An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations
Annual Report 2022

Information Notice

Reference: ComReg 23/60

Version: Final

Date: 04/07/2023

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:	23/60
Date:	04 July 2023

Content

Section Page

1 Introduction

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

2. This annual report on its activities is structured as follows:

   - Chapter 2: Covers Resilience and Network Incidents;
   - Chapter 3: Reviews network incidents for 2022;
   - Chapter 4: Outlines ComReg's work on Nuisance Communications;
   - Chapter 5: Details Other Projects undertaken by the NOU during 2022; and
   - Annex 1: Outlines the Obligations on Authorised Operators and Relevant ComReg powers.

2 Resilience and Network Incidents

2.1 Resilience of Networks and Services

3. 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 an Electronic Communications Network or Service ("ECN" or "ECS") coupled with the availability of that network or service, including any inherent redundancy.

4. The resilience of an ECN can be affected in its core network and in its distribution and access sections, all of which can then impact the provider, its customers, and other providers of ECN or ECS who might rely on wholesale access or interconnection. Furthermore, a large incident that affects a provider's network resilience, at the core or distribution level, such as international switching issues or damage to an international fibre network, can have effects that propagate outside of Ireland.

5. ComReg is engaged in understanding and assessing the risk management practices of providers including those providing publicly available electronic communications networks and services. Where appropriate, ComReg undertakes an assessment of risk management practices based on the information provided by the providers concerned.

6. This is a complex multi-year workstream and as such, entails seven phases, which are as follows:

    - 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 - Emergency Call Answering Service ("ECAS"); and
    - Phase 7 - Operator Provided CPE.

7. The final phases of this workstream were completed during the 2022 work programme.

Future Work

8. Work on the resilience of Networks and Services is a core ongoing workstream for ComReg's NOU. Over the next year the concentration of effort in this area will be to evolve the workstream by evaluating the learnings from the different phases, together with considering advances in the deployed network technologies.

2.2 Network Incidents

9. A network incident is now defined as a "security incident", pursuant to the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, No.4 of 2023 (the "Act of 2023")[1]. For the purposes of this report, a network incident is any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services. From 9 June 2023, such incidents are reported by providers to ComReg pursuant to section 11 of the Act of 2023.

10. During the period to which this Annual Report relates, network incidents, defined as breaches of security or losses of integrity that had a significant impact on the operators of networks or services, had to be notified to ComReg pursuant to Regulation 23(4)(a) of S.I. No. 333 of 2011, European Communities (Electronic Communications Networks and Services) (Framework) Regulations (the "Framework Regulations"). These Regulations have since been repealed[2] and the security provisions in those Regulations have been replaced by Part 2 of the Act of 2023. This Annual Report refers to the Framework Regulations where applicable.

11. The cause of network incidents can vary but typically can arise from:

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

[1] Section 5 of the Act of 2023.
[2] [2] By means of Regulation 116 of S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022, as inserted by S.I. No. 300 of 2023, the European Union (Electronic Communications Code) (Amendment) Regulations 2023.

- Third party damage: including, damage to physical infrastructure, vehicular impact, fibre cuts and cable damage;
- Malicious acts: Telephony Denial of Service ("TDoS") incidents, Distributed Denial of Service ("DDoS") incidents, cable theft, vandalism, espionage, and sabotage;
- Power outages due to weather, insufficient protection of mains supply, no or insufficient back-up power and poor maintenance of back-up power; and
- System failures including but not limited to hardware and software failure; insufficient redundancy; insufficient procedures and deficient supervision of both own and outsourced staff.

Incident Reporting and Thresholds

12. During 2022, Regulation 23(4)(b) of the Framework Regulations applied and provided, that when ComReg is notified of a breach of security or loss of integrity that had a significant impact on the operation of ECN or ECS; 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 also inform the NRAs in other MS and ENISA[3]. Incident reporting requirements under the Act of 2023, which is now the applicable legislation, are set out in section 11 of that Act.

13. ComReg must also submit a summary report annually to the Minister, the European Commission and ENISA regarding the incidents notified to it. The last such report was lodged with ENISA on 11 February 2023 and the summary statistics are presented in Chapter 3 below.

14. ComReg's approach to management of reported incidents and the coordination of its response to these incidents, was set out in Reporting & Guidance on Incident Reporting & Minimum Security Standards, ComReg Document 14/02[4] ("Document 14/02").

15. In 2022 ComReg completed a review of Document 14/02 and published its proposals for public consultation – "*Network Incident Reporting Thresholds, A consultation to revise and replace ComReg Document 14/02 (Reporting &*

[3] Going forward, the reporting obligation under the Act of 2023 is now section 11(5).
[4] Reporting & Guidance on Incident Reporting & Minimum Security Standards - https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg1402.pdf

Guidance on Incident Reporting & Minimum Security Standards)"[5]. This review was undertaken to update the guidelines considering the latest technological changes, the new legislative framework (Act of 2023) and changes introduced in the updated ENISA Technical Guidelines[6] (the "Revised Guidelines").

Future Work

16. The consultation closed on 25 May 2023 and ComReg is considering the responses received. ComReg expects to issue the Response to Consultation and associated Decision in due course, following careful consideration of the valuable responses received.

2.3 Network Security

General

17. Previously, Regulation 23 of the Framework Regulations placed obligations on providers of 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 included that they shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services and that measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks. Equivalent obligations are now contained in Part 2 of the Act of 2023[7].

Security of electronic communications networks

18. 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")[8], on 26 March 2019. Since then, ComReg has been working in close collaboration with the National Cyber Security Centre ("NCSC") to assist with the deliverables arising from Rec. 2335.

19. ComReg assisted the NCSC, which led Ireland's input into relevant EU working groups related to the deliverables of Rec. 2335. Further to this, ComReg has

[5] ComReg Document No. 23/36: https://www.comreg.ie/publication-download/network-incident-reporting-thresholds-a-consultation-to-revise-and-replace-comreg-document-14-02-reporting-guidance-on-incident-reporting-minimum-security-standards

[6] https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

[7] Parts 2 to 9 of the Act of 2023 were commenced on 9th of June 2023, by means of S.I. No. 299 of 2023. pdf (irishstatutebook.ie).

[8] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

provided input to the relevant ENISA and BEREC working groups and associated documents. This culminated in the publication of the report on the EU coordinated risk assessment on cybersecurity in Fifth Generation ("5G") networks[9] and the European Toolbox on the security of 5G networks[10] ("the Toolbox") on 29 January 2020.

20. The NCSC published its National Cyber Security Strategy 2019 – 2024 ("NCSS 2019 – 2024") in December 2019[11]. ComReg, as a stakeholder, has assisted 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.

Electronic Communications Security Measures ("ECSMs")

21. Since 2019, ComReg has been involved in supporting the development of the ECSMs with industry stakeholders.

22. The Department of the Environment, Climate and Communications ("DECC") consulted on the ECSMs on 23 November 2021[12] with the consultation having closed on 28 January 2022. ComReg has supported the DECC in the development of the Response to Consultation[13], ECSMs and forthcoming implementing legislation (Statutory Instruments ("S.I.")).

Future Work

23. Going forward, ComReg is responsible for the implementation of the ECSMs, and will assist DECC in relation to relevant secondary legislation in relation to same.

[9] https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049
[10] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127
[11] The National Cyber Security Strategy, 2019 – 2024:
https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

[12] https://www.gov.ie/en/consultation/6fc4c-technical-stakeholder-consultation-on-proposed-electronic-communications-security-measures-ecsms/
[13] 249308_81b8a7ef-530e-4e70-85be-26369cc48b23.pdf

24. This is a significant work programme which will establish and develop a framework, by which the security obligations of providers networks will be assessed, pursuant to Part 2 of the Act of 2023.

25. In order to prepare for this significant programme of work, ComReg took steps to establish a new Network Security Unit (“NSU”). Preparatory work is underway ahead of an S.I. to commence the ECSMs.

3 Network Incidents in 2022

3.1 General Commentary on 2022 ENISA Report for Ireland

26. All incidents reported to ENISA are derived from notifications made to ComReg via its incident reporting portal[14]. The information submitted populates an active database which facilitates efficient incident updates[15], even while incidents are still in progress. Once the incident has concluded, and following satisfactory finalisation of the root cause analysis, the incident report can be closed by the provider concerned.

27. This information enables ComReg to actively monitor trends, including but not limited to the type and occurrence of incidents. This along with other tools allows for the further investigation of events as necessary.

28. An incident report is provided to ENISA annually. A summary of the major incidents reported during 2022 is outlined below.

3.2 Overview of incidents reported to ENISA

29. There were twelve incidents reported to ComReg in 2022, compared to twenty-four in 2021 and the overall number of User Hours lost due to incidents reported also reduced.[16]

30. Of the twelve incidents reported, four exceeded the ENISA Threshold (in terms of User Hours lost), compared to twenty-one in 2021.

31. Notably however, there were no storms of any significance during the period, unlike the 2019 – 2021 and this generally explains the decrease in reported incidents.

32. Major causes of incidents in 2022 included faulty hardware, faulty software, or third-party failures, and where providers of other or ancillary services have caused or contributed to the outage. Again, ComReg notes that software replacement or upgrades, where feasible, should be thoroughly tested before being introduced into a production setting. Furthermore, ComReg also urges that upgrades take place out of hours (overnight) and that a clear testing and roll-back procedure is agreed in advance.

[14] See https://www.elicensing.comreg.ie/login.aspx .
[15] The guide to the new portal was published by ComReg as ComReg 19/98.
[16] The overall number of User Hours lost was 13,218,472, which is markedly less than the 2021 total of 50,609,004 User Hours lost.

33. ComReg notes that mobile, radio and overhead copper 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.

34. ComReg further 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 availability of communication services for the public in general. With the increase in remote working, following the COVID-19 pandemic, this is a matter of growing significance. With this in mind, ComReg commissioned the consultants DotEcon to undertake a foundational study in this area.

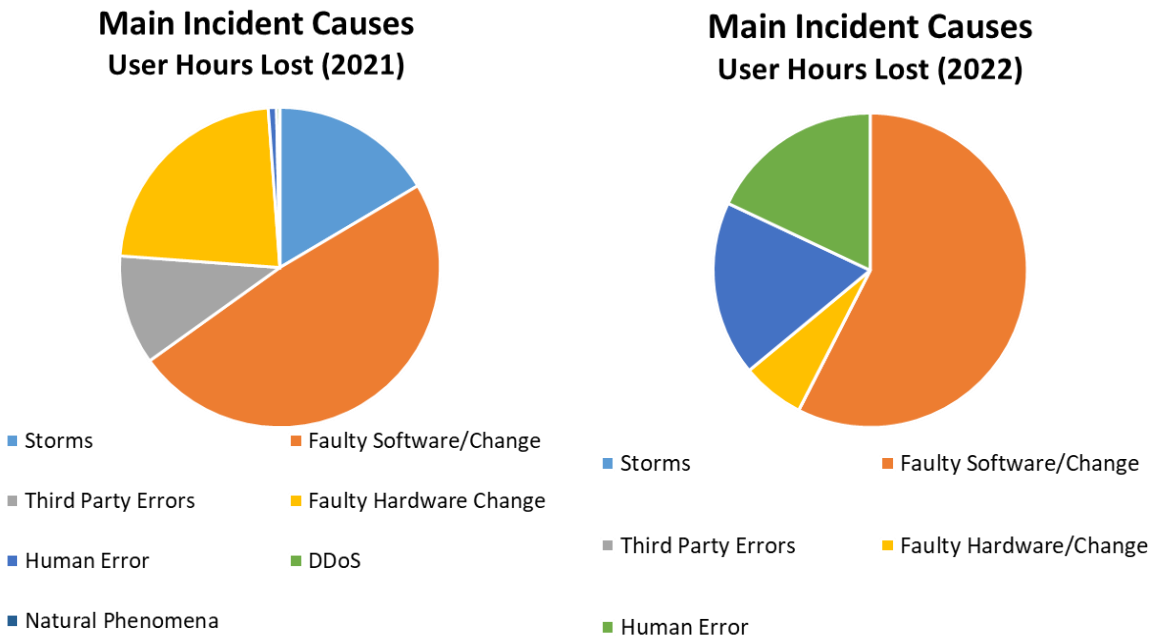

Figure 1 - Comparison of User Hours Lost 2021 to 2022

35. The DotEcon study has been published by ComReg as Document No. 23/59a and is available at www.comreg.ie

Future Work

36. ComReg will continue to fulfil its obligation to report significant incidents in 2023, in accordance with section 11 of the Act of 2023.

3.3 Storms and Other Natural Phenomena

37. In 2022, ComReg monitored both weather and space weather[17] events that could affect the provision of ECN and ECS in Ireland.

38. ComReg monitors warnings from Met Éireann, using 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, the most recent example of this was Storm Lorenzo in Autumn 2019[18].

39. Three separate storms were declared in 2022[19], thankfully none of which caused significant disruption. These were as follows:

- Dudley 16 February;
- Eunice[20] 17-18 February; and
- Franklin 20 February.

Further Work

40. During 2022 two projects in particular have helped to inform the work done by both the industry and ComReg in this regard and these are:

- Economic and Societal Impact of Incidents; and

[17] In relation to space weather, ComReg uses the tools offered by the NOAA and a useful information on space weather and its possible effects is here: https://www.swpc.noaa.gov/news/space-weather-educational-video

[18] 42. If an orange-level warning or named storm is announced by Met Éireann, then ComReg monitors it as it develops and engages with providers of national networks, where required NOU requesting the receipt of 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 DECC, as necessary. Requests for assistance from providers 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.

[19] The Western Europe Group (Met Éireann, Met Office and KNMI) named 6 storms (Arwen, Barra, Corrie, Dudley, Eunice and Franklin), while DMI named Malik. Seven named storms, in a season (2021-2022), is the joint 2nd (with 2019/20) lowest number of named storms since the project began.

[20] During the last storm season 2021/22, Eunice (February 2022) observed Ireland's highest sustained wind speeds of 106 km/h since Ellen's 111 km/h and highest 24-hr rainfall of 86.1 mm since Francis' 95.2 mm. Both storms Ellen and Francis occurred in August 2020.

- Climate Change and Adaptation of Telecommunications Networks.

Economic and Societal Impact of Incidents

41. ComReg procured expert advice from DotEcon to conduct a foundational study into the economic and societal costs of network incidents. This work is expected to provide guidance to providers in order that they can fulfil their obligations under Part 2 of the Act of 2023.

Climate Change and Adaptation of Telecommunications Networks

42. ComReg commissioned the study by Frontier Economics in late 2021, to consider in detail how communications networks are vulnerable to weather events that may increase in frequency and severity resulting from climate change. The report published as ComReg Document No. 22/100a presented findings on:

    - Communications networks' vulnerabilities to climate change;
    - Climate change preparation and adaptation measures implemented across networks; and
    - Potential steps to further adapt to climate change.

    The findings of the report were based on detailed information, including discussions undertaken with, communications network operators in Ireland, as well as climate and weather experts in Ireland (Climate Ireland and Met Éireann).

43. The infographic set out at figure 2 below, outlines the vulnerabilities of fixed and wireless communication networks to particular weather events; highlighting the three main areas of focus, for further improving the resilience of communication networks in light of climate change.

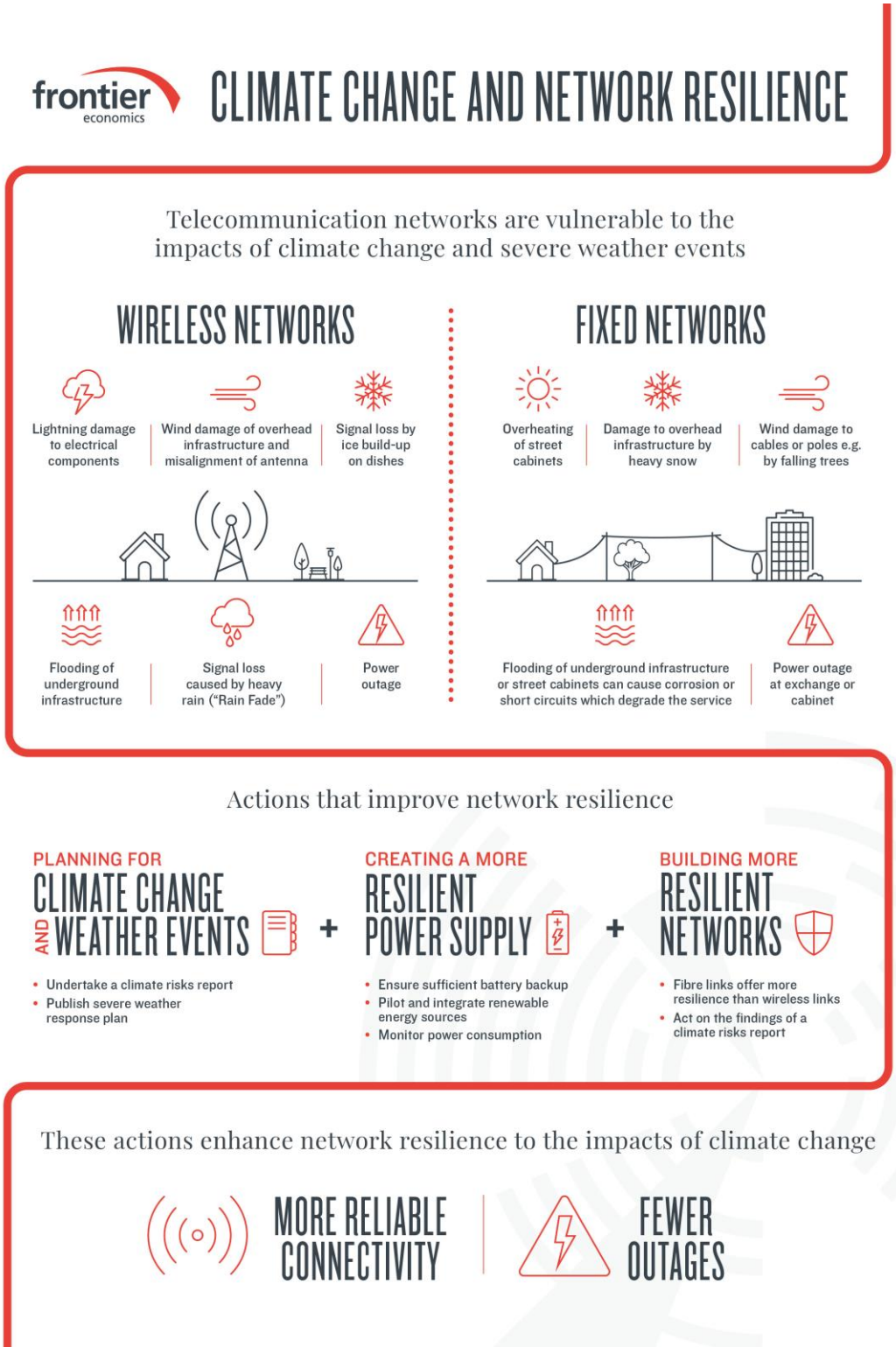

Figure 2. Climate Change and Network Resilience

4 Other Projects in 2022

4.1 Nuisance Communications

44. ComReg is actively working with the telecoms industry to mitigate the scourge of scam texts and calls in Ireland. Since early 2022, ComReg and the telecoms industry have been working together to restore trust in our telecommunications.

45. To help combat nuisance communications, ComReg has established an industry taskforce – the Nuisance Communications Industry Taskforce ("NCIT")[21], to bring together representatives of the telecoms industry, including fixed and mobile telecoms operators, meets regularly to develop what interventions are needed and how to implement them.

46. Several initiatives have resulted from this work item and the following documents have been published in 2022:

- IN 22/114 Nuisance Communications: Fixed CLI Blocking Intervention Arrangements for International Operations. Published 20/12/2022;
- IN 22/86 Nuisance Communications – Launch of 'Do Not Originate' Protocol. Published 24/10/2022;
- IN 22/86a Do Not Originate List – Guidance Note for organisations and Application Form. Published 24/10/2022; and
- IN 22/77 Nuisance Communications – Update on the Nuisance Communications Industry Taskforce. Published 30/09/2022.

47. The NCIT has met monthly since February 2022 and is chaired by an independent chairperson and secretariat.

48. More recently, on 16 June 2023, ComReg published its consultation on combatting scam calls and texts. Research commissioned by ComReg shows that in 2022 alone in Ireland there were:

- approximately 365,000 cases of fraud as result of scam calls and texts, (or 1,000 cases a day);
- up to 89 million annoying/irritating communications and 31 million distressing communications;
- over 5,000 businesses that were the victim of fraud after receiving scam calls and texts; and

[21] Nuisance Communications – Formation of the Nuisance Communications Industry Taskforce, 21/129 https://www.comreg.ie/publication/nuisance-communications-formation-of-the-nuisance-communications-industry-taskforce

- Overall, the total quantifiable harm to society arising is conservatively estimated at circa €309 million per annum.

49. ComReg is proposing that telecommunications operators implement a series of technical interventions to combat scam calls and texts all of which are detailed in ComReg Document 23/52 "*Combatting scam calls and texts, a consultation on network based interventions to reduce the harm from Nuisance Communications*" available at www.comreg.ie .

4.2 Network Monitoring

50. NOU has responsibility for ComReg's bi-annual drive testing programme. Two drive tests were conducted by AWTG on behalf of ComReg during 2022, the summer drive test report was published as ComReg 22/82, the winter 2022 drive test was published as ComReg 23/45.

Future Work

51. This work is expected to evolve to further assist with the verification and calibration of the outdoor mobile coverage maps. Any future drive tests may, for example, gather coverage measurements of targeted areas to review against other data sources.

4.3 Network KPIs

52. Following on from the work conducted during the COVID-19 pandemic, ComReg continues to monitor certain Key Performance Indicators ("KPI") of the providers of both Fixed and Mobile ECN and ECS, with a national footprint. The KPIs supplied are pursuant to section 13D(1)[22] of the Communications Regulation Act of 2002 (the "Act of 2002") and contain confidential data to allow ComReg to monitor the provider's security and integrity status. This has been in the exercise of ComReg's functions under sections 10(1)(a)[23] of the Act of 2002 and including ComReg's function, during the period to which this Annual Report relates, to enforce the security provisions of Regulation 23(1)[24] and 23(3)[25] of the Framework Regulations.

[22] Section 13D(1) of the Act of 2002 provides that: "*The Commission may at any time, by notice in writing, require an undertaking to provide it with such written information as it considers necessary to enable it to carry out its functions or to comply with a requirement made to it by the Minister under section 13B*."
[23] *"10.(1)(a) to ensure compliance by undertakings with obligations in relation to the supply of and access to electronic communications services, electronic communications networks and associated facilities and the transmission of such services on such networks".*
[24] *"23.(1) Undertakings providing public communications networks or publicly available electronic communications services 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."*
[25] *"23.(3) Undertakings providing public communications networks shall take all appropriate steps to guarantee the integrity of their networks, thereby ensuring the continuity of supply of services provided over those networks."*

This work will continue to evolve under Part 2 of the Act of 2023 which is now in force.

4.4 Mobile User Experience – Outdoor Mobile Coverage Mapping

53. ComReg's outdoor mobile coverage map 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 mobile connectivity requirements.

54. The outdoor mobile coverage map is regularly updated with three revisions taking place during 2022. The revisions account for new sites coming on-line and incorporate changes to the technology used. This not only affects coverage but can also lead to an improvement in the services offered in certain localities.

55. Following a consultation process ComReg published a response to consultation regarding 5G Outdoor Mobile Coverage Thresholds[26]. This paved the way for ComReg to map 5G as part of its Outdoor Mobile Coverage Map tool from its December 2022 revision onwards.

56. ComReg applies independent engineering calculations to the network data received from mobile network operators ("MNOs"). These calculations are then calibrated using a series of real-world Continuous Wave ("CW") measurements and targeted drive tests, at several locations throughout Ireland. Following calibration, the outdoor coverage map predictions are released via the ComReg website[27]. In addition to this, the analysis of the outdoor coverage predictions helps inform ComReg's current and future management of the radio spectrum.

57. ComReg remains one of the very first National Regulatory Authorities ("NRA") to make 5G available via its consumer facing mapping tools.

Future Work

58. In 2023 it is expected that this work will encompass the new bands assigned under the 2022 Multi-Band Spectrum Assignment[28], which facilitated an increase of 46% in the spectrum available for Wireless Broadband ("WBB") services.

[26] Response to ComReg Information Notice and study by Plum Consulting regarding 5G Outdoor Mobile Coverage Thresholds, 22/28 https://www.comreg.ie/publication-download/response-to-comreg-information-notice-and-study-by-plum-consulting-regarding-5g-outdoor-mobile-coverage-thresholds
[27] https://coveragemap.comreg.ie/map
[28] https://www.comreg.ie/industry/radio-spectrum/spectrum-awards/proposed-multi-band-spectrum-award/

4.5 Risks to Electricity Supply for ECN and ECS

59. Communications infrastructure has a critical dependency on the availability of secure electricity supply, the recent and continued heightened risk to electricity generation shortfall is a matter of concern for both ComReg and the telecommunications industry in general. During 2022, the impact of the war in Ukraine has also led to concerns regarding global energy supplies and its potential for subsequent impact to the secure supply of electricity, particularly in times of peak demand.

60. ComReg will continue to monitor the risk to electricity supply, in terms of the risks posed to the resilience of communications infrastructure and engage with undertakings of ECN and ECS regarding both the risk and possible mitigating factors in the coming year.

4.6 International Work

61. ComReg, via its NOU, contributes and participates in several international fora, primarily: the Body of European Regulators for Electronic Communications ("BEREC") including its 5G cybersecurity and NIS 2 Working Groups; and ENISA, in terms of the European Competent Authorities for Secure Electronic Communications ("ECASEC") group and its Working Groups.

Annex 1: Obligations on Authorised Operators and Relevant ComReg Powers

A 1.1 Obligations on Authorised Operators

A 1.2 During 2022, and until 9 June 2023, when Part 2 of the Act of 2023 was commenced[29], Regulations 23 and 24 of the Framework Regulations[30] were the legal provisions of key relevance to the activities of ComReg's NOU. Regulation 23 required that an undertaking that provides 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 undertaking providing a public communications network must also take appropriate steps to guarantee the integrity of that network.

A 1.3 In the event of a significant breach of security or integrity, the undertaking concerned was obliged to notify ComReg, who in turn had to inform the Minister[31]. Regulation 23(4)(b) provided that with the agreement of the Minister and where appropriate, ComReg also had to inform National Regulatory Authorities ("NRA") 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 could inform the public of a breach or require the undertaking concerned to do so.

A 1.4 Relevant ComReg Powers

A 1.5 Regulation 24 set out the powers available to ComReg and provided that, for the purposes of Regulation 23, ComReg could issue a direction to an undertaking requiring it to:

[29] By means of S.I. No. 299 of 2023, the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (Commencement) (No. 2) Order 2023.
[30] European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011). The Regulations were repealed on the commencement of Regulation 116 of S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022, as amended by S.I. No. 300 of 2023, the European Union (Electronic Communications Code) (Amendment) Regulations 2023.
[31] The Minister for the Department of the Environment, Climate and Communications.

- provide information needed to assess the security or integrity of its network / services; and/or

- submit to a security audit by a qualified independent body and to make the results available to ComReg.

A 1.6 These directions can also specify time limits for implementation and failure to comply with a direction is an offence.

A 1.7 A useful diagram from ENISA in the form of the virtuous triangle below (figure 1), relates undertakings' obligations under Regulation 23 to risk assessments made under Regulation 24. This is a prudent methodology for undertakings to adopt in reporting incidents. Following an incident, a risk could be lessened by adopting suitable mitigation measures, or failure to do so could result in ComReg issuing a security measures direction for such measures under section 14 of the Act of 2023.

A 1.8 Transposition of the EECC

A 1.9 The obligations regarding security that were contained in Regulations 23 and 24 of the Framework Regulations are, resulting from the transposition of the European Electronic Communications Code (the "EECC")[32] now contained within Part 2 of the Act of 2023. Furthermore, with the transposition of the EECC by inter alia section 11[33], which has now been commenced, the security incident reporting obligation now applies to "providers" as defined in section 5 of the Act of 2023[34].

A 1.10 ComReg notes that the relationships in the diagram shown below in figure 3, while being applicable to Regulations 23 and 24, are also generally applicable, going forward, to the methodology contained in Part 2 of the Act of 2023.

[32] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[33] By means of S.I. No. 299 of 2023, the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (Commencement) (No. 2) Order 2023.
[34] "provider" means a provider of public electronic communications networks or of publicly available electronic communications services.

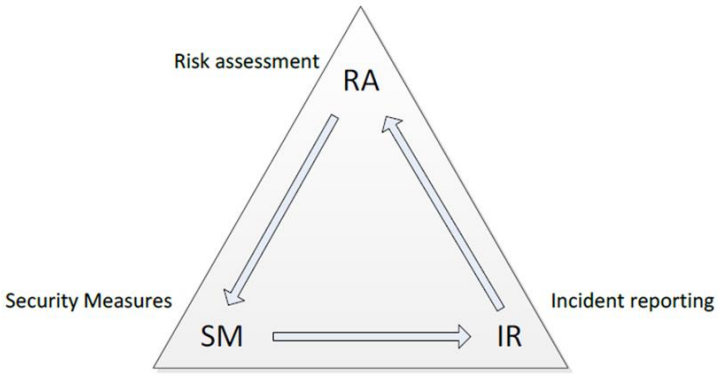

Figure 3: Relationships between Security Measures, Incident Reporting and Risk Assessment