EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TELECOM SECURITY INCIDENTS 2024

JULY 2025

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

More information about ENISA and its work can be found here: www.enisa.europa.eu

CONTACT

For content queries about this report, please email incidentreporting@enisa.europa.eu
For media or general queries about this document, please use info@enisa.europa.eu

Authors

Rossen Naydenov (ENISA), Nuno Rodrigues Carvalho (ENISA), Edgars Taurins (ENISA)

Acknowledgements

We are grateful for the review and input received from the members of the ENISA ECASEC expert group, which comprises national telecom regulatory authorities (NRAs) from the EU and European Economic Area, European Free Trade Association and EU candidate countries.

Legal notice

Copyright notice

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The present report provides anonymised and aggregated information about major telecom security incidents which occurred during 2024. Incident reporting is an important enabler of cybersecurity supervision and a support tool for policymaking at the national and EU levels.

In the EU, telecom operators notify significant security incidents to their national authorities. The national authorities send summary reports to ENISA. Under Article 40, the European Electronic Communications Code (EECC 2018/1972) reinforces the provisions ([1]) for reporting incidents, clarifying what incidents fall within its scope ([2]), as well as the technical guidelines ([3]) and the notification criteria. CIRAS is a platform that provides statistics, collects data from national authorities and provides a visual tool for displaying incidents through specific graphs ([4]). The incident reporting period for 2024 was from January 1st to February 24th 2025.

It is worth mentioning that as of 18 October 2024, the NIS2 Directive repeals Articles 40 – 41 of the EECC, which will consolidate the reporting of breaches of integrity and availability across multiple sectors including but not limited to providers of public electronic communications networks and providers of publicly available electronic communications services. The present report covers only 2024, where articles 40 - 41 of the ECCC are still valid.

Key findings in 2024 summary report

The 2024 annual summary contains reports of **188 incidents** submitted by national authorities from 26 EU Member States and 2 European Free Trade Association (EFTA) countries. This is an increase of 20,5% over the 2023 with 156 incidents from 26 EU Member States and 1 EFTA country.

Compared to 2022 and 2023, 2024 shows a significant drop in user hours lost.

A significant decrease of more than 50% of user hours lost was observed in 2024 compared to 2023. According to the data received, **1743** million user hours ([5]) were lost in 2024 while **3906** million user hours were lost in 2023. This is clearly a much lower number compared to last year, and returns at the levels of a decade ago, as we can see in **Figure 1**. A plausible hypothesis is that the trend may indicate the possibility of improved outage management, enhanced infrastructure, and increased system resilience.

([1]) The reporting of security incidents has been part of the EU's regulatory framework for telecoms since the 2009 reform of the telecoms package, in line with Article 13a of the framework directive (2009/140/EC) that came into force in 2011.
([2]) It is worth noting that since 2016 security incident reporting is also mandatory for trust service providers in the EU under Article 19 of the eiDAS regulation. In 2018, under the NIS directive, security incident reporting became mandatory for operators of essential services in the EU and for digital service providers, under Article 14 and Article 16 of the NIS directive.
([3]) ENISA technical guidelines on incident reporting under the EECC, including on thresholds and calculation of hours lost.
([4]) available on https://ciras.enisa.europa.eu
([5]) Derived by multiplying for each incident the number of users by the number of hours.

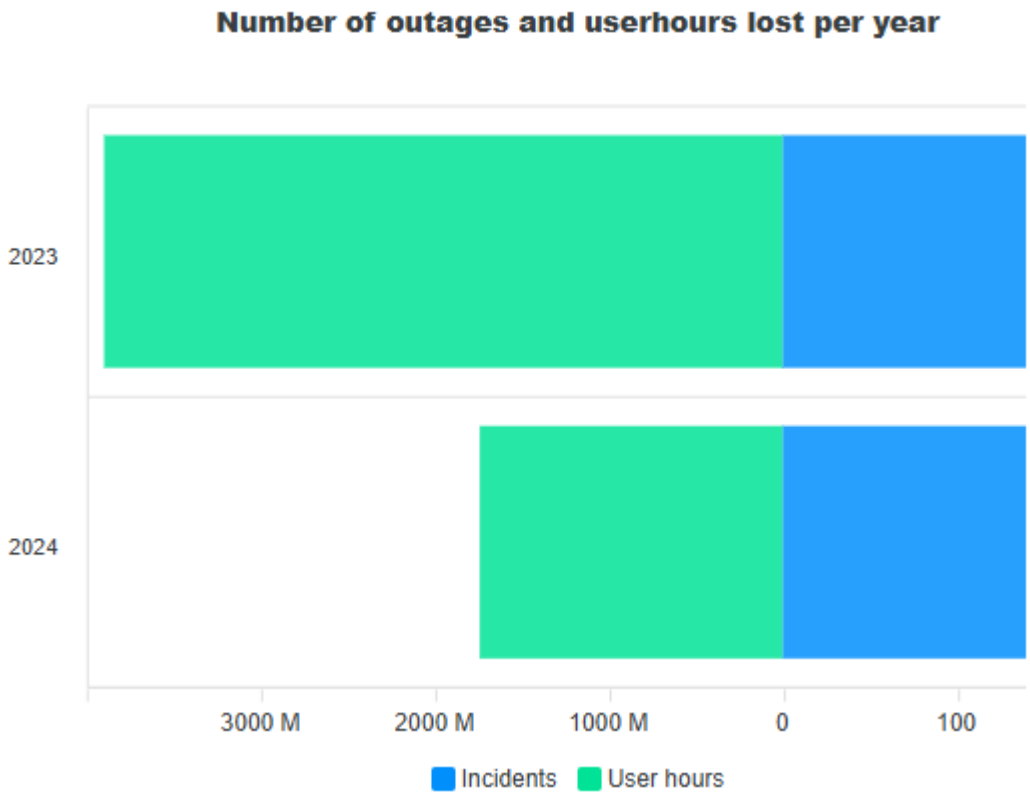

Figure 1: Number of incidents submitted by countries and user hours lost (2023–2024)

Additionally, the following findings can also be highlighted:

- Highest number of incidents to date (188) reported in electronic communications incident reporting to ENISA. Despite the rise in reported incidents, there was no corresponding increase in user hours lost.
- The distribution of incidents was as follows: service outage - 178, other impact on service - 4, Impact on other systems - 1, threat or vulnerability - 1, impact on redundancy - 2 and near miss - 1.
- **19,5% Increase in incidents** with very large impact from 77 (2023) to 92 (2024).
- Root causes key statistics**:**
    - **System failures** continued to largely dominate in terms of impact, reaching 60% in 2024 with 113 incidents, which is a slight decrease from 2023 (61%). They accounted for 548 million user hours lost or almost a third of all the user hours lost for 2024.
    - **Human errors** make a small decrease in percentage of incidents to 19% coming from 21% in 2023, however there is more than two times increase of user hours lost from 181 million to 402 million in 2024.
    - Incidents due to **natural phenomena** increased to 25 reaching a share of 13% leading to 605 million user hours lost, which is an increase of almost than 9 times the previous year (2023 - 72 million user hours lost).
    - **Malicious actions** accounted for 15 incidents representing 8% share of total incidents for 184 million user hours lost, which is lower than in 2023 with 16 incidents representing 10% and 214 million user hours lost.
- Affected services key statistics
    - **Mobile telephony** and **mobile internet** were again the most impacted sectors, with respectively 100 and 86 incidents, for a share of 57% and 49% similar to 2023.
    - Fhe fixed internet increased their share of incidents from 16% in 2023 to 26% in 2024.
- Technical causes
    - In 2024, **41 incidents were marked as cable cuts (23%)**, which gives it a 10 % lead over the next two technical causes, such as faulty software change/update (14%) and software

bugs (13%). The positions of cable cuts and faulty software change/update swap if we take into account the resulted user hours lost. Faulty software change/update incidents lead to 515 million user hours lost, while cable cuts to 331 million.

- In 2024, 65 incidents were flagged as **failures by third parties** which is a 25% increase compared to 2023 where 52 were reported.
- **No cross-border** incidents were reported.

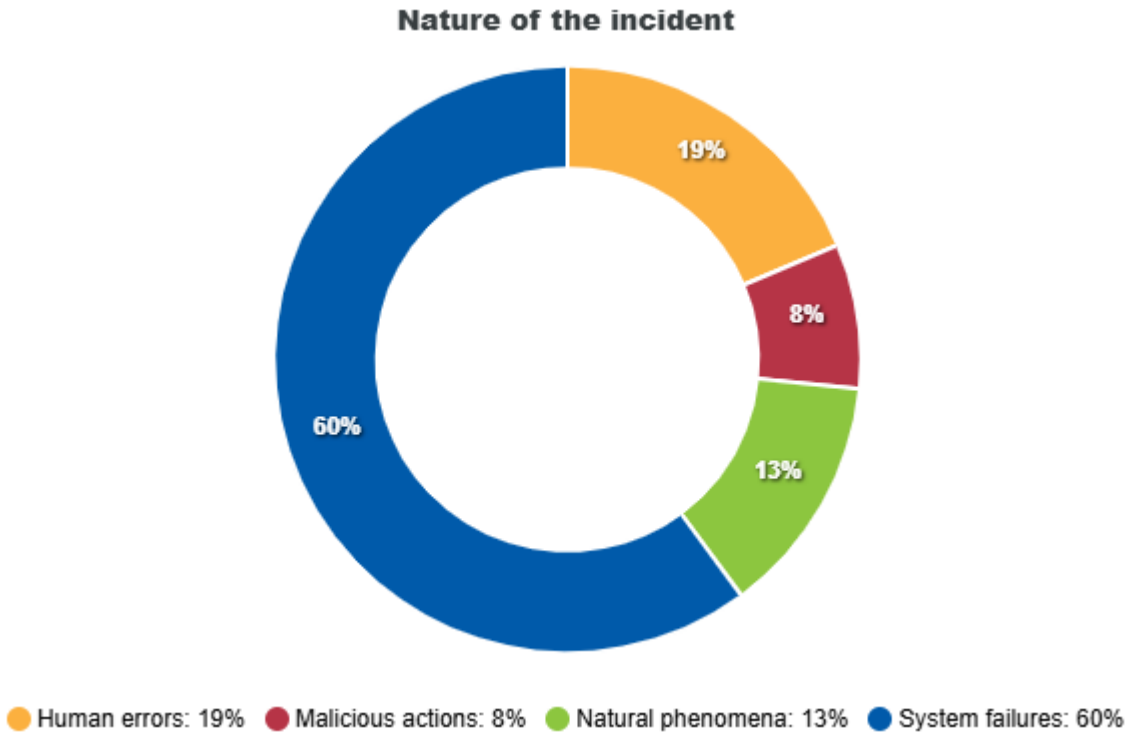

Figure 2: Root cause category

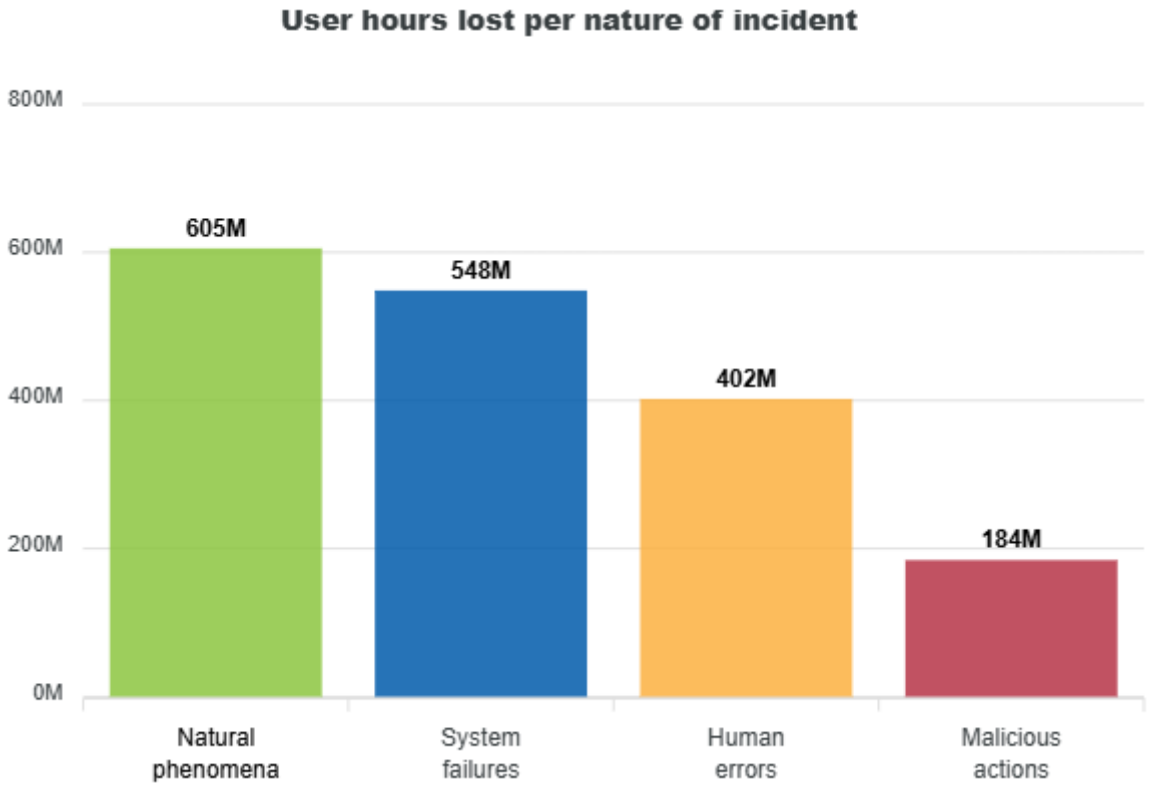

Figure 3: Share of user hours lost for each root cause category

Multiannual trends over the period 2012–2024

Over the 13 years, EU Member States reported **1 930** telecom security incidents, stored in the ENISA cybersecurity incident reporting and analysis system **(CIRAS)**. The statistics are accessible online ([6]).

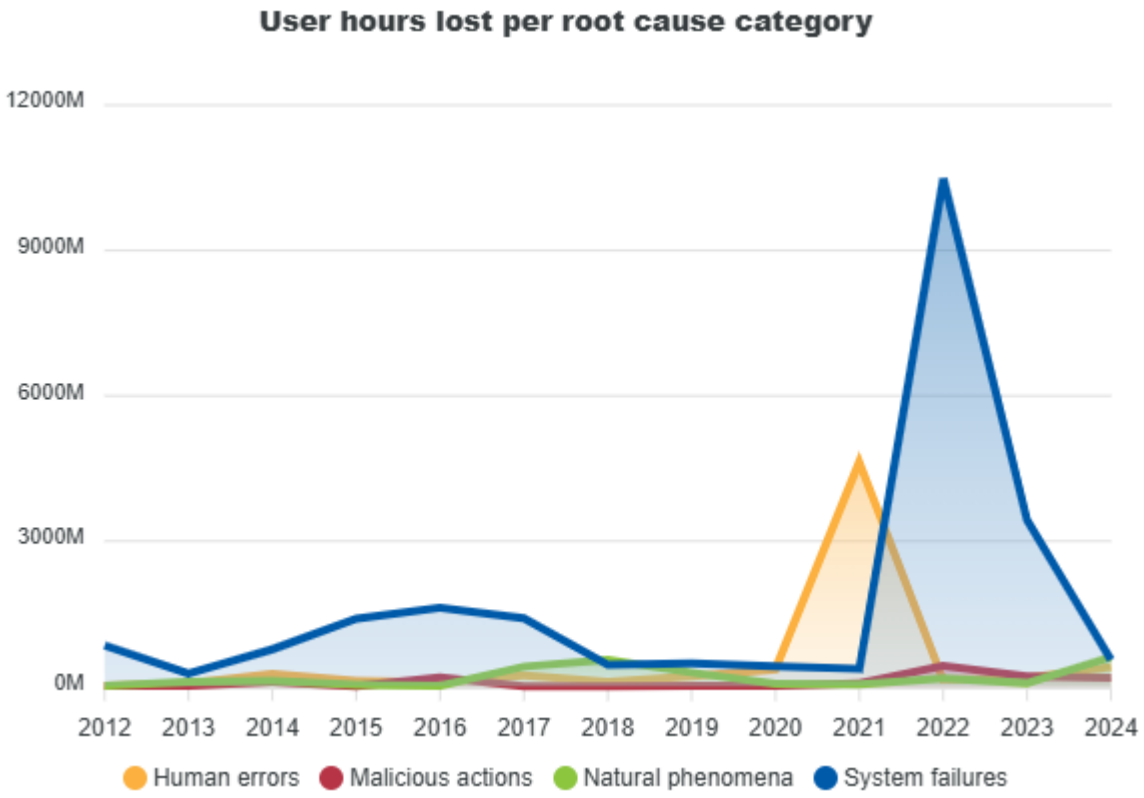

Figure 4: Root cause categories for telecom security incidents in the EU reported over the 2012–2024 period

An analysis of incident reports over the years suggests that European telecommunication networks may be becoming more robust and resilient, as the rising number of incidents has not resulted in an increase in user hours lost.

The following trends, in particular, have emerged:

- **System failures (Blue)** remains the top root cause over the years.
- **Malicious actions (Red)** remain relatively stable over time with minimal impact, suggesting they are not primary causes of major disruptions.
- **The most impacted services** remain **mobile telephony and mobile internet,** which is valid for the last 8 years**.**

ENISA will continue to work with the national authorities responsible for telecom security and the NIS Cooperation Group to find and exploit synergies between various pieces of EU legislation, particularly when it comes to incident reporting, incl. cross-border incidents.

([6]) Note that conclusions about trends and comparisons with previous years have to be made with caution, as national reporting thresholds change over the years. Indeed, reporting thresholds have been lowered in most countries in recent years, and reporting only covers the most significant incidents (not smaller incidents that may well be more frequent).

1. INTRODUCTION

Electronic communication providers in the EU have to report security incidents that have a significant ([7]) impact on the continuity of electronic communication services to the national telecom regulatory authorities (NRAs) in each EU Member State.

Every year the NRAs provide ENISA with a summary of the most significant incidents based on a set of agreed EU-wide thresholds. This document, *Telecom Security Incidents Report 2024*, aggregates the **188** incident reports received in 2024 and provides an overview of telecom security incidents in the EU.

The European Electronic Communications Code ([8]) (Art. 40 EECC), includes a broader scope on the requirements for incident reporting and requires mandatory incident reporting with a specific focus on security incidents with a significant impact on the functioning of each category of telecommunication services.

Over the years, the regulatory authorities (Art. 41 EECC) have agreed to primarily focus on network/service outages. ENISA has published guidelines for incident reporting under the ECCC ([9]). These guidelines outline the formats and procedures for cross-border and annual summary incident reporting. They focus specifically on two types of reporting: ad-hoc reporting between competent authorities and ENISA, and annual summary reporting from national authorities to the European Commission and ENISA.

This is the annual ENISA report on Incident Reporting for the electronic communications sector.

Mandatory incident reporting has been a part of the EU's telecom regulatory framework since 2009.

Article 40 of the European Electronic Communications Code is the legal basis for this document.

([7]) Note that the telecom security incidents that are reported to national authorities are only the major incidents, i.e. those with significant impacts.
([8]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32018L1972
([9]) https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

2. BACKGROUND AND CONTEXT

In this chapter, the policy context is explained, along with the main features of the incident reporting process, as described in *ENISA Technical Guideline on Incident Reporting* ([10]), which was developed in collaboration with national authorities.

2.1 POLICY CONTEXT

The European Electronic Communications Code (EECC), adopted in 2018 ([11]) and enforced from late 2020, modernised the EU telecom rules by broadening regulatory coverage to include over-the-top (OTT) communication providers like WhatsApp and Skype. A key pillar of the EECC is enhancing cybersecurity across all electronic communications services—requiring operators and OTT providers alike to implement strong security measures and incident reporting to safeguard networks and user data. This report stems from the art 40 of the EECC, which requires that MS provide annual summary reports to ENISA.

2.2 INCIDENT REPORTING FRAMEWORK

There are three types of incident reporting:

1) national incident reporting from providers to National Competent Authorities (NCA);
2) ad hoc incident reporting between NCAs and ENISA; and
3) annual summary reporting from national authorities to the European Commission and ENISA.

It bears noting that in this setup ENISA acts as a collection point, anonymising, aggregating and analysing the incident reports.

The different types of reporting are shown in **Figure 5** next page.

([10]) https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting
([11]) Security supervision changes in the new EU telecoms legislation – ENISA (europa.eu)

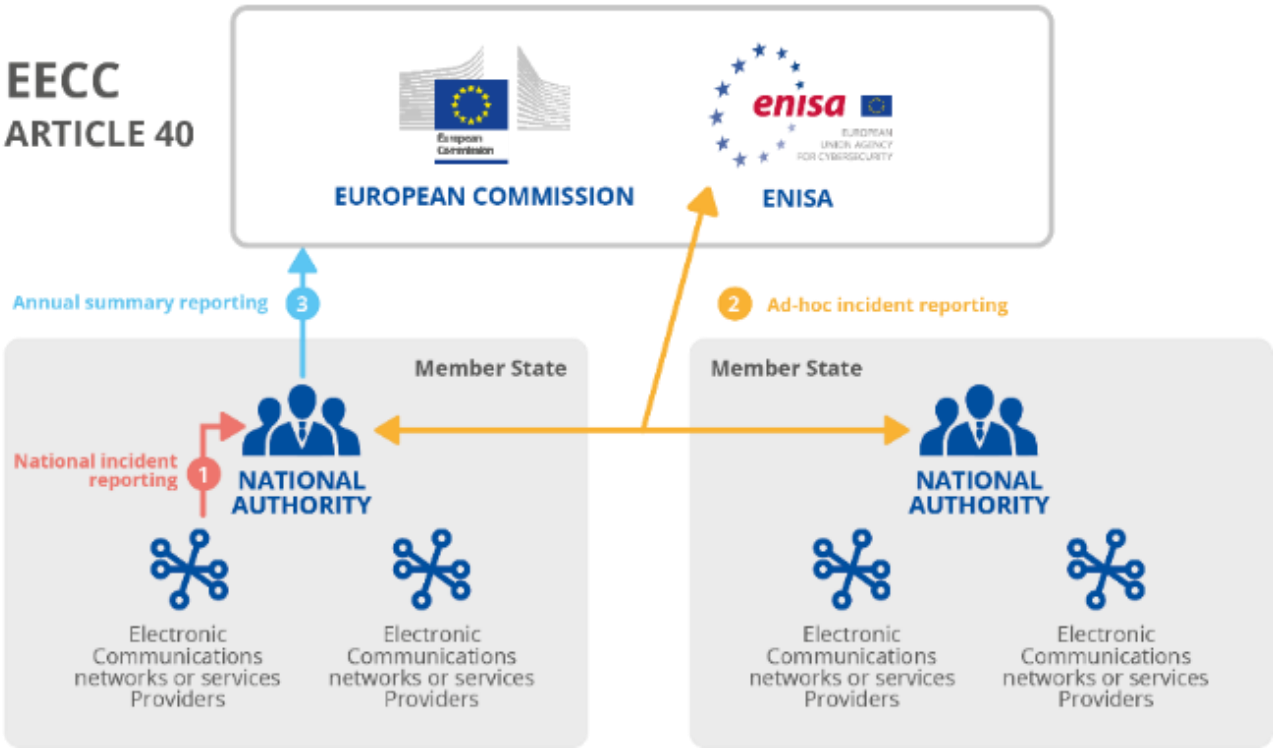

Figure 5: Incident reporting under Article 40 of the EECC

2.3 INCIDENT REPORTING TOOL

ENISA maintains the Cybersecurity Incident Reporting and Analysis System (**CIRAS**), for the authorities to upload reports and search for and study specific incidents.

For the general public, ENISA also displays an online visual tool, which is publicly accessible and can be used for custom analysis of data. This tool anonymises the country or operator involved.
Link: https://ciras.enisa.europa.eu/

CIRAS
is a free online tool where ENISA stores reported incidents and provides annual and multiannual statistics.

The reporting template starts with the type of incident (choice between six types of cybersecurity incidents, explained in **Figure 6**.

The field contains three parts:

1. **impact of the incident:** communication services impacted and by how much;
2. **nature of the incident:** the cause of the incident;
3. **details of the incident:** detailed information about the incident, including a short description, the types of networks, the types of assets, the severity level, etc.

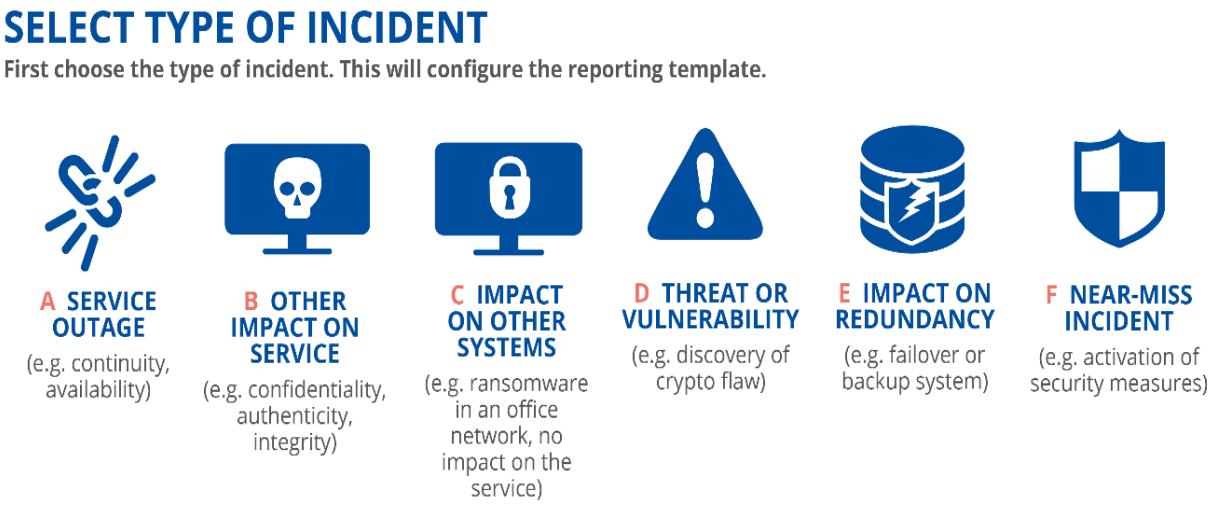

Figure 6: Types of cybersecurity incidents

- **Type A.** Service outage (e.g., continuity, availability).
  For example, an outage caused by a cable cut due to a mistake by the operator of an excavation machine used for building a new road would be categorised as a type A incident.

- **Type B.** Other impact on service (e.g., confidentiality, authenticity, integrity).
  For example, a popular collaboration tool has not encrypted the content of the media channels, which are being established when a session is started, between the endpoints participating in the shared session. This leads to the interception of the media (voice, pictures, video, files, etc.) through a man-in-the-middle attack. This incident would be categorised as a type B incident.

- **Type C.** Impact on other systems (e.g., ransomware in an office network, no impact on the service).
  For example, a malware being detected on several workstations and servers of the office network of a telecom provider would be categorised as a type C incident.

- **Type D.** Threat or vulnerability (e.g., discovery of crypto flaw).
  For instance, the discovery of a cryptographic weakness would be categorised as a type D incident.

- **Type E.** Impact on redundancy (e.g., failover or backup system).
  For example, one of two redundant submarine cables breaking would be categorised as a type E incident.

- **Type F.** Near-miss incident (e.g., activation of security measures).
  For instance, a malicious attempt that ends up in the honeypot network of a telecom provider would be categorised as a type F incident.

For more information about the incident reporting process, please refer to:
Technical Guideline on Incident Reporting under the EECC ([12])

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

3. ROOT CAUSE ANALYSIS

For the year 2024, 25 EU Member States, two European Free Trade Association countries participated in the annual process, reporting **188** significant incidents, compared to 156 in 2023, where we had 26 MS and 1 EFTA country.

188

telecom security incidents reported in 2024 by EU Member States.

3.1 ROOT CAUSES CATEGORIES

In 2024, there was a slight increase in incidents (113) related to **system failures**, representing 60% of the total compared to 2023 where 96 system failure (61%) of telecom incidents were reported. Software bugs and hardware failures each representing 19% of the top two technical causes for system failures in 2024.

Human errors consistently rank second after system failures, with 35 incidents representing 19% in 2024, which is similar in terms of percentage (20 %) for 2023 with 32 incidents reported. Cable cuts and faulty software/change update being the major technical cause with 40% and 37% for human errors in 2024.

Natural phenomena increased to 12% compared to 7% in 2023, with more than double the incidents in 2024 increasing to 25 from 12 in 2023. The most common technical causes were heavy wind (44%) and external causes (36%)([13])

Malicious actions accounted for 15 incidents in 2024 representing 8%, compared to 16 in 2023 for 10% representation. Major technical causes for the malicious actions were cable cuts representing 46% of all causes.

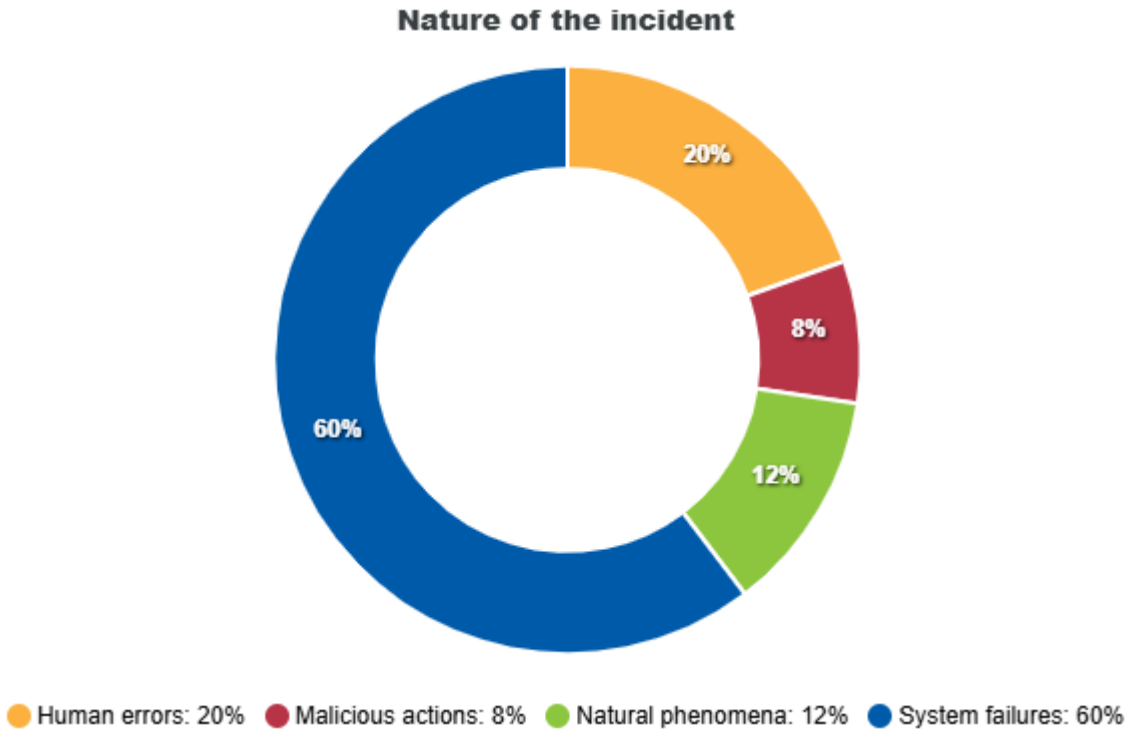

Figure 7: Root cause categories 2024

([13]) Multiple causes can be reported under one incident

In 2024, 65 incidents of all the 188 incidents were flagged as **failures by third parties** represented 37% of incidents compared to 38 incidents reported in 2023 for a representation of 24% of all incidents. This marks a more than 70% increase in incidents by third party failures for 2024.

The majority of incident reports, 42 of them, originated from system failures (65%), 19 from human errors (29%), 2 from malicious actions (3%) and 2 from natural phenomena (3 %) as shown in **Figure 8**.

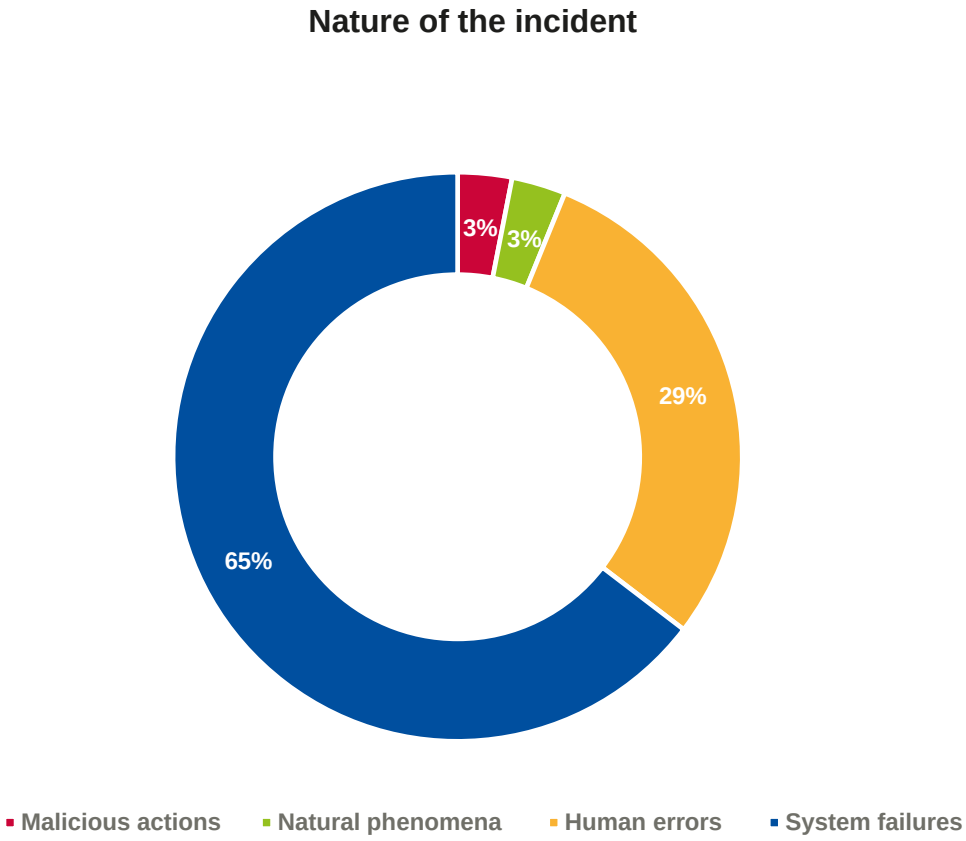

Figure 8: Root cause categories – third-party failures

3.2 USER HOURS LOST IN EACH CATEGORY OF ROOT CAUSES

- **System failures** accounted for 548 million user hours lost compared to 3 439 million in 2023. This is a decrease of more than 6 times compared to 2023. Faulty software changes/updates were among the top three with 183 million user hours lost. Power cuts come second with 160 million user hours lost. Third comes software bugs with 142 million hours lost.
- **Human errors** accounts for 402 million of user hours lost in 2023 for 35 incidents, compared to 181 million in 2023 for 32 incidents. Faulty software changes/updates is the top cause here with 341 user hours lost. Policy and procedure errors is the distant second cause with 27 Million user hours lost.
- User hours lost due to **natural phenomena** have increased significantly to 605 Million compared to 72 million in 2023. The main causes for that are floods (318 million), Heavy wind (277 million), External environmental causes (243 million) and cable cuts (216 million([14])). Natural phenomena ia also the most impactful root cause with 24.20 million user hours lost per incident with a total of 25 incidents reported for 2024.
- **Malicious actions'** number of user hours lost continue to decrease in 2024, reaching 184 million hours lost (for 15 incidents), compared to 214 million in 2023(for 16 inidents). Top three cause fo these losses were arson with 93 million, cable cut with 61 million and cable theft with 30 million user hours lost.

The most impactful root cause in 2024 is **natural phenomena.**

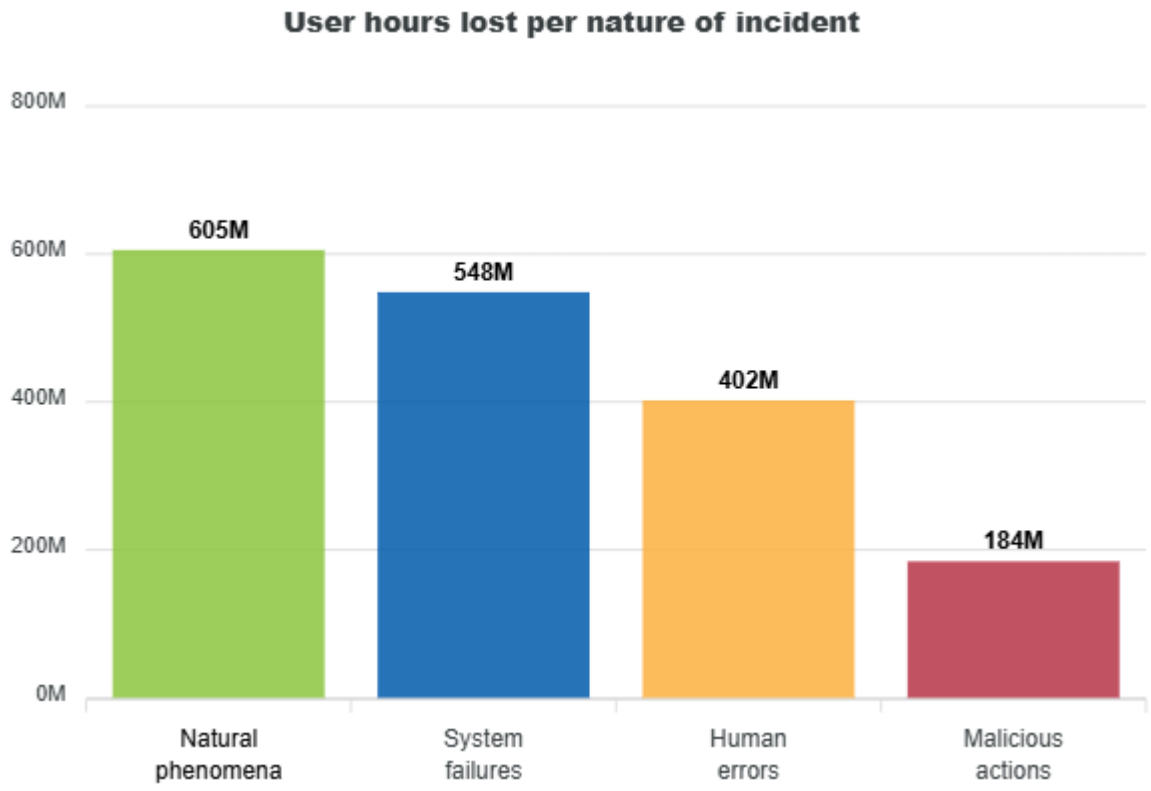

Figure 9: Share of user hours lost for each root cause category 2024

[14] One incident can have multiple causes

3.2.1 Detailed technical causes and user hours lost

Detailed technical causes for all incidents are tracked across all root cause categories in **Figure 10.** An incident is often a chain of events ([15]), therefore many technical causes can be part of an incident.
The most frequent technical cause appearing in incident reports for 2024 is cable cuts with 41 incidents. The most user hours lost is due to the faulty software change/updates.
The most impactful technical cause are the floods, which with 8 incidents are able to cause 318 million user hours lost of damage. The impact is more than 39 million user hours lost per incident.

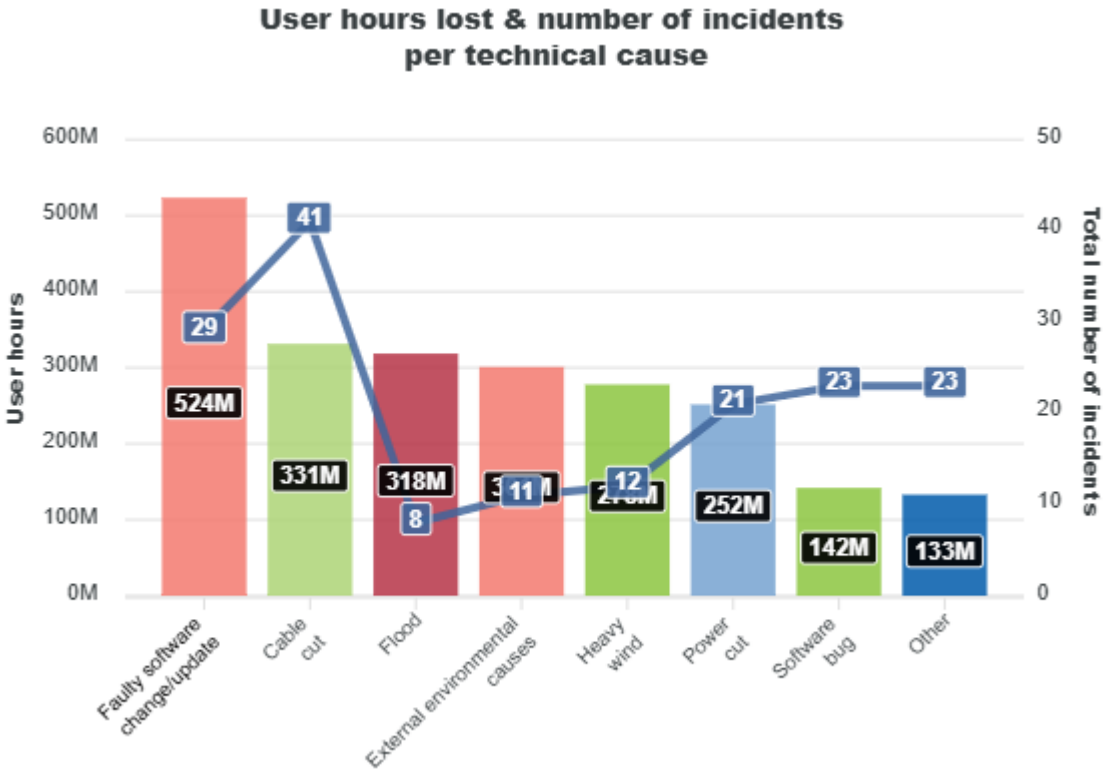

Figure 10: Detailed technical root causes

What follows is an overview of detailed causes and user hours lost for each category of incident in an effort to provide precision for each root cause, giving details about affected service, assets and technical causes.

3.2.1.1 Breakdown of system failures

System failures accounted for 113 incidents reports, meaning 60% of total incidents for 548 million user hours lost.

Faulty software change/update remains top technical cause in terms of user hours lost, with 183 million. However, in terms of number of incidents, **software bugs and hardware failures** with 22 incidents each come first.

It is worth noting that **external environmental causes** represent only 2 incidents but the user hours lost is 58 million, which makes it the most impactful root cause in system failures.

The most impactful technical cause of the system failures is **external environmental factors.**

([15]) For instance, an incident may be triggered by a storm, which tears down power supply infrastructure, cutting cables and thus power, which in turn results in a telecom outage. In this example, the root cause of the incident would be natural phenomenon and the detailed causes would be: heavy wind, cable cut, power cut and battery depletion.

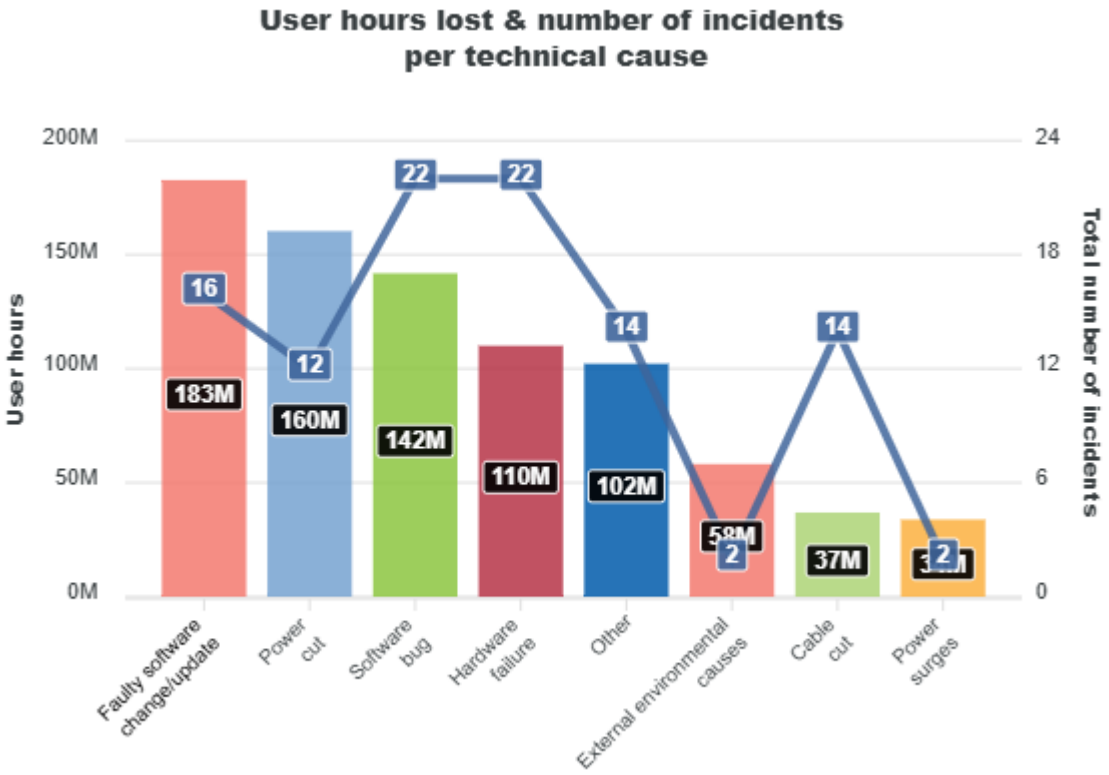

Figure 11: Root causes of system failure incidents vs user hours lost

Services affected by system failures

The most affected services by system failures are the mobile telephony (53% of the incidents) and the mobile internet (45 % of the incidents ([16])**.** The over the top (OTT) service providers account of the 23% of the incidents associated with the system failures. The fixed internet and fixed telephony are fourth and fifth impacted by the system failures with 20% and 19% respectively.

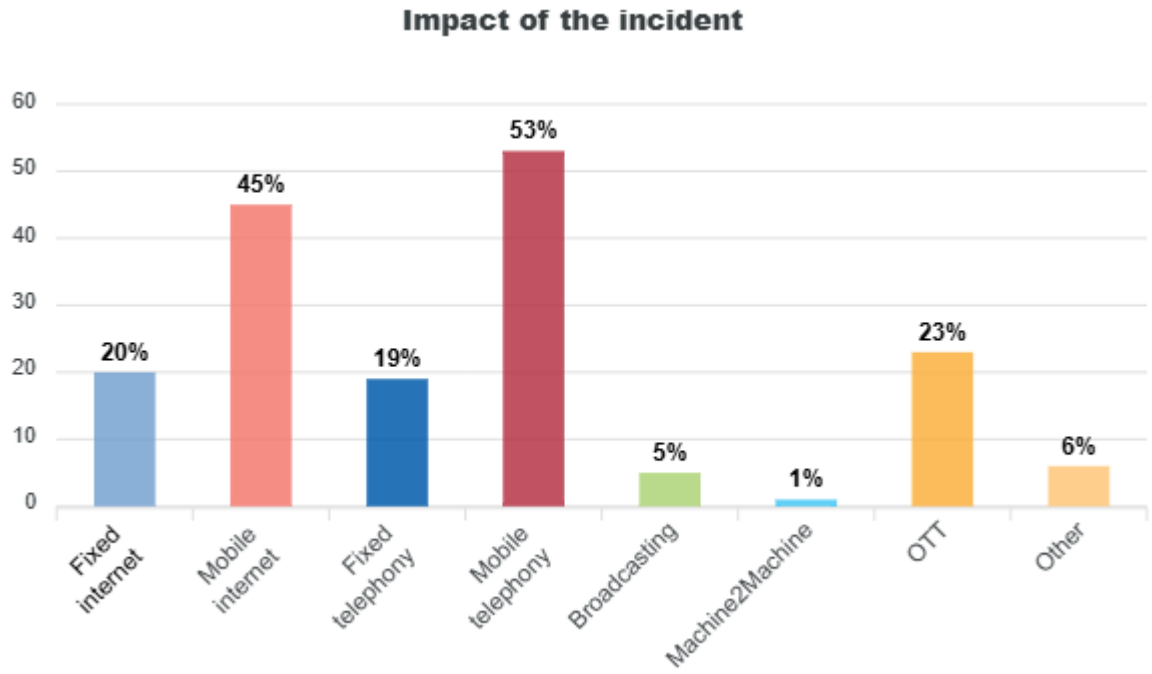

Figure 12: Services affected by system failure

[16] One incident can affect multiple services

Assets affected by system failures

The most affected technical assets by system failures are the switches and routers (18%), which is a decrease from 2023, where it was 30%. The mobile base stations and controllers remain the same as 2023 at 17%. Transmission nodes have not been reported for 2023, they remain last in 2024 with 16%. Mobile switches mark a small decrease with 13%, compared to 15% in 2023.

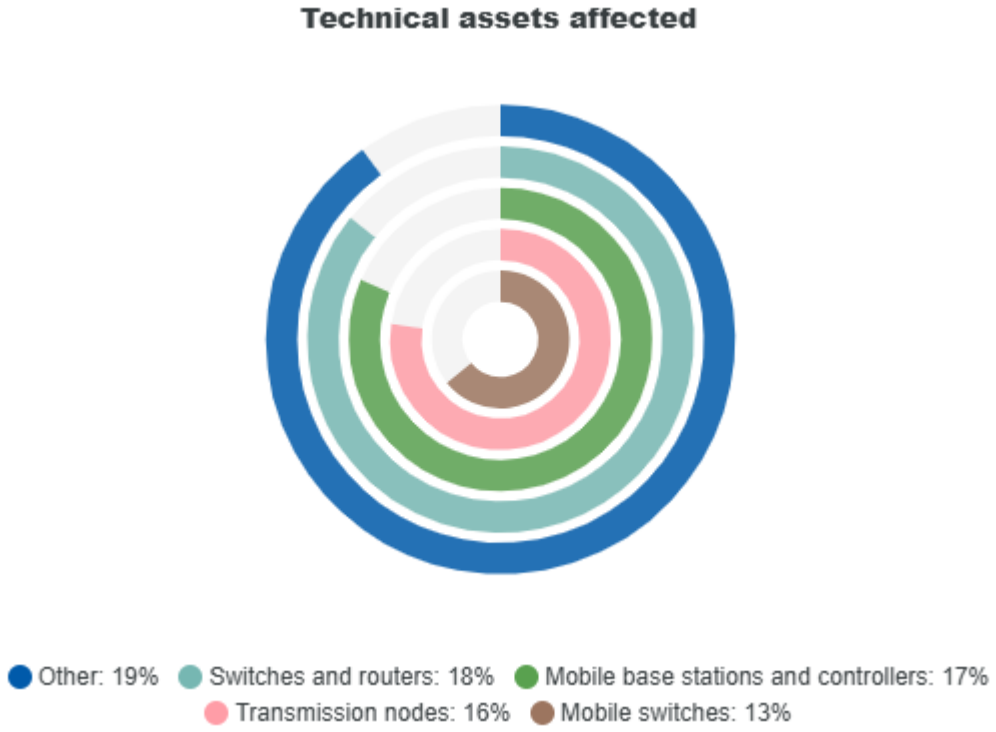

Figure 13: Assets affected by system failure

3.2.1.2 Breakdown of human errors

Human error remains similar to the previous year, reaching 19% of total incidents.
The 35 incidents accounted for 402 million user hours lost which is more than twice the amount lost in 2023 (180 million) from 32 incidents.
Faulty software change\update with 13 incidents rank top in terms of number of user hours lost. This cause is also the most impactful one with above 26 million user hours lost per incident.
Policy/procedure flaw comes second in terms of number of user hours lost with 27 million, with only 3 incidents reported.
Cable cut comes third with 14 incidents and 17 million of user hours lost.

The most impactful technical factor contributing to the human error root cause is a **faulty software change or update.**

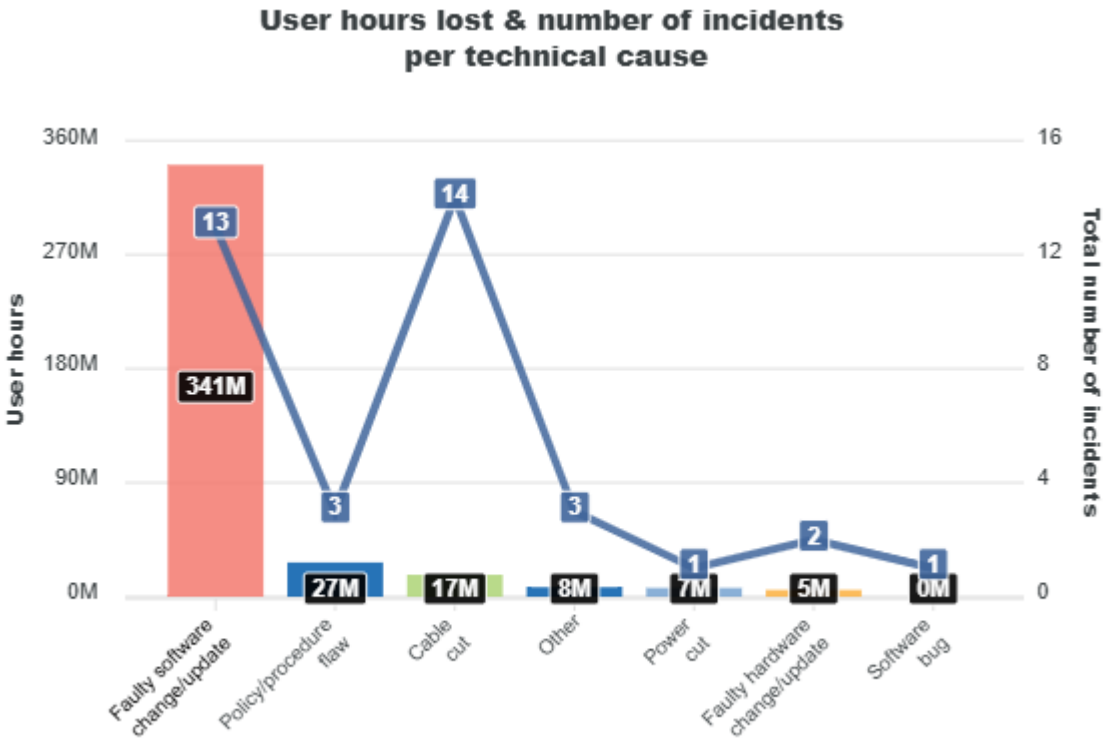

Figure 14: Technical causes –human errors

Services affected by human errors

The most affected service by human errors is the mobile telephony with 57%, which is lower than the previous year with 62% for 2023. The second affected service is the mobile internet with 48%, with also lower than 2023, where it was 53%. Third and fourth are the fixed telephony and fixed internet with an increase to 28% for 2024, while in 2023 fixed telephony was 25% and fixed internet was much lower with 15%. OTT remains with 25% for both years.

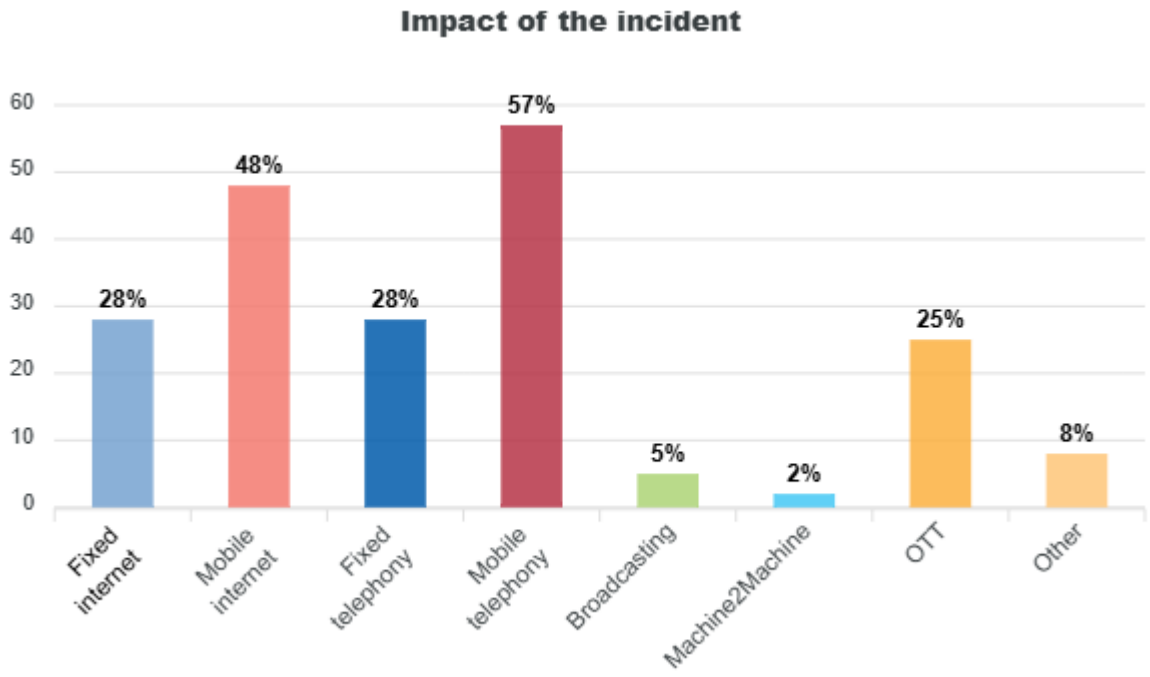

Figure 15: Services affected by human errors

Technical assets affected by human errors

The most affected asset by human errors are the mobile base stations and controllers with an increase to 31%, coming from 28% for 2023. Underground cables come second with 31%, while in 2023 no such incidents were reported. Mobile switches remain third with the similar results as in 2023 with 14%. Switches and router show a decline to 11% coming down from 25% for 2023. Addressing servers are last with 9% and no similar incidents reported in 2023.

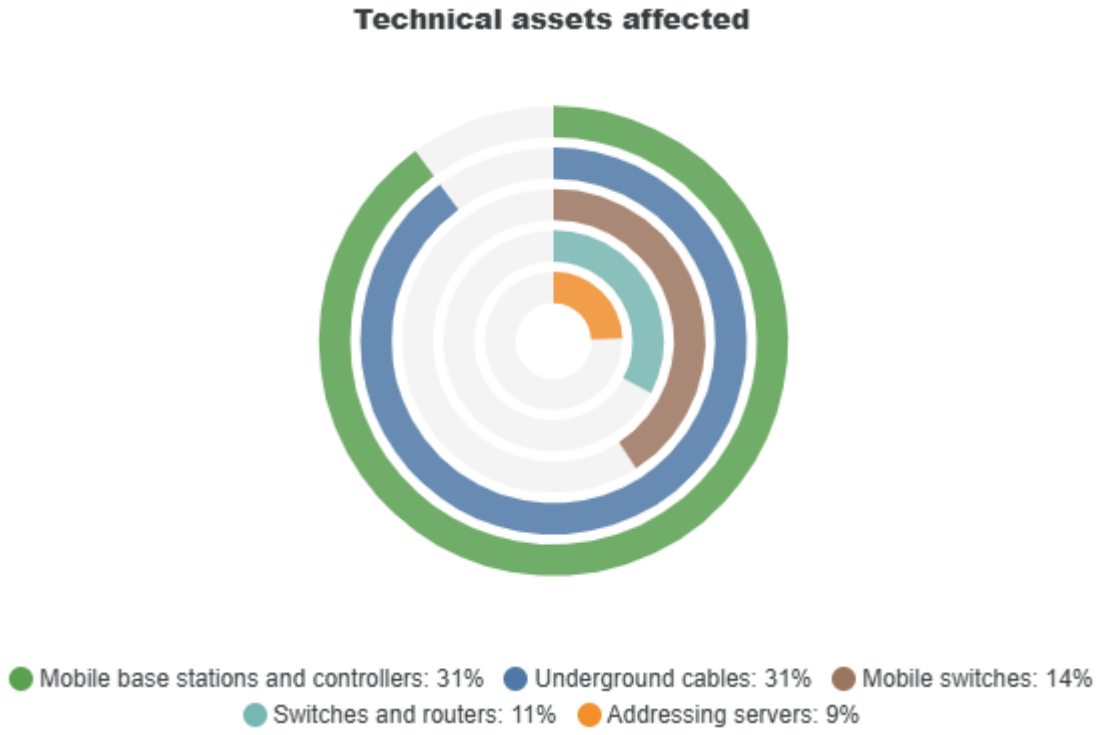

Figure 16: technical assets affected by human errors

3.2.1.3 Breakdown of natural phenomena

Natural phenomena accounted for 25 incidents and 13% of total incidents for 605 million user hours lost. This is an increase of almost 9 times the previous year with 72 million user hours lost and 12 incidents.

The floods are the top leading cause with 318 million user hours lost, which is a staggering increase compared to 6 million user hours lost in 2023. This technical cause is also the most impactful one with almost 40 million user hours lost per incident.

The heavy wind is the second leading cause for the natural phenomena with 277 million user hours lost. This constitutes an increase of almost 100 times compared to the previous year which was 3 million.

The external environmental causes are the third leading cause with 243 million user hours lost, which was not even registered last year as a cause for natural phenomena.

Forth in the leading causes is the **cable cut** which accounts for 216 million user hours lost. The cable cuts were not identified as a technical cause for the last 6 years.

The most impactful technical cause under the natural phenomena root cause is **flooding.**

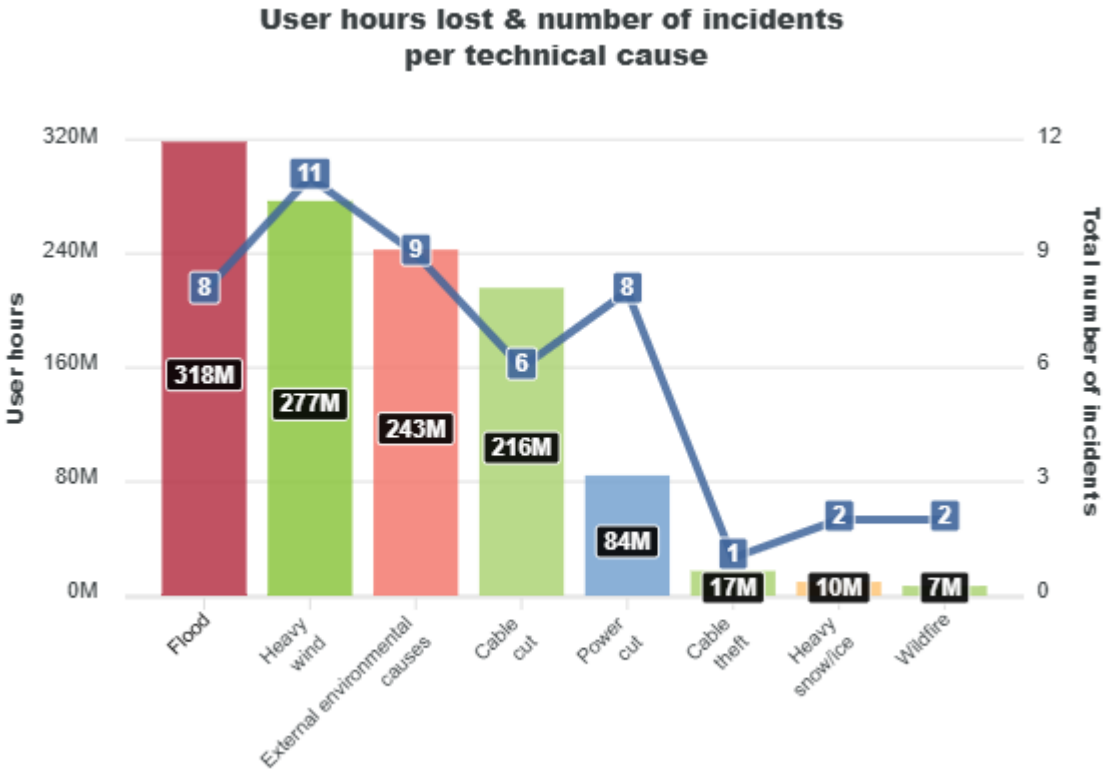

Figure 17: Root causes of natural phenomena incidents vs user hours lost

Services affected by natural phenomena

The most affected services by natural phenomena are the mobile telephony with 80%, which is lower than 2023 where it was with 91%. The mobile internet also marks a big decline in the affected services with 68%, compared to 91% in 2023. Fixed internet (52%) and fixed telephony (44%) show an increase of affected services in 2024, compared to 41% and 33% for 2023. Broadcasting also shows an increase in affected services to 20% from 8% for 2023. It seems that OTT services are the least affected services by natural phenomena with 4% a decrease from 8% in 2023.

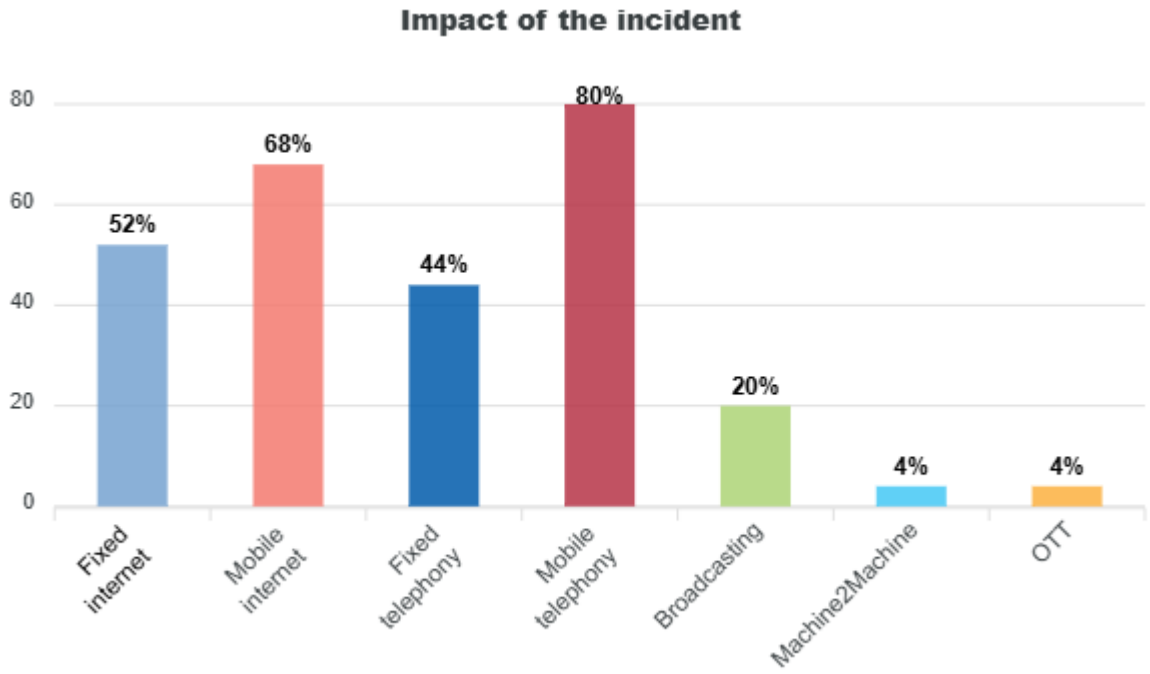

Figure 18: Services affected by natural phenomena

Technical assets affected by natural phenomena

The most affected assets by natural phenomena remain the mobile base stations and controllers marking a decrease from 83% in 2023 to 80% in 2024. Power supplies remain second with an increase to 44%, compared to 25% in 2023. Transmission nodes are third with 28% of incidents affected by natural phenomena, and no such incidents reported in 2023. Backup power supplies mark a decline to 12% in 2024 coming down from 17% in 2023. Overhead cables are last with 12% of incidents reported under natural phenomena, with non being reported for 2023.

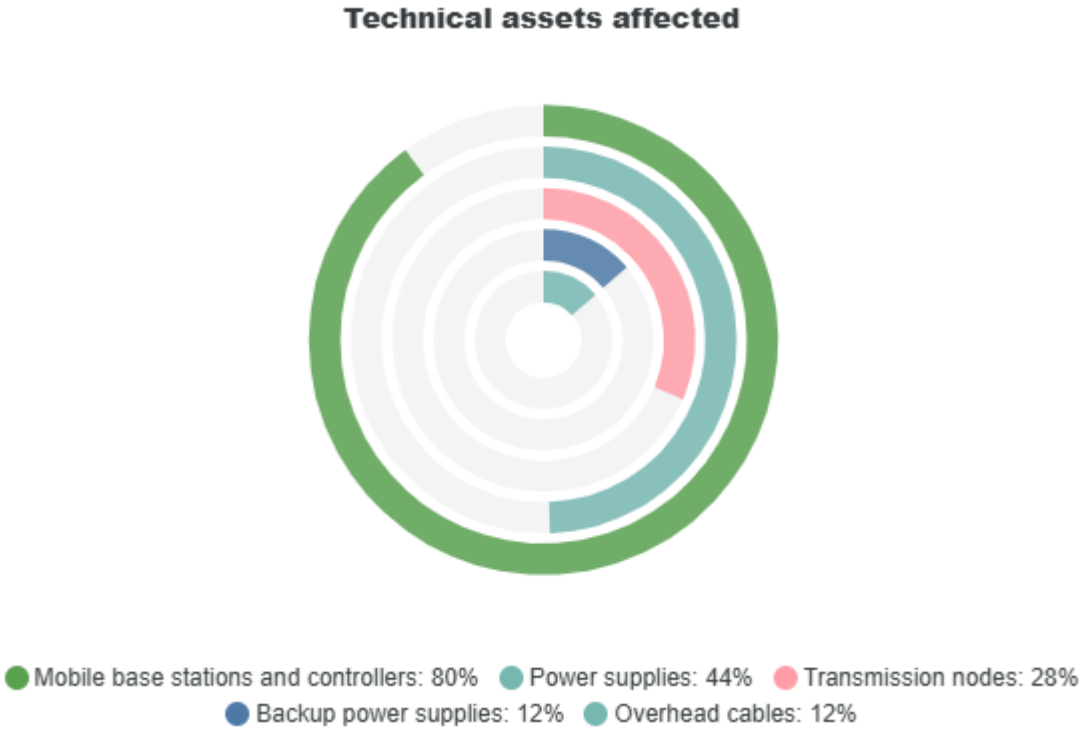

Figure 19: technical assets affected by natural phenomena

3.2.1.4 Breakdown of malicious actions

Malicious actions counted for 15 incidents representing 8% of all incidents, which is a decrease compared to 10% for 2023, although number of incidents is actually higher -16. The malicious actions lead to less user hours lost in 2024 - 184 million, compared to 214 million user hours lost in 2023.

The top cause for the malicious actions was **arson** with 93 million user hours lost and 3 incidents, which is an increase compared to 2023 where we had only 2 million user hours lost with one incident. Arson is also the most impactful technical cause with more than 30 million user hours lost per incident in average. This is likely to the fact that fire damages severely physical assets and leading to their replacement and/or rebuilding which requires time.

The second cause for malicious actions was **cable cuts**, with 7 incidents and 61 million user hours lost. In the previous year no cable cuts were reported under malicious actions.

The third cause for malicious actions was **cable theft** with 3 incidents and 30 million user hours lost. This is almost identical to 2023 where we had 4 incidents and 33 million user hours lost.

The most impactful technical cause under the malicious actions root cause is **arson**.

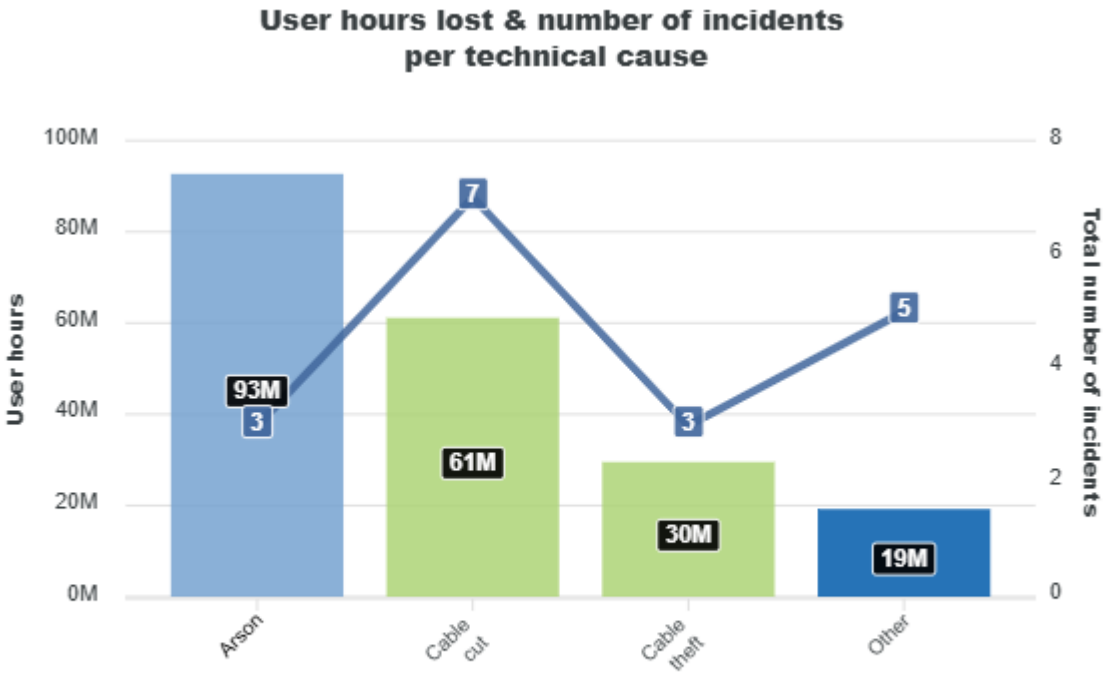

Figure 20: Root causes of malicious action incidents v user hours lost

Services affected by malicious actions

The most affected service in 2024 by malicious actions are the mobile telephony with 66%, an increase from 56% in 2023. The OTT affected services come into strong second place with an increase to 60%, compared to 31% in 2023. The mobile internet comes third with an increase to 60%, coming from 50% for 2023. Fixed internet is least affected with a decrease to 26%, compared to 37% in 2023. Broadcasting and fixed telephony do not have reported incidents for 2024, while in 2023 we had 18% and 31% respectively.

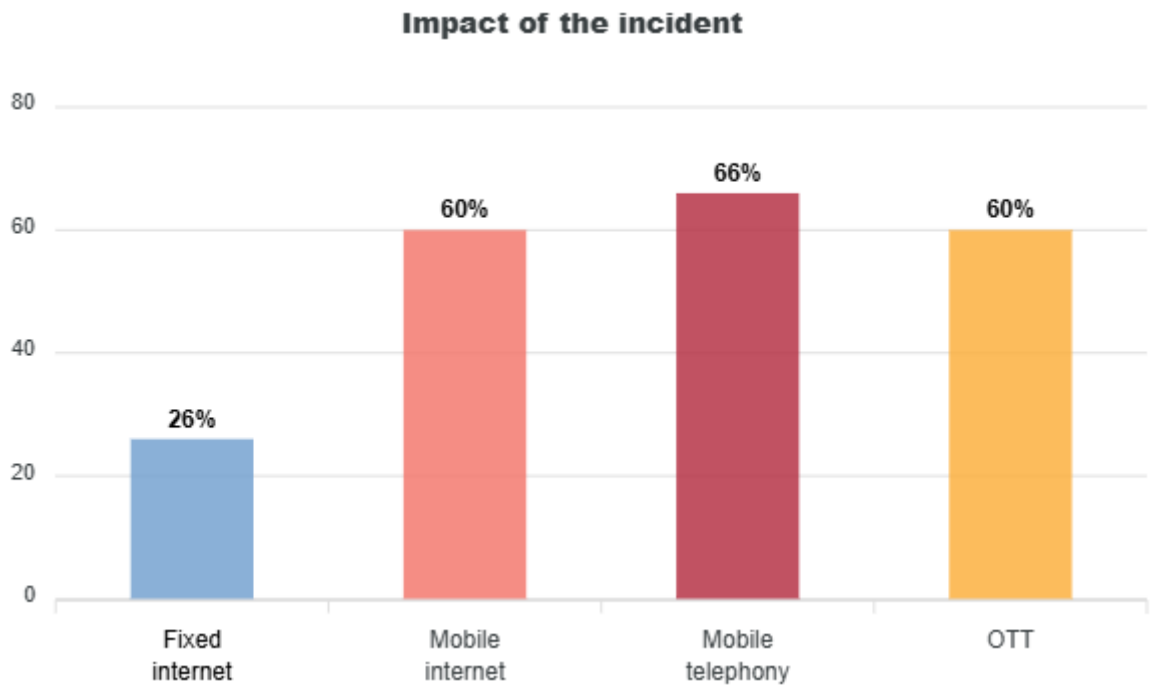

Figure 21: Services affected by malicious actions

Technical assets affected by malicious actions

Mobile ase stations and controllers remain the most affected asset by nalicious actions with a decrease of 27%, compared to 31 % in 2023. Mobile switches have the same percentage of incidents affecting them for 2024 with 27%, and no incidents reported in 2023. The next three assetss are similar with 20% shares of the incidents in malicious actions. The addressing servers are showing an increase compared to 6% in 2023. Submarine cables have no similar incidents reported in 2023. Switches and routers remain similar share with 19% in 2023.

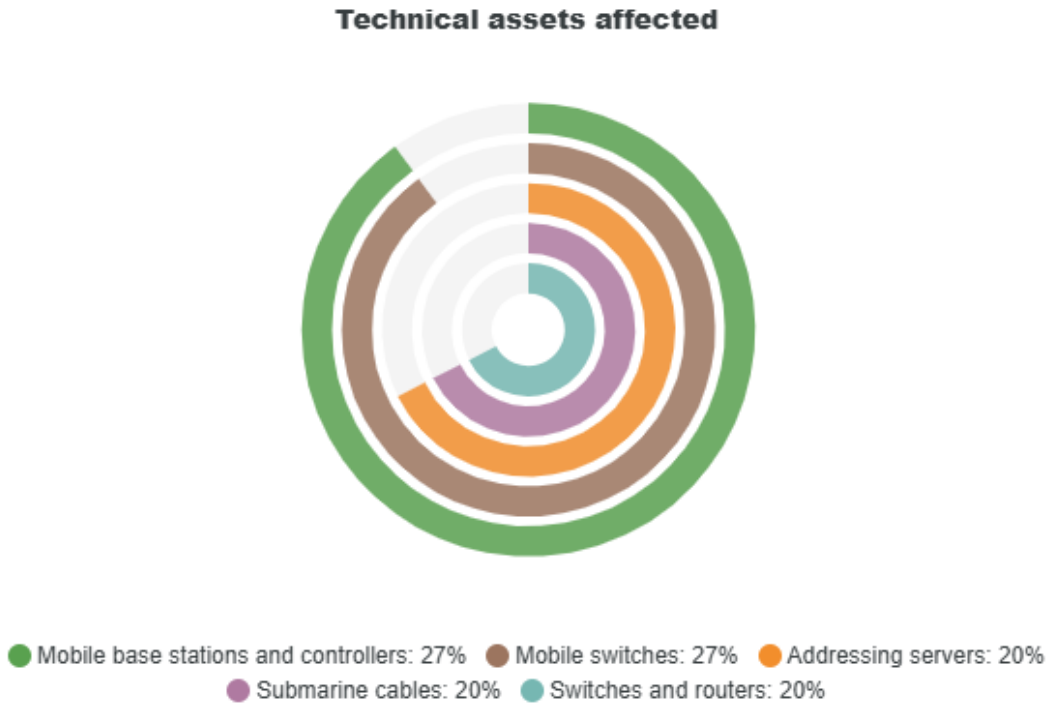

Figure 22: Technical assets affected by malicious actions

4. OVERVIEW OF AFFECTED SERVICES

This paragraph examines in **Figure 24** the services affected by incidents – from mobile and internet telephony, fixed internet and telephony, broadcasting and OTT services according to EECC-type of services.

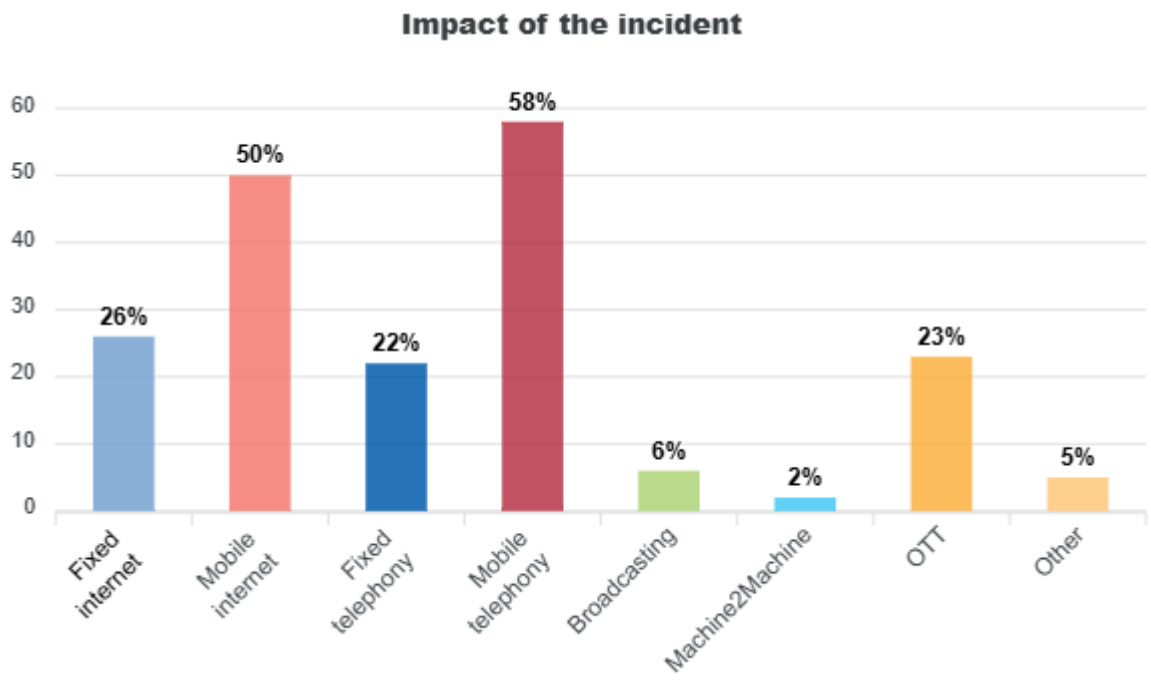

Figure 24: Services affected ([17]) – all incidents 2024

Again, most of the reported incidents affected **mobile services**. In 2024, 58**%** of reported incidents had an impact on **mobile telephony** which is similar to 2023 with 57%. Mobile telephony remains the top affected service for the last 8 years.

Mobile internet followed with 50% in 2024, a slight increase compared to 47% in 2023. Mobile internet has been the seond most affected services for the last 8 years, while in 2016 it was the most affected service.

Reported incidents affecting **OTT services** ([18]) marks a slight increase to 23%, with 22 % in 2023. The OTT services remain at the level of 22-25% since the reporting period 3 years ago.

Traditional services like **fixed internet services** mark a increase of incidents with 26%, coming from 16% in 2023. **Fixed telephony** remains similar share of incidents with 21% in 2023 and 22% in 2024. **Broadcasting** incidents have decreased to 6%, coming down from 12% in 2023.

([17]) Caveat 'Methodology". It bears noting that for most reported incidents there was an impact on more than one service, which explains why the percentages in Figure add up to more than 100 %.
([18]) These newly introduced services and data still need to be consolidated and normalised over 3 years. In 2022, these services counted for 26 % of total incidents, when in 2021, OTT represented 4 %.

5. OVERVIEW OF AFFECTED TECHNICAL ASSETS

Each incident report also describes the (secondary) assets affected during the incident.
Figure 25 shows the assets most affected, knowing that "other" means that detailed information was not provided ([19]).

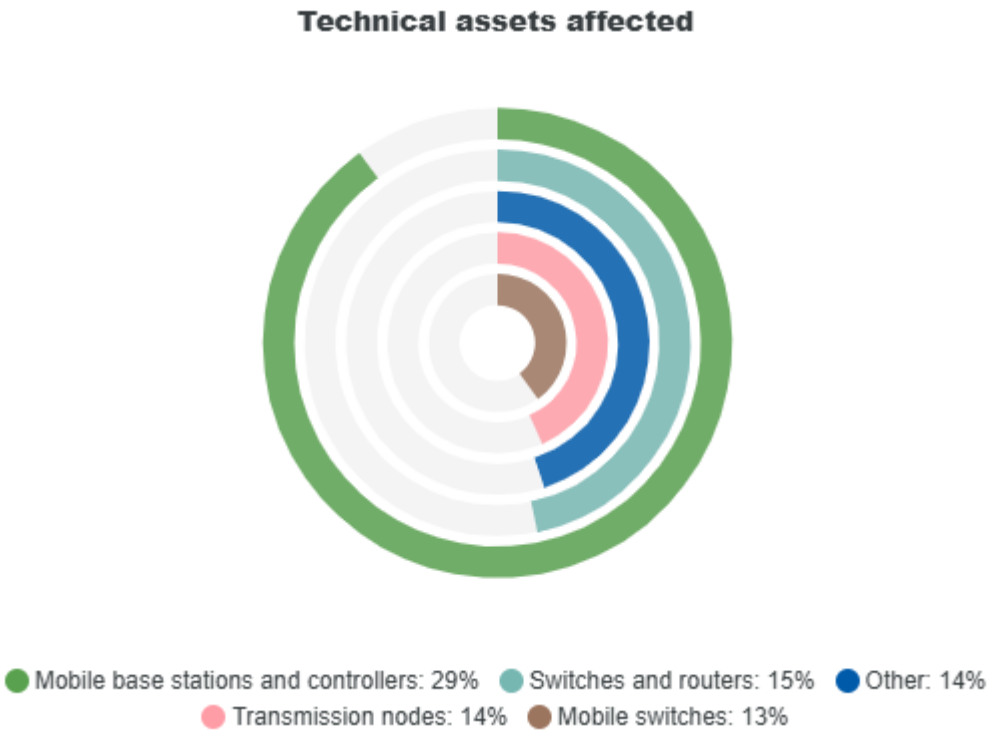

Figure 25: Assets affected – all incidents 2024

Mobile base stations and controllers constitute the most affected assets with 29%, which is a small increase to what we have seen 26% in 2023. These assets have been the most affected for the last three years.

Switches and routers mark a decrease for 2024 with 15%, compared to 26% in 2023. These assets have also been second most affected assets for the last three years, while in 2021 they were the most affected assets.

Transmission nodes are third with 14% of incidents while none were reported for 2023.

Mobile switches remain at the same level as 2023 with 13% of incidents affecting them. For the last three years mobile switches have increased their share of incidents coming from 8% in 2022.

([19]) Caveat 'Other". In the future, more information will need to be provided by Member States to improve the analysis of incidents. Caveat 'Taxonomy'. Incidentally, reassessing the asset taxonomy will also be needed to improve incident reporting.

6. OVERVIEW OF THE TECHNICAL CAUSES

This section contains an in-depth review of the most high-profile technical causes behind reported incidents, focusing on 2024 comparing it with the prevoious year. We will focus on the top three causes.

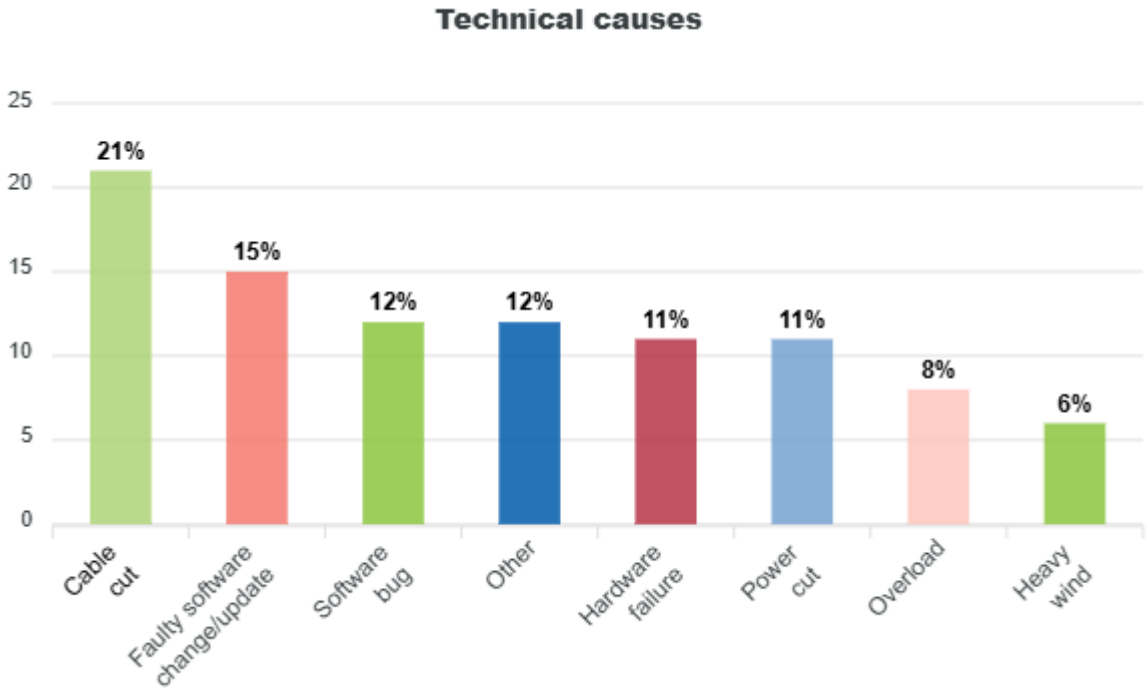

Figure 26 – Technical causes – all incidents 2024

In 2024 41 **cable cuts** incidents were reported overall. Cable cuts have steadily increased their share of incidents from 2022 with 5%, to 2023 with 11% and to 21% in 2024. Cable cuts also represent 331 million of user hours lost for 2024, which is the second most hours lost only to Faulty software changes or updates. It should be noted that for 2023 almost zero hours were lost due to cable cuts.

Faulty software changes or updates represent 15% of the incidents, which is exactly the same to what was in 2023. It marks a slow decrease over the last five years where it was 24% of all incidents (top cause). For 2024 with its 29 incidents, it led to 524 million user hours lost which is the most user hours lost due to a cause. This is still more than 5 times less than what was lost in 2023 where we have seen 2731 million hours lost.

Software bugs mark an increase of their share of incidents to 12% coming from 10% for 2023, this also represent an increase in number of incidents with 16 for 2023 to 23 for 2024. The impact however on user hours lost is diminishing with 142 million user hours lost in 2024, while in 2023 they were 222 million user hours lost.

7. MULTIANNUAL TRENDS

ENISA has been collecting and aggregating incident reports since 2012.

This is the highest number of incidents (188) recorded by ENISA so far in electronic communication incident reporting.

In this section, we present multiannual trends over the last 13 years, from 2012 to 2024.

This dataset contains **1930** reported incidents in total, as we can see in **Figure 27**.

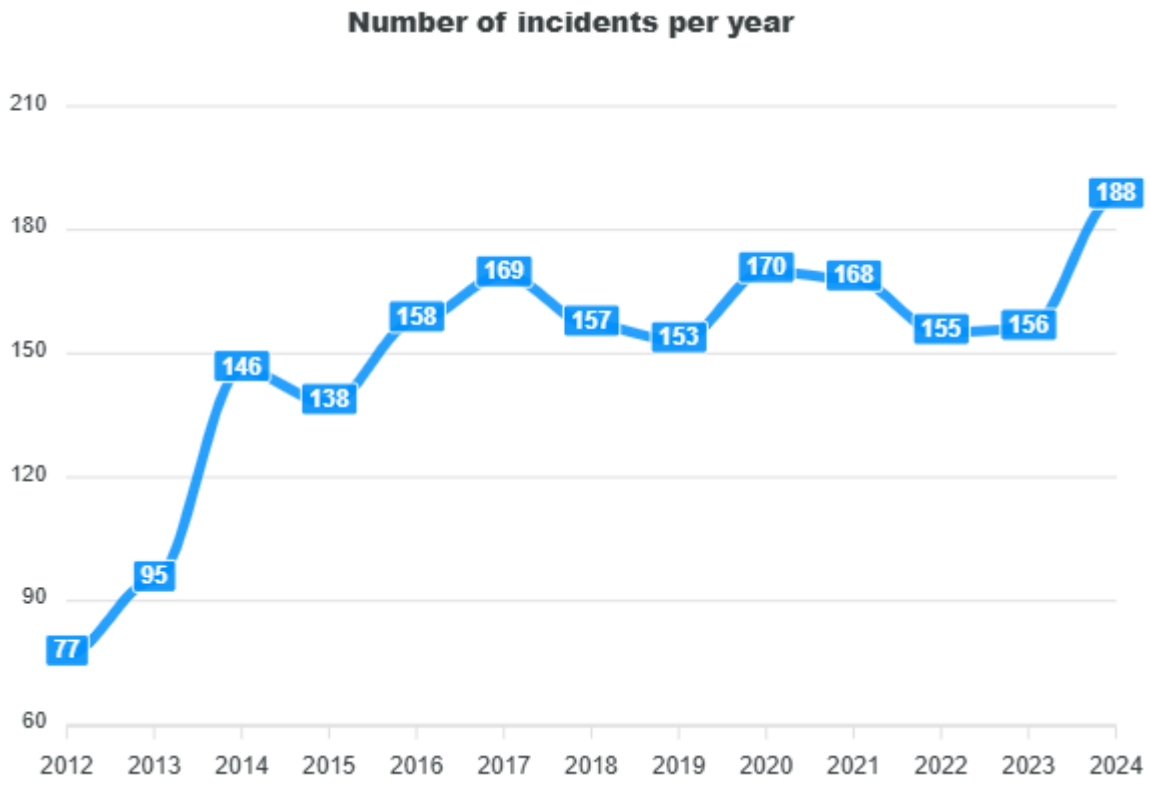

Figure 27: Number of incidents reported per year (2012–2024)

Over the course of the last 10 years, the number of reported incidents has been steadily increasing. Nevertheless, the numbers of user hours lost has not increased, in fact it has remained at the same level as 10 years ago. Based

on the number of incidents an average of one incident occurs every 2 days. The peak of incidents in 2021 and 2022 can be due to the new type of area covered in incident reporting, namely the over-the-top providers.

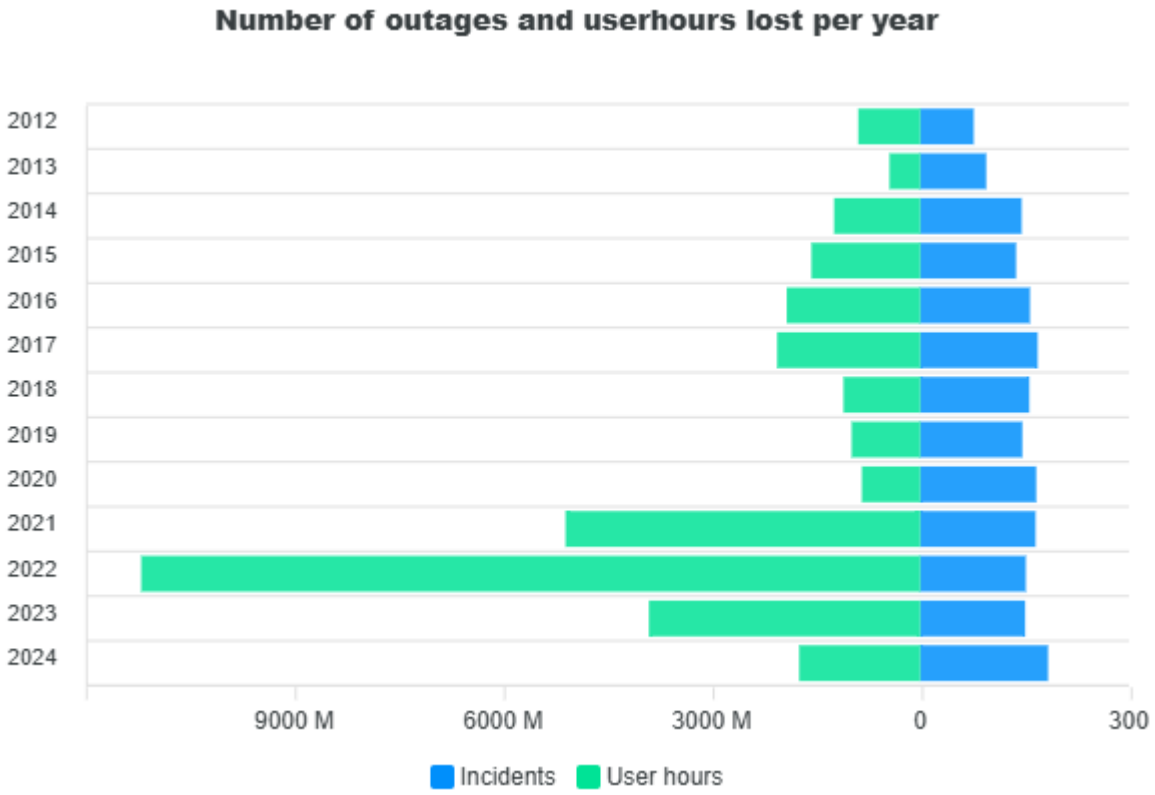

Figure 28: Number of outages and user hours lost over the years 2012-2024

7.1 ROOT CAUSE MULTIANNUAL TRENDS

Over the years we can see a steady increase of natural phenomena incident especially in the last three years. Human errors remain at the 20% mark, while malicious actions and system failures mark a small decrease over the previous one year.

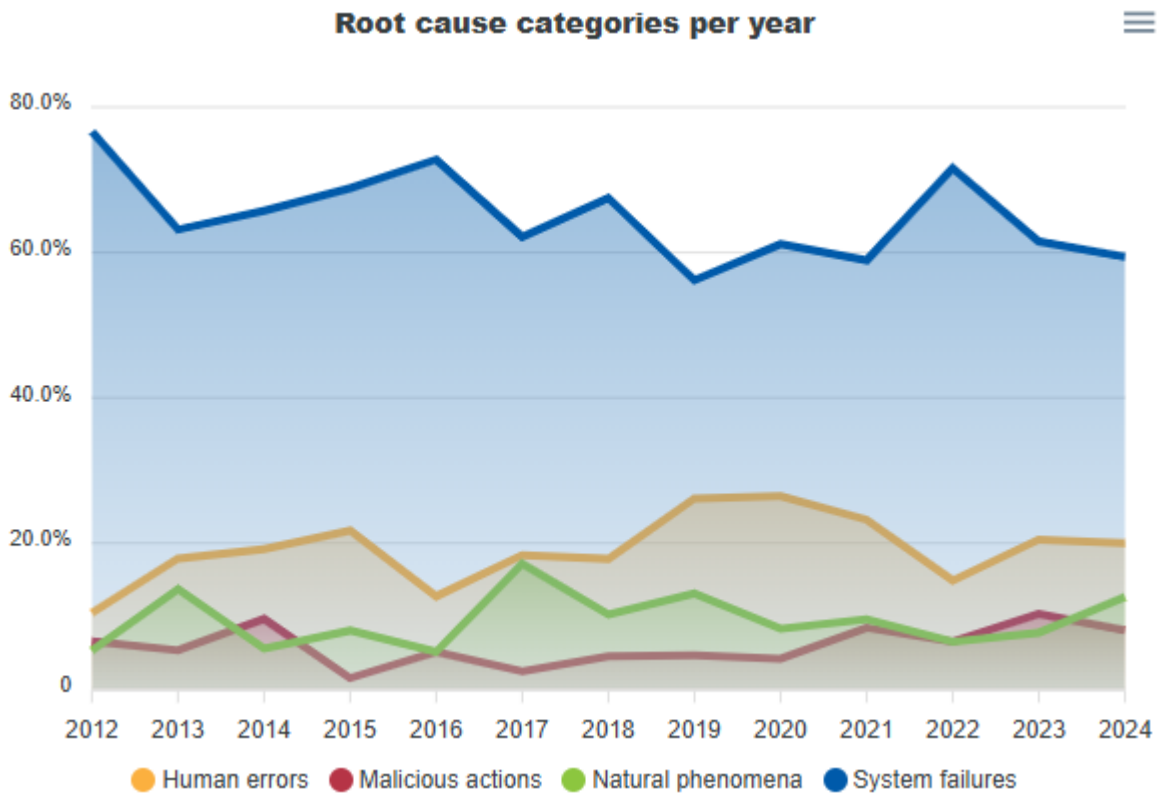

Figure 29: Root cause categories – Telecom security incidents in the EU reported over 2012–2024

Every year, from 2012 to 2024, **system failures** were the most common root cause with average 65% of all incidents. In total, system failures accounted for **1 245** incident reports. The top three causes for system failures over the 13 years are hardware and software bugs, as well as the faulty changes of software or updates.
The second most common root cause was **human errors**, with nearly a fifth of total incidents (20%, 376 incidents in total). The top three causes for the human errors were faulty changes of software or updates, cable cuts and policy or procedure flaws.

Natural phenomena come third, with a tenth of total incidents (10 %, 186 incidents in total). Top three causes during the years were power cuts, heavy wind and heavy snow or ice.

Only 6% of incidents have been categorised as **malicious actions**, with 114 incidents over the course of 13 years. In the 2012–2024 period, nearly half of malicious actions consisted of denial-of-service attacks (48%), while the next two cause were cable cuts (16%) and arson (9%). Only 2% was attributed to vulnerability exploitation (former malware and viruses). Additionally, 28% of technical causes are being classified as 'other'. This highlights the need to update the taxonomy of malicious actions – something that has been noted before.

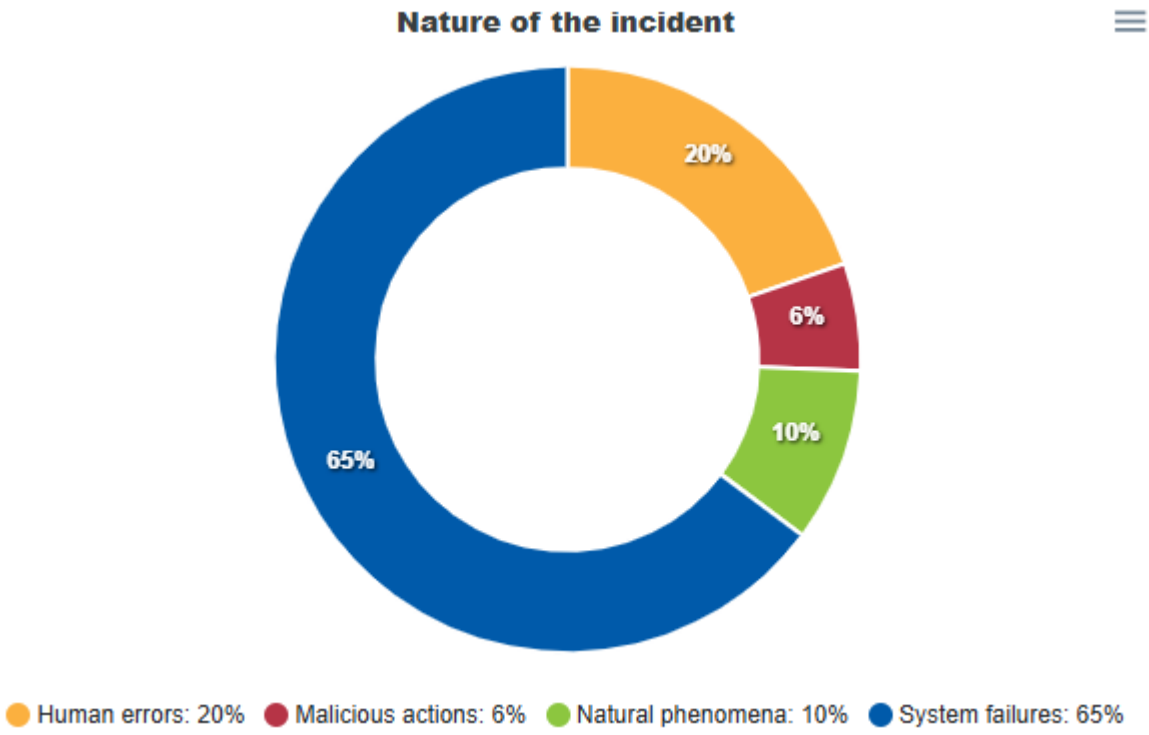

Figure 30: Root cause categories – Telecom security incidents in the EU reported over 2012–2024

Interestingly, the **assets** affected by malicious actions differ significantly from the overall categorisation of affected assets. Addressing servers came first, with 20%, followed by switches and routers, at 19%. Mobile base stations are forth with 13% and last are the underground cables with 9% overall. "Other" category remains with 19%.
Moreover, with respect to services affected by malicious actions, 52% were associated to fixed internet and 44% to mobile internet services, whereas 15% referred to OTT services.

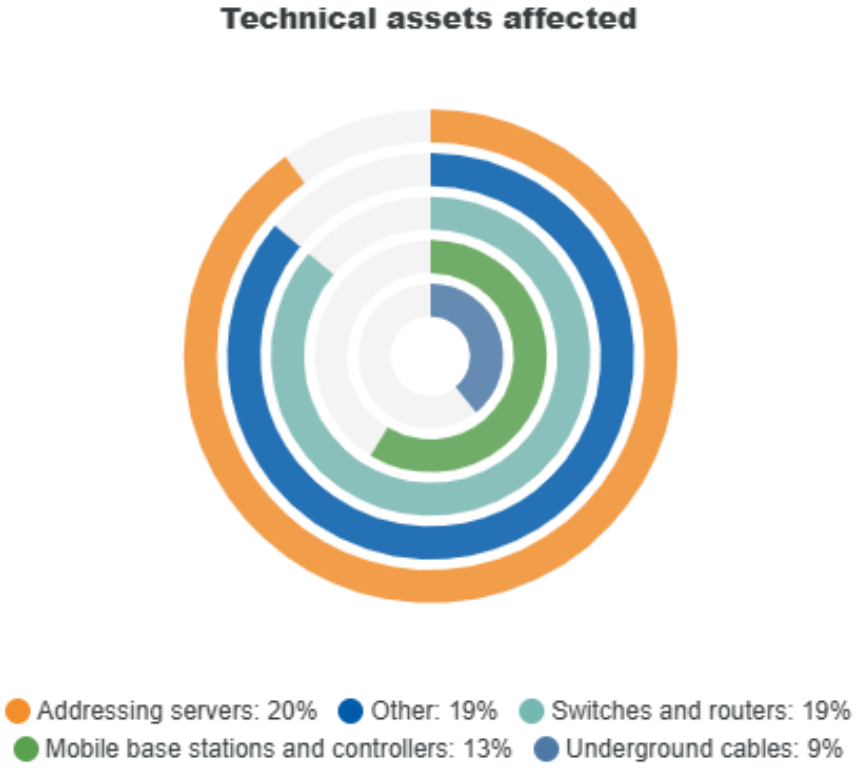

Figure 31: affected technical assets by malicious actions 2012–2024

7.2 MULTIANNUAL TRENDS – SERVICE IMPACT

Over the period, mobile telephony and mobile internet were once more the most impacted by incidents - 58% and 50%, respectively in 2024.

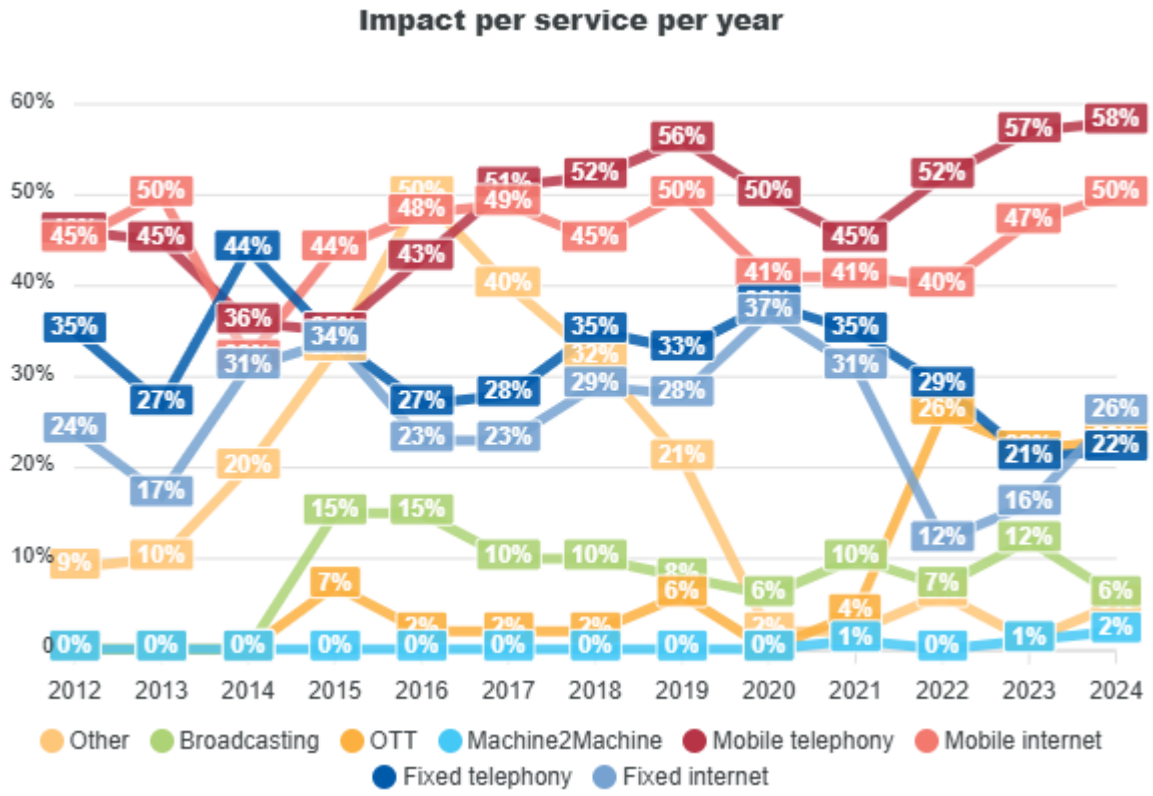

Figure 32: Trends on impact for each service reported over 2012–2024

Fixed internet incidents continue their rising since 2022 to 26% in 2024, while fixed telephony services remained at almost the same level as in 2023. Interesting to note that incidents in machine to machine continue to be very low compared to all other, but they mark an increase from 1% to 2%.

7.3 MULTIANNUAL TRENDS – SEVERITY OF IMPACT OF INCIDENTS

ENISA has published technical guidelines on incident reporting under the EECC ([20]), including on thresholds, severity estimation and calculating hours lost. Relevant multiannual trends may be found in **Figure 33.**

Since 2021, an **increase** in reports of **very large incidents** is observed, from 62 in 2021 to 92 in 2024. Contrary to very large incidents, there has been a steady decline in **large incidents** since 2021, from 62 in 2021 to 52 in 2024. **Minor incidents** show an increase compared to last year coming from 26 to 44 in 2024, after a steady decline for about three years.

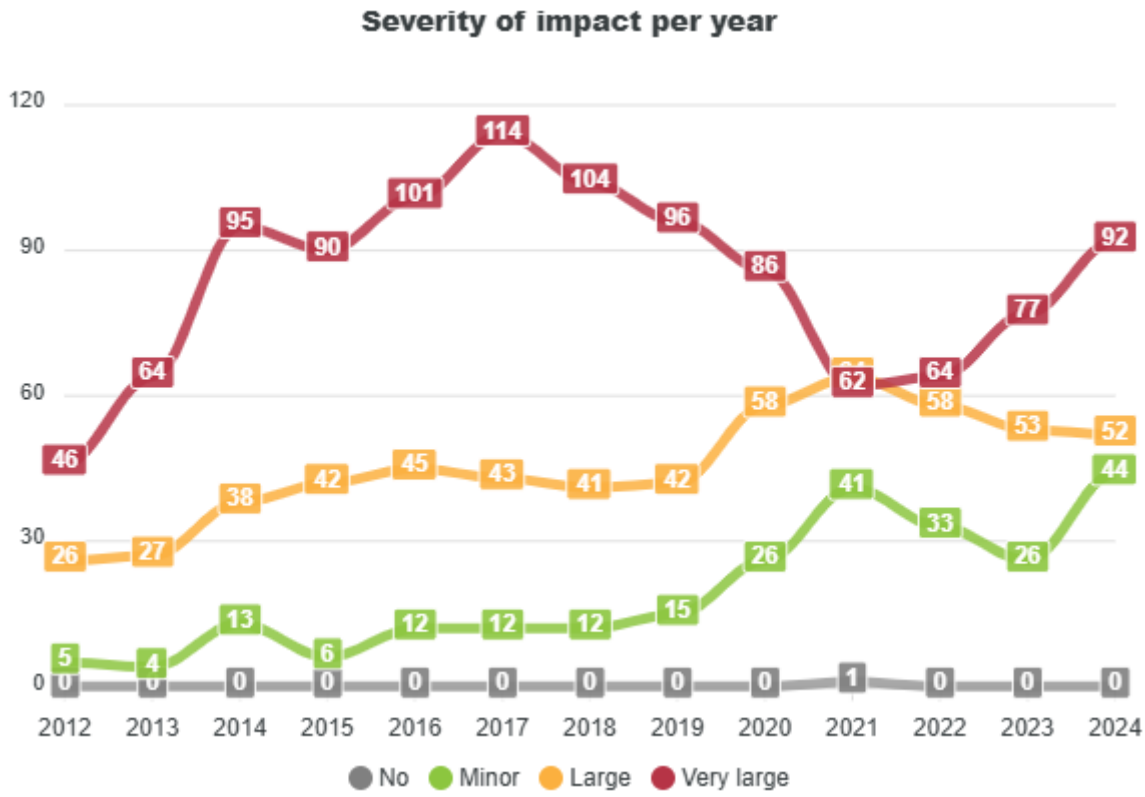

Figure 33: Severity of impact for each year – multiannual trends 2012–2024 (number of incidents)

([20]) https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc, March 2021.

7.4 MULTIANNUAL TRENDS – NUMBER OF INCIDENTS AND USER HOURS LOST

Over the years, the number of incidents has increased steadily and is now at the highest point so far 188 incidents. Contrary to the increase of incidents the hours lost continue to decline and are around the same as 10 years ago.

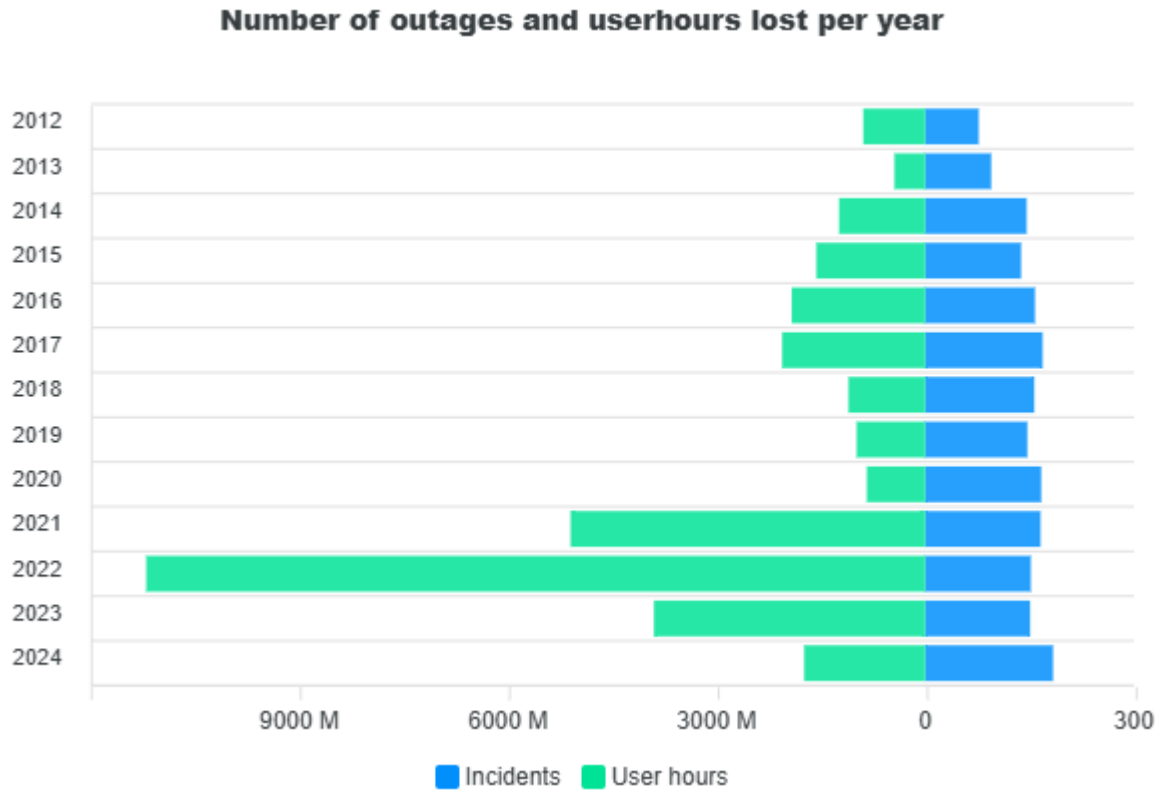

Figure 34: Number of incidents and user hours lost each year over 2012-2024

8. CONCLUSIONS

To conclude, here are the main findings and some general observations about this process and the broader policy context.

Main findings

- Highest number of incidents to date (188) reported in electronic communications incident reporting to ENISA.
- **Steady Increase** in incidents with **very large impact** for the last four years from 62 to 92
- Increase in numbers of incidents though doesn't constitute an increase of user hours lost. It actually shows continuous decline over the last three years and returns to similar numbers as ten years ago in 2014.
- In 2024, 65 incidents were flagged as **failures by third parties** which is an increase compared to 52 reported in 2023.
- **System failures** continued to largely dominate in terms of impact, reaching 60% in 2024 with 113 incidents. They globally accounted for 548 million user hours, which compared to 2023 is 6 times less (3439 million).
- While an increase of incidents is recorded, 188 compared to 156 in 2023, an enormous decrease in total user hours lost is documented. This leads to the conclusion that the telecom infrastructure and processes likely are becoming more resilient to incidents.
- Incidents due to **natural phenomena** continue to increase reaching a share of 13% with an increase from 72 million user hours lost to 605 million for 2024.
- **Human errors** incidents have stayed the same in terms of share of incidents at 19% compared to last year. However, we see an increase in user hours lost from 181 million to 402 million user hours lost.
- **Malicious actions** continue to decrease in both share of incidents reported 15 for 204 with 16 for 2023, as well as the numbers of user hours lost from 184 million user hours lost in 2024 to 214 million in 2023.
- **Mobile telephony** and **mobile internet** were the most impacted sectors, with respectively 58% and 50% of incidents.
- **Fixed internet** continued to increase in terms of number of incident reports and share in the last three years from 12% to 26% in 2024.
- **No cross-border** incidents were reported.

Policy observations

- It should be noted that as of 18 October 2024, the NIS2 Directive repeals Articles 40 – 41 of the EECC, which will consolidate the reporting of breaches of integrity and availability across multiple sectors including but not limited to providers of public electronic communications networks and providers of publicly available electronic communications services.
- During the transition period in 2025, ENISA will continue to work with national authorities through the ECASEC expert group, as well as the NIS Cooperation Group, to find and exploit synergies between different pieces of EU legislation, particularly when it comes to incident reporting and cross-border supervision.
- Additionally, the CIRAS methodology and guidelines may also be reviewed during our regular discussions with member states to better reflect new developments and to facilitate reporting and alleviate the administrative burden.

ENISA will continue to work with the national authorities responsible for telecom security and the NIS Cooperation Group to implement security incident reporting efficiently and effectively, and takes the opportunity to thank all the contributors of this report.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu