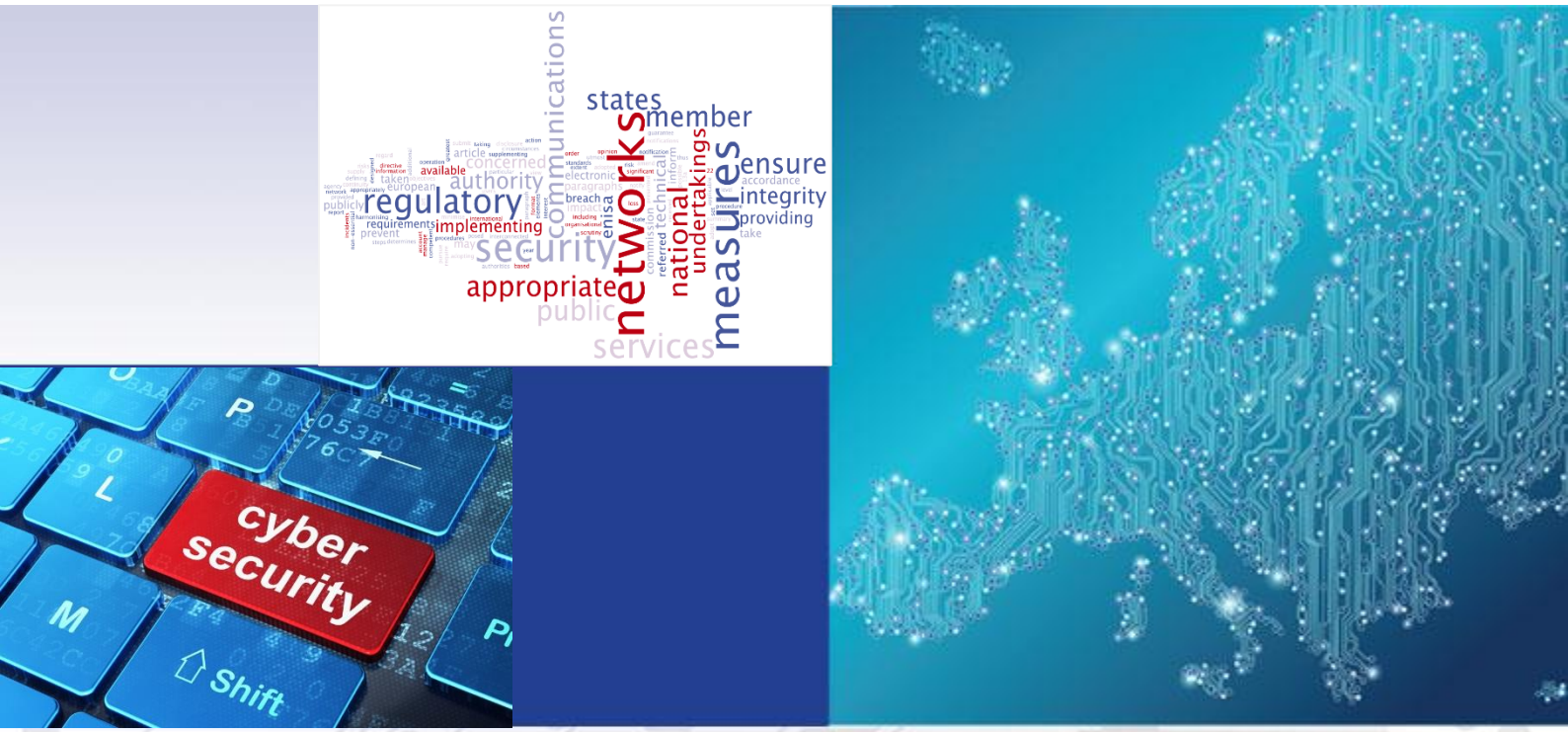


Annual Incident Reports 2014

Analysis of Article 13a annual incident reports

AUGUST 2015

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Christoffer Karsberg and Christina Skouloudi.

Contact

For contacting the authors please use resilience@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For the completion of this report ENISA has worked closely with a group of experts from National Regula-tory Authorities and ministries from across Europe. Listing the organizations (in no particular order): PTS (SE), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ADAE (GR), Centre for Cyber Security - CFCS (DK), RTR (AT), ANCOM (RO), CRC (BG), Ministry of Economics, Finance and Industry (FR), Bundes-netzagentur (DE), BIPT (BE), Agentschap Telecom (NL), MINETUR (ES), MPO (CZ), CTO (CZ), CERT LT (LT), Teleoff (SK), ILR (LU), PECSRS (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), Nkom (NO), RIA (EE), NMHH (HU), ITSIRI (LV), OEC (PL), AKOS (SI), OFCOM (CH), and HAKOM (HR).

ISBN: 978-92-9204-126-7, DOI: 10.2824/24249

Table of Contents

Executive Summary

For the fourth year, ENISA publishes the annual report about significant outage incidents in the European electronic communications sector, which are reported to ENISA and the European Commission under Article 13a of the Framework Directive (2009/140/EC), by the National Regulatory Authorities (NRAs) of the different EU Member States.

This report covers the incidents that occurred in 2014 and it gives an aggregated analysis of the incident reports about severe outages across the EU. This report does not include details about individual countries or providers.

The aim of the incident reporting scheme is to provide transparency to society and to learn from past incidents in the electronic communications sector in order to systematically improve the security in the networks and services. This report provides an overview on an aggregated level of what services and network assets are impacted and the root causes of the incidents. Conclusions on the main patterns of incidents are drawn, contributing to discussions at policy level on strategic measures to improve the security in the electronic communications sector.

The main conclusions from this year's incident reporting are the following:

- **137 major incidents reported:** This year 25 countries including one EFTA country reported 137 significant incidents that occurred in 2014 while four countries reported they had no significant incidents.
- **Fixed telephony most affected:** In 2014 most incidents affected fixed telephony (Nearly half of all reported incidents). This was a change compared with the previous reporting years, when mobile telephony and mobile Internet represented the services most impacted by incidents.
- **Impact on emergency calls:** 29 % of the major incidents also had an impact on 112 emergency calls.
- **Technical failures cause most outages:** Most of the incidents were caused by technical failures (65 % of all reported incidents), mainly software bugs and hardware failures affecting switches and routers.
- **Faulty software changes and updates have most impact:** Incidents caused by human errors and particularly faulty software changes and updates had most impact in terms of users impacted in combination with the duration of the incidents.

These patterns need particular attention when carrying out risk and vulnerability assessments in the electronic communications sector.

Based on results from the annual incident reports, ENISA has over the years studied and provided recommendations in the areas of: power supply dependencies, national roaming for resilience, ICT procurement in the telecom sector, and mitigating cable cuts.

This year ENISA is assessing the impact of the implementation of the incident reporting scheme mandated in Article 13a of the EU Telecom Framework Directive. ENISA is also studying what indicators are being used when measuring the impact of incidents in the telecom sector. Thirdly, ENISA is providing a vocabulary covering the relevant threats to the continuity of telecom networks and services and the relevant network assets that are at risk.

ENISA chairs since 2010 the NRA Article 13a Expert Group that meets periodically to draft technical guidelines in the area of Article 13a. This NRA group of experts also exchanges experiences and good practices regarding security requirements, incident reporting and how providers and NRAs have addressed certain major incidents.

ENISA, together with the European Commission and NRAs in the EU Member States, will continue addressing specific incidents in more detail within the Article 13a Expert Group. ENISA will also continue to give support to other sectors that are developing network and information security incident reporting schemes.

1. Introduction

This is the fourth iteration of the report "Annual Incident Reports", which summarises significant outage incidents reported to ENISA and the European Commission (Commission), under Article 13a of the Framework Directive (2009/140/EC), a new article introduced in the 2009 reform of the EU regulatory framework for electronic communications. This year ENISA and the Commission received 137 incident reports from NRAs, about severe outages in the EU's electronic communication networks or services which occurred in 2013. This report provides an aggregate analysis of these 137 incidents.

Please note that in this document we do *not* provide details from the individual incident reports. The analysis is only an aggregation in terms of averages and percentages across the EU, and it does not contain references to specific countries or specific providers. Individual incidents are discussed in more detail with the NRAs in the Article 13a Expert Group.

This document is structured as follows: Section 2 and Section 3 briefly summarize Article 13a and the details of the technical implementation of Article 13a, as agreed in the Article 13a Expert Group by the different NRAs of the EU Member States. Section 4 analyses the incidents from 2014 which were reported to ENISA and the Commission and provides examples of incidents. Section 5 provides the conclusions.

In annex A-D we show graphs with the trend over the years to allow for the reader to make a comparison with data from previous years. This comparison should however be done with caution, as the methodology for details in the reporting has been improved over the years and the thresholds have been lowered year by year allowing for more incidents to be reported.

2. Article 13a of the Framework Directive: 'Security and Integrity'

The reform of the EU regulatory framework for electronic communications, which was adopted in 2009 and was transposed by most EU countries around May 2011, adds Article 13a to the Framework Directive. Article 13a addresses the security and integrity[1] of public electronic communications networks and services. The legislation concerns National Regulatory Authorities (NRAs) and providers of public electronic communications networks and services (providers).

Article 13a states:

- Providers of public electronic communications networks and services should take measures to guarantee security and integrity of their networks.
- Providers must notify competent national authorities about breaches of security or loss of integrity that have had significant impact on the operation of networks or services.
- National Regulatory Authorities should notify ENISA and national authorities abroad when necessary, for example in case of incidents with cross-border impact.
- Annually, National Regulatory Authorities should submit a summary report to ENISA and the European Commission about the incidents.

These incident reporting flows (incident notification and annual reporting) are shown in the diagram below. This document analyses the incidents from 2014 that have been reported to ENISA and the Commission (the black dashed arrow).

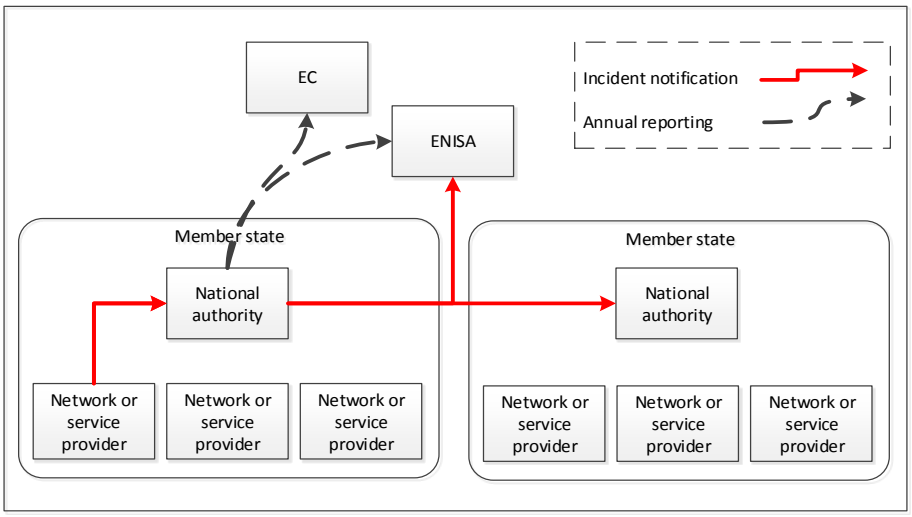


Figure 1: Incident reporting in Article 13a.

[1] Here integrity means network integrity, which is often called availability or continuity in information security literature.

3. Article 13a Expert Group and Incident Reporting Procedure

In 2010, ENISA, Ministries and NRAs initiated a series of meetings (workshops, conference calls) to achieve a harmonised implementation of Article 13a of the Framework directive. In these meetings, a group of experts from NRAs, called the Article 13a Expert Group, reached agreement on two non-binding technical documents providing guidance to the NRAs in the EU Member States:

- Technical Guideline on Incident Reporting[2]
- Technical Guideline on Security Measures[3]

Later on, in 2014, the group of experts agreed on the third non-binding technical document:

- Technical Guideline on Threats and Assets[4].

The Article 13a Expert Group continues to meet several times a year to develop the technical guidelines and to discuss the implementation of Article 13a (for example, on how to supervise the electronic communications sector) and to share knowledge and exchange views about past incidents, and how to address them.

3.1 Incident reporting procedure

In spring 2012, the Commission agreed with the EU Member States (in meetings of the Communications Committee, COCOM) to do the first round of annual summary reporting on the 2011 incidents impacting the continuity of supply of electronic communications services. The decision included a recommendation to use the reporting template agreed within the Article 13a Expert Group and published by ENISA. Following the COCOM meeting, ENISA implemented the technical procedure by deploying a basic electronic form based on the Article 13a Technical Guideline on Incident Reporting. There was also an agreement that in the coming years, annual reporting would be carried out by the end of February each year.

In autumn 2012, ENISA developed an online incident reporting tool (called CIRAS), which replaces the electronic forms exchanged by email. CIRAS allows NRAs to exert greater control over the data reported and provides the NRAs with better access to data about incidents reported across the EU. In 2015 ENISA is providing the possibility for the NRAs to extract graphs from CIRAS based on their search results.

We briefly explain the main features of the incident reporting procedure, as described in the Article 13a Technical Guideline on Incident Reporting, which was developed in collaboration with the NRAs.

3.1.1 Services in scope

NRAs should report about incidents affecting the following electronic communication services:

- Fixed telephony (e.g. PSTN, VoIP over DSL, Cable, Fibre, etc.),
- Mobile telephony (e.g. GSM, UMTS, LTE, etc.),
- Fixed Internet access (e.g. over DSL, Fibre, Cable, etc.),
- Mobile Internet access (e.g. GPRS/EDGE, UMTS, LTE, etc.)

[2] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting
[3] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[4] https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

NRAs may also report about incidents affecting other types of services, e.g. TV broadcast, SMS and e-mail, however these services are not in scope of this report.

3.1.2 Security incidents in scope

NRAs should report security incidents, which had a significant impact on the continuity of supply of electronic communications services.

3.1.3 National user base

NRAs should provide estimates of the total number of users of each service in their country.

- For fixed telephony and Internet, NRAs should use the number of subscribers or access lines in their country.
- For mobile telephony, NRAs should use the number of active telephony SIM cards.
- For mobile Internet, NRAs should sum up[5]:
    1. The number of standard mobile subscriptions, which offer both telephony and Internet access, and which have been used for Internet access recently (e.g. in the past 3 months).
    2. The number of subscriptions dedicated for mobile Internet access, which are purchased separately, either standalone or on top of an existing voice subscription.

3.1.4 Thresholds

The threshold for the annual summary reporting is based on the duration and the number of users of a service affected as a percentage of the national user base of the service.

NRAs should send an incident report, as part of the annual summary reporting, if the incident:

- lasts more than an hour, and the percentage of users affected is higher than 15 %,
- lasts more than 2 hours, and the percentage of users affected is higher than 10 %,
- lasts more than 4 hours, and the percentage of users affected is higher than 5 %,
- lasts more than 6 hours, and the percentage of users affected is higher than 2 %, or if it
- lasts more than 8 hours, and the percentage of users affected is higher than 1 %.

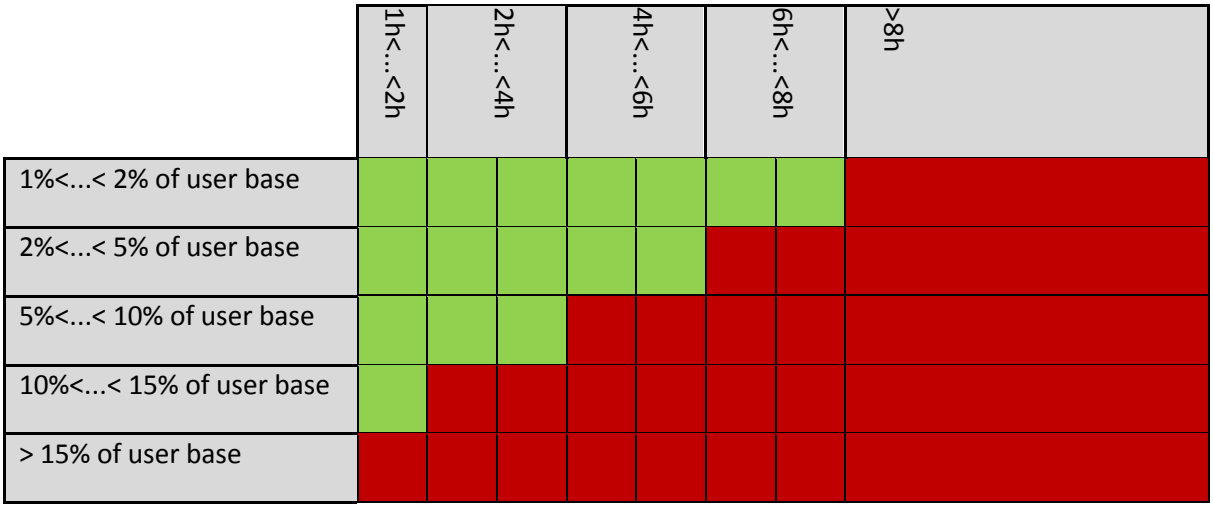


Figure 2: Threshold for annual summary reporting based on a combination of duration and the percentage of the national user base.

[5] Reference is made to the definition agreed in the COCOM meetings.

The threshold should be understood on a "per service" basis. In other words, if an incident impacts multiple services, then for one of the services the threshold should be passed in order to trigger the reporting mechanism. NRAs have the discretion to also report incidents with impact graded below the threshold.

For 2013, we introduced a new optional threshold for annual summary reporting, based on absolute impact, in order to allow for NRAs in large Member States to include larger incidents but that would not exceed the relative thresholds. This absolute threshold has been lowered for 2014 and has now become mandatory. NRAs should include incidents when the product of duration and number of user connections affected exceeds 60 million user minutes, or 1 million user hours. Note that the introduction of this mandatory and lowered absolute threshold has led to an increase in the number of reported incidents to ENISA and the Commission.

3.1.5 Root cause categories

In the incident reports four categories of root causes have been outlined plus one category that is used in conjunction with one of the other four categories.

- **Natural phenomena** – This category includes incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on.
- **Human errors** - This category includes incidents caused by errors committed by employees of the provider or outside the provider, during the operation of equipment or facilities, the use of tools, the execution of procedures, etc. E.g. an excavator cutting off a cable.
- **Malicious attacks** - This category includes incidents caused by a deliberate act by someone or some organisation, e.g. a Denial of Service attack disrupting the service, or a cable theft.
- **System failures** – This category includes incidents caused by technical failures of a system, for example caused by hardware failures, software bugs or flaws in manuals, procedures or policies.
- **Third party failures** – This category includes incidents caused by a failure or incident at a third party. The category is used in conjunctions with one of the other four root cause categories.

3.1.6 Detailed causes

In the incident reports, detailed causes are specified in terms of "initial cause" and "subsequent cause". "Initial cause" is the event or factor that *triggered* the incident. Often incidents involve a chain of events or factors, and by specifying a "subsequent cause" NRAs may indicate a cause that subsequently played a role in the incident. In the ENISA annual reports the initial and subsequent causes are equally presented in the graphs of the detailed causes. These detailed causes are referred to as "threats" in the Article 13a Technical Guideline on Threats and Assets[6]. In the report, which is used by the NRAs as a guide for the annual summary reporting, the causes/threats are listed and described.

3.1.7 Assets affected

Optionally NRAs may indicate what network assets were affected by the incidents, e.g. HLRs, routers and switches, underground cables etc. These assets are listed and described in the Article 13a Technical Guideline on Threats and Assets.

[6] https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

4. Analysis of the incidents

In total, all 28 EU Member States and 1 EFTA country participated in this process. Of these, 24 Member States and 1 EFTA country reported in total 137 significant incidents and 4 countries reported there were no significant incidents.

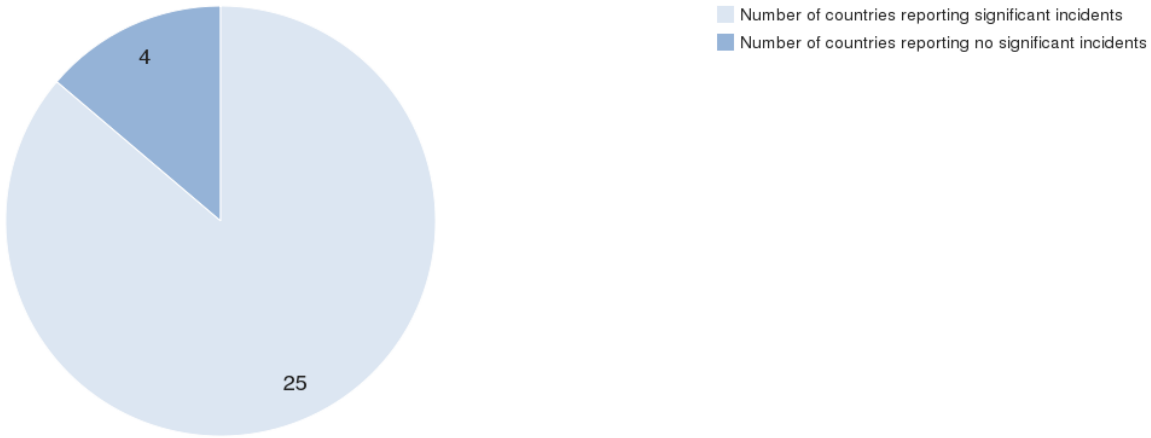


Figure 3: Countries involved in the annual summary reporting over 2013.

In this section, the 137 reported incidents are aggregated and analysed. First, the impact per service is analysed (in Section 4.1), then the impact per root cause category is analysed (Section 4.2), and in Section 4.3 detailed causes are examined. In Section 4.3.5 the impact, as a product of user connections affected and duration of the incidents, is analysed, and in Section 4.4 the components or assets affected by the incidents are considered. Throughout the text we provide anonymized descriptions (in blue italic) of actual large-scale incidents which occurred in 2014. In annex A-D we show graphs including the previous two years to allow the reader to make a comparison. This comparison should however be done with caution, see below.

Note about statistical conclusions: Readers should be cautious when drawing conclusions from the statistics in this report. In particular, they should take into account that:

1. The scope of reporting major security incidents is restricted to incidents with an impact on the *continuity* of public electronic communication services and networks. There are many other types of incidents with an impact on security of services and networks which are not in scope of annual reporting. For example, if attackers would wiretap undersea cables without causing any outages, then such a security incident would not be included in the annual reporting.
2. The scope of reporting includes major, or *significant,* incidents scoring above the agreed reporting thresholds. Smaller incidents are not reported at EU level, meaning that the view is skewed towards the larger incidents.
3. Year by year we are in collaboration with the NRAs lowering the thresholds for the annual summary reporting. This fact, in combination with continuously improved national reporting mechanisms, lead to increasing numbers of reports submitted to ENISA and the Commission each year. This doesn't necessarily mean that the number of incidents throughout the EU is increasing.
4. We are continuously working in collaboration with the NRAs for improved quality in the incident reporting. There are still changes, more details and improvements in the way national and EU reporting is being implemented, including the lowering of reporting thresholds and refinements of parameters for reporting. Statistical conclusions about multi-annual trends should therefore ***be drawn with caution***.

4.1 Impact of incidents

First we look at the electronic communications services and compare them with each other in terms of incidents.

4.1.1 Impact per service

In 2014 most of the reported incidents affected fixed telephony although there was quite an even spread among the services. This is a break in the trend compared to the earlier reporting years when most incidents affected mobile communications (see Annex A.1).

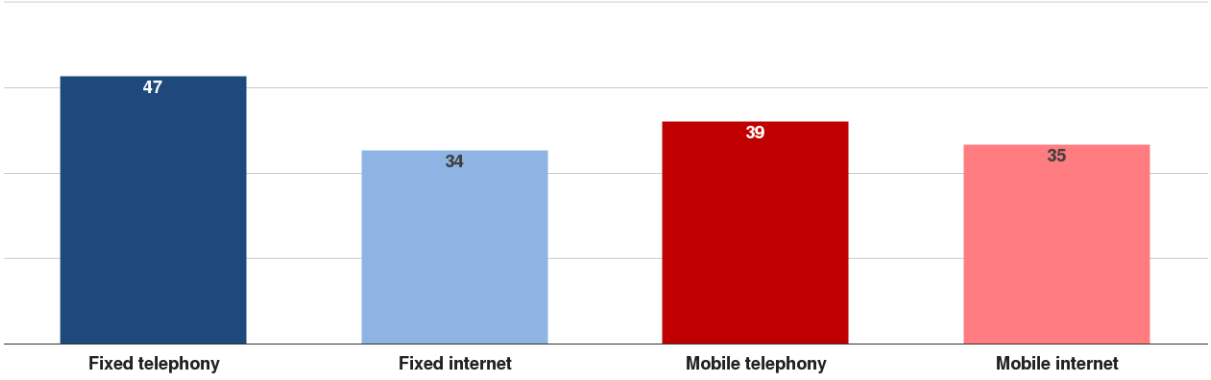


Figure 4: Incidents per service (percentage)

Note that most reported incidents usually have an impact on more than one service in the same incident (which is why the percentages in the chart add up to more than 100 %).

A software bug caused fixed telephony to fail for millions of users (duration: hours, connections: millions, cause: system failure): *A metro router[7] in an exchange suffered a software crash and lost connection to the core network but continued to advertise available BGP routes to access network swtiches. Some more exchanges continued to be affected but they were misdiagnosed as fixed, which delayed restoring the service.*

4.1.2 Number of user connections affected

Mobile Internet outages affected most user connections compared to the other services, with an average of 1.7 million user connections affected per reported incident. Also in past reporting years mobile internet failures affected most user connections, and mobile telephony failures came in second place, see Annex A.2.

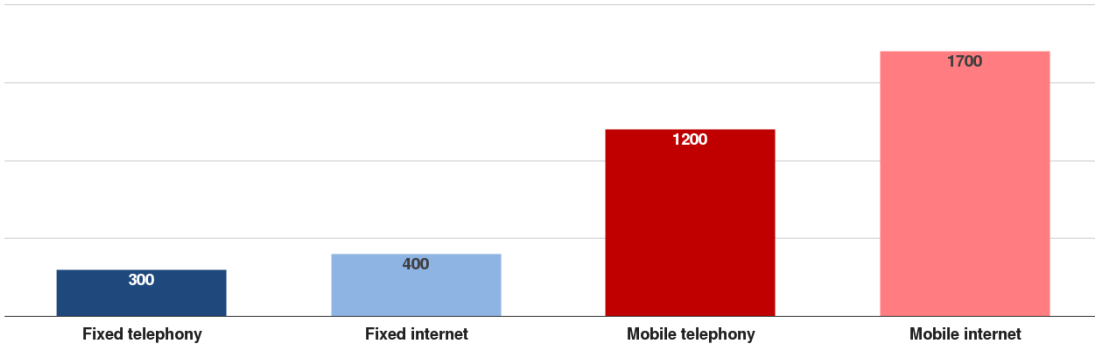


Figure 5: Average number of user connections affected per incident per service (1000s).

[7] Metro router = system for routing traffic in metropolitan area networks.

Note that the averages in these diagrams include both small and large countries, so EU averages shown in the diagram above are not necessarily representative for the size of incidents occurring nationally. The average size of national incidents can be very different, depending on the size of the population and the national network topology. What is interesting to note is the comparison between the affected services in terms of affected user connections.

The difference between mobile and fixed may partly be due to the fact that some of the impacted components, we call them assets, in the mobile networks, were more centrally located parts of the networks as compared to the failed assets for fixed services, thus affecting more user connections per incident. We can see this pattern for the last three years, see Annex A.2.

4.1.3 Percentage of the national user base affected

Mobile Internet outages impacted about 13 % of the national user base for mobile Internet user connections on average, which is a slight increase compared to the previous year, see annex A.3. Despite an increased number of smaller incidents reported in 2014 compared to earlier years, due to lowered reporting thresholds, the percentage of the national user base affected increased. All four years, mobile Internet has been reported to suffer the most impact in terms of percentage of its national user base compared to the other services.

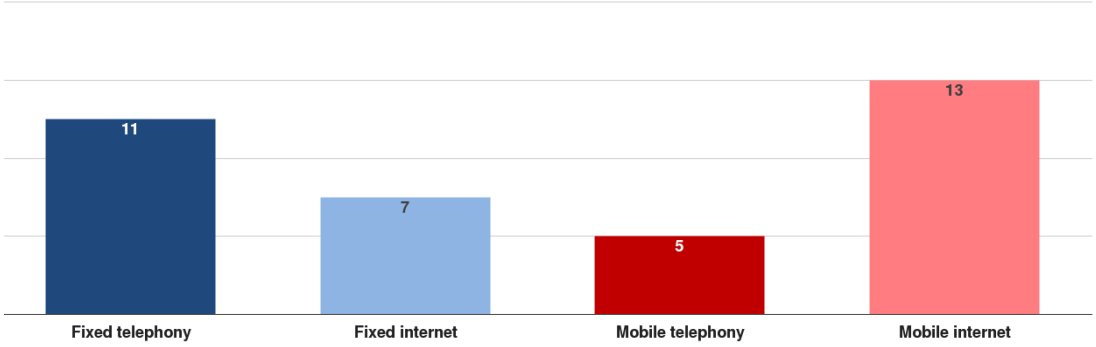


Figure 6: Percentage of national user base affected on average per incident per service.

Distributed Denial of Service attack caused mobile Internet to fail (duration: hours, connections: millions, cause: Malicious action): *Intermittent DDos attacks were carried out by hijacking customer equipment. The equipment was used to create an amplification attack by issuing malicious DNS requests towards certain customers' domains. The amplification attack created an overload situation in the load balancers for the DNS servers which caused the mobile Internet services to fail for approximately 50 % of the customers, although the provider was not the target of the attack.*

4.1.4 Impact on emergency services

In 29 % of incidents reported, emergency calls were impacted - i.e. the possibility for users to contact emergency call-centres using the emergency number 112. Compared to the previous year this figure has increased, see Annex A.4.

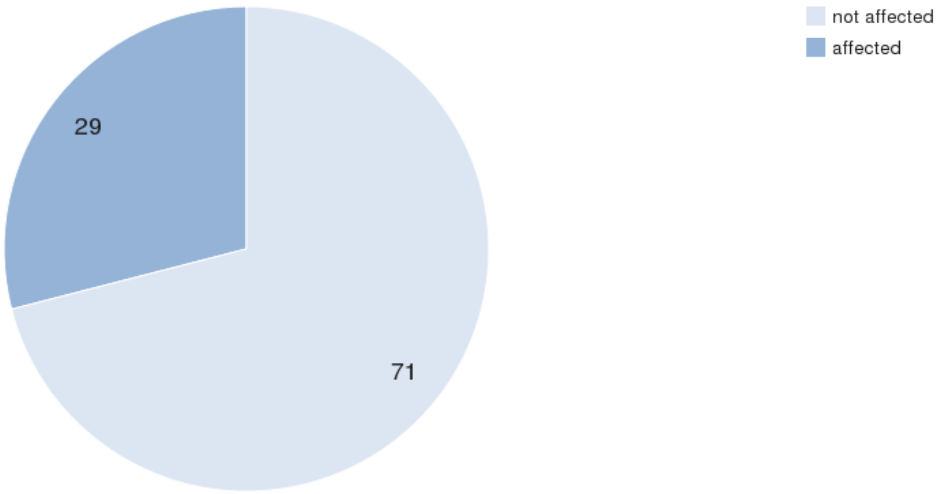


Figure 7: Impact on emergency calls.

4.1.5 Impact on interconnections

In 12 % of incidents reported there was an impact on interconnections between providers. Compared to previous year also this figure has increased, see Annex A.5. This calls for incentives for information sharing between interconnected providers to inform about disruptions and to share mitigation measures.

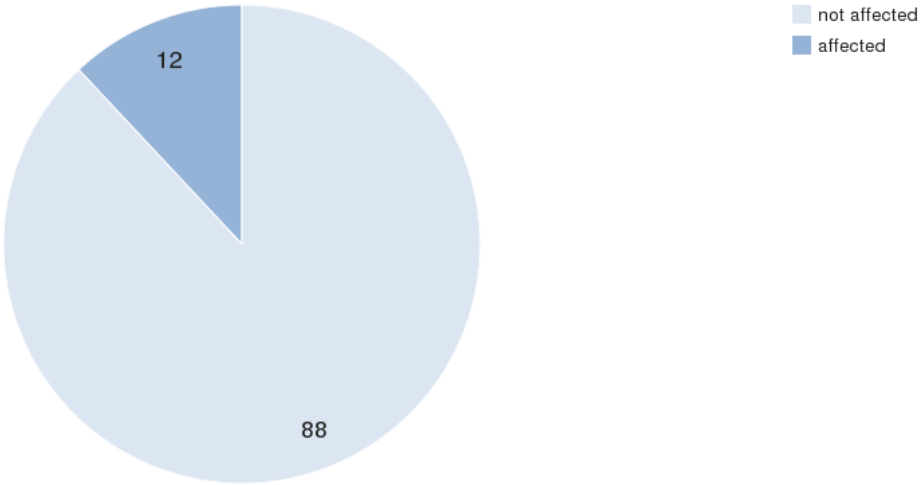


Figure 8: Impact on interconnections

4.2 Root cause categories

In this section we look at the main root cause categories of reported incidents. For a description of the root cause categories, see section 3.1.5.

4.2.1 Incidents per root cause category

In 2014 most of the reported incidents, 65 % of the incidents, were in the root cause category system failures or technical failures, a ratio which is consistent compared to the previous year, see Annex B.1. For all reporting years, system failures has been the most commonly impacted root cause category. In second place, 20 % of the incidents were caused by human errors, also this was consistent with previous years. In 9 % of the reported incidents ”malicious actions” were detected, which is a slight increase compared with the previous year. Last year this category surpassed ”natural phenomena”, which had a decrease compared to the earlier years.

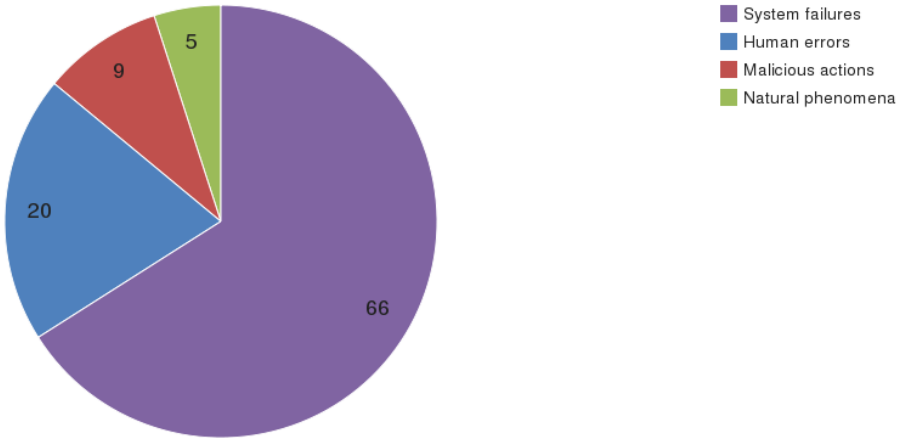


Figure 9: Incidents per root cause category (percentage).

Hardware failure caused disruptions for millions of mobile telephony users (duration: hours, connections: millions, cause: system failure): *A failure in some cross-connector circuits in town X isolated a Mobile Switching Centre, MSC, from the rest of the network, causing overload in the Home Location Register, HLR. Due to this overload, millions of users across the country were not able to make phone calls for several hours.*

4.2.2 Third party failures

About 16 % of the incidents reported were categorized as third party failures, a slight increase compared to the previous year, see Annex B.2.

Figure 10: Third party failures and non-third party failures of all incidents (percentages).

Below we show the root cause categories for the reported third party failures.

In 2014 third party failures basically had the same distribution of root causes as the reported incidents in general, with system failures as the most common type of third party failures. Human errors, however, were more frequent in third party failures than in the reported incidents in general.

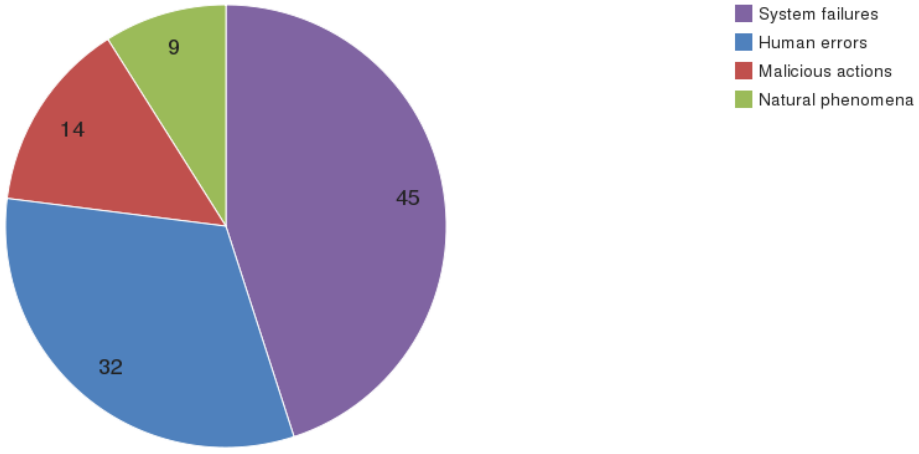


Figure 11: Third party root causes (percentage).

External power failure caused fixed telephony and internet to fail (duration: hours, connections: thousands: cause: third party system failure): *The incident was caused by a power failure from the energy supplier and power surges coming from the power network. This affected a number of central systems, applications and circuits that had to be reestablished and in some cases repaired.*

4.2.3 Root cause categories per service

In this section we look at the root causes for each of the four services separately: fixed telephony, fixed Internet access, mobile telephony and mobile Internet access.

In 2014, system failures was the dominant root cause for all services respectively. For mobile telephony and mobile internet, this was the case also the previous years, whereas the dominant root cause for fixed telephony and fixed internet the previous years was natural phenomena, see Annex B.3.

4.2.3.1 Fixed Telephony

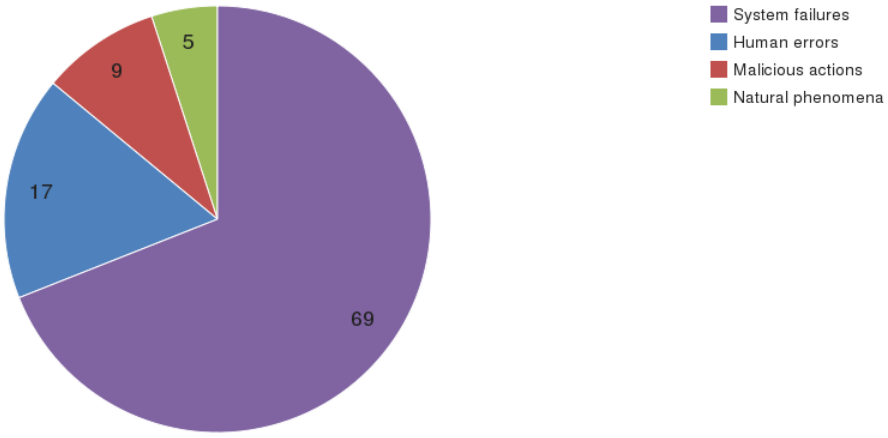


Figure 12: Root cause categories for fixed telephony (percentage).

4.2.3.2 Fixed Internet

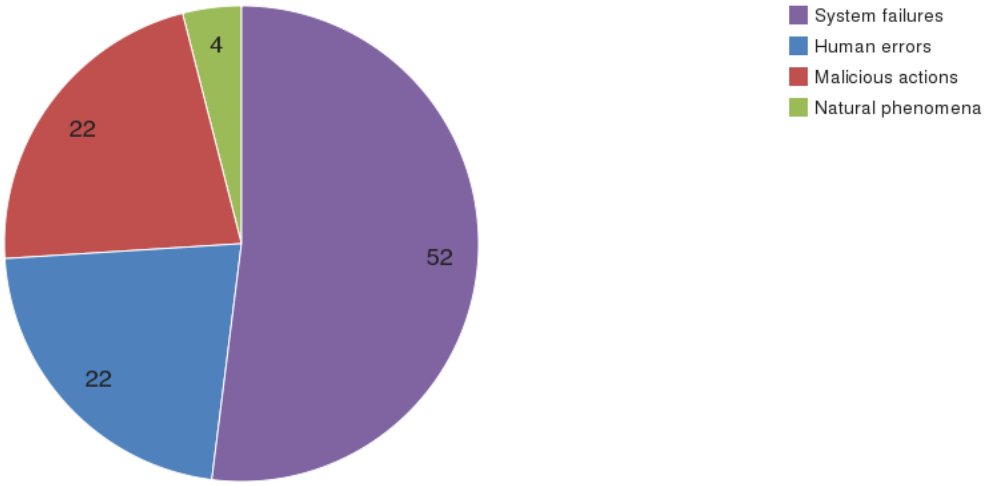


Figure 13: Root cause categories for fixed Internet (percentage).

4.2.3.3 Mobile telephony

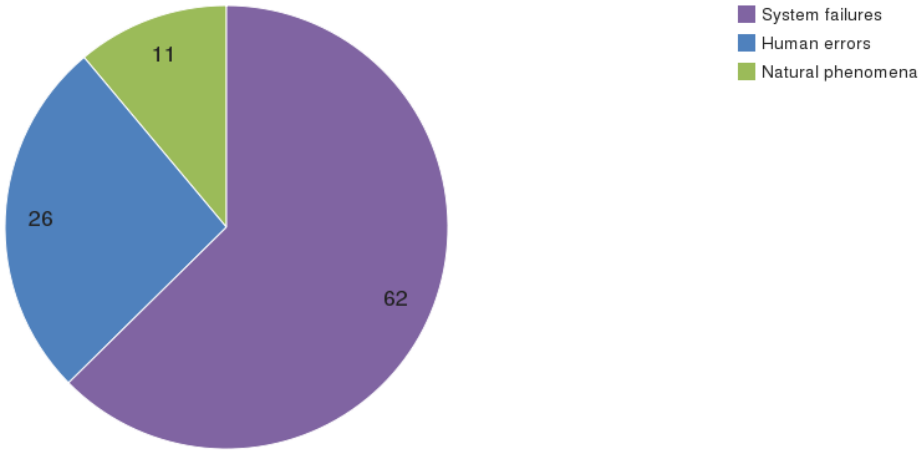


Figure 14: Root cause categories for mobile telephony (percentage).

4.2.3.4 Mobile internet

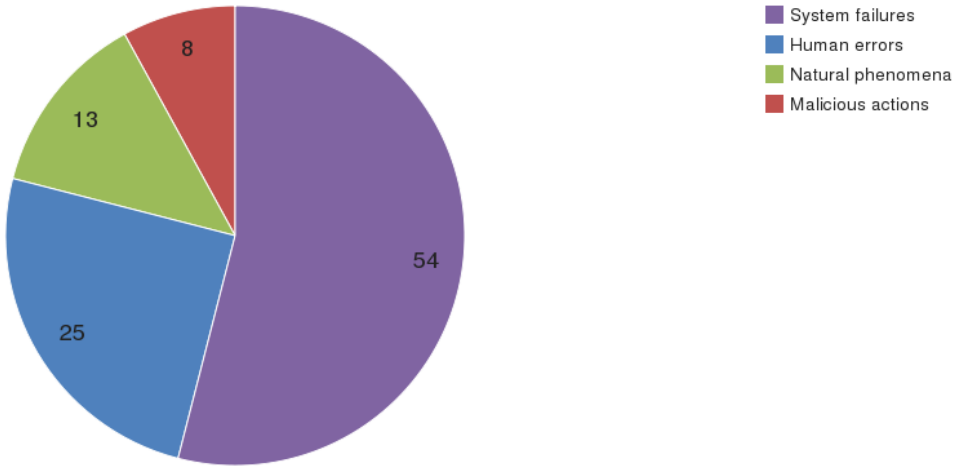


Figure 15: Root cause categories for mobile Internet (percentage).

4.2.4 Average number of user connections affected per root cause category

In 2014 human errors affected most user connections, on average about 3 million user connections per incident. In the previous year, system failures affected most connections.

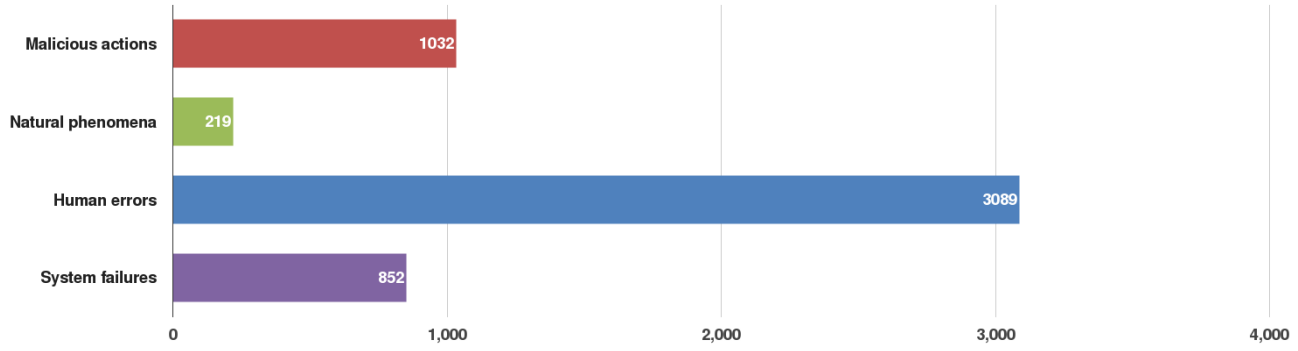


Figure 16: Average number of user connections affected per incident per root cause (1000s)

Excavator cut a cable causing all services to fail for millions of users for several hours (duration: hours, connection: millions, cause: human error and third party failure*): An electricity company was doing excavation works, and in order to avoid cable damages, it had asked the relevant telecom provider to come and show where in the ground it had its infrastructure. The provider didn't show one interconnection cable between the two countries, and it was cut. Soon after, it was discovered that due to a configuration error in a router in the capital of the other country, the traffic didn't route automatically to the secondary interconnection. This caused major lack of capacity in the abroad connections.*

4.2.5 Average duration of incidents per root cause category

The reported incidents caused by natural phenomena had the longest recovery time on average per incident (81 hours), the highest figure since the annual incident reporting started, see Annex B.4. The trend is unsurprisingly that incidents caused by natural phenomena are the most difficult incidents to manage in terms of recovery time.

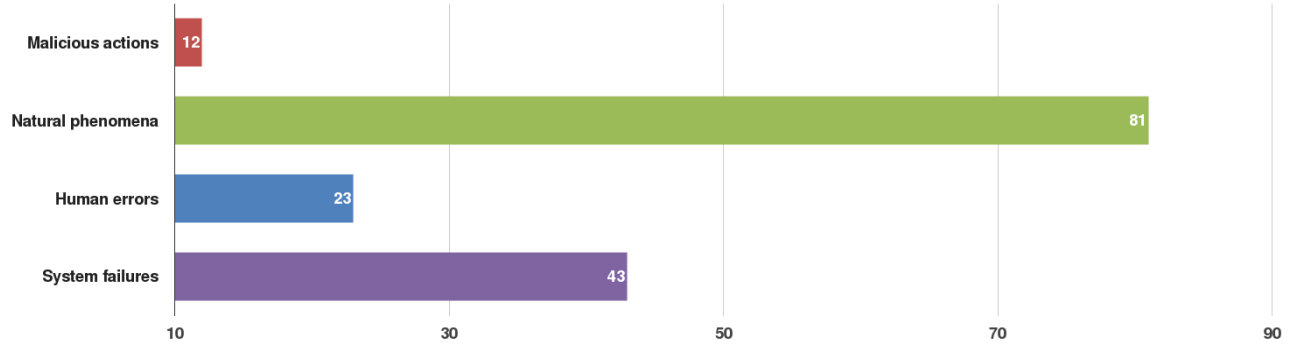


Figure 17: Average duration of incidents per root cause category (hours).

Ice storm caused outages in all services for up to two weeks (duration: weeks, connection: thousands, cause: natural phenomena): *Due to heavy sleet and fierce ice storms, providers experienced a lengthy interruption of*

services. Affected were users in the wide area of the country. The loss of services was impacting users for one day up to two weeks. The main cause for the loss of services was the interruption of power supply, because heavy ice on cables destroyed a large number of power lines and pillars. All services including the emergency call service were interrupted.

***Heavy snow shut down power supply causing mobile networks to fail (duration: days, connection: thousands, cause: natural phenomena and third party failure**): Due to severe weather conditions with heavy snow and ice, the electricity supplier was affected. Because of the lack of power supply, the equipment became inoperable until the situation was remedied by the supplier. Due to the weather conditions, roads were closed. This made the access to base station sites with problems very difficult, so the actions taken to remedy the situation were delayed.*

4.2.6 User hours lost per root cause category

Considering the number of user connections affected and the duration of the incident, yields a value that allows us to measure the total impact of an incident. We call the latter ”user hours lost”. In 2014 human error clearly had most impact in terms of user hours lost. However, the previous year natural phenomena had most impact.

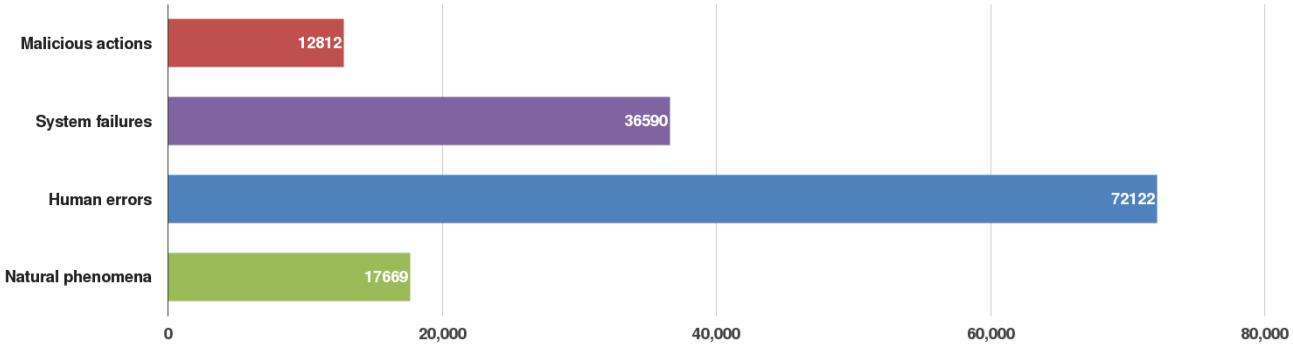


Figure 18: Average user hours lost per incident per root cause category.

***A procedure flaw caused fixed network to fail: (duration: hours, connections: thousands, cause: human error):** Provider Edge routers at two POP sites became isolated due to planned optical fibre works by third party fibre provider. Planned works ran over schedule and upon completion of works the provider equipment was not correctly reconnected.*

4.3 Detailed causes

Root cause categories are rather broad but give a good summary of the most common types of incidents. In this section we break down the root cause categories in predefined detailed causes of incidents.

An incident is often not only triggered by one cause but often by multiple causes and a chain of causes. For instance an incident may initially be triggered by heavy winds, which tear down power supply infrastructure causing a power cut, which in turn leads to an outage. For this incident both heavy winds and power cut are detailed causes. These detailed causes are equally represented in the statistics, because both causes may be addressed by the provider in terms of security measures.

4.3.1 Detailed causes of all incidents

In 2014, the most common causes of incidents were software bugs and hardware failures. This can now be considered a trend as this has been the case all the previous years. Also cable cuts were among the top four causes during all three years as well as power cuts. Denial of service attacks increased to being the seventh most common cause for service disruptions.

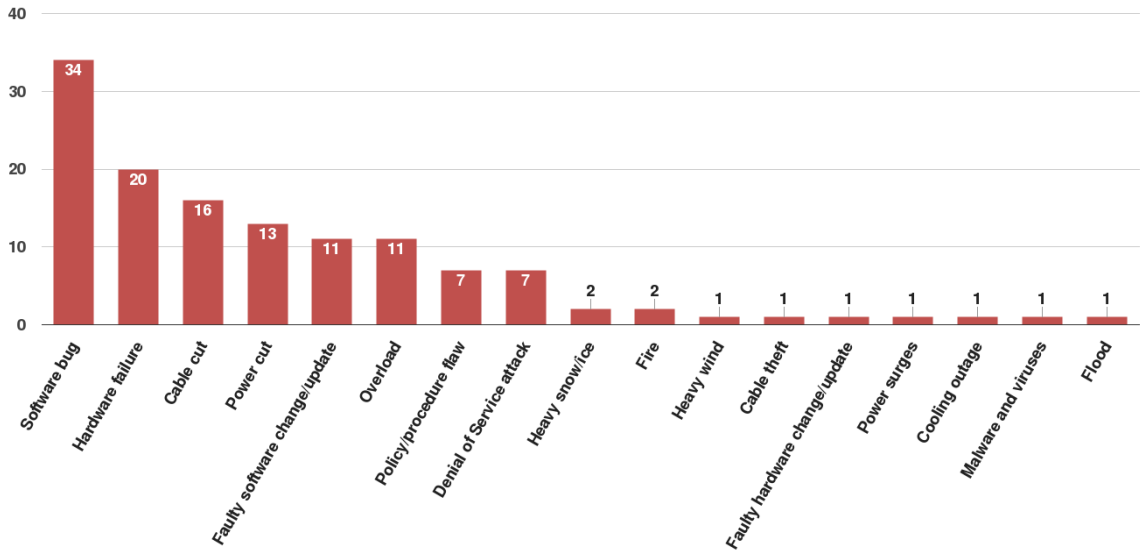


Figure 19: Detailed causes of reported incidents (percentage)

Software bug/vulnerability in CPEs[8] caused DDOS attacks outside operator's network (duration: hours, connections: thousands, cause: software bug): *Compromised CPEs generated DDoS to domain outside operator's own network. Grown traffic affected operator's DNS-servers so that occasionally DNS requests could not be answered.*

4.3.2 Detailed causes per service

In this section we show the detailed causes of incidents for each of the four services (fixed telephony, fixed Internet, mobile telephony and mobile Internet) - see figures 20 to 23 below. Software bugs and hardware failures were the most common causes for failures in three of the four services; fixed telephony, mobile telephony and mobile internet. For fixed Internet the most common cause was power cuts. Fixed Internet was also compared

[8] Customer Premises Equipment (e.g. home routers)

with the other services and in absolute terms quite significantly impacted by denial of service attacks and this trend has increased over the years.

4.3.2.1 Fixed Telephony

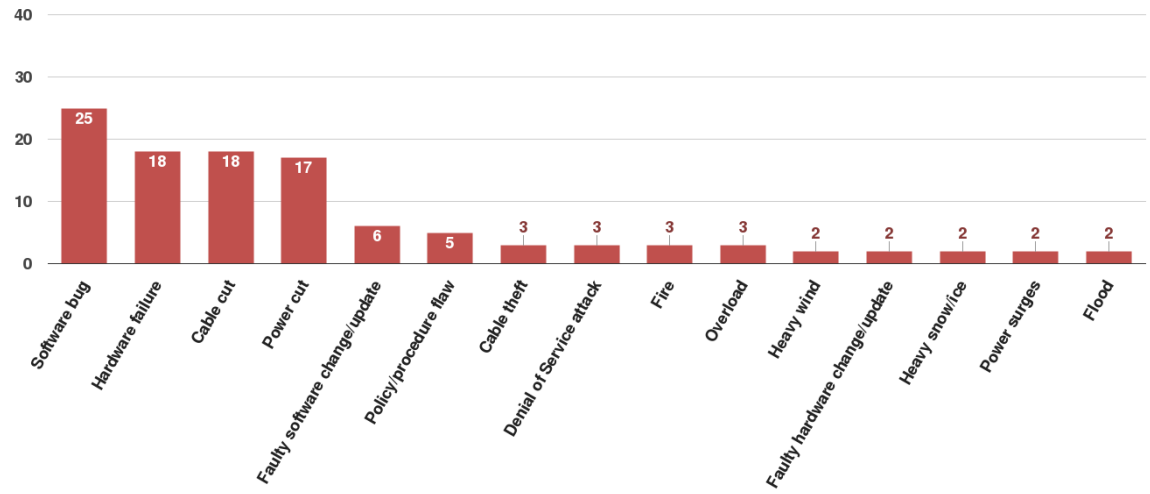


Figure 20: Detailed causes for fixed telephony (percentage).

4.3.2.2 Fixed Internet

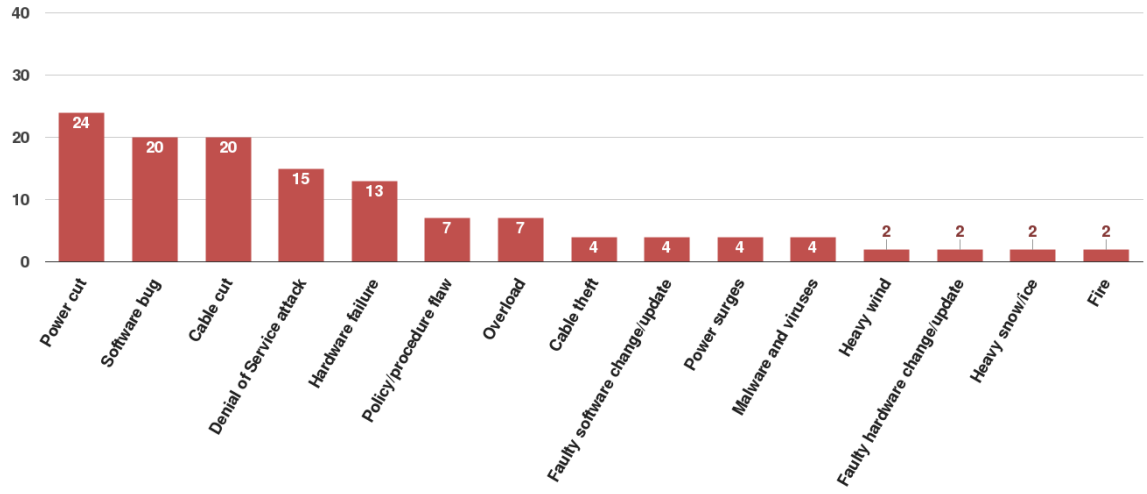


Figure 21: Detailed causes for fixed Internet (percentage).

4.3.2.3 Mobile Telephony

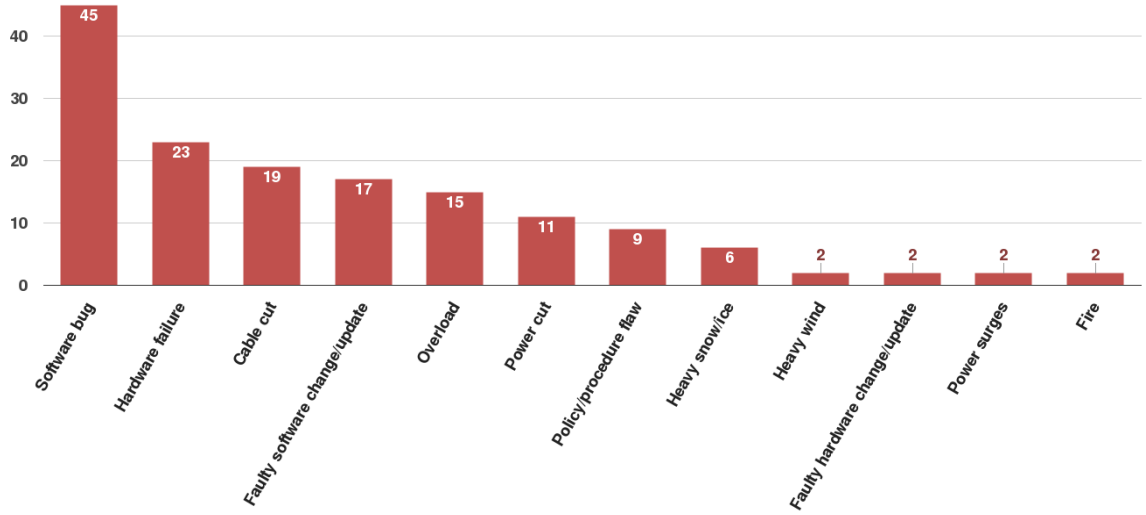


Figure 22: Detailed causes for mobile telephony (percentage).

4.3.2.4 Mobile Internet

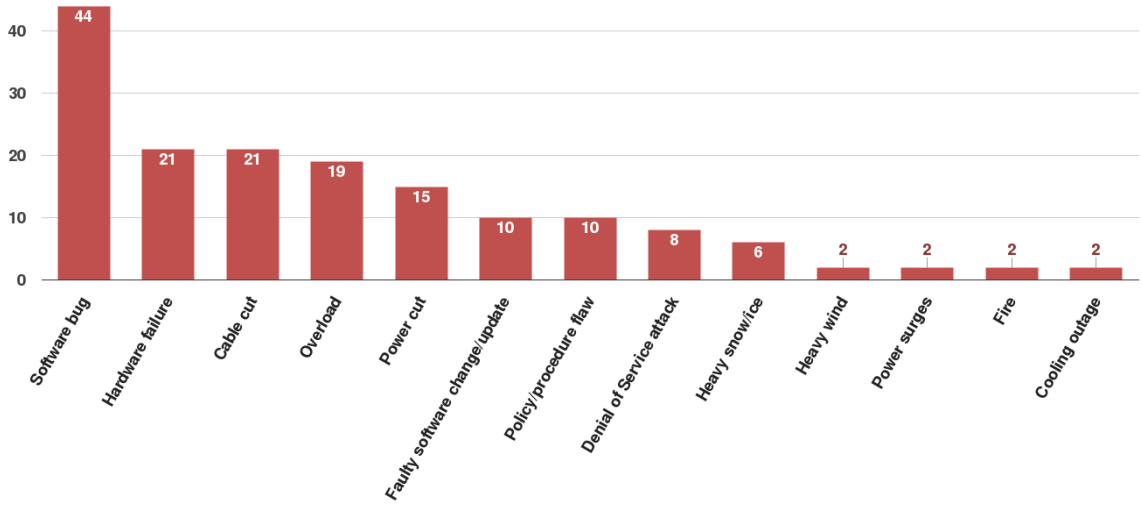


Figure 23: Detailed causes for mobile Internet (percentage).

4.3.3 Average number of user connections affected per detailed cause

In 2014 there was a small number of reported incidents caused by cooling outage affecting over 6 million user connections on average. Otherwise the number of user connections affected per incident was quite evenly spread over policy/procedure flaws, overload, denial of service attacks and software bugs.

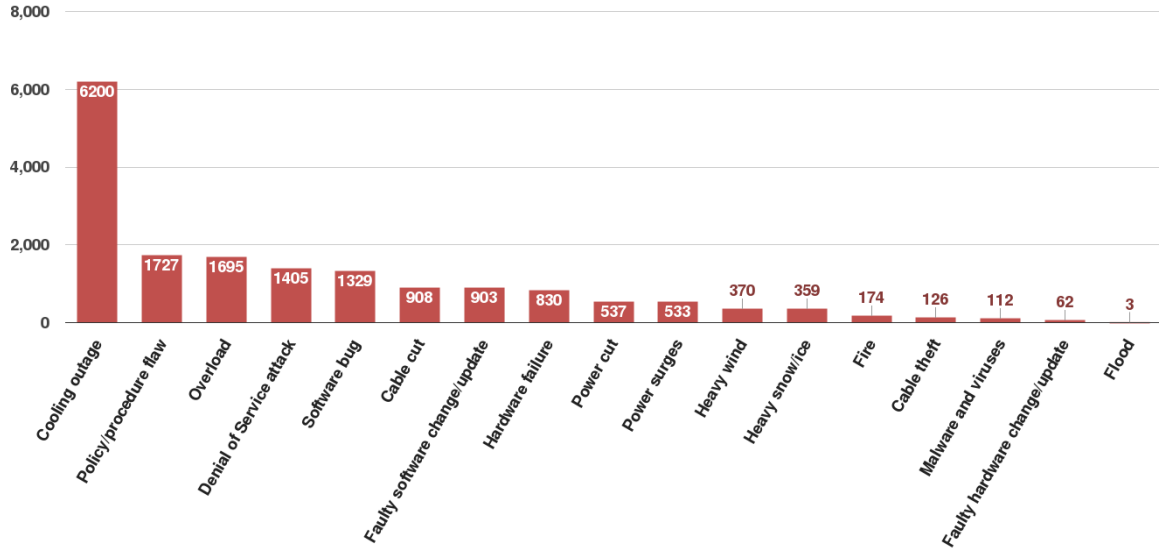


Figure 25: Average number of user connections affected per incident per detailed cause (1000s).

Faulty air conditioning led to power failure causing outage for millions of mobile Internet users (duration: hours, connections: millions, cause: cooling outage*): There was a power failure at a Provider's data centre. This impacted the mobile Internet service for millions of users for several hours. The loss of power resulted in customers experiencing problems when trying to make new data connections and when sending SMS/MMS. Mobile virtual network operators also experienced issues making voice calls. The initial cause was faulty air conditioning units which resulted in overheating, leading to a power failure. Temporary air conditioning units were set up in the rooms to reduce temperature while the air conditioning units were repaired. When temperatures returned to normal, power was restored and services started to restore. Full service was restored after six hours.*

DDoS-attack on website caused loss of mobile internet for all customers (duration: hours, connections: millions, causes: *Denial of Service attack): A distributed denial of service attack was carried out on a foreign gaming-site through old ADSL-modems. This caused DNS-overload and subsequently total loss of mobile data for the provider's customers all over the country.*

4.3.4 Average duration of incidents per detailed cause

For 2014, reported incidents caused by faulty software changes and updates had the longest duration (almost 5 days per incident on average). This figure should be considered with caution, as one of the incidents caused by faulty software changes and updates had a considerably high duration driving up the average figure. Heavy snowfall had the second longest average duration per incident (4 days) followed by heavy winds (3 days), fire and hardware failures (2,5 days).

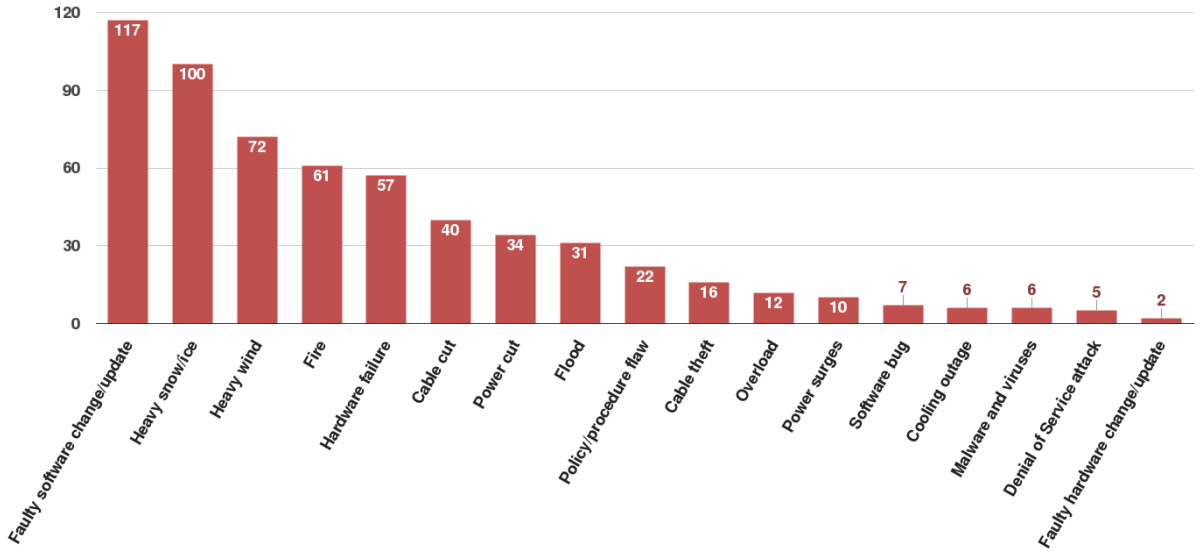


Figure 24: Average duration of incidents per detailed cause (hours).

Faulty software update caused a large scale mobile communication failure: (duration: days, connections: thousands, cause: faulty software update): *After migration of a HLR on to a new platform, subscribers experienced difficulties registering to the network and thus using the services. Subscribers didn't manage to setup calls and transfer data, etc.*

4.3.5 User hours lost per detailed cause

This graph shows the impact in terms of user hours lost per detailed cause. Faulty software changes and updates was for 2014 the cause having the most impact among the incidents. The previous year it was power cuts. This points towards the dependency on ICT equipment and services and the need to have security measures in place to deal with software changes and upgrades, such as good agreements with third party vendors, educated personnel, test environments, redundant systems and roll back routines etc.

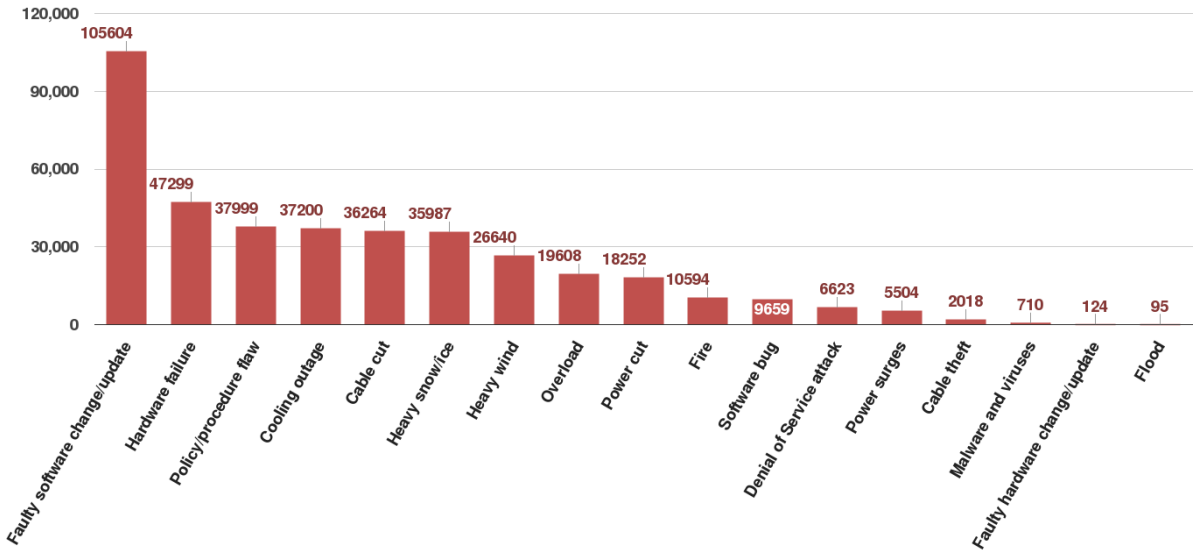


Figure 26: Average user hours lost per incident per detailed cause.

Faulty upgrade caused service failure for mobile communications (duration: hours, connections: thousands, cause: *faulty software change/update): While upgrading software affecting the Provider Edge (PE) in routing elements, there was a failure and redundant data paths did not work correctly.*

Faulty configuration caused outage in all services for millions of users (duration: hours, connections: millions, cause: human error): *A faulty executed command caused massive propagation of wrong configuration across an IP backbone of a provider. The incident originated from a network element and then flooded as a domino effect on other nodes of the operator's IP backbone, causing lack of IP connectivity among switches and HLRs and on the signaling network. The incident impacted access to mobile and fixed services for millions of users in parts of the national territory for several hours.*

4.4 Assets affected

For the third year we received reports from NRAs about which components or assets of the electronic communications networks were affected by the incidents. This provides some more information about the nature of the outages and what assets of the infrastructure that were primarily involved in them.

4.4.1 Assets affected overall

In 2014 switches and routers were the assets most affected by incidents. The previous year it was base stations and controllers, followed by switches and routers, see Annex D.1. In 2014 there were also many problems affecting underground cables.

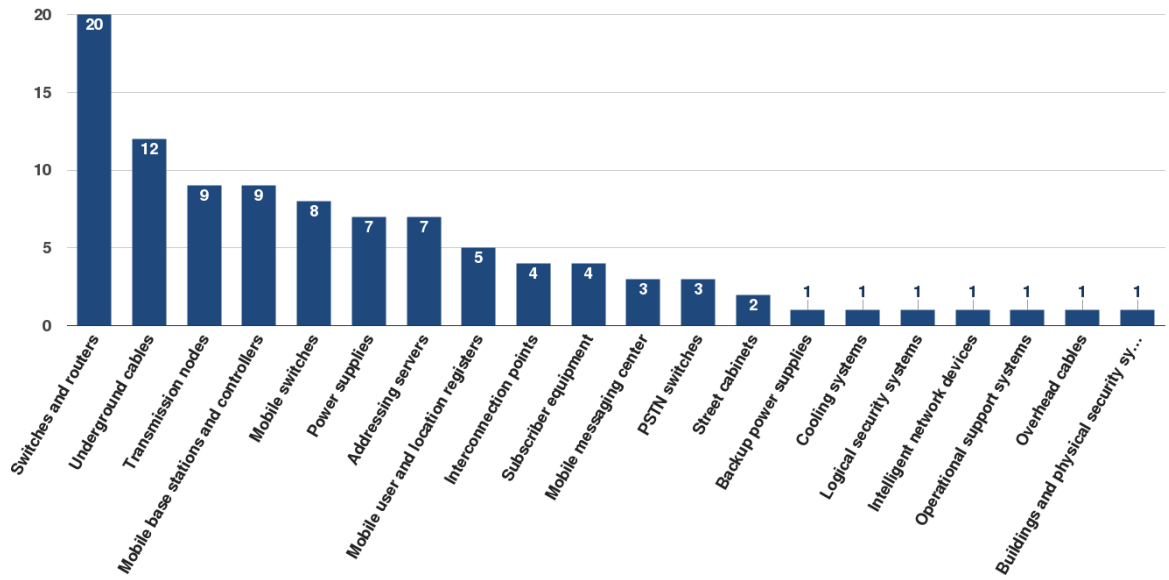


Figure 27: Assets affected by the incidents (percentage).

Software bug caused outage in VoIP services for thousands of users (duration: hours, connections: thousands, cause: Software bug): *Failure of both SIP[9] Session Management processes on the main Operator SIP Switch prevented set up of all inbound and outbound calls.*

[9] **Session Initiation Protocol** (**SIP**) is a communications protocol for signaling and controlling multimedia communication sessions.

4.4.2 Affected assets in system failures

As for all previous reporting years, system failures (or technical failures), was the most common root cause category in 2014[10]. In these system failures the most common assets that failed were switches and routers, mobile switches (MSC), transmission nodes, power supply equipment and mobile user and location registers (e.g. HLR). Also the previous year mobile switches, and switches and routers were the most common assets to fail in this root cause category.

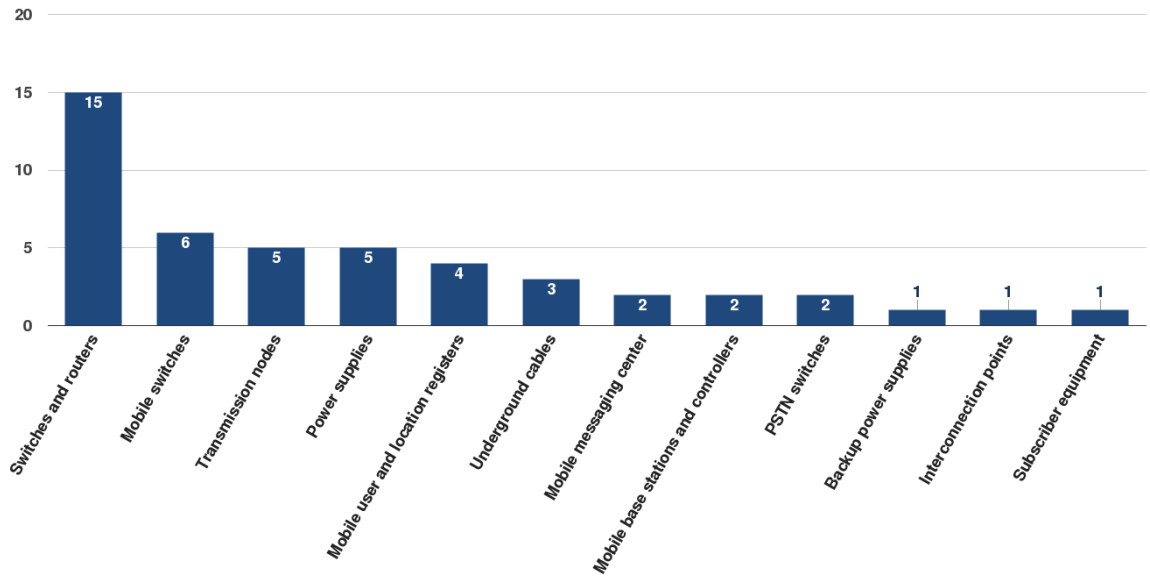


Figure 28: Assets affected by system failures (percentages).

Software bug caused outage in VoIP services for thousands of users (duration: hours, connections: thousands, cause: Software bug): *Thousands of xDSL-users could not use the VoIP service. A software bug of the switch appliance caused the outage. After the error had been identified, the appliance was relaunched.*

[10] The root cause System failure includes incidents caused by technical failures of a system, for example caused by hardware failures, software bugs or flaws in manuals, procedures or policies.

4.4.3 VoIP versus PSTN

We also split the service fixed telephony into traditional circuit switched fixed telephony (PSTN) and fixed IP based telephony (VoIP) to see if the detailed causes show any particular differences. Both PSTN and VoIP were mostly affected by software bugs last year and PSTN had more problems compared to VoIP. PSTN was also more affected by hardware failures compared to VoIP, and both PSTN and VoIP were affected by cable cuts. VoIP had more problems than PSTN with policy/procedure flaws.

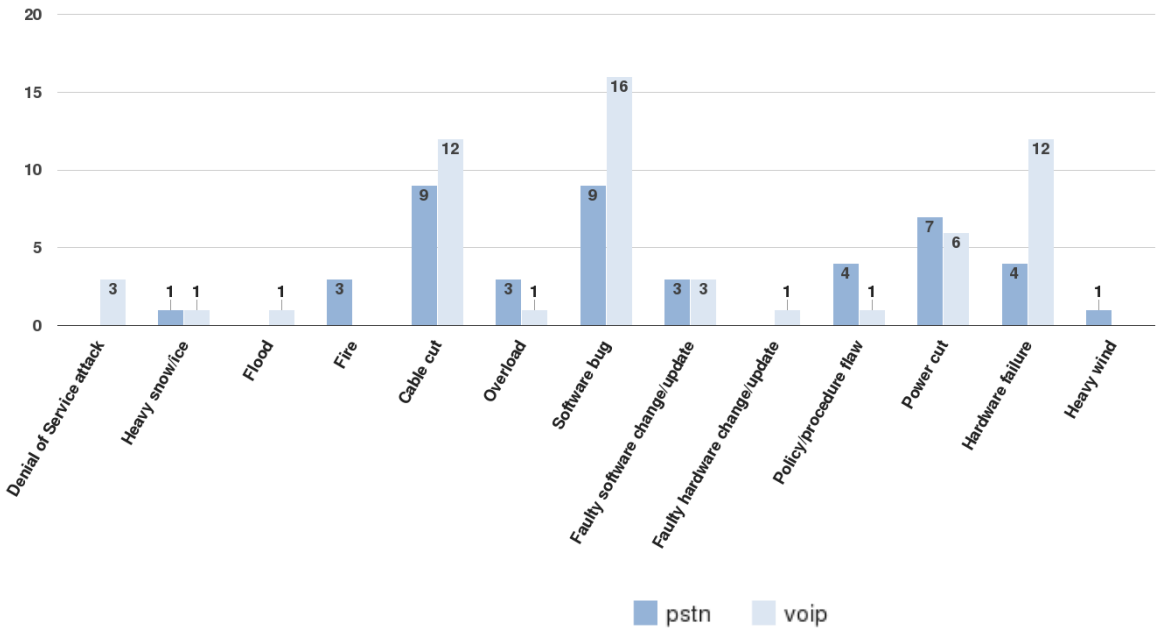


Figure 29: Detailed causes for incidents affecting PSTN and VoIP (percentage).

5. Conclusions

In this Report ENISA summarized and analysed the outage incidents that were sent by the National Regulatory Authorities, NRAs, to ENISA and the European Commission in 2015 concerning incidents in 2014, as mandated by Article 13a of the Framework Directive (2009/140/EC). ENISA and the Commission received, as part of the fourth round of reporting from the NRAs, 137 reports about major outages/disruptions impacting electronic communications services that occurred in 2014.

From the 137 significant incidents reported to ENISA and the Commission, the following conclusions can be drawn, first looking at services and network assets affected and then at the causes of the incidents.

Services and network assets affected:

- **Fixed telephony most affected:** In 2014 most incidents affected fixed telephony (47 % of all reported incidents). This was a change compared with the previous reporting years, when mobile telephony and mobile Internet represented the services most impacted by incidents.
- **Mobile network outages affect many users:** Incidents affecting mobile Internet or mobile telephony affected most users (around 1.7 million users and 1.2 million users respectively per incident). Centrally located network assets seemed to constitute single points of failure.
- **Emergency Services are affected by incidents**: In 29 % of the incidents there were problems in reaching the 112 emergency services, a small increase since the previous year.
- **Interconnections between providers are affected by incidents**: In 12 % of the incidents there were problems in interconnecting between providers, an increase compared with previous years. This calls for enhancing cooperation between providers in terms of information sharing and mitigation measures.
- **Switches and routers most affected by incidents:** Overall, switches and routers were the network components most affected by incidents.

Causes of incidents:

- **System failures are the dominant causes of incidents:** Most incidents were caused by causes in the root cause category system failures or technical failures (65 % of the incidents). This has been the dominant root cause all the reporting years so far. System failures was also the most common root cause for all the services when looking at them separately. In the category system failures, software bugs and hardware failures were the most common causes. The assets most often affected by system failures were switches and routers, and mobile switches. System failures followed by human errors, e.g. cable cuts and faulty software updates, were the most common root cause category for third party failures, which calls for improved cooperation between providers, construction workers and third party vendors of equipment and managed services.
- **Human errors affect many users:** Last year human errors was the root cause category involving most users affected, around 3 million user connections on average per incident.
- **Natural phenomena cause long lasting incidents:** Incidents caused by natural phenomena (mainly heavy snow/ice and heavy winds) had, like for all previous years and not surprisingly, most impact in terms of duration, on average over three days per incident.
- **Faulty software changes and updates have most impact:** Incidents caused by human errors and particularly faulty software changes and updates had most impact taking into account user connections affected and the duration of the incidents.

These patterns and trends need particular attention in the risk and vulnerability assessments carried out in the electronic communications sector.

Based on the annual summary reporting of 2011 and 2012 incidents, ENISA analysed in 2013 the dependencies in the electronic communications sector on power supply and issued recommendations regarding the sector's ability to withstand and act efficiently after power cuts. ENISA also studied in 2013 national roaming for increased resilience in mobile networks. Last year, based on the annual summary reporting of 2012 and 2013 incidents, ENISA has issued recommendations for providers about how to manage security requirements for vendors of ICT equipment and outsourced services used for core operations. Based on the 2012 and 2013 summary reporting ENISA has also studied national initiatives to reduce the number of underground cable breaks caused by mistakes.

In 2015 ENISA is assessing the impact of the Article 13a Incident Reporting Scheme in the EU. A study is also being carried out this year to analyse alternative indicators for measuring impact in electronic communications services. Thirdly, ENISA is providing a guideline on relevant threats to the continuity of telecom networks and services and the relevant network assets to secure.

ENISA, in the context of the Article 13a Expert Group, will continue discussing specific incidents in more detail with the NRAs, and if needed, discuss and agree on mitigating measures.

ENISA would like to take this opportunity to thank the NRAs, Ministries and the European Commission for a fruitful collaboration and we look forward to leveraging this kind of reporting to further improve the security and resilience of the electronic communications sector in the EU and more generally for supervision of security also in other critical sectors.

References

Related ENISA papers

- The Article 13a Expert Group technical guidelines on incident reporting, security measures, and threats and assets respectively: https://resilience.enisa.europa.eu/article-13
- ENISA's reports about the 2011 and 2012 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- ENISA's study 2013 on Power Supply Dependencies in the Electronic Communications Sector: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies
- ENISA's study 2013 on National Roaming for Resilience: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience
- ENISA's study and guide 2014 to Electronic Communications Providers when procuring ICT products and outsourced services for core operations: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors
- ENISA's study 2014 on information sharing systems for announcing civil works in order to protect underground communications infrastructure from cable cuts: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure
- ENISA's whitepaper from 2012 on cyber incident reporting in the EU shows Article 13a and how it compares to some other security articles mandating incident reporting and security measures: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
- For the interested reader, ENISA's 2009 paper on incident reporting shows an overview of the situation in the EU 6 years ago: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1

EU legislation

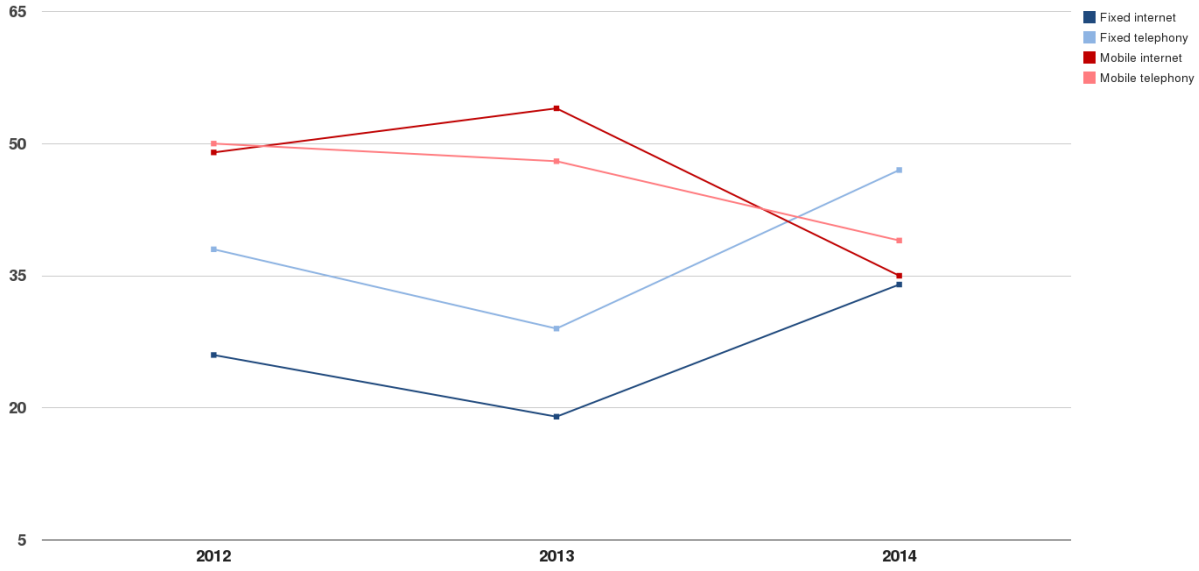
- Article 13a of the Framework directive of the EU regulatory framework for electronic communications: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140
- The EU regulatory framework for electronic communications (incorporating the Framework Directive including Article 13a): https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf
- In 2013 the European Commission issued a European Cyber Security Strategy and proposed a directive on Cyber Security. Article 14 of the proposed directive is similar to Article 13a, requiring operators to take appropriate security measures and to report significant incidents.

Annex

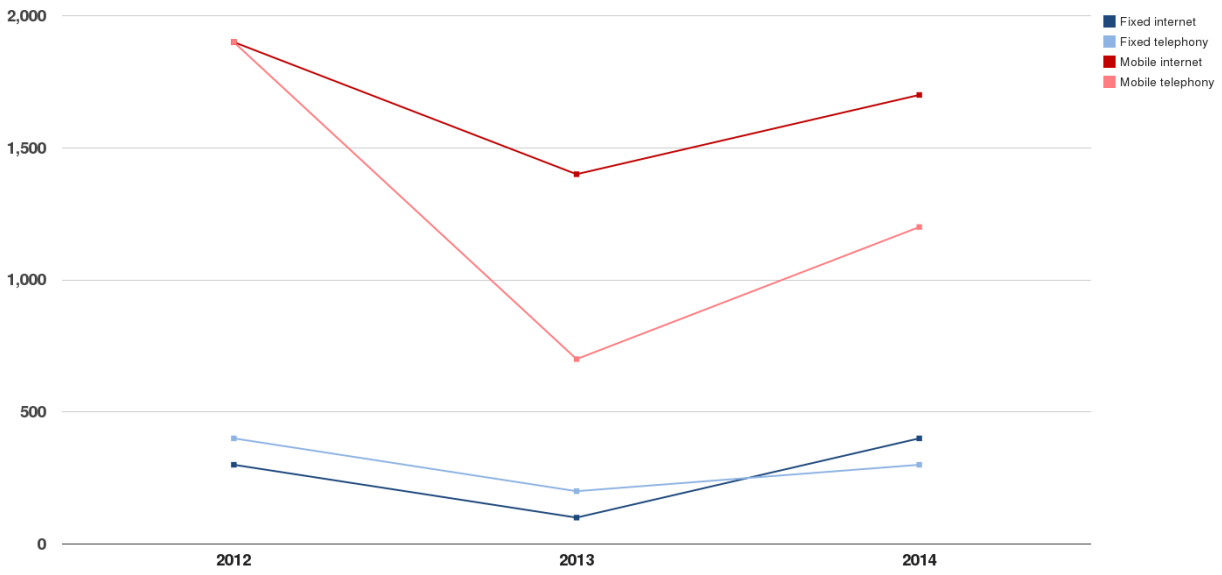
In this annex (A-D) we present graphs showing the situation between 2012 and 2014 based on the annual summary reporting by the NRAs to ENISA and the Commission. The graphs provide a brief comparison betweeen the years, but conclusion should be drawn with care, as the threshold for the incidents in scope has been lowered from year to year, and thus the number of reported incidents has increased over the years, and the list of causes and assets has been developed over the years.

Annex A: A Impact of incidents

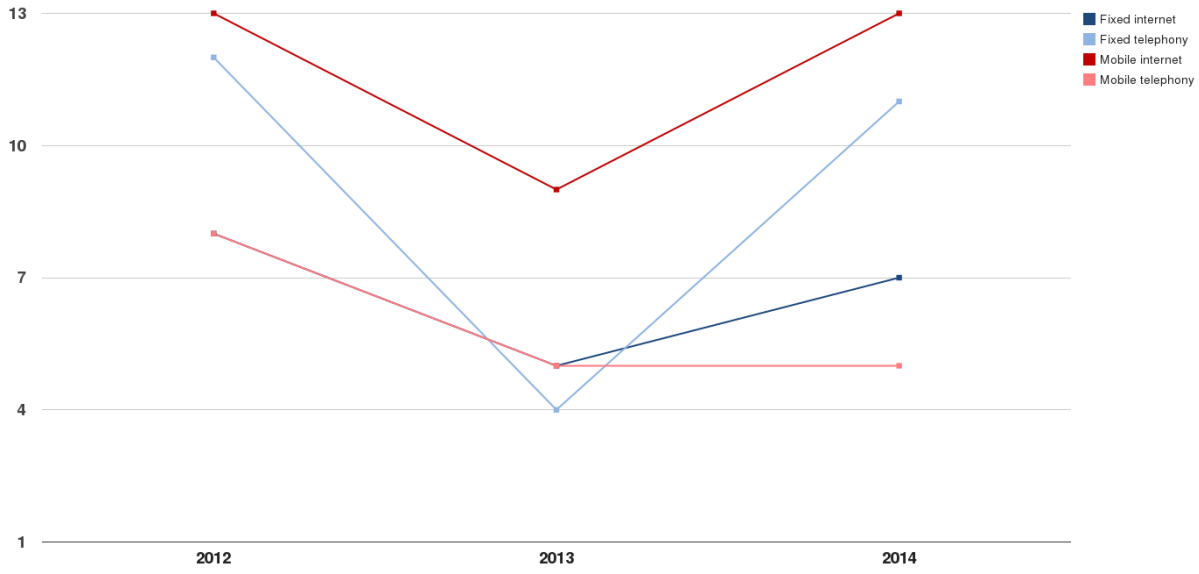
A.1 Impact per service



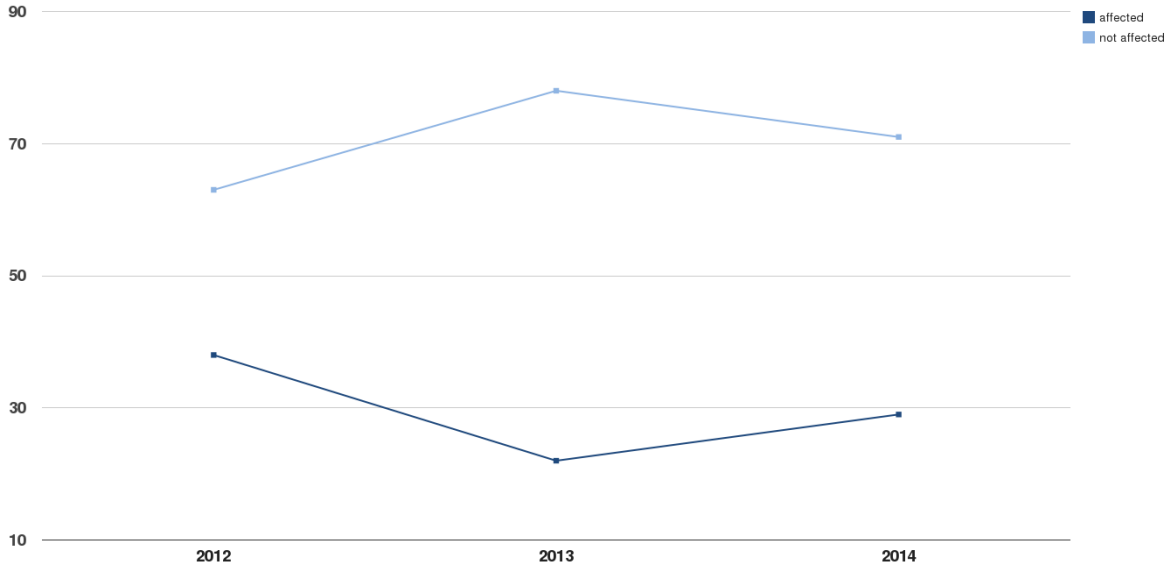
A.2 Number of user connections affected



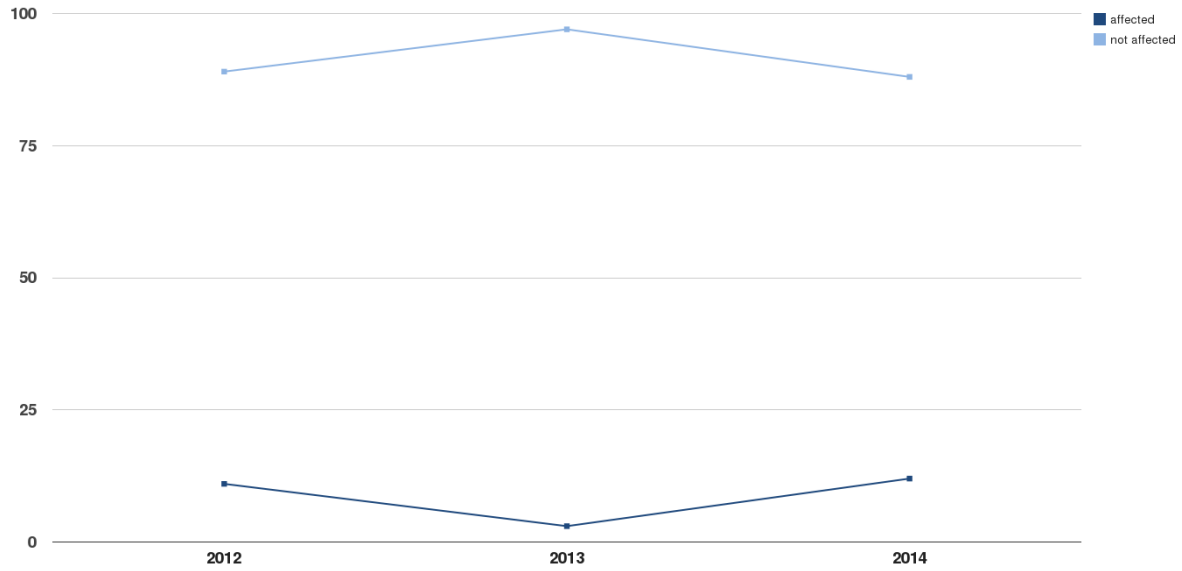
A.3 Percentage of the national user base affected



A.4 Impact on emergency services

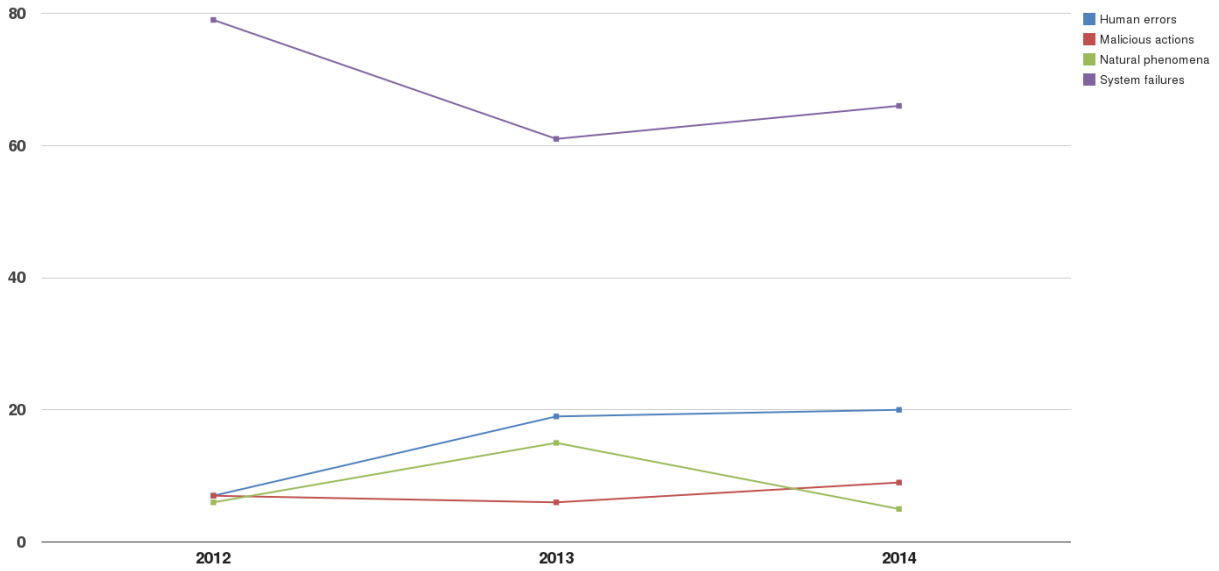

90
70
50
30
10
2012
2013
2014
affected
not affected

A.5 Impact on interconnections

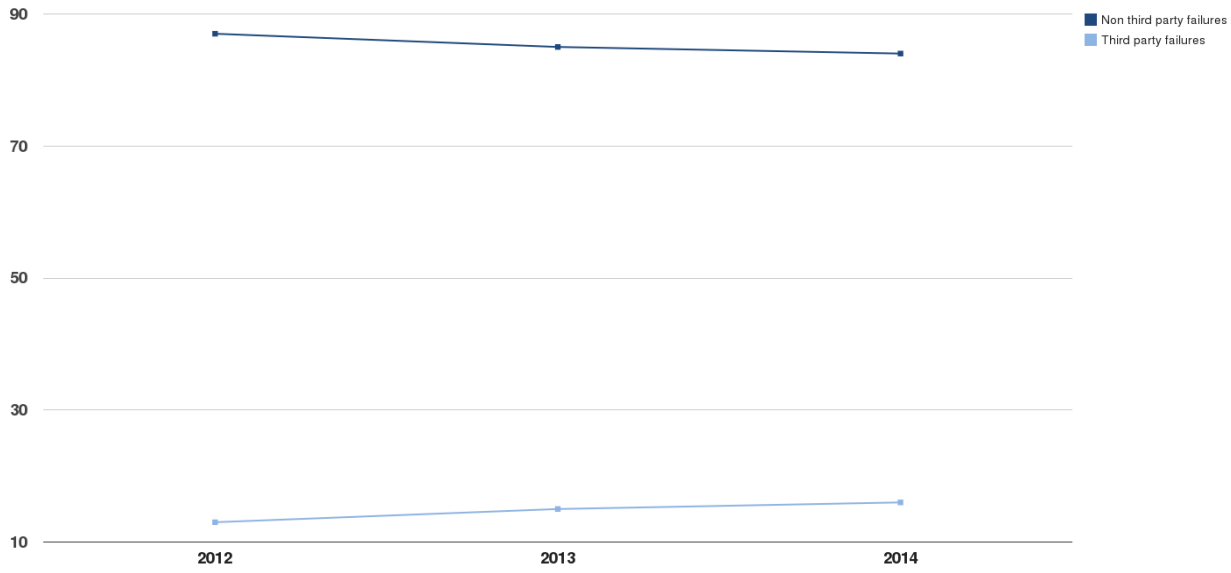


Annex B: Root cause categories

B.1 Incidents per root cause category

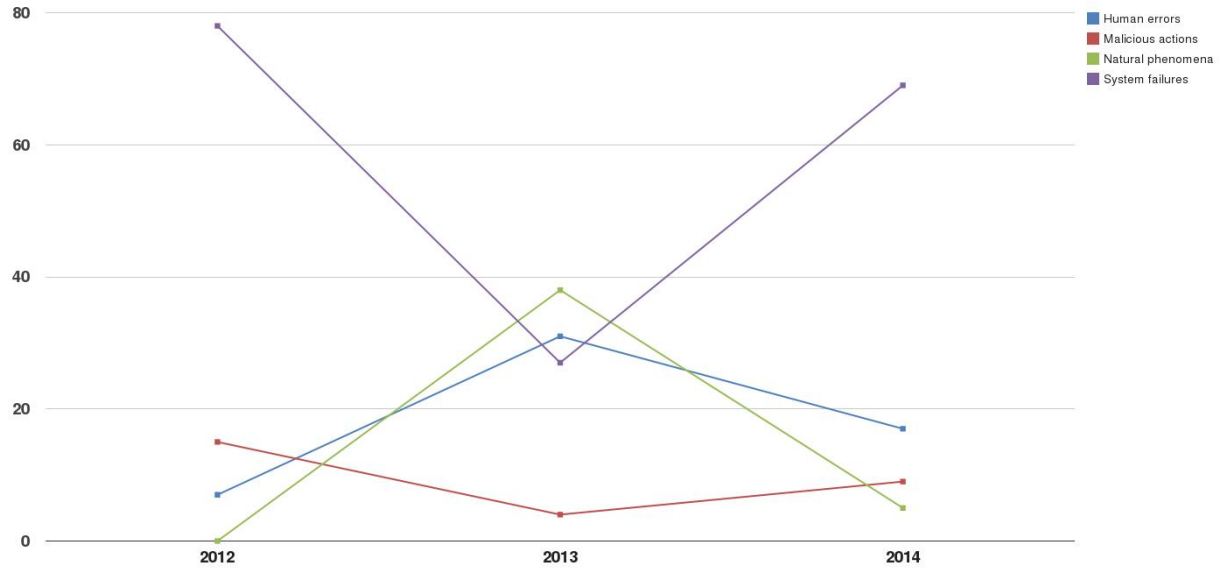


B.2 Third party failures

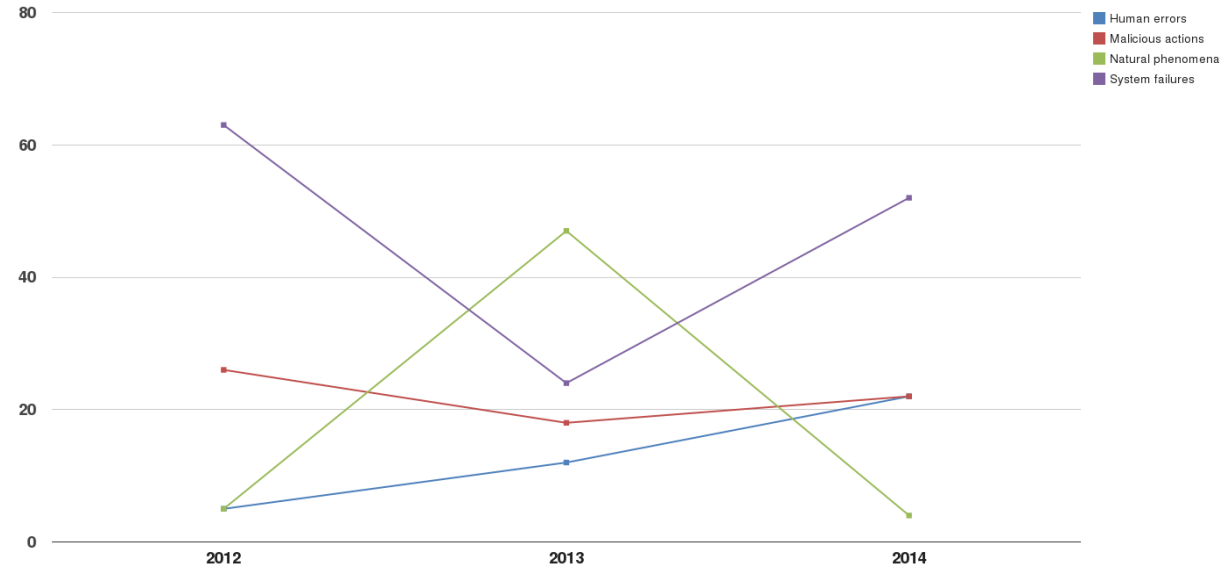


B.3 Root cause categories per service

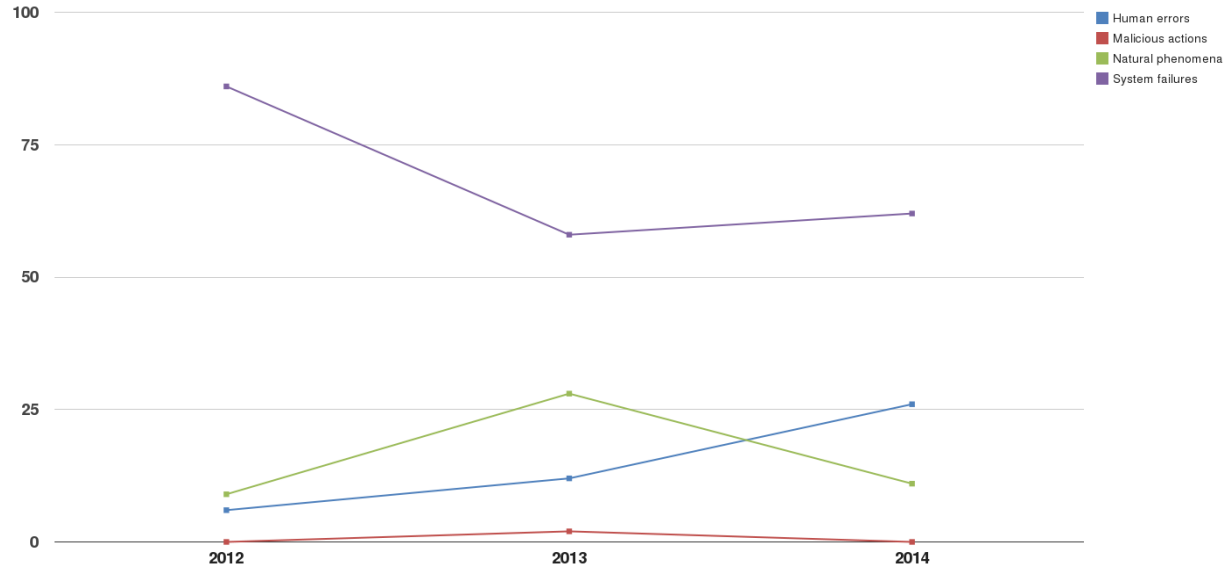
Fixed Telephony



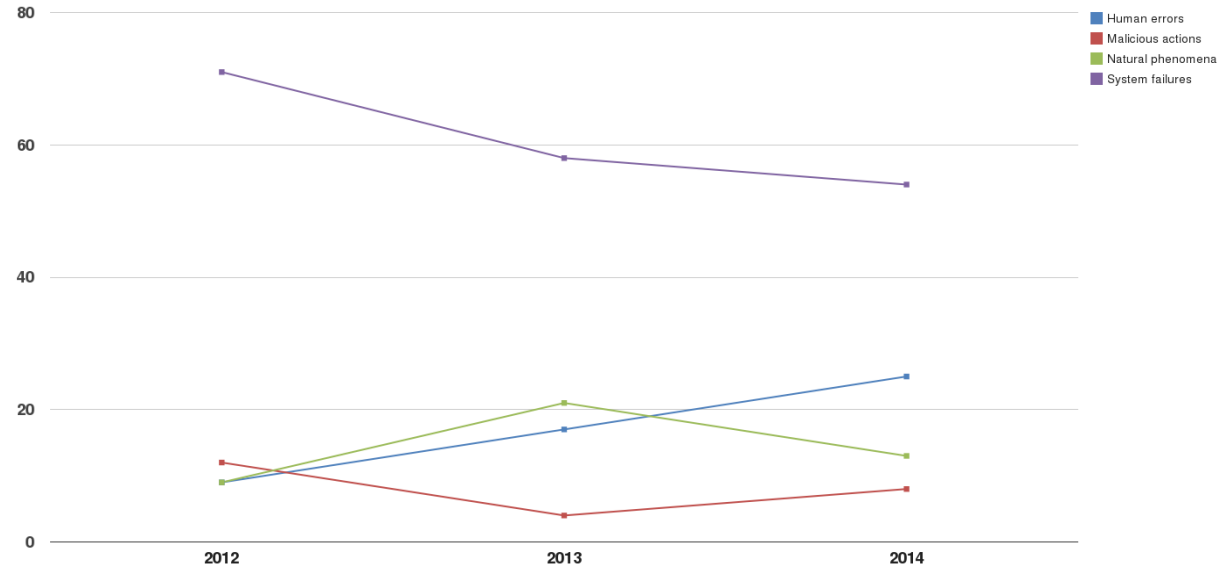
Fixed Internet



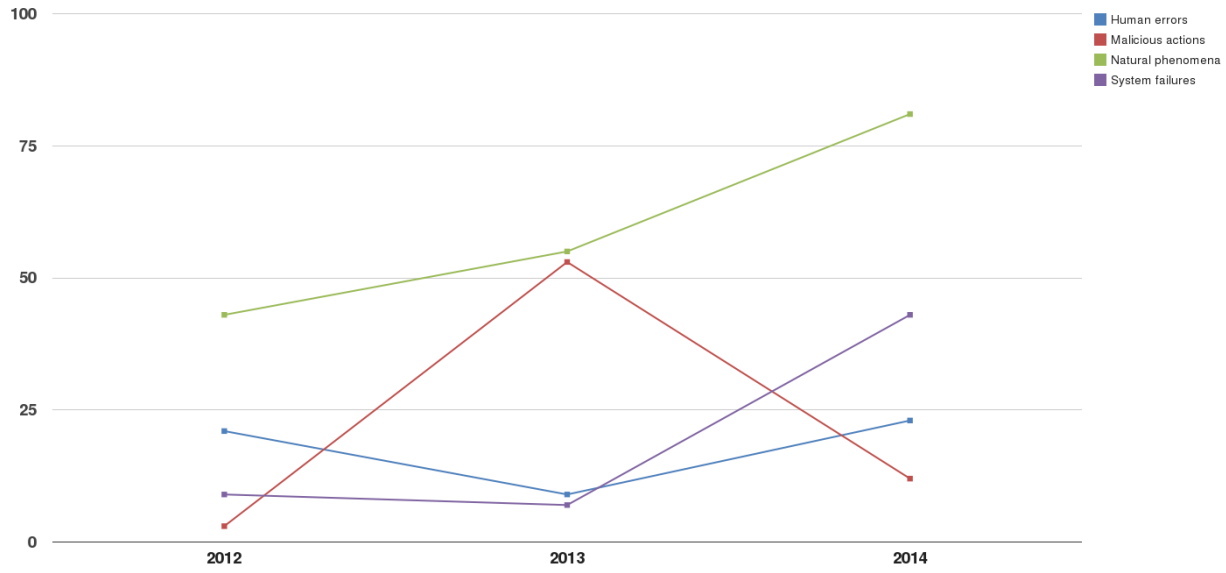
Mobile telephony



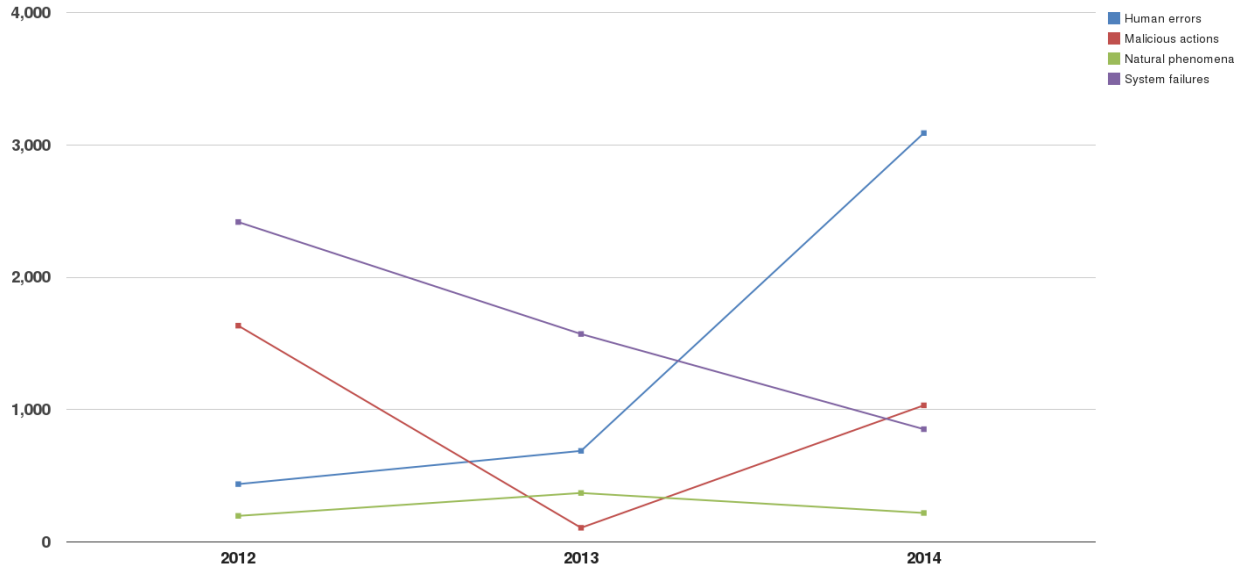
Mobile internet



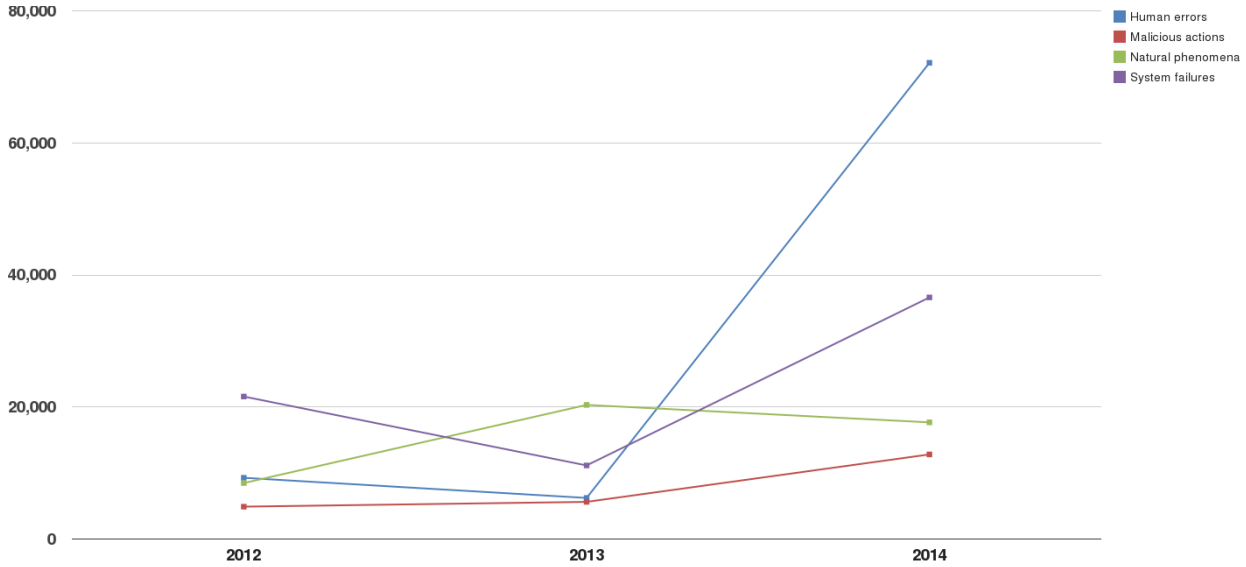
B.4 Average duration of incidents per route cause category



B.5 Average number of user connections affected per route cause category

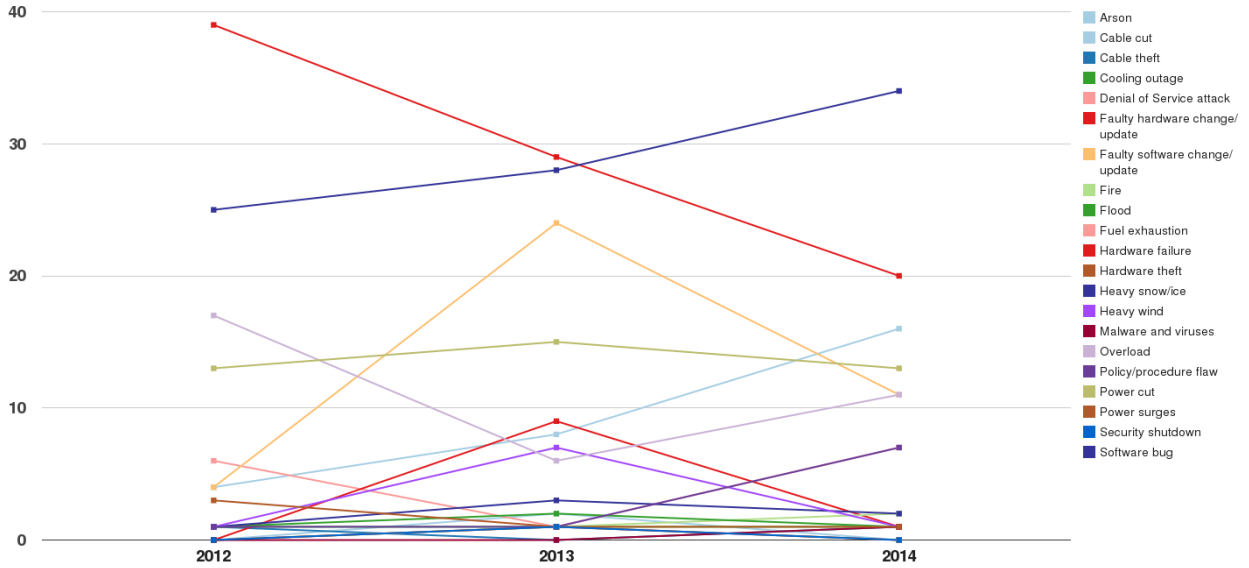


B.6 User hours lost per route cause category



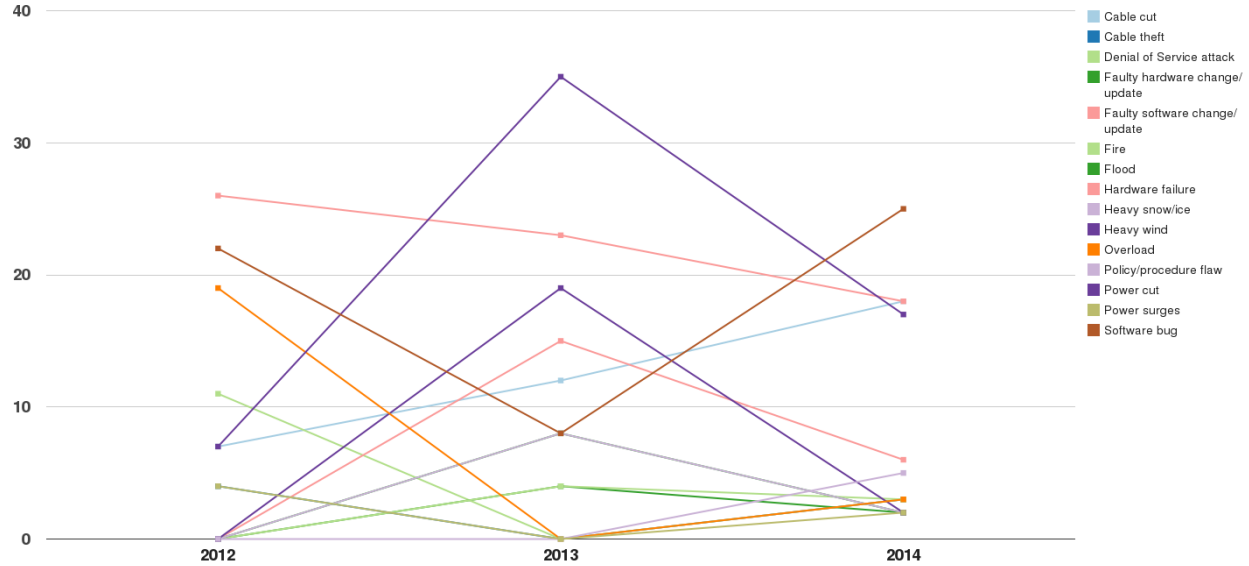
Annex C: Detailed causes

C.1 Detailed causes of all incidents

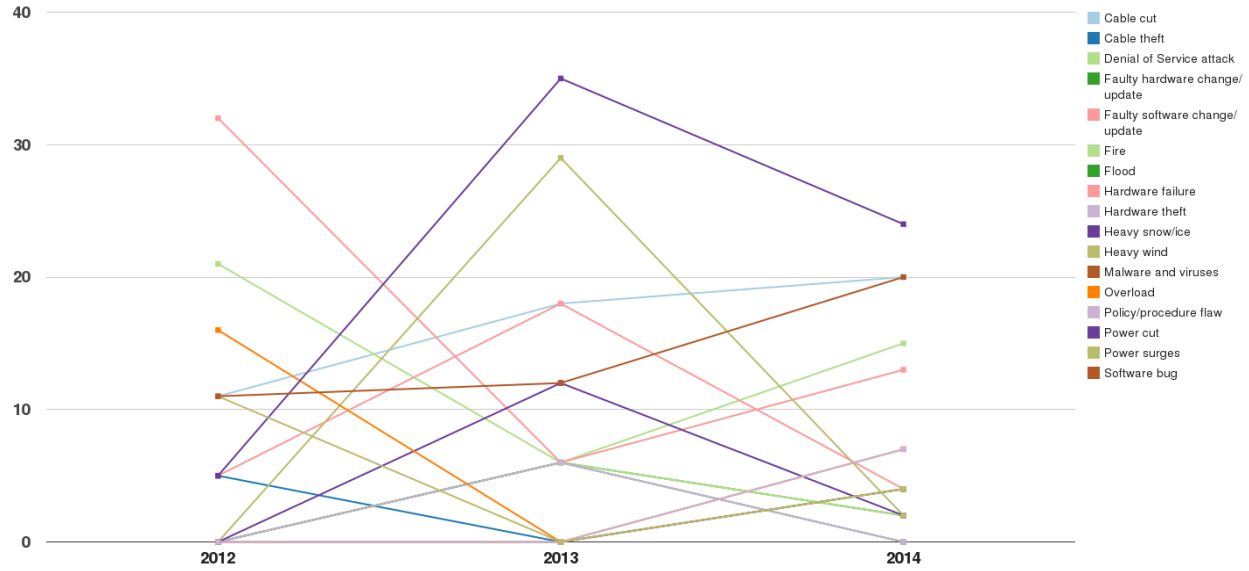


C.2 Detailed causes per service

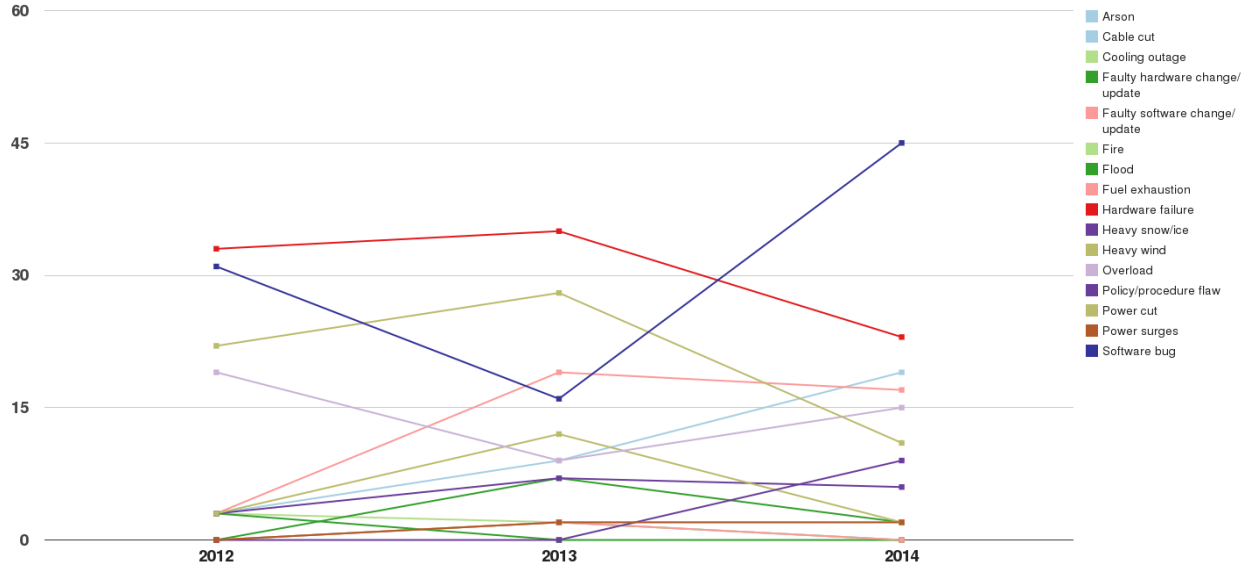
Fixed Telephony



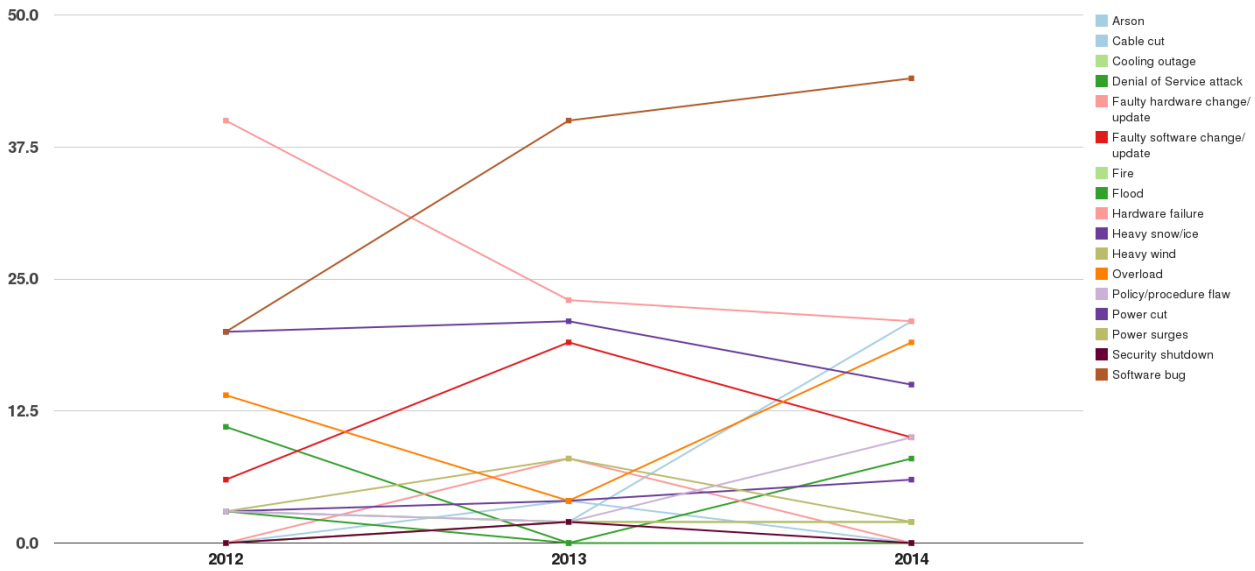
Fixed Internet



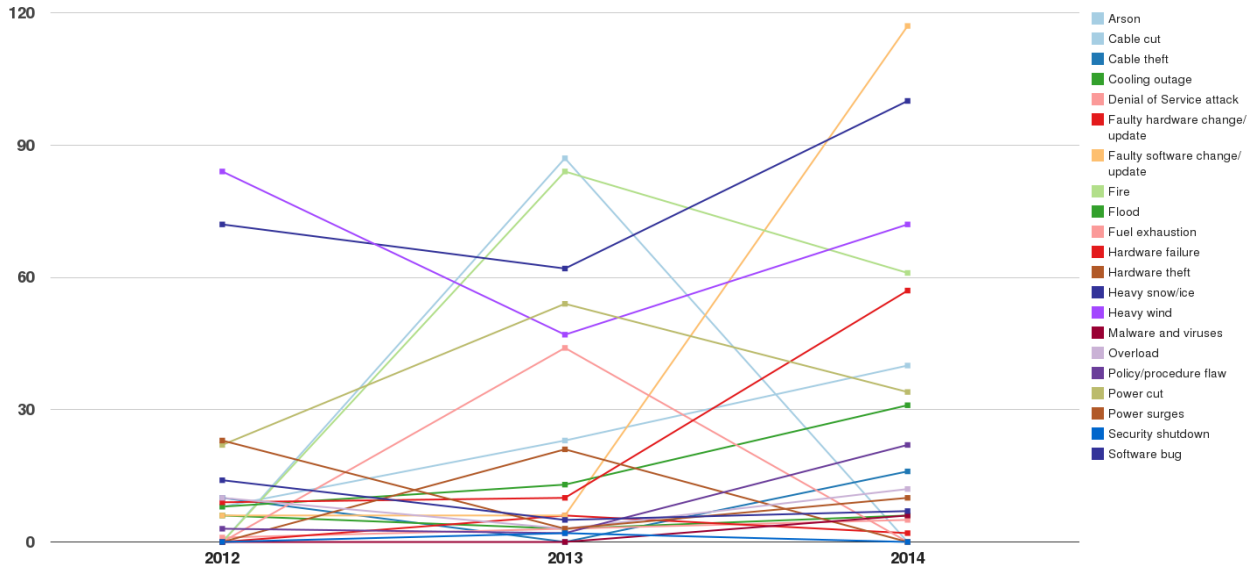
Mobile Telephony



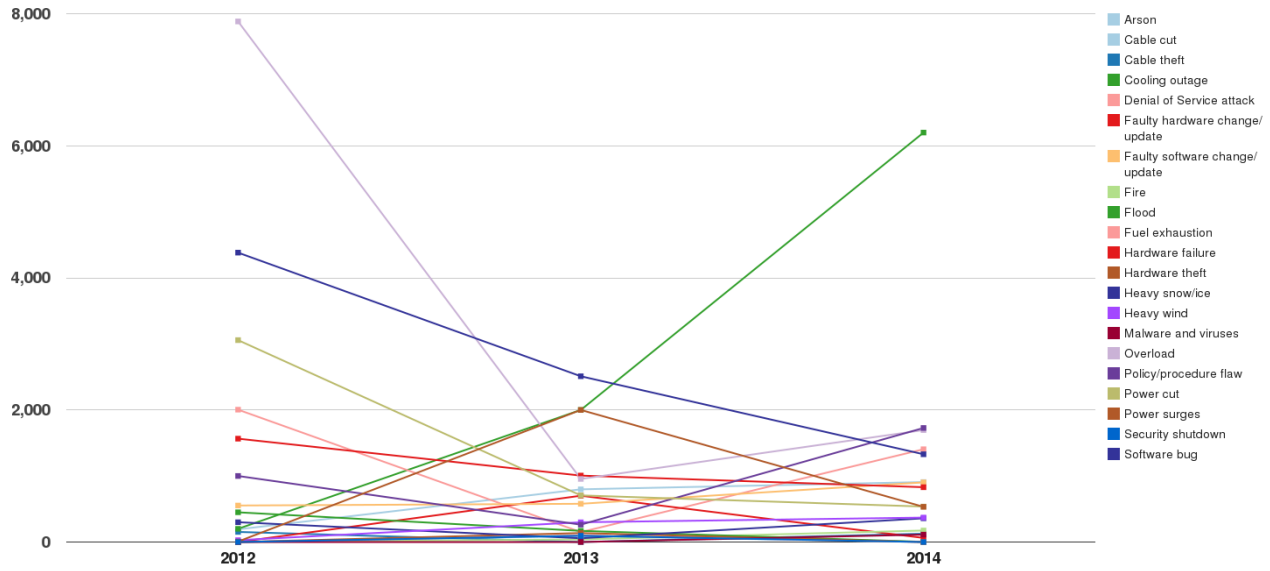
Mobile Internet



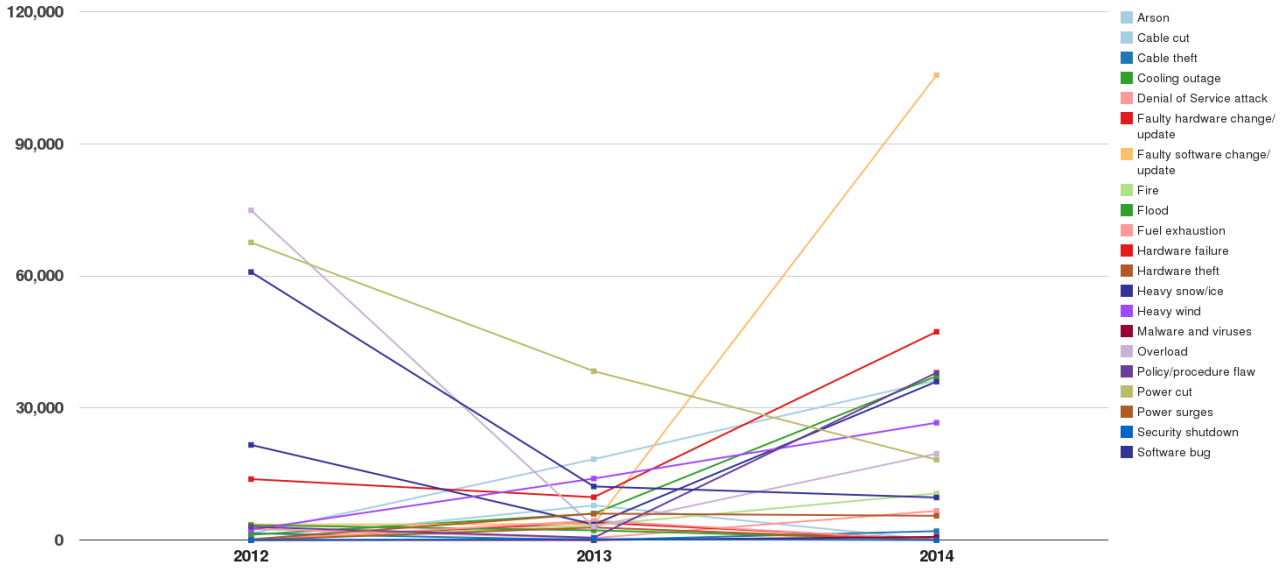
C.3 Average duration of incidents per detailed cause



C.4 Average number of user connections affected per detailed cause

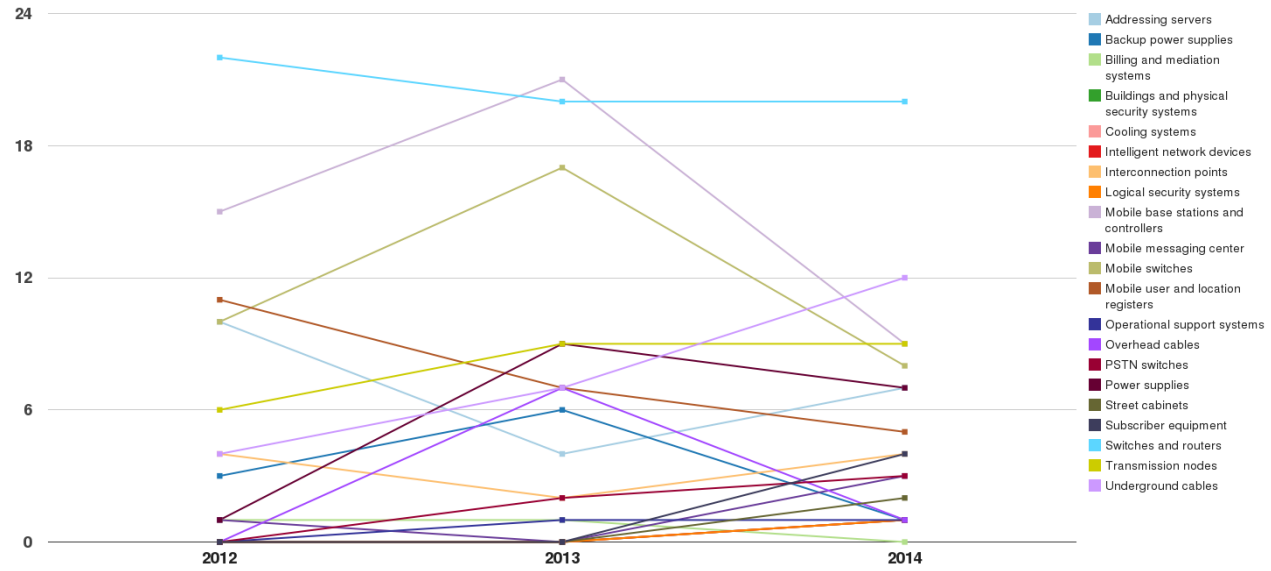


C.5 User hours lost per detailed cause

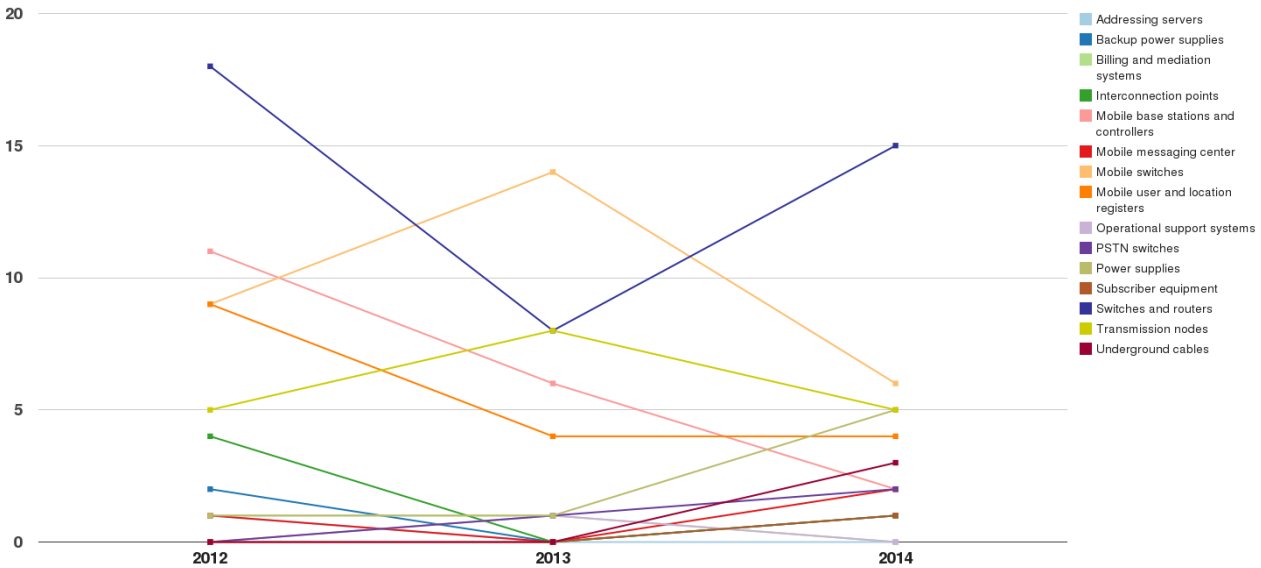


Annex D: Assets affected

D.1 Assets affected overall



D.2 Affected assets in system failures



ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number: TP-AD-15-001-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-126-7
DOI: 10.2824/24249