An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations
Annual Report 2021

Information Notice

Reference:	ComReg 22/44
Version:	Final
Date:	09/06/2022

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:	22/44
Date:	09 June 2022

Content

Section Page

1 Introduction

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

2. This annual report is structured as follows:

   - Chapter 2: Outlines the Obligations on Authorised Operators and Relevant ComReg Powers;

   - Chapter 3: Covers Resilience and Network Incidents;

   - Chapter 4: Reviews network incidents for 2021;

   - Chapter 5: Outlines ComReg's work on Nuisance Communications;

   - Chapter 6 Details Other Projects undertaken by the NOU during 2021;

2 Obligations on Authorised Operators and Relevant ComReg Powers

2.1 Obligations on Authorised Operators

3. Regulations 23 and 24 of the Framework Regulations[1] are of particular relevance to the activities of ComReg's NOU. Regulation 23 requires that 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. Equivalent obligations, on authorised undertakings, are expected to be maintained in the context of the transposition of the European Electronic Communications Code (the "EECC")[2].

4. In the event of a significant breach of security or integrity, the undertaking concerned is obliged to notify ComReg, who in turn must inform the Minister[3]. With the agreement of the Minister and where appropriate, ComReg must also 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 may inform the public of a breach or require the undertaking concerned to do so.

2.2 Relevant ComReg Powers

5. 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.

[1] European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011)
[2] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[3] The Minister for the Department of the Environment, Climate and Communications.

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

7. The current powers, pursuant to this Regulation, are expected to be broadly maintained in the context of the transposition of the European Electronic Communications Code[4].

8. 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 prudent methodology for undertakings to adopt in reporting incidents. Following an incident, a risk could be lessened by adopting suitable mitigation measures.

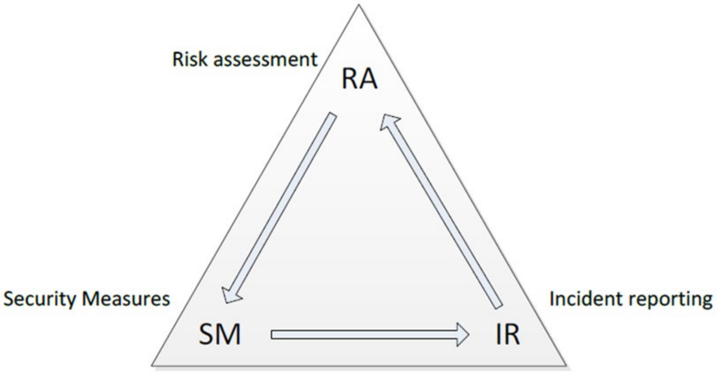


Figure 2: Relationships between Security measures, incident reporting and Risk assessment under Regulation 23 and 24 of the Framework Regulations.

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

3 Resilience and Network Incidents

3.1 Resilience of Networks and Services

9. 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.

10. The 2016 Directive on Security of Network and Information Systems ("NIS Directive")[5] 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.

11. The resilience of an electronic communications network can be affected in its core network 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 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.

12. Since late 2019, ComReg has been engaged in understanding and assessing the risk management practices of undertakings including, operators of publicly available electronic communications networks and services. Where appropriate, ComReg undertakes an assessment of risk management practices based on the information provided by the network operators and service providers.

13. This is a complex multi-year workstream and as such, has entailed seven phases, which are as follows:

[5] 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

- 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;

14. So far, phases 3, 4 and 5 – respectively have been in the main completed during the 2021 work programme. Furthermore, in late 2021, commenced on phase 6.

Future Work

15. Work on the resilience of Networks and Services is a core ongoing workstream for ComReg’s NOU and over the next year the concentration of effort, in this area, will be to complete phases 6 and 7.

3.2 Network Incidents

16. 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.

- Third party damage: including, vehicular impact, cable theft; fibre cuts, deep diving submarines, remotely operated vehicles ("ROV"), anchor, cable plough or trawler related, cable damage.

- Malicious acts: theft, Telephony Denial of Service ("TDoS") incidents, Distributed Denial of Service ("DDoS") incidents, 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. This is of significant concern to ComReg and as such, in 2021, ComReg commenced a project to study this.

- System failures including but not limited to hardware and software failure; insufficient redundancy; poor procedures, particularly 'roll-back' procedures[6]; poor supervision of both own and outsourced staff.

Incident Reporting and Thresholds

17. 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.

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

18. 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 14 February 2022 and the summary statistics are presented in Chapter 4 below.

19. 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[7] ("Document 14/02"). This 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 undertakings 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[8].

Future Work

20. ComReg expects to begin a review of the Reporting & Guidance on Incident Reporting & Minimum Security Standards, Document 14/02, this year. It is intended that this work will update Document 14/02 for changes in both technological focus, for example 5G, and in terms of the new legislative framework post EECC. This in the main, will reflect the changes in the updated ENISA Technical Guidelines[9]. As such, it is likely to include Number Independent Interpersonal Communications Services ("NIICS"), more commonly known as Over The Top ("OTT") providers.

[7] Reporting & Guidance on Incident Reporting & Minimum Security Standards - https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg1402.pdf

[8] 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

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

3.3 Network Security

General

21. Regulation 23 of the Framework Regulations places obligations on undertakings 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 include 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.

Security of electronic communications networks

22. 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")[10], on 26 March 2019. Since then, ComReg has been working in close collaboration with the NCSC to assist with the deliverables arising from Rec. 2335.

23. ComReg assisted the NCSC, as it led Ireland's input into relevant EU working groups related to the deliverables of Rec. 2335. Further to this, ComReg has provided input into the relevant ENISA and BEREC working groups and subsequent output documents in respect of this matter. This culminated in the publication of the report on the EU coordinated risk assessment on cybersecurity in Fifth Generation ("5G") networks[11] and the European Toolbox on the security of 5G networks[12] ("the Toolbox") on 29 January 2020.

24. The NCSC published its National Cyber Security Strategy 2019 – 2024 ("NCSS 2019 – 2024") in December 2019[13]. ComReg, as a stakeholder, has been involved in 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.

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

- 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")

25. ComReg has been closely involved with the NCSC in running the various workshops to support the development of the ECSMs with industry stakeholders. These workshops included: speakers from security stakeholders on several relevant topics and a discussion of the principles underlying each of the ECSMs. The Department of the Environment, Climate and Communications ("DECC") consulted on the ECSMs on 23 November 2021[14] with the consultation having closed on 28 January 2022.

Future Work

26. ComReg will be responsible for the implementation of the ECSMs post transposition European Electronic Communications Code ("EECC"), this will be a significant work programme to establish and develop a framework by which to assess operator networks. ComReg will continue to work in close co-operation with the NCSC to assist it in the delivery of the measures contained in the NCSC 2019-2024 strategy throughout the coming period.

[14] https://www.gov.ie/en/consultation/6fc4c-technical-stakeholder-consultation-on-proposed-electronic-communications-security-measures-ecsms/

4 Network Incidents in 2021

General Commentary on 2021 ENISA Report for Ireland

27. All incidents reported to ENISA are drawn from notifications made to ComReg in accordance with Document 14/02[15].

28. The incident reporting portal[16], employed for this purpose, uses two-factor authentication and only registered undertakings can access it. Information submitted populates an active database, securely storing the information. This allows for easier incident updates[17] while the incident is still in progress. Once the incident has concluded, and provided the root cause analysis has been completed satisfactorily, the incident report can be closed by the undertaking concerned.

29. This information facilitates ComReg 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 as necessary..

30. An incident report is provided to ENISA annually. A summary of the major incidents experienced during 2021 is outlined below.

4.1 Overview of incidents reported to ENISA

31. There were twenty-four incidents reported to ComReg in 2021, compared to seventeen in 2020. The overall number of User Hours lost due to incidents reported in 2021 are on a par with 2020.

32. Major causes of incidents in 2021 included: software bugs, poorly implemented software updates and hardware failures. ComReg notes and is concerned with the number of major incidents involving Firewalls (6). Undertakings must be most thorough in the testing, scaling, updating and replacement of these essential resources.

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

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

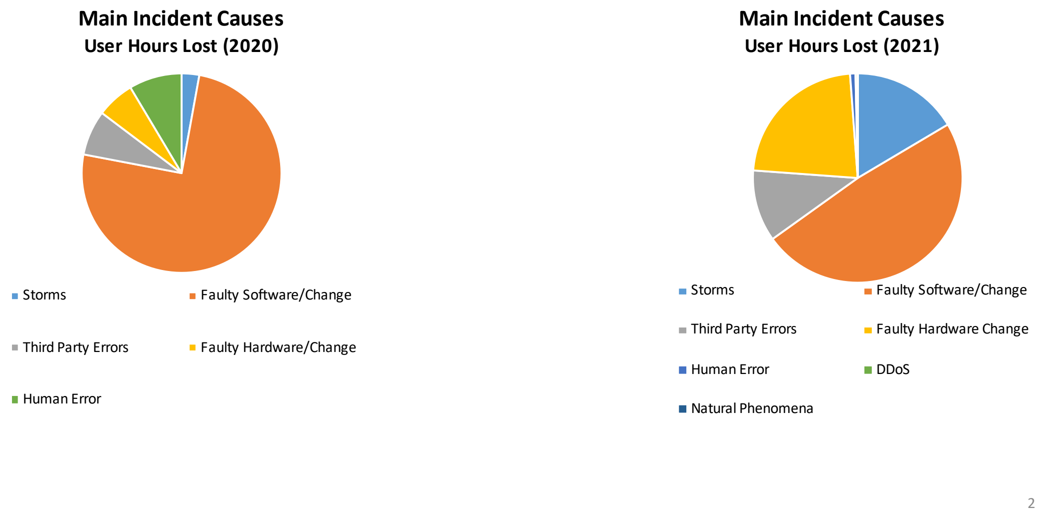
[17] The guide to the new portal was published by ComReg in 2019, see ComReg 19/98

33. Again, in common with 2020, the number of hours lost was often compounded by procedural flaws. These incidents typically arose during hardware and software network changes.

34. 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 the fixed underground plant tends generally to be more vulnerable to flooding, caused by storm surges and heavy rain.

35. 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 increase in remote working, arising from the COVID-19 pandemic, this is a matter of growing significance.

2020-2021 Above Threshold Incident Comparison: Main Incident Causes



4.2 Storms and Other Natural Phenomena

36. In 2021, ComReg monitored three separate weather events, of which only Storm Barra caused significant disruption. ComReg monitors warnings from Met Éireann and uses 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 recent example of this being Storm Lorenzo in Autumn 2019.

Named Storms and duration in 2021:

Arwen	25 November
Barra	7 – 9 December

37. Of the 2021 meteorological events, only Storm Barra caused outages above normal levels, totalling 9,822,864 User Hours lost, which was notably greater than the 2020 experience.

38. If an orange-level[18] warning or named storm[19] is announced by Met Éireann, then ComReg monitors 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 DECC, as necessary.

39. 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.

Future Work

40. Over the coming year, two new projects and an ongoing workstream will influence the work done by ComReg in this regard and these are:

[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).

- Economic and Societal Impact of Incidents; and
- Climate Change and Adaptation of Telecommunications Networks.

Economic and Societal Impact of Incidents

41. As part of its work on both network incidents and on the forthcoming transposition of the European Electronic Communications Code ("EECC"),

42. ComReg procured expert advice to develop a model to estimate the economic and societal costs of a network incident. This work is underway and expected to conclude in 2022.

Climate Change and Adaptation of Telecommunications Networks

43. During 2021 and given the increasing intensity and incidence of storms and weather events and their subsequent effect on undertakings, ComReg commenced a project seeking expert advice on the relationship between network incidents and meteorological events. This work is now underway and expected to conclude in 2022.

Ongoing Workstream: ENISA Report 2022 and NOU Annual Report 2022

44. Through the work of its 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, ComReg will issue its Annual Report for 2022, which will summarise the work carried out in respect of the work of its NOU, including but not limited to, incident reporting and incident types that have emerged during the year.

5 Nuisance Communications

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

46. Irish society and its economy have become ever more reliant on telecommunications technology. While it is deeply integrated into all areas of the economy and society, this constant in our lives comes with its own threats and vulnerabilities.

47. Fraud using electronic communications networks and services has become a low-risk form of crime. The reduced cost and increased availability of the equipment needed has seen incidents of fraud multiply in Ireland. Our daily use of electronic communications networks and services is exploited by criminals, who use social engineering type attacks, for example: vishing, smishing and CLI spoofing; with the intention of illegally acquiring personal consumer information, ultimately to abet financial fraud.

48. At its heart, this fraud is the abuse of telecommunications products (mainly telephones and mobile phones) or services, with the specific intention of illegally acquiring money from a communication service provider or its customers. Criminals prey on our daily use of electronic devices and continuously seek out new ways to exploit vulnerabilities and access information.

49. Consumers are being inconvenienced, confused and threatened by the volume of nuisance communications. With the clear and present danger that consumers can be manipulated into providing sensitive personal information, such as Personal Public Service Numbers (PPSN) and banking information. This also has systemic effects, for example the Commission for Communications Regulation ("ComReg") is aware of anecdotal cases of businesses needing to advise customers that their calls may come from unknown numbers, to ensure they will be answered. This implies that nuisance communications are leading to missed appointments and lost business. In short, trust is being lost in electronic communications services, and this is in turn impacting consumers and the economy at large.

50. Given the increasing frequency of nuisance communications and the damaging effects on public confidence in the integrity and trustworthiness of electronic communications, ComReg convened an industry taskforce to address the matter, with the full support of the DECC.

Nuisance Communications Industry Taskforce

51. To help combat nuisance communications, ComReg has established an industry taskforce – the Nuisance Communications Industry Taskforce (“NCIT”), to bring together representatives of the electronic communications industry.

52. ComReg issued an Information Notice[20] to extend this invitation to members of the electronic communications industry. Membership of NCIT is limited to persons employed by organisations who have and operate within the State under a General Authorisation and carry voice calls and/or SMS messages.

53. The NCIT continues meet monthly and is being chaired by an independent chairperson and secretariat, reporting to ComReg.

[20] Nuisance Communications – Formation of the Nuisance Communications Industry Taskforce, 21/129, 17th December 2021.

6 Other Projects in 2021

6.1 COVID-19

54. The COVID-19 pandemic and the Government's Public Health restrictions; led to continued work for, the industry and ComReg. This was in response to the need for employees to work from home, due to public health restrictions in place to mitigate the spread of COVID-19 and to ensure business continuity where possible.

55. Again, during 2021, ComReg's NOU acted as a central coordination point between undertakings and DECC to continue monitoring network stability and resilience. Ensuring that essential services, such as telecommunication networks, could support the increased load on both fixed and mobile data services and fixed and mobile voice services, this involved sourcing information on network stability directly from the undertakings. Regular meetings with undertakings, DECC and other stakeholders were necessary to discuss the impact of public health restrictions and/or issues that arose consequently.

Network Monitoring

56. The NOU has responsibility for ComReg's current bi-annual drive testing programme. However, due to the COVID-19 pandemic and subsequent Government Public Health restrictions, ComReg, with the agreement of Advanced Wireless Technologies Group Limited ("AWTG") suspended this work during 2020 and the first half of 2021.

57. Following the relaxation of the travel restrictions in the second half of 2021, AWTG conducted the winter 2021 Drive Test on behalf of ComReg and in January 2022, ComReg issued a report[21] on the results of the drive test.

Mobile User Experience – Outdoor Mobile Coverage Mapping

58. 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 connectivity requirements.

[21] https://www.comreg.ie/publication/assessment-of-mobile-network-operators-compliance-with-licence-obligations-coverage-winter-2021

59. The outdoor mobile coverage map is regularly updated, both in terms of new sites coming on-line, as well as incorporating changes to the technology used on the sites. This not only affects coverage but can also lead to an improvement in the services offered in that locality.

60. 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, undertaken at several locations throughout Ireland. Following calibration, the outdoor coverage map predictions are released via the ComReg website[22]. In addition to this, the analysis of the outdoor coverage predictions helps inform ComReg's current and future management of the radio spectrum.

Future Work

61. Over the next year it is expected that a further release of the mobile coverage map will include updates to include 5G bands and technologies. Furthermore, this project will continue to evolve for both newly assigned frequency bands and technological updates.

6.2 Secure supply of power

62. The matter of secure supply of power is a matter of concern for ComReg and the telecommunications industry. In the lead into winter 2021, ComReg engaged with undertakings of ECN and ECS regarding the risk posed to the continuity of networks and services. While not unique to Ireland, the impact of the war in Ukraine has led to further concerns regarding energy supply and its subsequent impact on the secure supply of power.

63. ComReg will continue to monitor the situation and engage with undertakings of ECN and ECS regarding the risk in the coming year.

[22] https://coveragemap.comreg.ie/map

6.3 International Work

64. 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.

65. During the COVID-19 pandemic, this work has been done remotely using web-based video conferencing tools. This has facilitated both regularly scheduled and ad-hoc meetings, with ComReg being able to fully participate and contribute to the work.