An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations
Annual Report 2018

Information Notice

Reference: ComReg 19/31

Version: Final

Date: 29/03/2019

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:	19/31
Date:	29 March 2019

Content

Section Page

1: Introduction

1. This is the first annual report on the activities of the Network Operations Unit ("NOU") of the Commission for Communications Regulation ("ComReg"), following the NOU's formation in Q2 2018.

2. The NOU is a specialised unit and a centre of expertise on technical network issues. The NOU sits within the Market Framework Division but does not 'belong' to any Division and is intended to support ComReg across all of its functions, as required.

3. Since its establishment, and with the cooperation of ComReg's Wholesale and Retail Divisions, the NOU has recruited several specialist staff with relevant expertise and experience. The NOU has also had the full support of the Corporate Services Division, and IT and Facilities sections, in facilitating the required resources.

Figure 1: ComReg Monitoring Room at Dockland Central

4. This annual report is structured as follows:

- Chapter 2 covers the background to the report;
- Chapter 3 introduces the concepts of network resilience and incidents;
- Chapter 4 reviews network resilience incidents for 2018; and
- Chapter 5 presents an overview of future work for the NOU.

2: Background

5. 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.

6. 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]

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

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

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

Obligations on Authorised Operators

9. Of particular relevance to the NOU is regulation 23 of the Framework Regulations. 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. In the event of a significant breach of security or integrity, the undertaking concerned must notify ComReg and ComReg in turn must inform the Minister and, with the agreement of the Minister and where appropriate, ComReg must also inform national regulatory authorities in other EU Member States and ENISA. And 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.

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

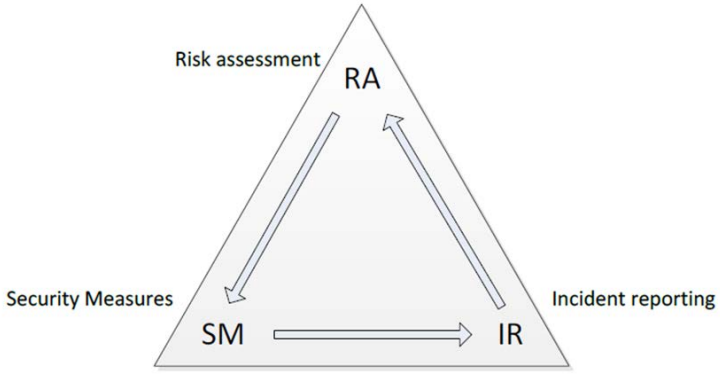


Figure 2: Relationships between Security measures, incident reporting and Risk assessment under Regulation 23 and 24 of the Framework Regulations.

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

3: Resilience, Network Incidents and Special Events

Resilience

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

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

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

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

What are Network Incidents?

14. As described in Chapter 3, 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, Article 4 of the NIS Directive defines an "incident" as 'any event having an actual adverse effect on the security of network and information systems'. Typical incidents include:

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

Figure 3: Typical causes of Incidents that affect Network Resilience

Incident Reporting and Thresholds

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

16. ComReg must also annually submit 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 26 February 2019 and the summary statistics are presented in Chapter 4 of this Document.

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

- Exceed 1 hour with more than 15% of users affected;
- Exceed 2 hours with more than 10% of users affected;
- Exceed 4 hours with more than 5% of users affected;
- Exceed 6 hours with more than 2% of users affected; or
- Exceed 8 hours with more than 1% of users affected.

Special Events

18. The NOU also acts as a central coordination point between ComReg and undertakings in monitoring network resilience for special events, such as international sporting events (i.e. UEFA Euro 2020), State visits with high media interest (e.g. the 2018 Papal visit), large music festivals, and the St. Patrick's Day parade.

19. The NOU also works with ComReg's Licensing unit and Spectrum Intelligence and Investigations unit to ensure that all special events are properly covered in terms of network resilience and effective management of radio frequency spectrum.

4: Network Incidents in 2018

20. The summary statistics as presented from the ENISA portal for 2018 are shown in the figure below.

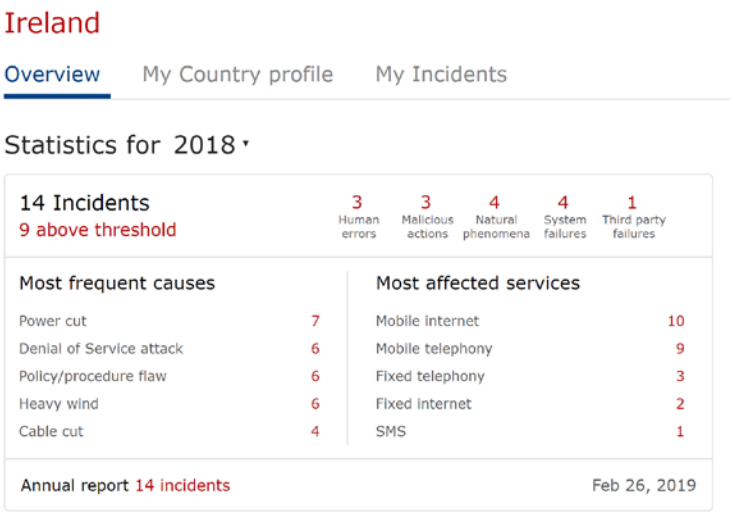


Figure 4: Summary Statistics as presented on ENISA portal for 2018

General Commentary on 2018 ENISA Report for Ireland

21. All incidents reported to ENISA are based on notifications made to ComReg using ComReg reporting form 14/02[8] and sent to ComReg at incident@comreg.ie. When an incident report form is submitted, the NOU may go back to the undertaking concerned for further information about the outage and any actions taken to prevent or reduce the risk of a recurrence or to mitigate the effects. Once the NOU is satisfied that an incident has been dealt with sufficiently, the report is anonymised and uploaded to the ENISA portal.

22. Most reported outages are power outages, mostly caused by storms. Mobile and radio networks are more prone to the effects of adverse weather (wind damage, ice, and heavy rain) while fixed underground plants is more vulnerable to flooding, caused by storm surges and heavy rain.

23. The next largest causes of outages were Distributed Denial of Service ("DDoS") attacks and Policy and Procedure flaws. This latter category results from poor or

[8] See Annex 1 for an example of the Incident Reporting Form.

lack of Standard Operating Procedures ("SOPs") which typically come to light during network changes (hardware and software). It can also be worsened by poor supervision and poorly trained outsourced staff.

Storms and Other Natural Phenomena

24. In 2018, the NOU monitored 23 separate weather events, from Storms Eleanor and Fionn in January 2018 through to Storm Diana in November 2018. The 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 is to include Atlantic storms which could pass over Ireland, the most famous example being Storm Ophelia in October 2018.

25. If an Orange Level warning or named Storm is announced by Met Éireann, the NOU can monitor from two locations and can communicate with operators of national networks and the NOU receives twice daily reports from such operators. This information is then passed on to the National Emergency Coordination Group ("NECG") and/or the Department of Communications Climate Action and Environment ("DCCAE"), as necessary. Requests for assistance from network operators can be passed via the NECG to appropriate State agencies, in order to achieve a quicker resolution of any outage than the operator could achieve without such assistance.

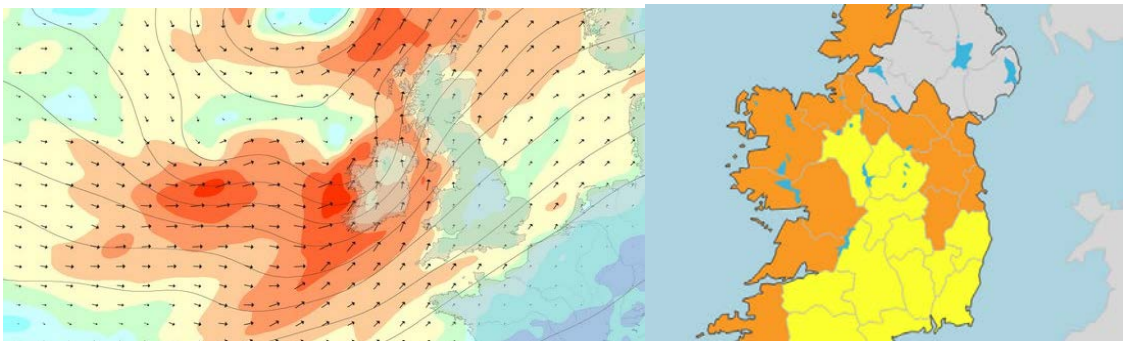


Figure 5: Storm Ali; Screenshot from Magic Seaweed and Met Éireann Warning Map

Named Storms[9] in 2018:

Eleanor	2-3	January	2018;
Fionn	16	January	2018;
Georgina	23-24	January	2018;
Hector	13-14	June	2018;
Ali	19	September	2018;
Bronagh	20-21	September	2018;
Callum		12-13 October	2018;
Deirdre		15-16 December	2018

Storms named by other Agencies;

Winter Storm Emma,	26 February-05 March,	2018
Storm Diana	27-30 November	2018

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

5: Future Work

Incident Reporting Portal

26. The NOU, in conjunction with the Corporate Services IT section, is developing a new portal to streamline the notification of incidents. The format will remain as set out in Form 14/02 but the form will be submitted to ComReg electronically (to incident@comreg.ie) rather than in hardcopy form.

27. The new portal will include two-factor authentication, with only registered undertakings able to use it, and it will enable modification and updating of submitted information while an incident is still in progress. If an incident has ended and if the cause analysis has been satisfactorily completed by the undertaking concerned to ComReg satisfaction, then the incident report can be closed. Should it be required by an undertaking, the NOU in exceptional circumstances and at its sole discretion may reopen an Incident Report, in order to allow the undertaking to make any corrections or to submit further information.

28. The portal will allow the NOU to actively monitor trends including but not limited to the type and occurrence of incidents; as the active form will populate a database. This would allow for the further investigation of events if deemed necessary by the, Market Framework, Retail and Wholesale Divisions ("Operational Divisions"), within ComReg.

Adaptation

29. As can be seen from both the amount of Storms and weather events discussed in the previous Chapter. ComReg considers it prudent, that the links to network incidents and meteorological issues is investigated. ComReg intends to consult on this in the next work-plan year 2019-2020. While it is too early to say what the outcome of this work will be, it could usefully be used to act as guidelines for AO to consider when hardening their ECN or ECS to meteorological factors.

ENISA Report 2019 and NOU Annual Report 2019

30. The NOU will fulfil its obligation under Regulation 23 of the Framework regulations and once again will summarise the incident types in the NOU Annual Report 2019.

European Electronic Communications Code ("EECC")

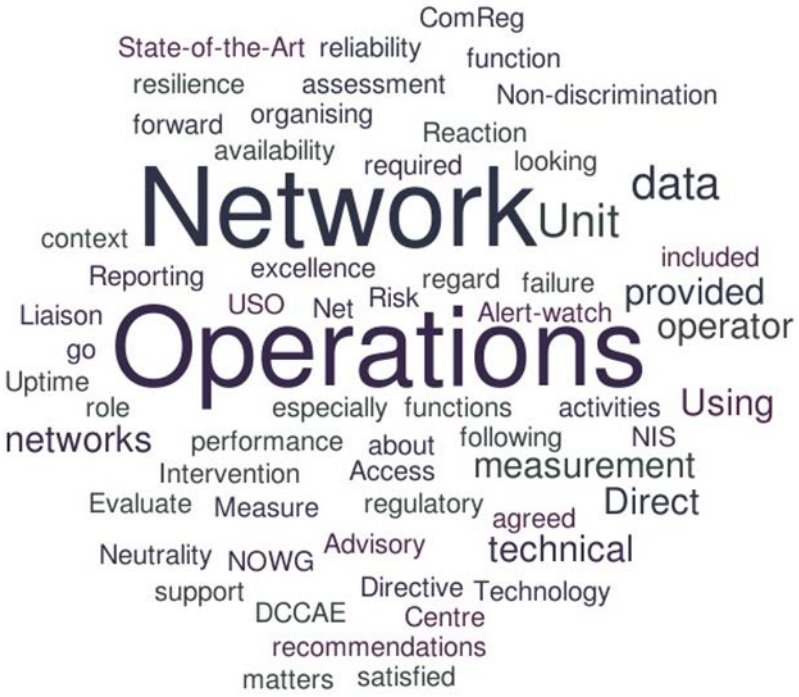
31. The NOU will support ComReg's Operational Divisions with technical advice on any factors under consideration during the Transposition of the EECC into Irish law by DCCAE.

Network Monitoring

32. The NOU has assumed responsibility for ComReg's bi-annual drive testing programme which was conducted between 18 November 2018 and 18 December 2018, by its contractor Advanced Wireless Technologies Group Limited ("AWTG") and has issued the first summary report in this regard[10].

33. In conjunction with ComReg's Spectrum Intelligence and Investigations ("SII") Unit, the NOU plan to advance ComReg's remote radio frequency spectrum monitoring capabilities in the coming work year, 2019-2020. In relation to the monitoring of ECN and ECS in general and in conjunction with ComReg's Operational Divisions the NOU is actively exploring methodologies and suitable technologies in this regard.

[10] https://www.comreg.ie/publication/assessment-of-mobile-network-operators-compliance-with-licence-obligations-coverage-winter-2018/


ComReg
State-of-the-Art
reliability
function
resilience
assessment
Non-discrimination
forward
organising
Reaction
availability
required
looking
Network
Unit
data
context
included
Reporting
excellence
regard
failure
provided
Liaison
USO
Net
Risk
Alert-watch
Operations
operator
go
Uptime
role
especially
functions
activities
Using
networks
performance
about
following
NIS
Intervention
Access
measurement
Evaluate
Measure
regulatory
Direct
agreed
Neutrality
NOWG
Advisory
technical
support
Directive
Technology
DCCAE
Centre
recommendations
matters
satisfied