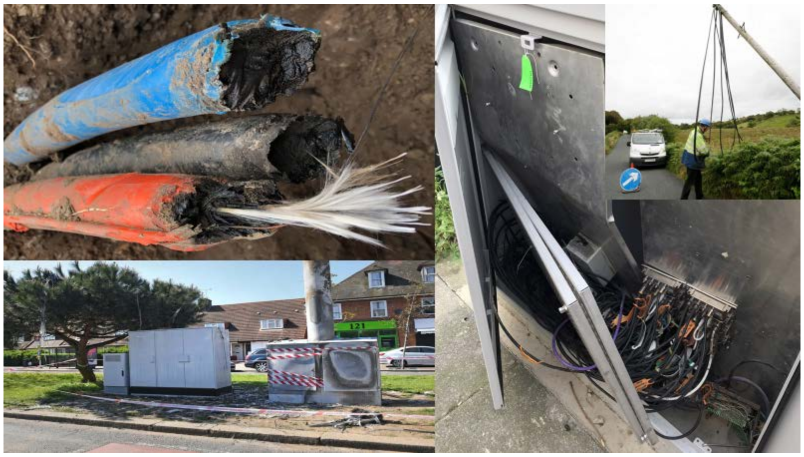


Figure 5: Plant Damage, including Arson, Vandalism and Theft

- 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 including but not limited to: hardware and software failure; insufficient redundancy; poor procedures, particularly 'roll-back' procedures[11]; poor supervision of both own and outsourced staff.

Incident Reporting and Thresholds

21. 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 the Environment, Climate and Communications (the "Minister") of the notification and, with the agreement of the Minister and where appropriate, ComReg shall also inform the NRAs in other MS and ENISA.

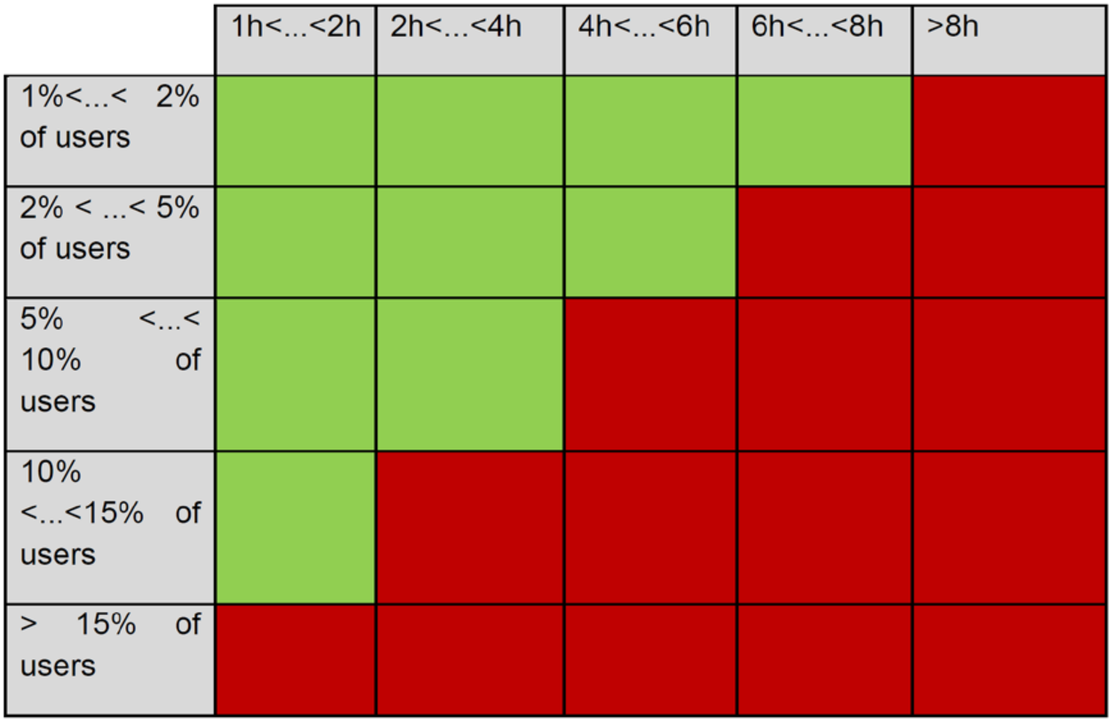
22. ComReg must also submit annually a summary report to, the Minister, the European Commission and ENISA on incidents notified to it. The last such report was lodged with ENISA on 12 February 2021 and the summary statistics are presented in Chapter 4 below.

23. Under the current ENISA Guidelines, the threshold for annual summary reporting is based on the duration and number of user connections affected for a particular service

[11] This is where a software or hardware change is restored to is original state prior to the implementation of the change.

(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.



	1h<...<2h	2h<...<4h	4h<...<6h	6h<...<8h	>8h
1%<...< 2% of users	🟩	🟩	🟩	🟩	🟥
2% < ...< 5% of users	🟩	🟩	🟩	🟥	🟥
5% <...< 10% of users	🟩	🟩	🟥	🟥	🟥
10% <...<15% of users	🟩	🟥	🟥	🟥	🟥
> 15% of users	🟥	🟥	🟥	🟥	🟥

Figure 6: ENISA Thresholds for Incident reporting, as per ENISA Technical Guidelines document

24. ComReg's approach to management of reported incidents and the coordination of its response to these incidents, is set out in Reporting & Guidance on Incident Reporting & Minimum Security Standards, ComReg Document 14/02. The document outlines the appropriate thresholds for reporting incidents and the requisite timing for submission of incident reports. The thresholds and process for reporting are provided as guidance to operators providing public communications networks or publicly available electronic communications service. ComReg's approach takes into

consideration guidance provided by ENISA in its document: Technical Guideline on Reporting Incidents[12], as set out earlier in this section. The NOU expect to begin a review of the Reporting & Guidance on Incident Reporting & Minimum Security Standards, ComReg Document 14/02, in 2022.

[12] Technical Guideline on Reporting Incidents Article13a Implementation Version 1.0 – https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0

4 Network Incidents in 2020

General Commentary on 2020 ENISA Report for Ireland

25. All incidents reported to ENISA are drawn from notifications made to ComReg using the template outlined in ComReg reporting form 14/02[13]. Since October 2019, this has been incorporated in and is carried out electronically via the incident reporting portal accessible via ComReg's e-licensing platform.

26. The incident reporting portal[14], uses two-factor authentication and only registered undertakings can use it. Information submitted populates an active database, securely storing the information. This allows for easier incident updates [15] while the incident is still in progress. Once the incident is over and if the cause analysis has been completed to ComReg's satisfaction, then the incident report can be closed by the undertaking concerned.

27. The information from the portal facilitates the NOU in actively monitoring trends, including but not limited to the type and occurrence of incidents. This along with other tools allows for the further investigation of events, if deemed necessary by ComReg.

28. Once NOU is satisfied that an incident has been appropriately dealt with, by the undertaking concerned, the report is closed. Following this, the report is anonymised in order to upload the incident report to the ENISA portal. A summary of the major incidents for 2020, as uploaded to ENISA, is presented at figure 4 below.

29. Major causes of incidents in 2020 included: software bugs, poorly implemented software updates and hardware failures. The amount of hours lost, to each outage, was commonly compounded by, policy and procedural flaws. This often arose from inadequate, or in some instances a lack of, Standard Operating Procedures ("SOPs"). These incidents typically arose during network changes (including to both hardware and software) where poor supervision and training of staff and contractors, were also notable factors.

30. There have been seventeen incidents, reported to ComReg in 2020, compared to eleven in 2019. The overall number of User Hours lost due to incidents reported in 2020 was 50,726,256, which is approximately 10 times that of 2019.

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

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

[15] The guide to the new portal was published by ComReg in 2019, see ComReg 19/98

31. Several of the reported incidents relate to power outages, which are typically 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 plant tends generally to be more vulnerable to flooding, caused by storm surges and heavy rain.

32. ComReg notes, that these incidents have both an economic cost, in terms of the loss of services, impacting productivity and commerce; as well as a societal cost, limiting communications options for the citizens of the state. With the adoption of remote working, this has proved of particular importance during the COVID-19 pandemic. As such, NOU proposes to explore this topic further in the forthcoming work programme[16].

Storms and Other Natural Phenomena

33. In 2020, NOU monitored 8 separate weather events, from Storm Brendan in February 2019 through to Storm Aiden in December 2020. 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 storms originating as Atlantic Hurricanes which could pass over Ireland, a previous example of this would be Storm Lorenzo in Autumn 2019.

Named Storms and duration in 2020:

• Brendan	11 – 17 January
• Ciara	4 – 12 February
• Dennis	12 – 20 February
• Ellen	18 – 27 August
• Francis	24 – 27 August
• Aiden	30 October – 1 November

Storms named by other Meteorological Agencies;

• Jorge[17]	25 February – 5 March

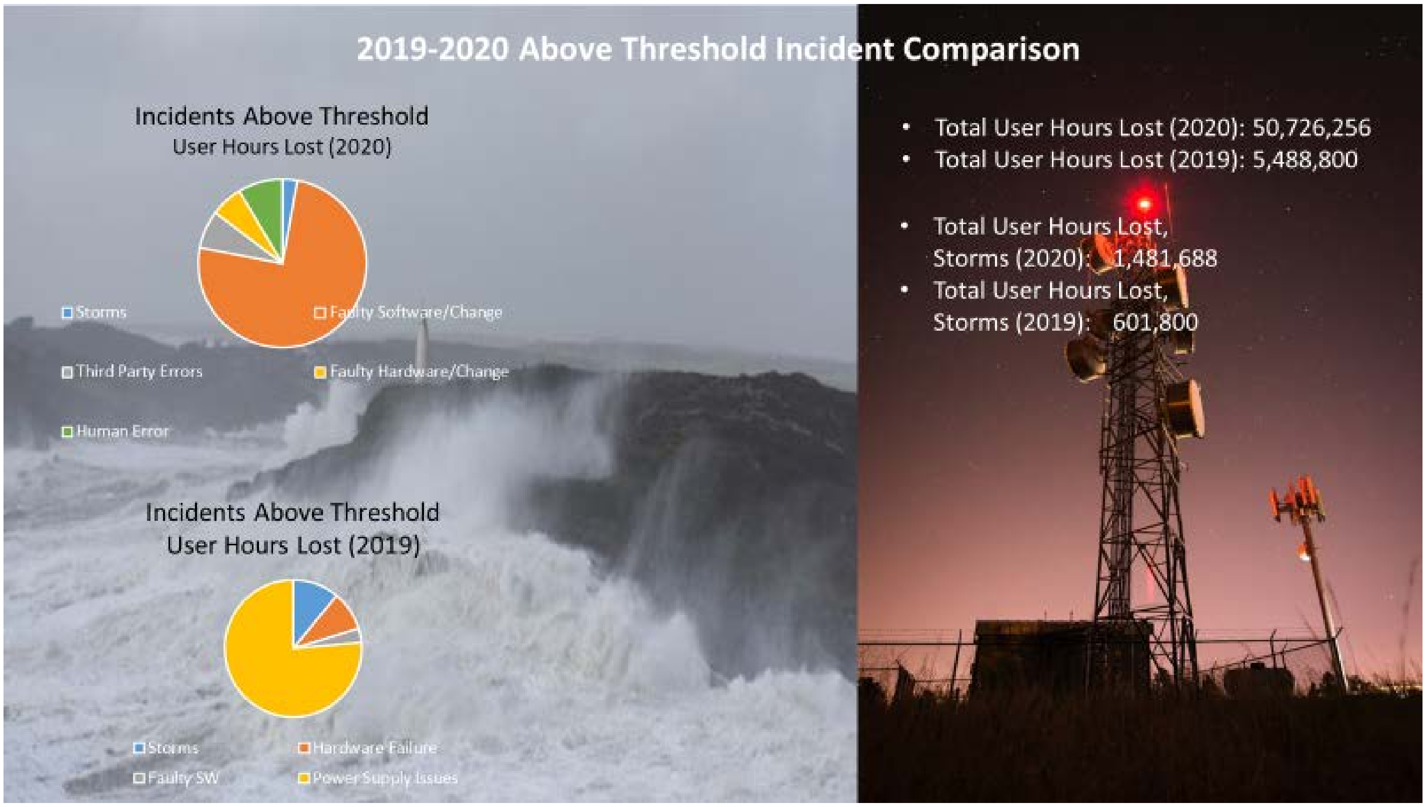
[16] See Chapter 7.

[17] Named by the Spanish State Meteorological Institute (AEMET)

34. Of the 2020 meteorological events, Storms Brendan, Ciara and Dennis caused outages above ‘business as usual’ levels, totalling 1,481,688 User Hours lost, notably greater than the 2019 experience. During Storms Ellen, Francis, Jorge and Aiden the networks operated normally.

35. If an orange-level[18] warning or named Storm[19] is announced by Met Éireann, then NOU monitor it as it develops and can communicate with operators of national networks, with NOU receiving twice daily reports (six hours apart) from these operators. This information is then passed on to the National Emergency Coordination Group (“NECG”) and/or the Department of the Environment, Climate and Communications (“DECC”), as necessary.

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



2019-2020 Above Threshold Incident Comparison

- Total User Hours Lost (2020): 50,726,256
- Total User Hours Lost (2019): 5,488,800
- Total User Hours Lost, Storms (2020): 1,481,688
- Total User Hours Lost, Storms (2019): 601,800

Figure 7: Comparison of above threshold Incidents 2019 vs. 2020

[18] 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

[19] Storms in Ireland are named by Met Éireann, the Met office (UK) and the Royal Netherlands Meteorological Institute (KNMI).

5 Review of Programmatic Work for 2020

COVID-19

37. Due to the world-wide COVID-19 pandemic and subsequent International and Domestic travel restrictions, no special events were held. However, the Government's Public Health restrictions led to unforeseen work for, the Industry, ComReg and NOU. This was in response to the need for employees to work from home to prevent the spread of COVID-19 and to ensure business continuity where possible.

38. During 2020, NOU acted as a central coordination point between ComReg and undertakings, monitoring network stability and resilience, in order that essential services, such as telecommunication networks, were capable of supporting the increased load on both fixed and mobile data services and fixed and mobile voice services. This has involved regular meetings with undertakings, DECC and other stakeholders.

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

40. During 2020, the NOU advanced its Strategic Technical Support ("STS") function and provided support to ComReg's Market Framework, Retail and Wholesale Divisions, through delivery of programmes under its control. This includes but is not limited to: Network Monitoring, Radio Frequency Monitoring Network, Outdoor mobile coverage mapping and handset testing.

41. Furthermore, the STS function also provides centralised expertise on emerging technologies and technical advice, assisting policy and compliance decisions within ComReg. This function interacts with industry, research bodies and other expert bodies as part of its core objectives.

Network Monitoring

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

Group Limited ("AWTG") and during 2020, NOU issued a report[20] on the results of the drive test.

43. Due to the world-wide COVID-19 pandemic and subsequent Government Public Health restrictions, ComReg, with the agreement of AWTG has currently suspended this work. ComReg plans to reactivate this work, as soon as the circumstances reasonably permit.

44. During 2020, NOU advanced ComReg's remote radio frequency spectrum monitoring capabilities. In relation to the monitoring of ECN and ECS more generally, NOU is actively involved in work to enhance ComReg's capabilities in this regard. This included the purchase of licences for an outage detection product, which covers not just IP based OTT providers, ECN and ECS providers, but also voice and text.

Handset Testing

45. Several factors affect the quality of the mobile connectivity, that a user experiences at any given location and Figure 9 below outlines these. Most of these factors vary over time and by location, and this can be seen from the results of the drive testing programme[21]. One factor that can impact connectivity from the mobile user's perspective, is the mobile handset.

46. ComReg's aim is to allow users to understand the factors that affect the connectivity experience, including those introduced by mobile handsets.

47. Since 2019, NOU has been responsible for the ComReg mobile handset testing performance measurement programme for 2G, 3G and 4G technology, which includes the publication of reports on the measurement of antenna performance of mobile handsets.

48. As current and future technologies, such as 5G progress, the methodology of informing and allowing users to understand the factors which affect connectivity experience may evolve. Therefore, NOU will strategically engage in a review of the best communication methodology to allow users to understand the impact of handset performance, taking into account current and future technologies.

49. Again, due to the world-wide COVID-19 pandemic and subsequent Government Public Health restrictions, affecting both domestic and international travel, the performance of this task has been affected, both in terms of travel to the testing

[20] https://www.comreg.ie/publication/assessment-of-mobile-network-operators-compliance-with-licence-obligations-coverage-winter-2019

[21] https://www.comreg.ie/publication/assessment-of-mobile-network-operators-compliance-with-licence-obligations-coverage-winter-2019

facilities and the provision of instrument calibration. As such, ComReg has published a single report regarding the Data performance of Mobile Handsets: ComReg Document 20/121[22].

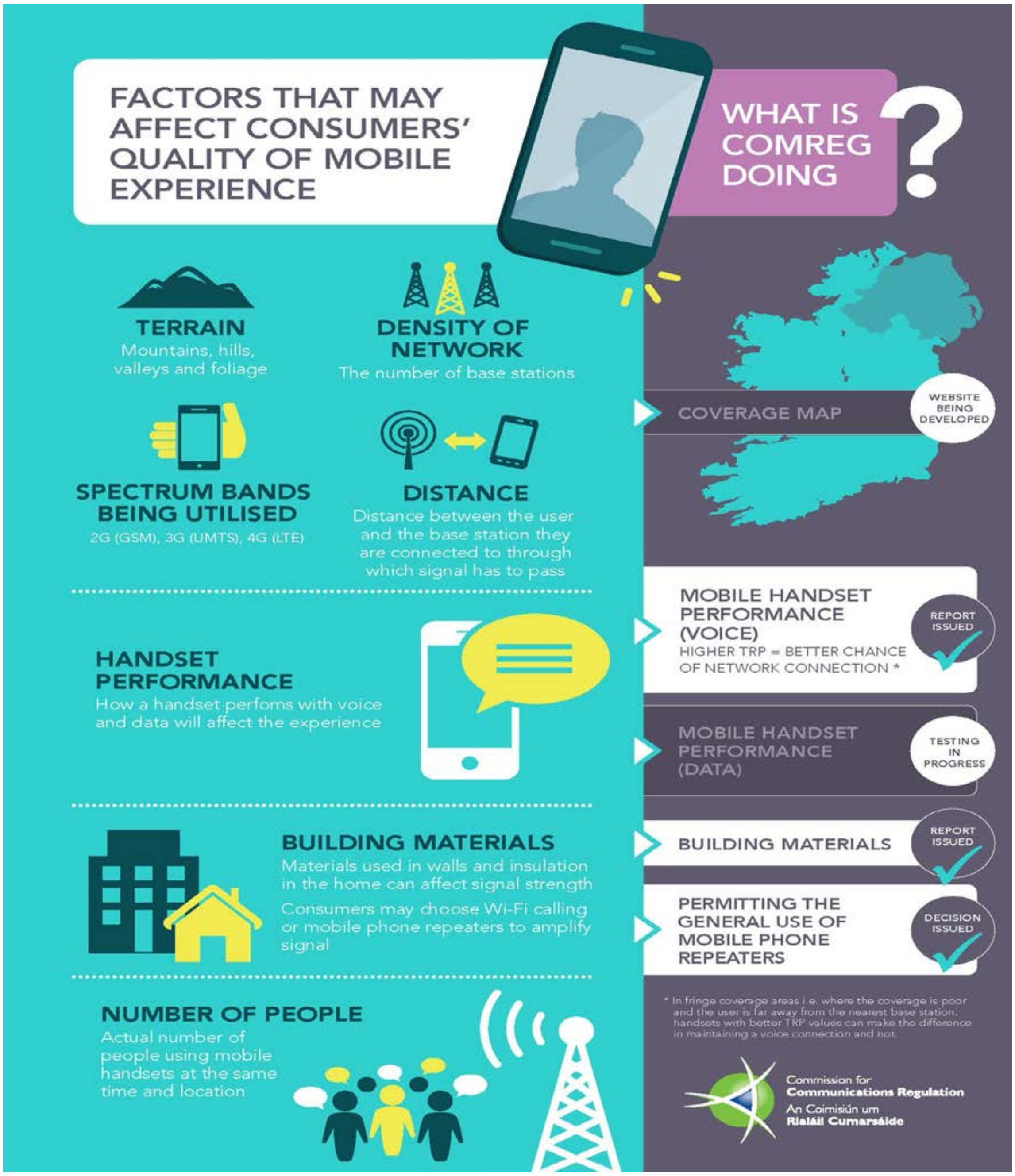

FACTORS THAT MAY AFFECT CONSUMERS' QUALITY OF MOBILE EXPERIENCE
WHAT IS COMREG DOING ?
TERRAIN
Mountains, hills, valleys and foliage
DENSITY OF NETWORK
The number of base stations
SPECTRUM BANDS BEING UTILISED
2G (GSM), 3G (UMTS), 4G (LTE)
DISTANCE
Distance between the user and the base station they 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
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 9: Some factors that affect end-user experience of mobile networks

[22] https://www.comreg.ie/publication/mobile-handset-performance-data-3

Mobile User Experience – Outdoor Mobile Coverage Mapping

50. Developed in conjunction with ComReg's Retail division, the outdoor mobile coverage map[23], allows consumers to assess the level of mobile coverage they might reasonably expect to experience in their own localities. Amongst, other things, this information helps consumers to make an informed choice regarding their connectivity requirements.

51. As part of its STS function, NOU apply independent engineering calculations to network data received from mobile operators ("MNOs") to allow outdoor coverage map predictions to be available on the ComReg online website. Additionally, analysing the outdoor coverage predictions helps inform ComReg's current and future management of the radio spectrum.

International Work

52. NOU plays a role in a number of international forae, primarily: the Body of European Regulators for Electronic Communications ("BEREC") including its 5G, NIS 2 and cybersecurity Working Groups; ENISA, in terms of the ECASEC (formerly, Article 13a) group and its Working Groups.

53. During the COVID-19 pandemic, this work has been taking place by correspondence with meetings taking place, using web-based video conferencing tools. This has facilitated both regularly scheduled and ad-hoc meetings, with NOU being able to fully participate and contribute from home.

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

6 Cyber Security of Networks and Network Resilience

General

54. 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. Measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

55. One of the threats to the resilience of ECN and ECS includes cyber-attacks. Because 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 DECC, which is the lead agency for Ireland within the Cyber domain.

Cybersecurity of networks

56. The background to this continuing work item was the publication of the European Union Commission Recommendation on Cybersecurity of 5G networks C(2019) 2335 final ("Rec. 2335")[24], on 26 March 2019. Since then, NOU has been working in close collaboration with the NCSC to assist with the deliverables from this Recommendation

57. NOU has provided assistance to the NCSC as it led Ireland's input into relevant EU working groups related to the deliverables of Rec. 2335. Further to this, the NOU has regularly provided input into the relevant ENISA and BEREC working groups and subsequent output documents. This culminated in the publication of the report on the EU coordinated risk assessment on cybersecurity in Fifth Generation ("5G") networks[25] and the European Toolbox on the security of 5G networks[26] ("the Toolbox") on 29 January 2020.

58. The NCSC published its National Cyber Security Strategy 2019 – 2024 ("NCSS 2019 – 2024") in December 2019[27]. ComReg, as a stakeholder, has been involved in

[24] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks
[25] https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049
[26] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127
[27] The National Cyber Security Strategy, 2019 – 2024:
https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

assisting the NCSC 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 security measures to support the cyber security of telecommunications infrastructure in the State.

7 Future Work

Economic Impact of Incidents

59. As part of its work on the forthcoming transposition of the EECC, NOU, along with the Economic Unit of the Market Framework Division, will investigate and develop a model which can give an indication of the economic and societal cost of a network incident.

Cybersecurity of telecommunications networks

60. NOU will continue to work in close co-operation with the NCSC to assist them in the delivery of the measures contained in the NCSS 2019-2024 Strategy over the coming year.

European Electronic Communications Code ("EECC")

61. NOU has been supporting ComReg's various operational units with technical advice on any relevant factors under consideration during the transposition of the EECC into Irish law by DECC.

ENISA Report 2021 and NOU Annual Report 2021

62. Through the work of the NOU, ComReg will fulfil its obligation to report significant incidents to both the Minister and ENISA under Regulation 23 of the Framework regulations. This is expected to continue under the transposed EECC. Following this, NOU will issue its Annual Report for 2021, which will summarise the work carried out in respect of incident reporting and incident types that have emerged during the year.

Review of ComReg Document No. 14/02 on Incident Reporting

63. Following the expected transposition of the EECC, ComReg intends to undertake a review of its Document 14/02 with regard to Incident Reporting and minimum security standards. This is to update both the reporting requirements, undertakings and other operators that will be in scope, such as Number Independent Interpersonal Communications Services providing certain Over The Top ("OTT") services, following the future transposition of the EECC.

Climate Change and Adaptation of Telecommunications Networks

64. Given the increasing incidence of storms and weather events as outlined , ComReg intends to engage with the sector and consult on the matter of network incidents and meteorological events during the next reporting period.

Strategic Technical Support

65. 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.