Annual Incident Reports 2015

Analysis of Article 13a annual incident reports in the telecom sector

SEPTEMBER 2016

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.

Contact

For contacting the authors please use resilience@enisa.europa.eu.
For media enquiries 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 Regulatory 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).

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-176-2, doi: 10.2824/10420

Table of Contents

Executive Summary

For the fifth 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 (EC) 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 2015 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:

- **138 major incidents reported:** This year 21 countries including two EFTA countries reported 138 significant incidents that occurred in 2015 while 9 countries reported they had no significant incidents.
- **Mobile internet most affected service:** In 2015 most incidents affected mobile internet (44% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 where fixed telephony was the most affected.
- **Impact on emergency calls**: In 15 % of the incidents there were problems in reaching the 112 emergency services, a small decrease since the previous year.
- **System failures are the dominant root cause of incidents:** Most incidents were caused by system failures or technical failures (70 % of the incidents) as a root cause. This has been the dominant root cause for all the reporting years so far. In the system failures category, software bugs and hardware failures were the most common causes affecting switches and routers, and mobile base stations.
- **Human errors affected on average more user connections per incident:** In 2015 human errors was the root cause category involving most users affected, around 2.6 million user connections on average per incident. The second place was taken by system failures with 2.4 million user connections on average per incident.
- **Malicious actions are not focused on causing disruptions:** the total number of incidents caused by malicious actions dropped to 2.5% from higher previous values (9.6% in 2014). This may indicate that the malicious actions are not necessarily aiming at causing unavailability of services, but might have other objectives.
- **Malicious actions started causing long lasting incidents:** Incidents caused by malicious actions (e.g. DDoS), although the volume was not high, had most impact in terms of duration, on average almost two days per incident.
- **New services affected:** TV broadcasting / Cable TV Networks (14%) and SMS/MMS (13%), public email (5%), IPTV (4,4%), VOIP services (3,7%) were the most affected services among the new ones that started being collected from this year.

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

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.

In late 2015 the EC started the process of revising the regulatory framework on electronic communications in order to "assess the current rules and to seek views on possible adaptations to the framework in light of market and technological developments, with the objective of contributing to the Digital Single Market Strategy"[1]. A public consultation concerning the evaluation and review of the current regulatory framework ended in December 2015. In this context, ENISA along with the Article 13a Expert Group submitted an opinion on the evaluation and review of Article 13a and 13b of the Framework Directive. One of the main observations made jointly by ENISA and the group is the lack of harmonisation and sometimes the overlapping between different EU provisions that impact the telecom sector. Harmonisation between the newly adopted NIS Directive and the upcoming Telecom Framework would be desirable. A draft of the new regulatory framework is expected until the end of the year.
ENISA, together with the EC 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] https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-regulatory-framework-electronic-communications

1. Introduction

This is the fifth iteration of the report “Annual Incident Reports”, which summarises significant outage incidents in the telecom sector reported to ENISA and the EC, under Article 13a of the Framework Directive (2009/140/EC), an Sometimes article introduced in the 2009 reform of the EU regulatory framework for electronic communications. This year ENISA and EC received 138 incident reports from NRAs, about severe outages in the EU’s electronic communication networks and/or services which occurred in 2015. This report provides an aggregate analysis of these 138 incidents. The main difference from last year is the inclusion of new services besides the four basic ones covered in the previous years (fixed telephony and internet, mobile telephony and internet).

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 EFTA countries, 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 2015 which were reported to ENISA and the EC 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 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, added Article 13a to the Framework Directive. Article 13a addresses the security and integrity[2] 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 EC about the incidents.

These incident reporting flows (incident notification and annual reporting) are shown in the diagram below. This document analyses the incidents from 2015 that have been reported to ENISA (the black dashed arrow).

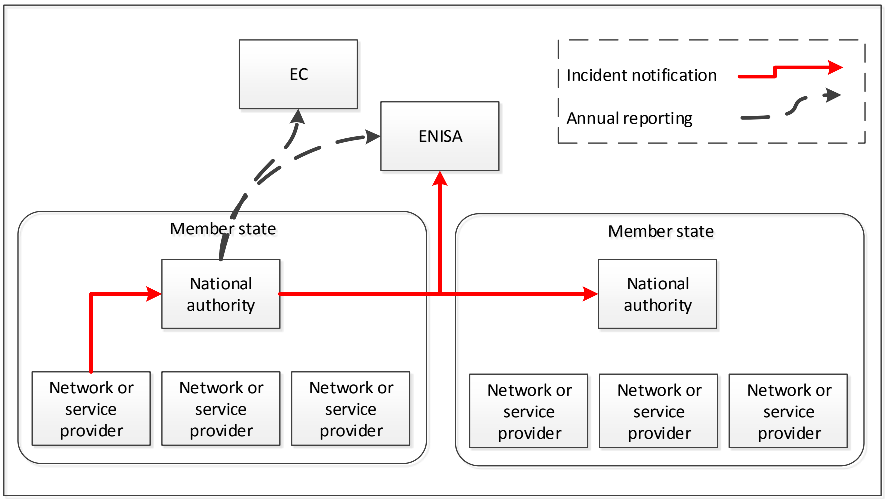

EC
ENISA
Incident notification
Annual reporting
Member state
National authority
Network or service provider
Network or service provider
Network or service provider
Member state
National authority
Network or service provider
Network or service provider
Network or service provider

Figure 1: Incident reporting in Article 13a.

Late 2015 the EC has started the process of revising the regulatory framework on electronic communications in order to “assess the current rules and to seek views on possible adaptations to the framework in light of market and technological developments, with the objective of contributing to the Digital Single Market Strategy”[3]. A public consultation concerning the evaluation and review of the current regulatory framework was ended in December 2015. In this context, ENISA along with the Article 13a Expert Group submitted an opinion on the evaluation and review of Article 13a and 13b of the Framework Directive, area which is at the core of ENISA expertise and competence. A draft of the new regulatory framework is expected until the end of the year.

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

[3] https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-regulatory-framework-electronic-communications

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[4]
- Technical Guideline on Security Measures[5]

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

- Technical Guideline on Threats and Assets[6].

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 EC 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

Although the focus of this report is still on the main 4 types of classic services, due to latest technological and legal advancements, we have decided to extend the number of services. As some of those services become more and more important in today's EU digital market, and some countries already cover them through their national level regulations, their inclusion in ENISA's annual report is a preparatory work in order to cover them in the future.

Nevertheless the inclusion is still in a test phase and concrete actions, whether to remove some of them or insert new ones, will be taken at a later stage. Besides the 4 classic services, others were added as follows:

[4] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

[5] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures

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

CLASSIC SERVICES	NEW SERVICES	NEW INTERNET RELATED SERVICES
Fixed telephony	SMS	IXPs - Internet Exchange Points
Mobile telephony	MMS	ccTLDs - Country Code Top Level Domains
Fixed Internet access	Satellite communication services	IPTV
Mobile Internet access	International roaming	Video on demand
	Voice mail	Public WIFI hotspots
	RADIO broadcasting	Web based voice services
	TV broadcasting	Web-messaging services
	Cable television networks (Cable TV)	Voice over Internet Protocol (VoIP) services
		Public email services

Table 1. Services in scope

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. As explained, not all incidents types are reportable under Art. 13a provisions. Depending on the national implementation of Art. 13a, if one incident does not affect the continuity of the service (availability), although confidentiality or integrity might be affected, the incident needs no reporting.

3.1.3 National user base

NRAs should provide estimates of the total number of users of each service in their country. The national user base is used for determining the significance of incidents, in cases where the threshold is relative to the national user base.

- 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[7]:
    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.
- For other types of services that are still in a test phase no national user base was collected at this point.

3.1.4 Thresholds

NOTE*: Art. 13a provisions state that Member States (MS) shall ensure that electronic communication providers will “notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services”. However, the thresholds for defining significant incidents were not established through the Directive and the EC has not issued any implementing measures in this sense leaving the matter open for discussions and unrestricted for national implementation. At this point the activities of ENISA and Art. 13a expert group have proved to be very useful by defining a set of* ***informal and non-binding EU thresholds*** *to help Member States in reporting or setting up their own national level thresholds. In this respect a set of EU thresholds were adopted by the Art. 13a expert group that are known and accepted by every country, but it has remained at the discretion of each Member State to adopt its own national thresholds. All incidents reported within*

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

the annual report to ENISA and EC, and presented within this report, are based on the thresholds established at national levels, which can be above or below (in most of the cases they are below) the EU thresholds. For an analysis of incidents based on the informal EU level thresholds pls. see Section 4.5.

The EU thresholds for the annual summary reporting are 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 %.

	1h<...<2h	2h<...<4h		4h<...<6h		6h<...<8h		>8h
1%<...< 2% of user base	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥
2%<...< 5% of user base	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥
5%<...< 10% of user base	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥
10%<...< 15% of user base	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥
> 15% of user base	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

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

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.

Since 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 was 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 EC.

In case of the newly added services no thresholds were established. Member states could report incidents that they consider significant.

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[8]. 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.

3.1.8 Impact evaluation on the implementation of Article 13a incident reporting scheme

As several years have passed since the publication and implementation of the Framework Directive including Art. 13a, an impact evaluation of the new article was carried out. This was done by ENISA along with the Article 13a Expert Group in 2015. The evaluation had the purpose of assessing the changes in outcome that can directly be attributed to the provision of Art. 13a, the effects caused by this particular set of obligations within the Telecom Package. The evaluation focused on 5 key areas, where we tried to identify possible outcomes:

- The new security measures implemented in the member states ;
- The transparency resulting from the incident reporting process;
- The learning process resulting from incidents;
- The level of collaboration between the stakeholders ;
- The harmonization of the procedures within the European Union.

The evaluation done within this project has brought to light some important outcomes that have definitely contributed to increasing the resilience and security of the telecommunications infrastructures in Europe. In a European Union which was highly diversified in terms of security measures, Art. 13a brought a certain amount of uniformity in the approach taken regarding security of telecommunication services, but more importantly contributed to strengthening the European telecom infrastructure’s resilience and services availability across the EU. The role of ENISA, especially in the coordination of Art. 13a expert group, was most beneficial as it helped considerably in bringing more harmonization within the implementation process and collaboration among stakeholders (NRAs and providers). The report has served as an input to the EU Commission in the telecom framework evaluation process. The full report along with findings and conclusions can be found here.

[8] 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 2 EFTA country participated in this process. Of these, 19 Member States and 2 EFTA countries reported in total 138 significant incidents and 9 countries reported there were no significant incidents. A slight decrease from previous year where we had 25 countries reporting significant incidents.

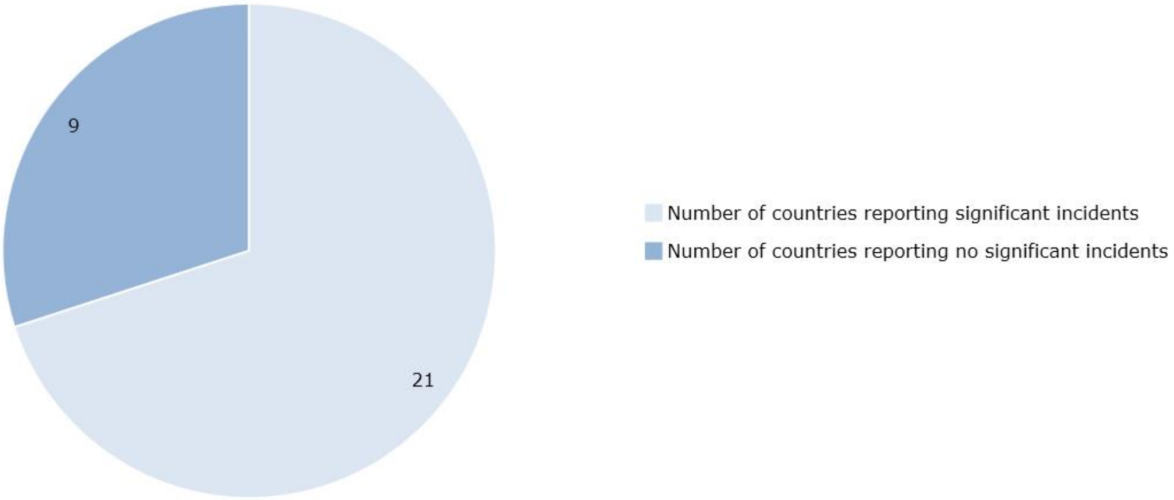


Figure 3: Countries involved in the annual summary reporting in 2015.

In this section, the 138 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 2015. 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 and in some cases the thresholds that define the significance of incidents are modified. This may cause the number of reported incidents to fluctuate. Until now the thresholds have only been lowered, causing in some years an increase in the number of incidents. 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***.

5. All incidents reported within the annual report to ENISA and EC, and presented within this report, are based on the thresholds established at national levels, which can be above or below (in most of the cases they are below) the EU thresholds. For an analysis of incidents based on the informal EU level thresholds pls. see Section 4.5.

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 2015 most of the reported incidents affected mobile internet. This is return to the previous trend where mobile was the most affected service. In 2014 the most affected service was fixed telephony (see Annex A.1).

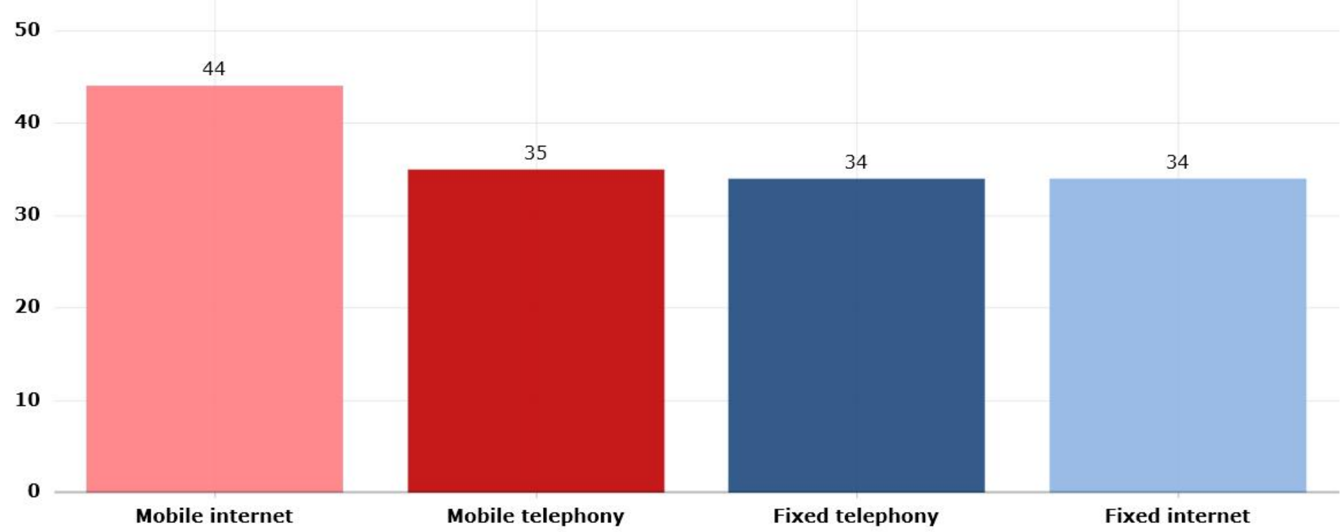


Figure 4: Incidents per classic services (percentage)

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 faulty hardware change/update caused fixed internet and mobile internet to fail for millions of users (duration: hours, connections: millions, cause: human error): *A misconfigured router hardware replacement performed incorrectly affecting mobile data capacity approximately 60-70%. Although both fixed internet and mobile internet user connections were affected, mobile internet user connections affected were four times more. Incident was resolved by configuring the new equipment correctly, however it took a few hours to recover connectivity.*

FIGURES ABOUT THE NEW SERVICES ADDED:
The most affected services among the new ones added this year's report are TV broadcasting / Cable TV Networks (13,7%) and SMS/MMS (13%).
Most affected internet related services were public email (5,8%), IPTV (5,1%), VOIP services (4,3%).

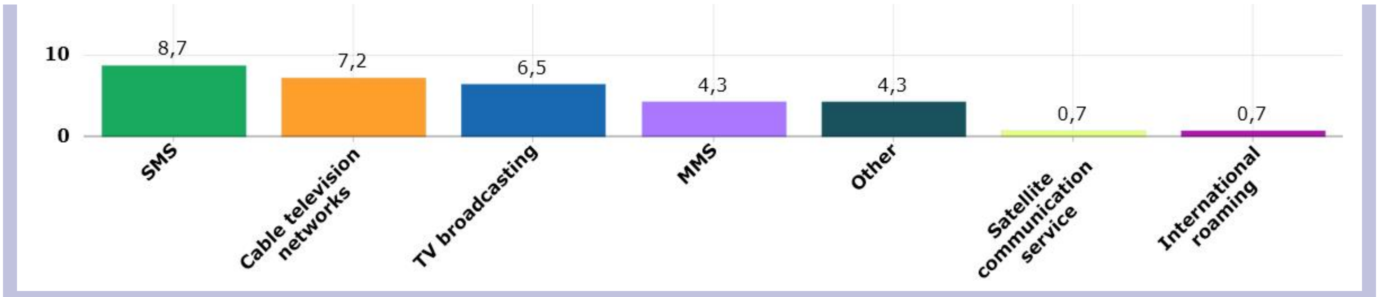


Figure 5: Incidents per other service (percentage)

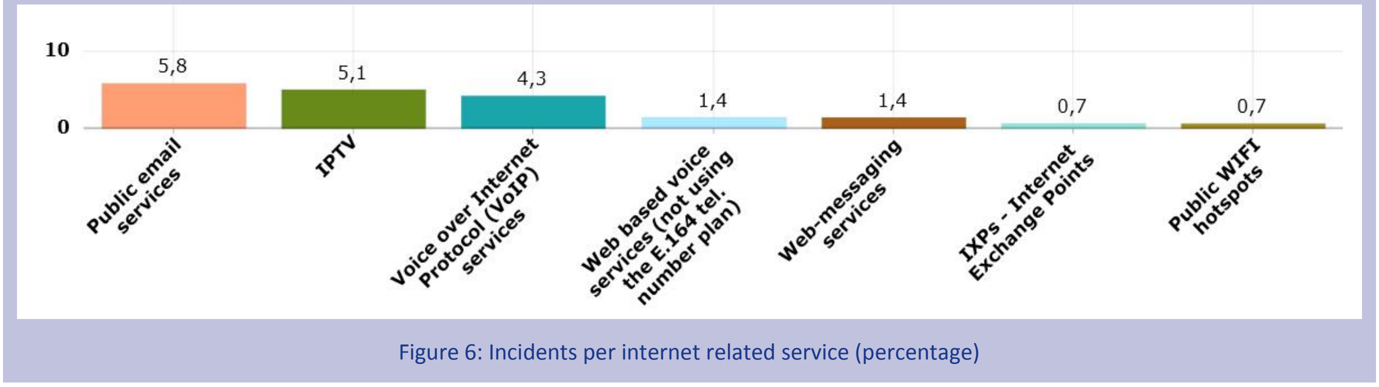


Figure 6: Incidents per internet related service (percentage)

4.1.2 Number of user connections affected

Mobile Internet outages affected most user connections compared to the other services, with an average of 1.3 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.

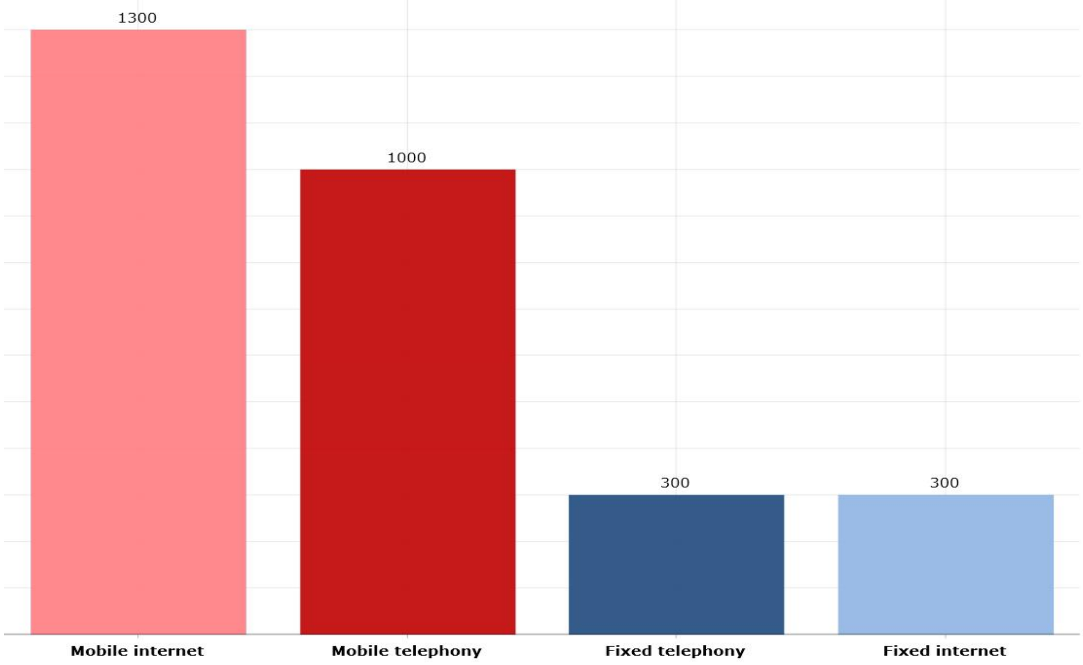


Figure 7: Average number of user connections affected per incident per classic service (1000s).

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 evolution of the number of affected connections can be seen in Annex A.2.

FIGURES ABOUT THE NEW SERVICES ADDED:
The number of connections affected for SMS/MMS (1.3 million) services is in the same range as mobile telephony/mobile internet underlining the interconnection between the two.
As expected, Internet Exchange Points (IXPs) related incidents are causing a lot of damages, with an average of 6 millions affected connections.
Public email services related incidents affected in general 1 million users.

4.1.3 Percentage of the national user base affected

Mobile Internet outages impacted on average 18% of the national user base for mobile Internet user connections, which is a slight increase compared to the previous years, see annex A.3. All five 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.

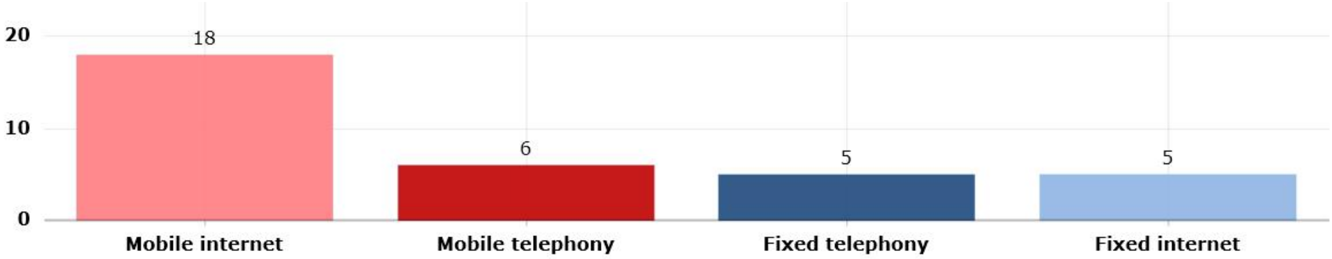


Figure 10: Percentage of national user base affected on average per incident per service.

A faulty hardware change/update caused mobile internet to fail for more than an hour impacting a significant number of user connections (duration: hours, connections: millions, cause: system failure): *Initialy the outage of two network core elements during maintenance work caused an outage of GPRS,HSDPA,and LTE. The incident was resolved by rebooting the two network core elements.*

4.1.4 Impact on emergency services

In more than 20% 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 percentage has a slight decrease, see Annex A.4.

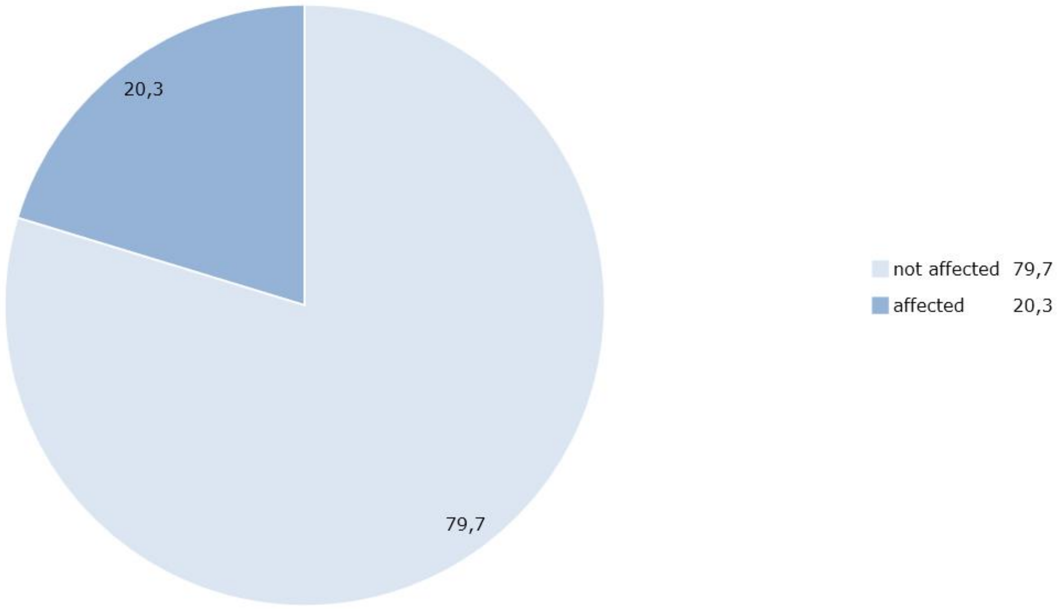


Figure 11: Impact on emergency calls.

4.1.5 Impact on interconnections

In 4,3 % of incidents reported there was an impact on interconnections between providers. Compared to previous year also this figure has a decrease, see Annex A.5.

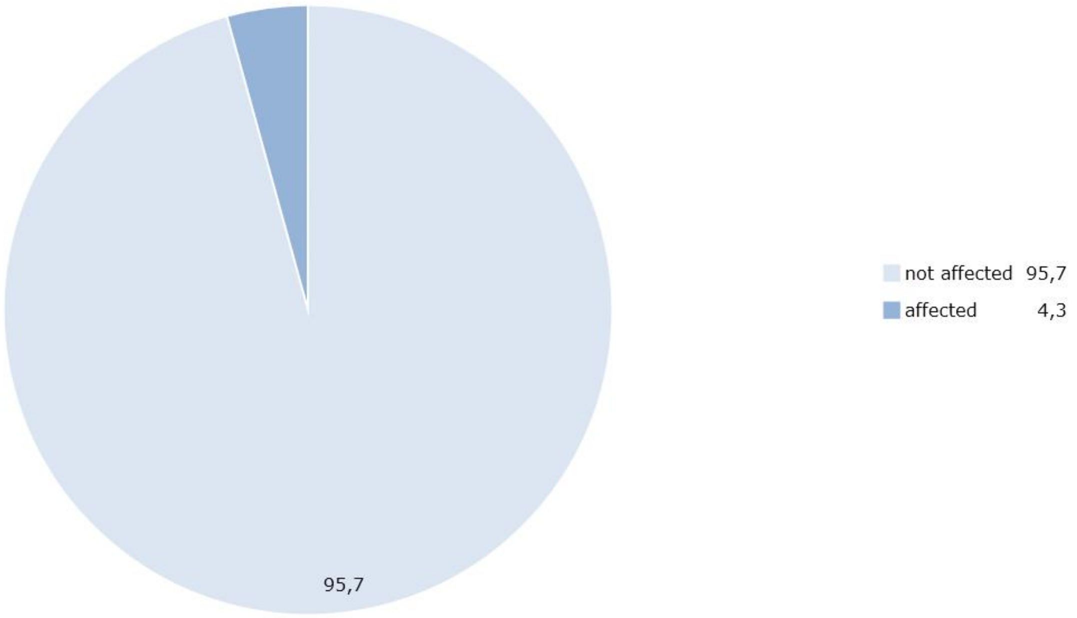


Figure 12: Impact on interconnections (percentage)

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 2015 almost 69% of the reported 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, 20.7% of the incidents were caused by human errors, also this was consistent with previous years. In case of malicious actions the recorded percentage was way smaller than previous year (9.5% in 2014, 5.3 % in 2013).

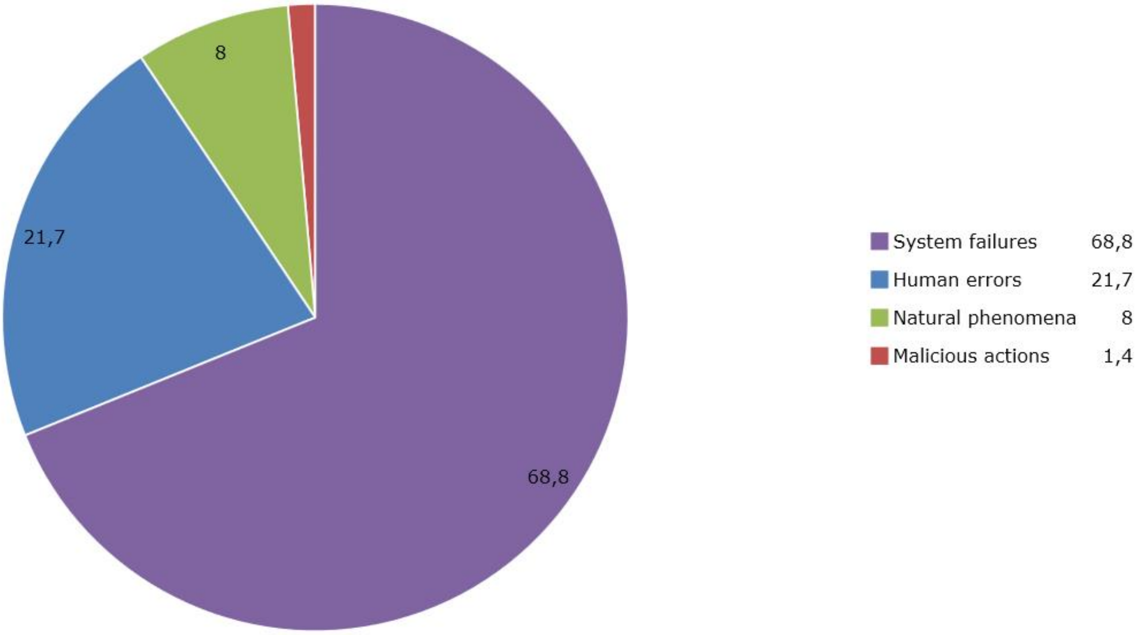


Figure 13: Incidents per root cause category (percentage).

System failure caused disruption in telecommunication services to one of the major providers in a country affecting millions of users (duration: hours, connections: millions, cause: system failures): *Routing problems in the network core were caused by a technical problem with one of the network cards, which sendt wrong signal packets and broadcast on the network with the other routers, and resulted in a total lack of access to services Mobile Data (2G, 3G, LTE), CDMA, APN Corpo. In order to respond to the incident, the provider invoked the emergency and crisis management procedure, as part of the analysis undertaken was diagnosed with the problem of routing in the network core. The problems were eliminated by gradually switching routers over to parts of the network that is working correctly.*

4.2.2 Third party failures

About 15.2 % of the incidents reported were categorized as third party failures, a slight decrease compared to the previous year (16.4%), see Annex B.2.

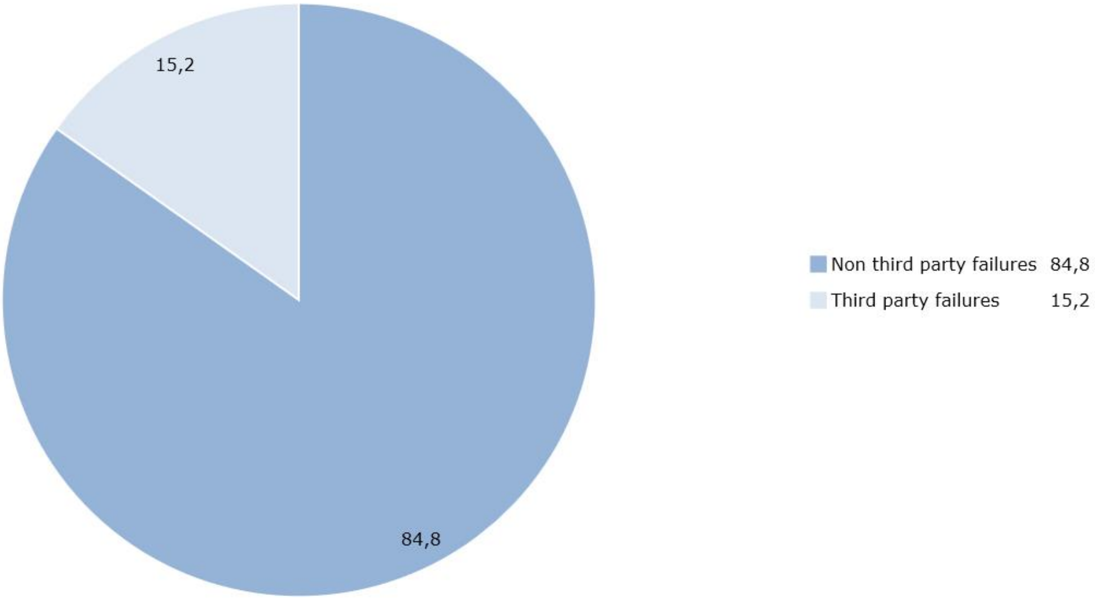


Figure 14: Third party failures and non-third party failures of all incidents (percentages).

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

In 2015 third party failures basically had a similar distribution of root causes as the reported incidents in general, with system failures as the most common type of third party failure. Errors caused by natural phenomena, however, were more frequent in third party failures than in the reported incidents in general.

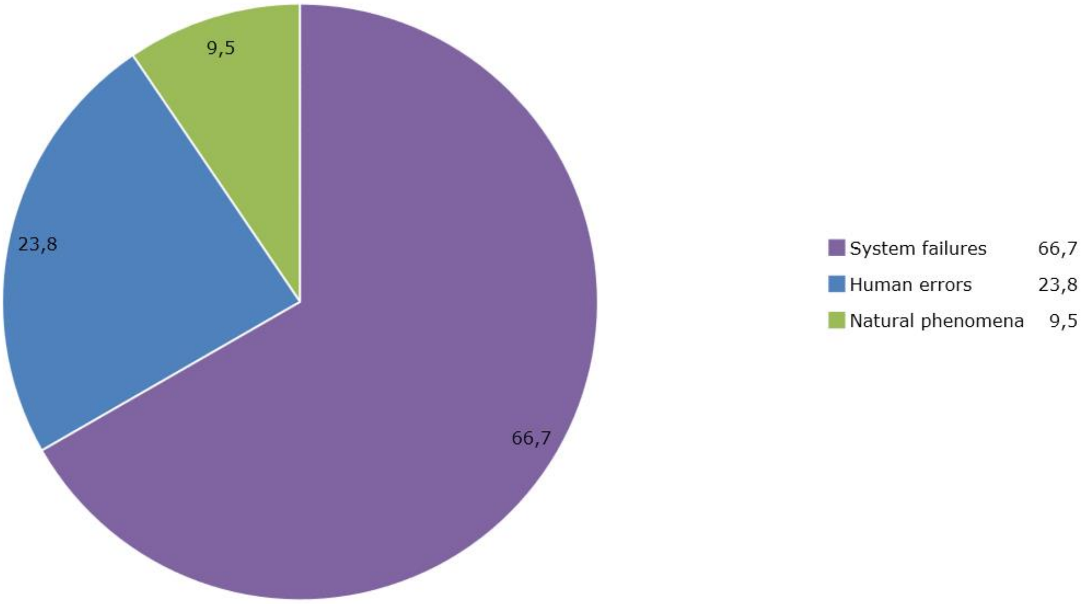


Figure 15: Third party root causes (percentage).

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 2015, system failures was the dominant root cause for all services respectively, counting in all cases for more than half of the incidents reported. For mobile telephony and mobile internet, this was the case also in the previous years, whereas the dominant root cause for fixed telephony and fixed internet oscillated in the previous years between natural phenomena and system failures, see Annex B.3.

System failure caused unavailability of telecommunication services to approximately a million users for more than ten hours (duration: hours, connections: thousands, cause: system failures): A change over switch subsequently caused a power cut leading to a hardware failure of the Dense Wavelength Division Multiplexing Equipment.

4.2.3.1 Fixed Telephony

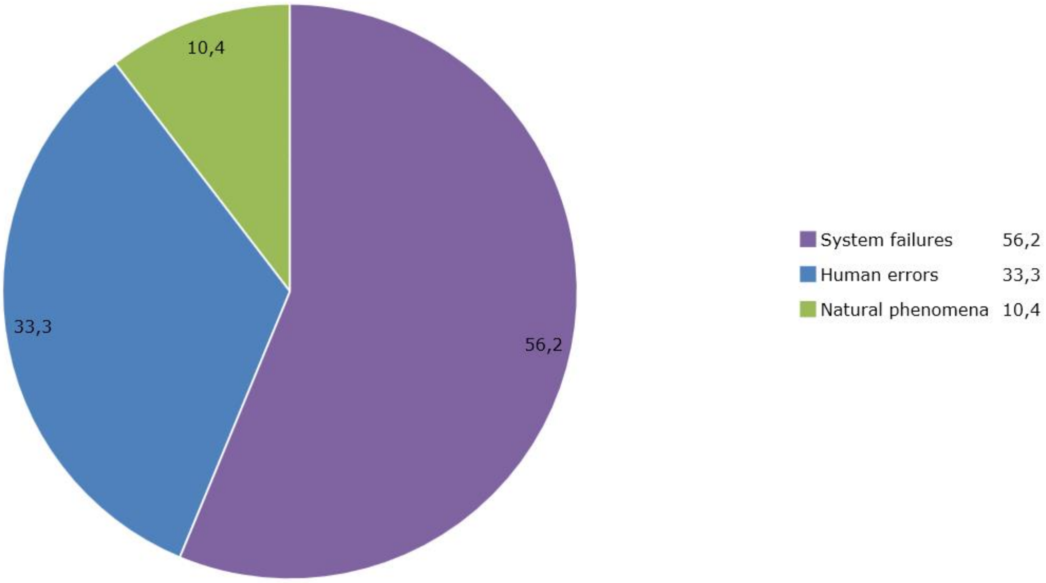


Figure 16: Root cause categories for fixed telephony (percentage).

4.2.3.2 Fixed Internet

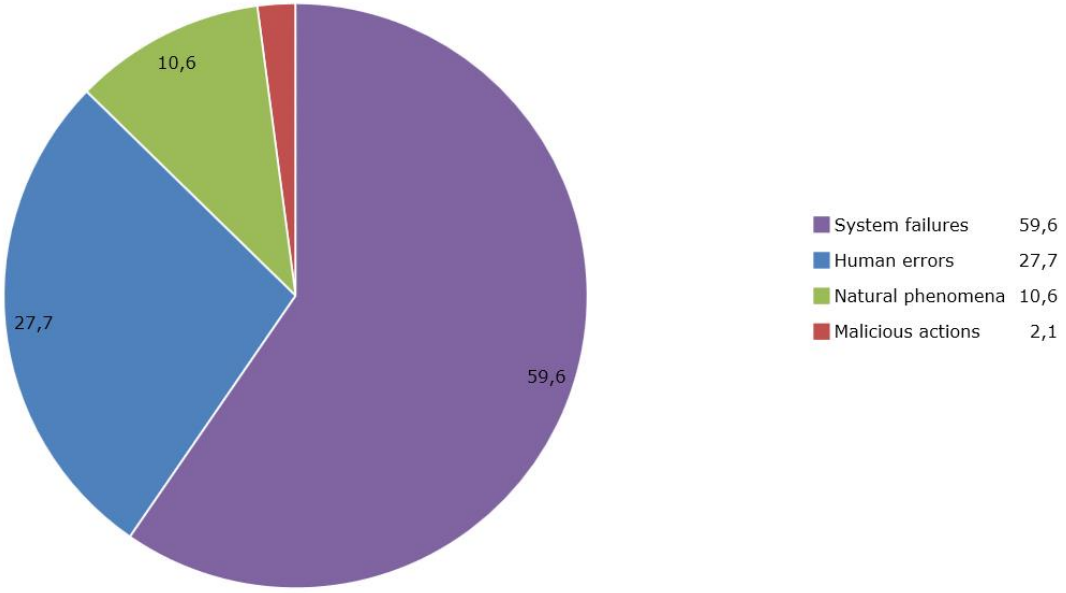


Figure 17: Root cause categories for fixed Internet (percentage).

4.2.3.3 Mobile telephony

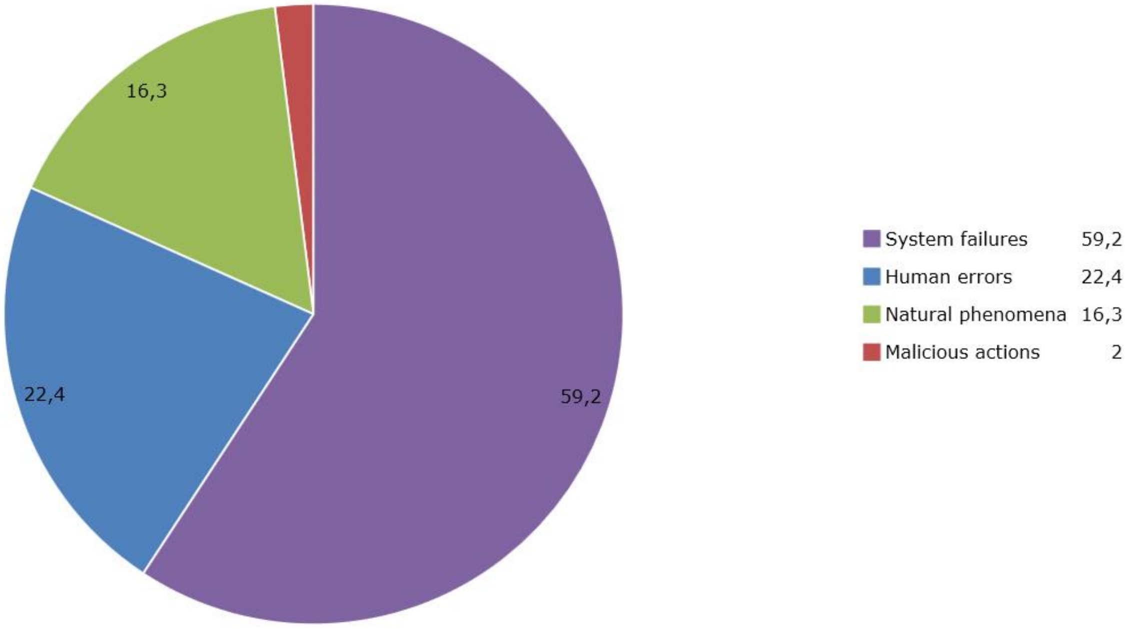


Figure 18: Root cause categories for mobile telephony (percentage).

4.2.3.4 Mobile internet

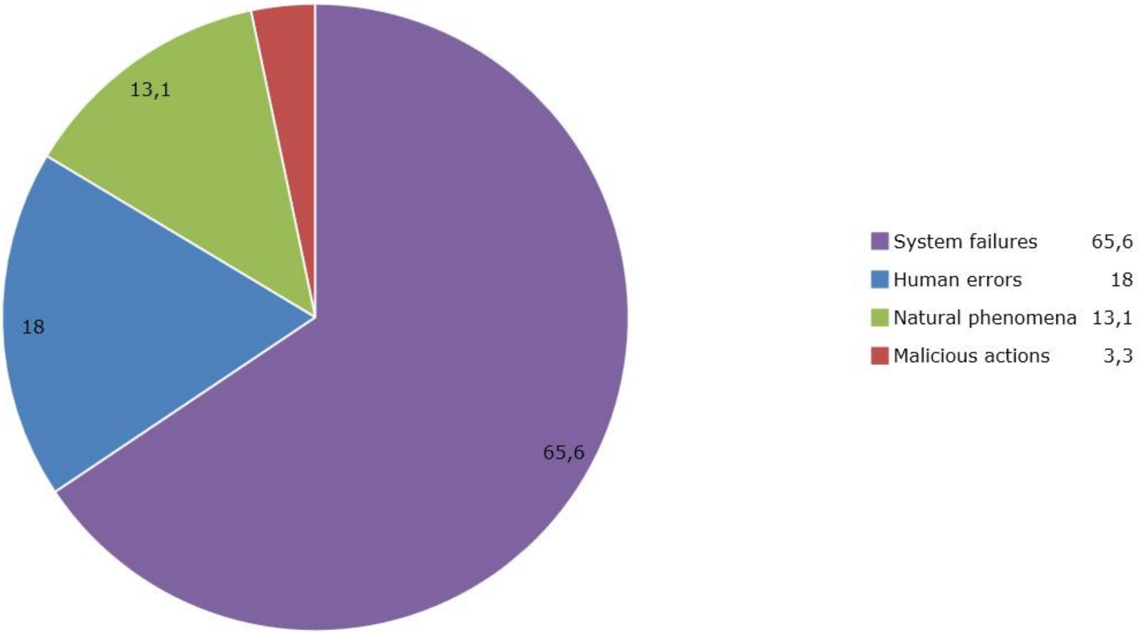


Figure 19: Root cause categories for mobile Internet (percentage).

4.2.3.5 Newly added services

System failures is also the main root cause for all new services, with a percentage of 75,6% (other services) to 85,2% (internet related services) depending on the service.

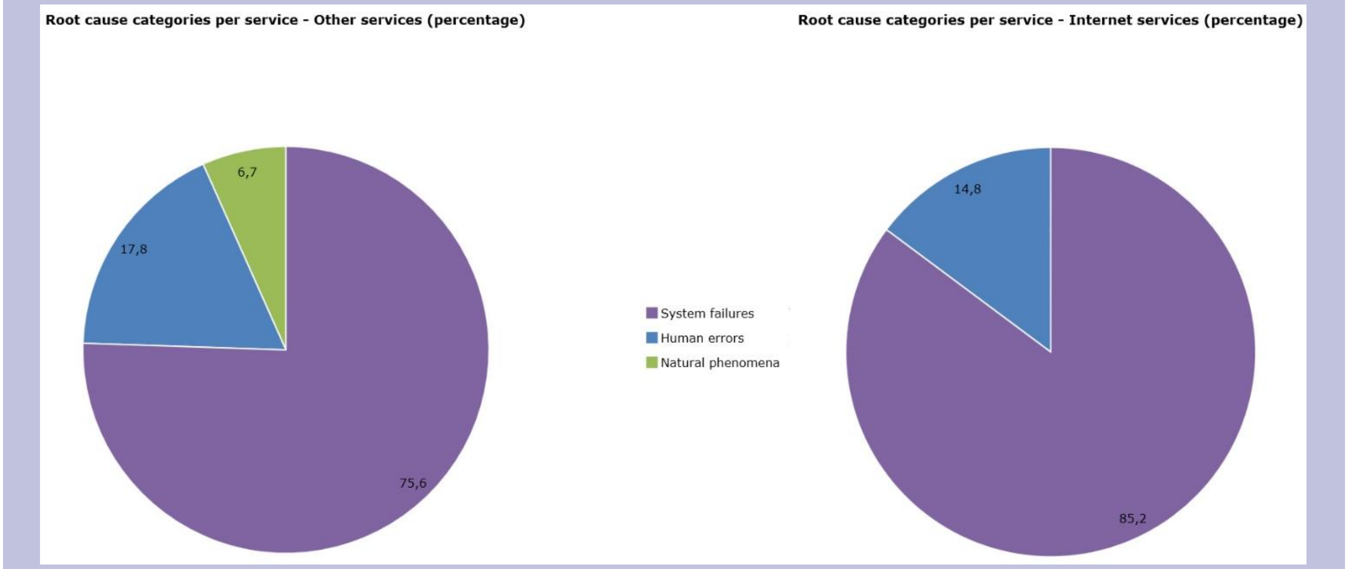


Figure 20: Root cause categories for other services (percentage).

4.2.4 Average number of user connections affected per root cause category

In 2015 system failures affected most user connections, on average about 1.6 million user connections per incident. In the previous year, system failures affected most connections.

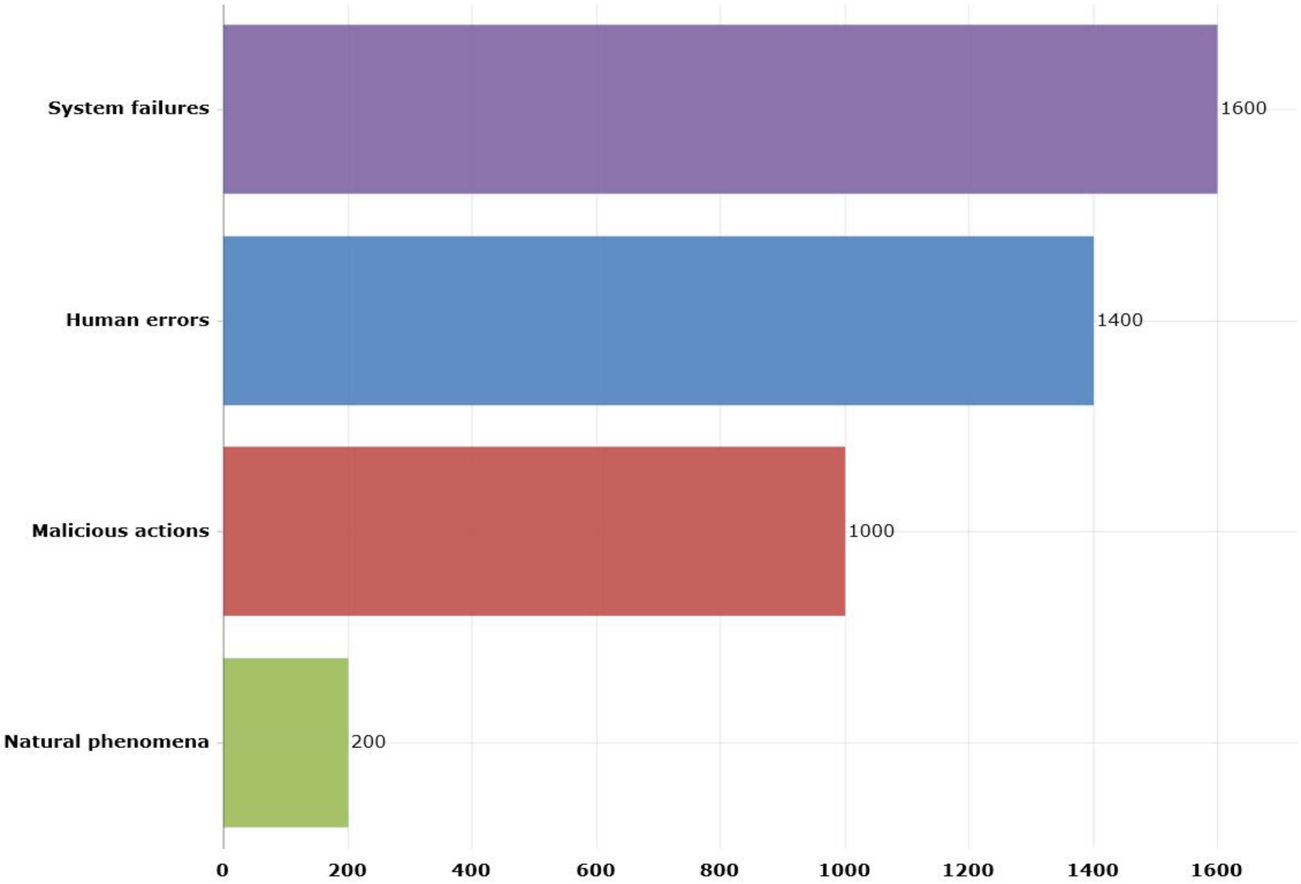


Figure 22: Average number of user connections affected per incident per root cause (1000s)

***A software bug caused an unintentional Denial of Service disrupting fixed telephony and fixed internet services for millions of users for several hours (duration: hours, connection: millions, cause: system failures, third party failures**): A malformed DNS (DNSSEC) unintentionally caused the crash of DNS servers because of a vulnerability introduced into a corrective patch the week before. The crash was amplified by the saturation of the load balancers. Addressing servers were the assets affected by this crash. Upon detection an incident management team was set up to analyse, evaluate and implement the initial actions. After several attempts, the Arbor filtering and rate limiting mechanism was activated to stop the saturation and the services restart. A new corrective patch was deployed, as a post-incident action, in order to stop the vulnerability effect. More hardware capacity has been added to load balancers. Timers on the load balancers have been obtimized. An evolution of the DNS architecture has been studied.*

4.2.5 Average duration of incidents per root cause category

The reported incidents caused by malicious actions had the longest recovery time on average per incident (47 hours). Usually incidents affecting the most in terms of duration are the ones caused by natural phenomena. For the evolution in time of the average duration pls. check Annex B.4.

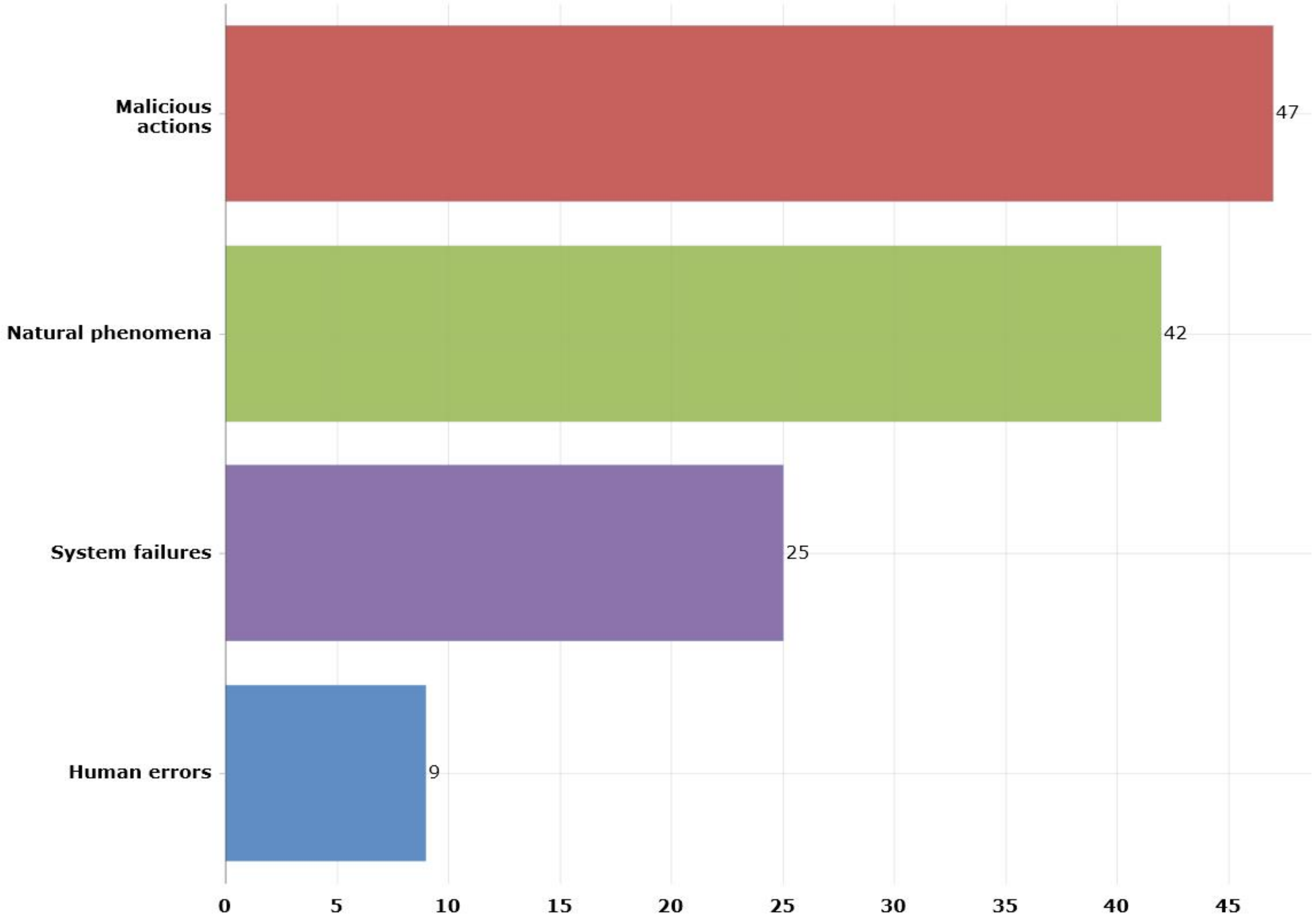


Figure 23: Average duration of incidents per root cause category (hours).

Denial of service attack caused an outage of both mobile services for ninety three hours (duration: days, connection: thousands, cause: malicious actions): *A DDoS attack affected mobile routers, which had an impact on in-home femtocell connectivity. This caused some impact (although not total service loss) for a number of customers for several days. Assets affected: Switches and routers.*

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 2015, the most common causes of incidents were hardware failures and software bugs. This can now be considered a trend as this has been the case all the previous years, with the first position being occupied by one or the other. Also cable cuts and cable cuts were among the top four causes during all four years.

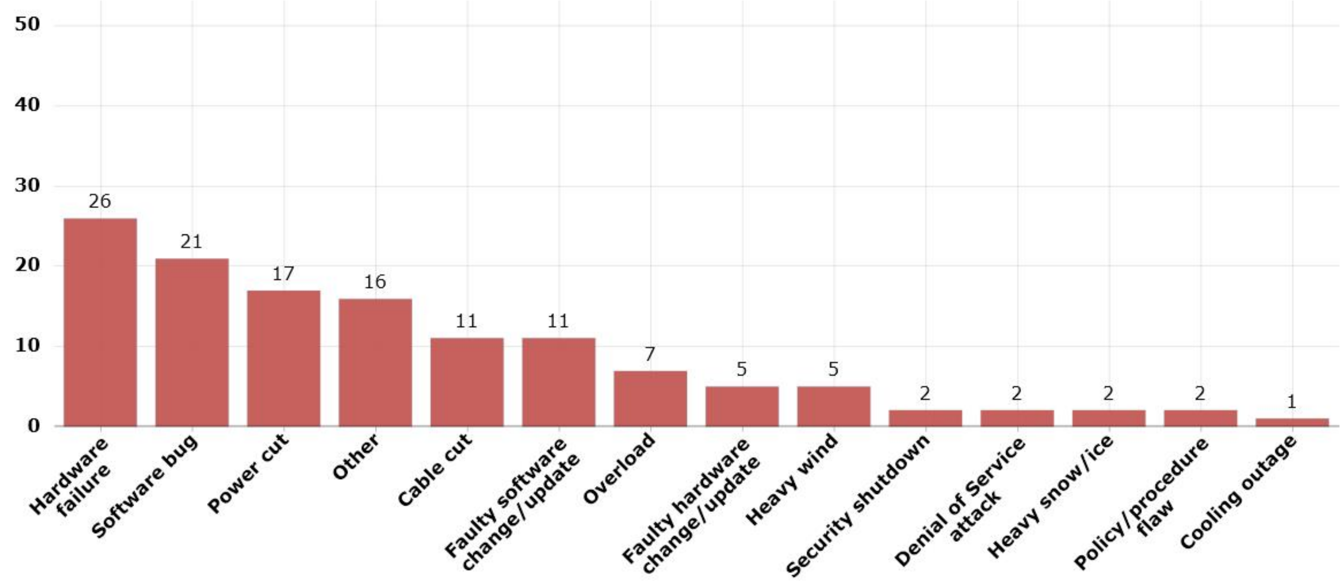


Figure 25: Detailed causes of reported incidents (percentage)

Hardware failure resulted to loss of mobile services and SMS services for more than a million of users (duration: days, connections: millions, causes**: s**ystem failure): *An HLR fault resulted in disruption of mobile services, both mobile telephony and mobile internet, for more than two days for millions of users.*

4.3.2 Detailed causes per service

In this section we show the detailed causes of incidents for each of the main four services (fixed telephony, fixed Internet, mobile telephony and mobile Internet) - see figures 20 to 23 below – and for the newly added services. Hardware failures were the most common causes for failures in all the main four services

4.3.2.1 Fixed Telephony

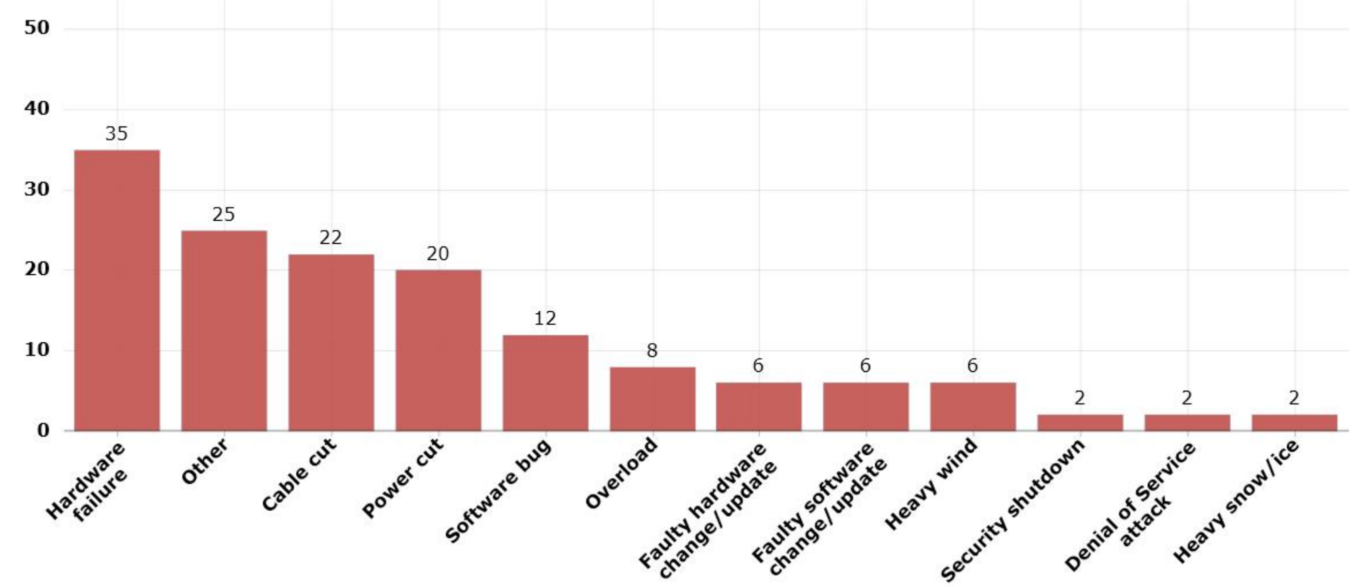


Figure 26: Detailed causes for fixed telephony (percentage).

4.3.2.2 Fixed Internet

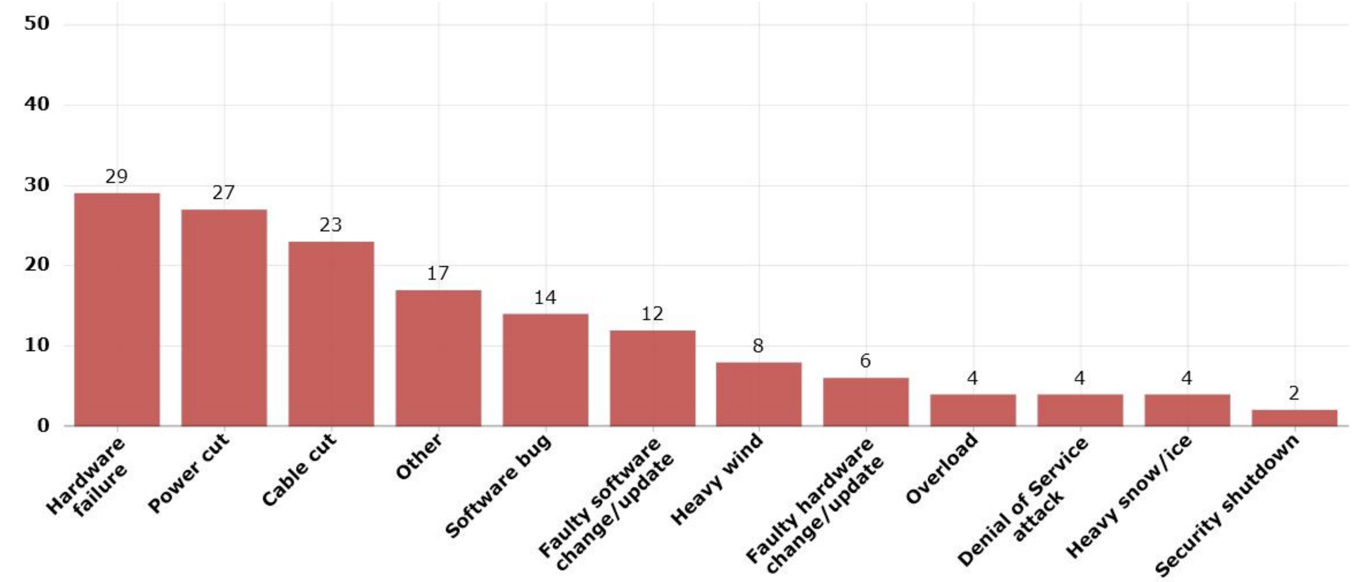


Figure 27: Detailed causes for fixed Internet (percentage).

4.3.2.3 Mobile Telephony

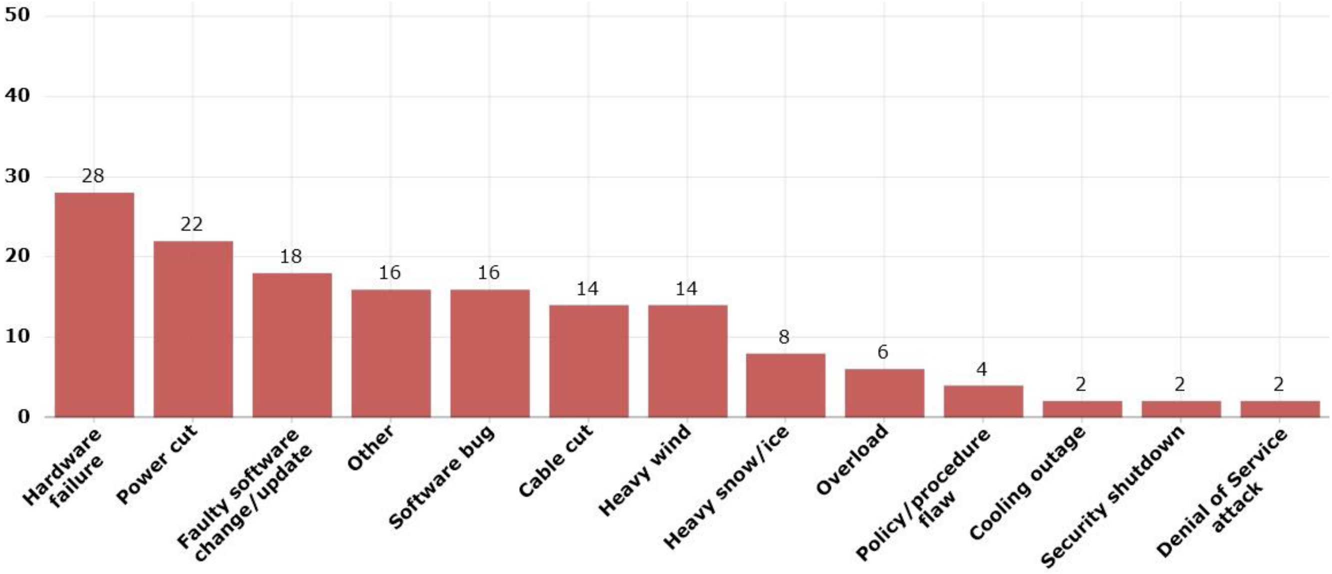


Figure 28: Detailed causes for mobile telephony (percentage).

4.3.2.4 Mobile Internet

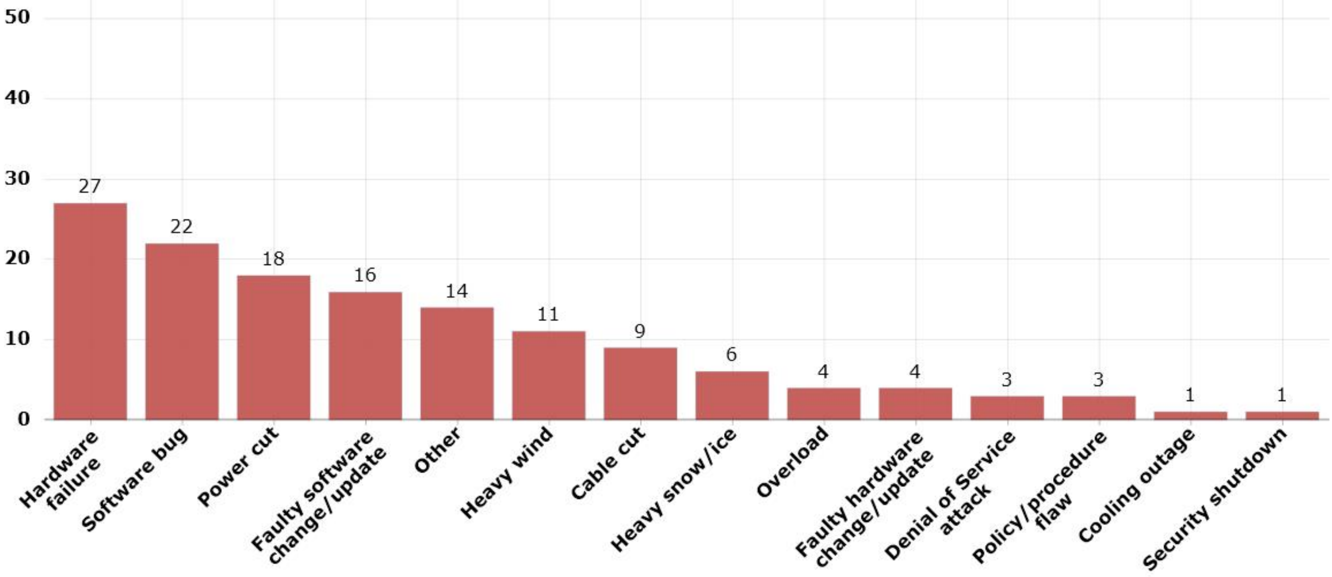


Figure 29: Detailed causes for mobile Internet (percentage).

4.3.2.5 Newly added services

The main detailed causes for all new added services were “Power cuts” affecting 26%. Software bugs and Hardware failures are following affecting 24% of all incidents (the percentages per service are the following: Cable TV, IPTV and TV Broadcast).

"Software bug" is the detailed cause impacting the most internet related services, such as Public email services. Another cause with great impact was "Hardware failure" which impacted both types of new services, with SMS and IXPs scoring highest.

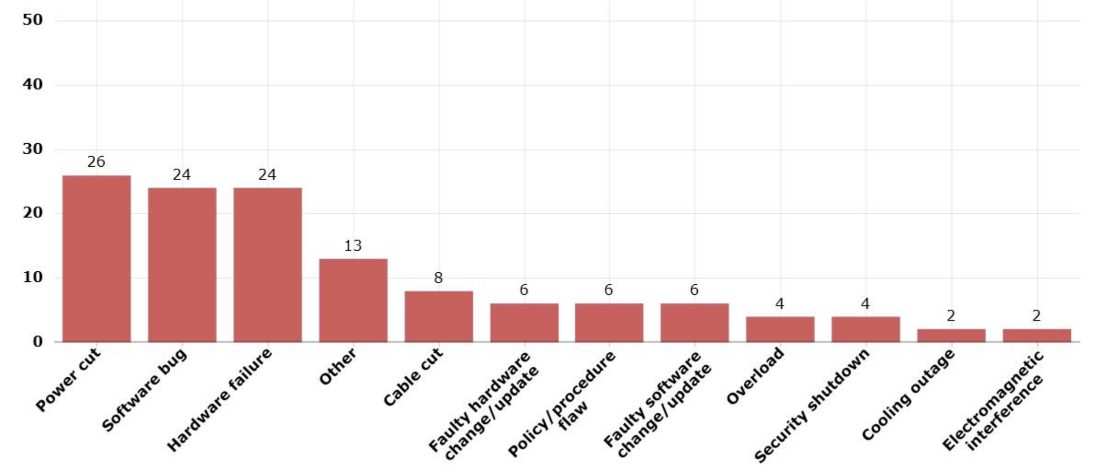


Figure 30: Detailed causes for other services (percentage).

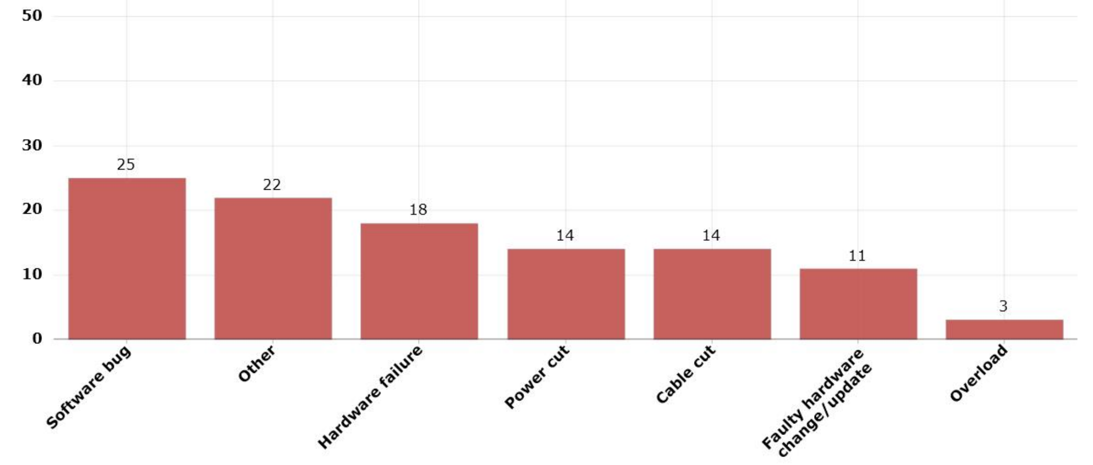
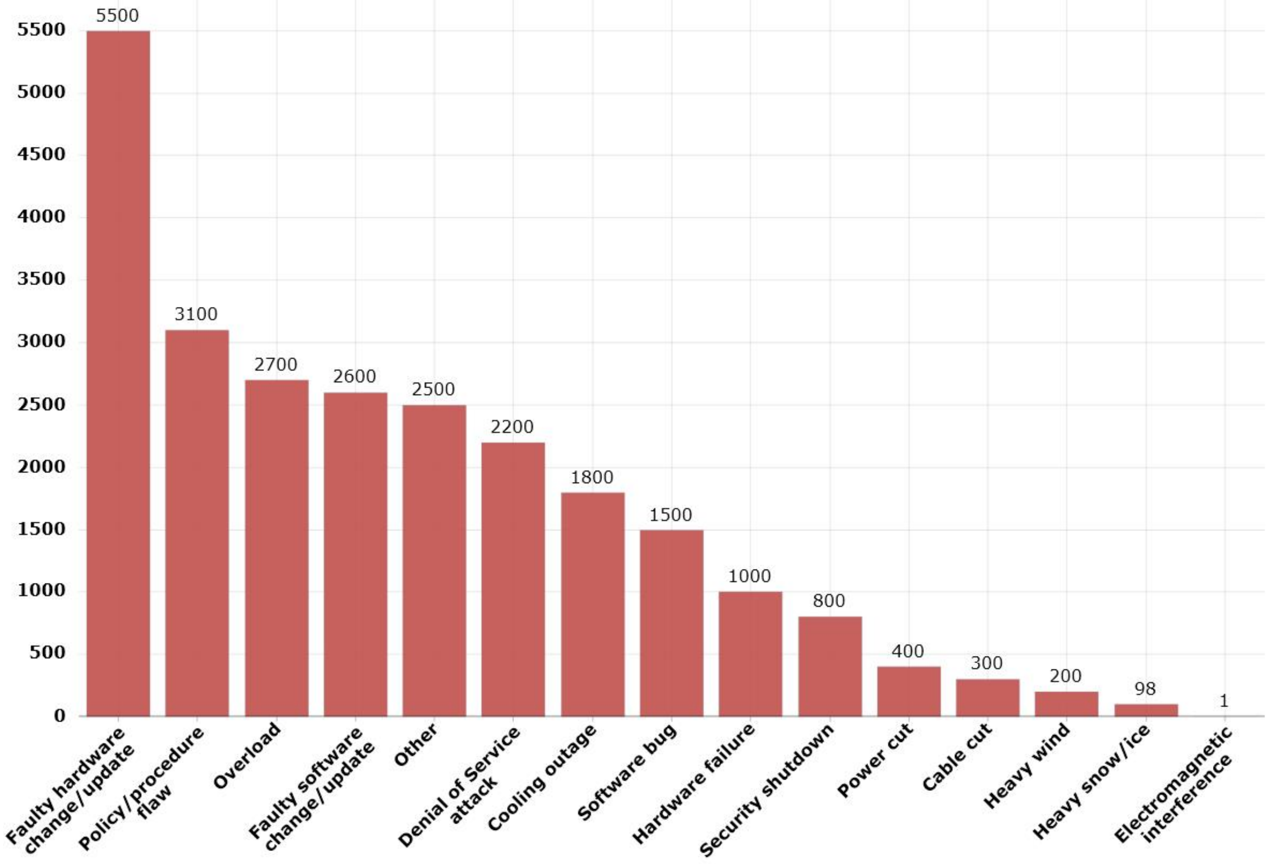


Figure 31: Detailed causes for Internet related services (percentage).

4.3.3 Average number of user connections affected per detailed cause

In 2015 Faulty hardware changes affected in average the most number of user connections (5.5 mil.). Other important causes were procedure flaws, overloads, faulty software changes, DoS etc.



Faulty hardware change/update resulted to loss of mobile internet and other internet related services for millions of users (duration: hours, connections: millions, causes: System Failure): *Failure of key server resulted in dysfunctional cellular data throughout the country for millions of users. Identification of errors, replacing defective hardware as well as services group changes key server for a new one was the immidiate response of the provider to resolve the incident.*

4.3.4 Average duration of incidents per detailed cause

For 2015, reported incidents caused by heavy winds had the longest duration (almost 3.5 days per incident on average). Hardware failures caused incidents that on average a little more than 2 days.

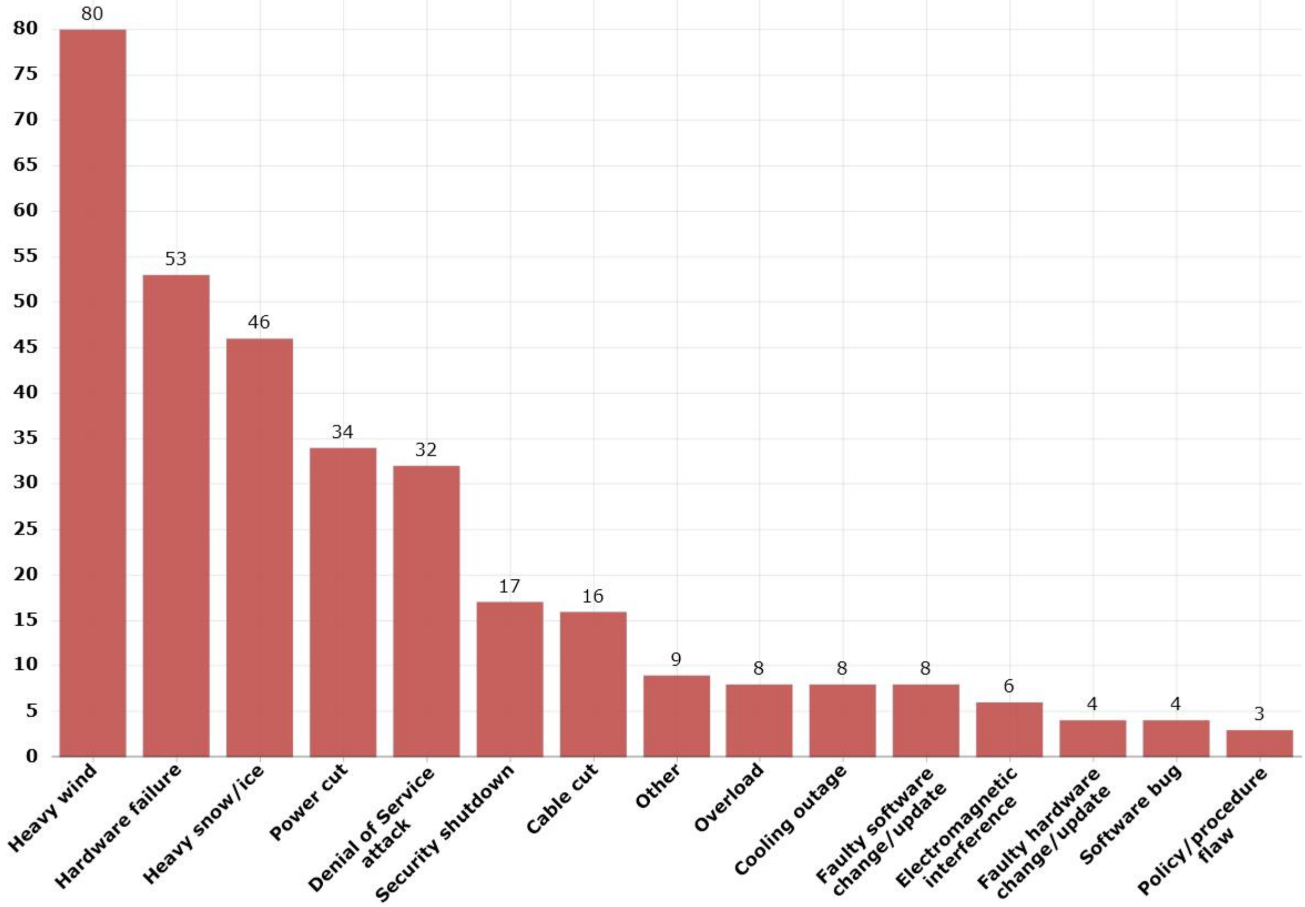


Figure 33: Average duration of incidents per detailed cause (hours).

Heavy wind led to a power cut causing a large scale mobile communication outage for approximately a week: (duration: days, connections: thousands, cause: Natural phenomena): *Widespread storms lead to major damage to mains power and subsequent power failure to mobile basestations across a region.*

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 2015 switches and routers were the assets most affected by incidents, followed by mobile base stations and transmission nodes. The previous year the ranking was more or less the same, with underground cables being on second place. For more details pls. see Annex D.1.

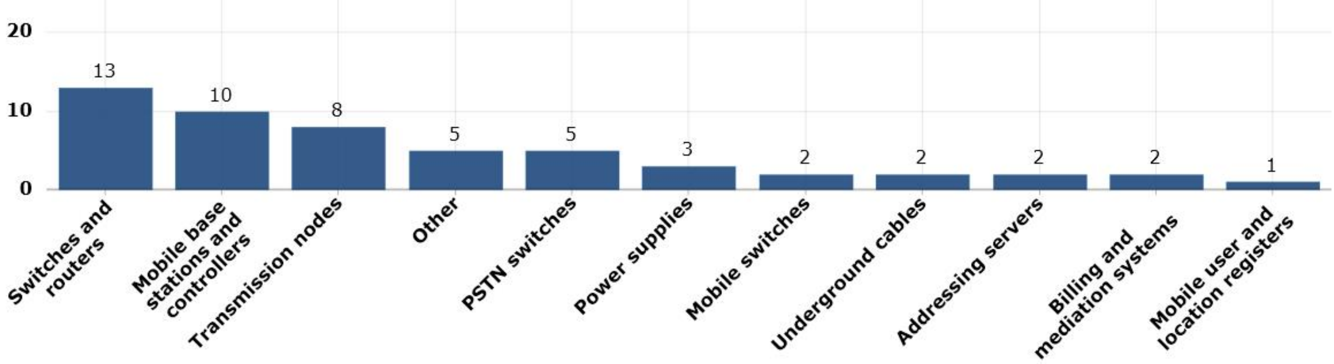


Figure 35: Assets affected by the incidents (percentage).

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 2015[9]. In these system failures the most common assets that failed were switches and routers, transmission nodes, mobile switches (MSC), 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.

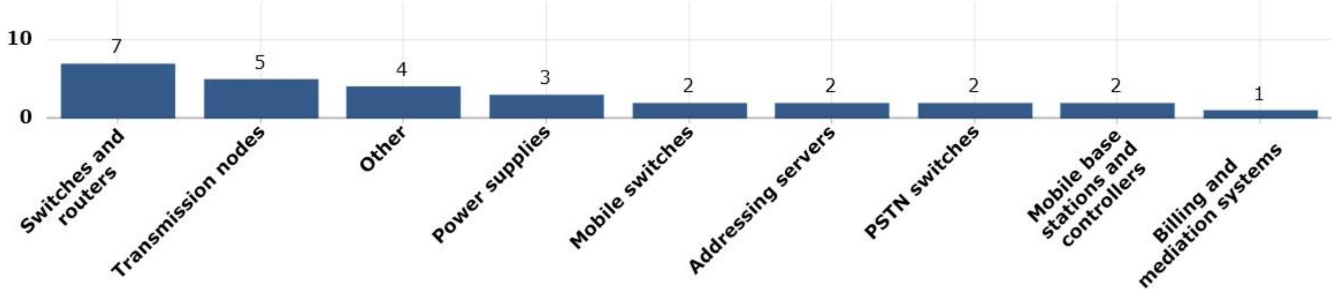


Figure 36: Assets affected by system failures (percentages).

[9] 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.

Faulty software change caused overload of systems disrupting all services for millions of users (duration: hours, connections: thousands, cause: human error): *A planned job on core routers and a bad configuration led to connection of two networks that should not be connected, which in turn led to signalling overload and significant capacity reduction (up to almost 10%.). Disconection of the two networks resolved the unavailability issue. Furthermore, the provider made changes in the configuration mangement and automated further the configurations and segmentation of the core network in order to prevent similar future events.*

4.5 EU thresholds vs. national level thresholds

Art. 13a provisions state that member states shall ensure that electronic communication providers will "notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services". But the thresholds for defining significant incidents were not established through the Directive and the EC has not issued any implementing measures in this sense leaving the matter open for discussions and unrestricted as regards the national implementation. At this point the activities of ENISA and Art. 13a expert group have proved to be very useful by defining a set of **informal and non-binding EU thresholds** to help member states in reporting or setting up their own national level thresholds. In this respect a set of EU thresholds were adopted by the Art. 13a expert group that are known and accepted by every country, but it has remained at the discretion of each Member State to adopt its own national thresholds. All incidents reported within the annual report to ENISA and EC, and presented within this report, are based on the thresholds established at national levels, which can be above or below (in most of the cases they are below) the EU thresholds. This section presents a short analysis of incidents based on the informal EU level thresholds.

According to our estimations more than half of the EU member states have thresholds below the ones defined by ENISA while others use the same thresholds.

The total number of incidents reported that exceed the informal EU relative and absolute thresholds is ***90***, representing 67% of all reported incidents.

In the chart below you can also see the evolution of the number of incidents in the past years.

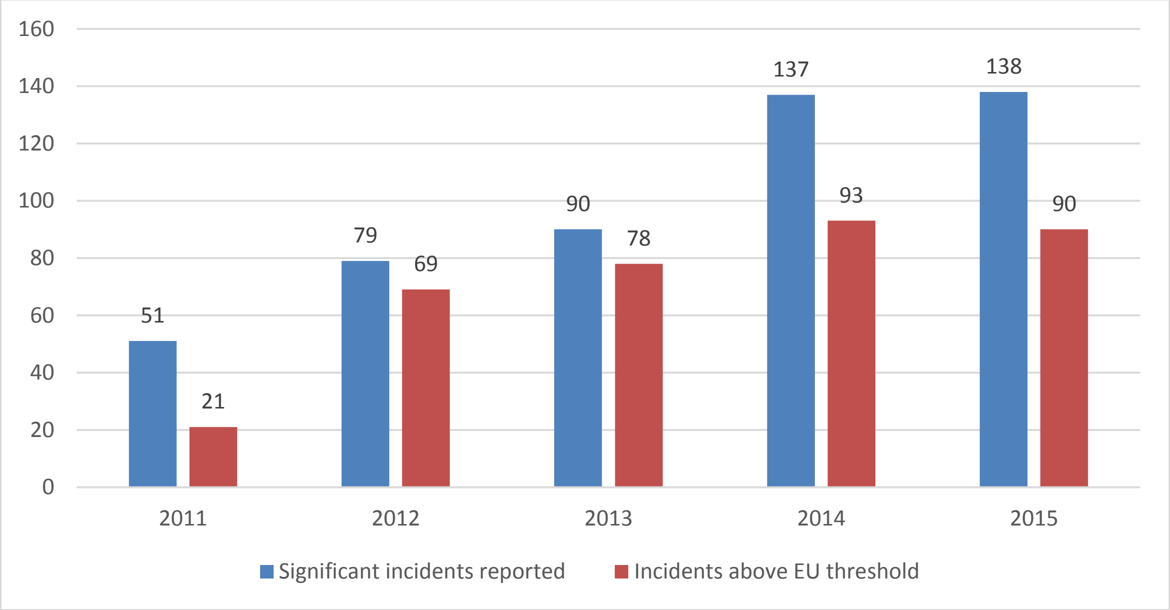


Figure 37: Total number of incidents: national threshold vs. EU thresholds.

5. Conclusions

In this Report ENISA summarized and analysed the outage incidents that were sent by the National Regulatory Authorities (NRAs) from member states and EFTA countries, to ENISA and the EC in 2016 concerning incidents in 2015, as mandated by Article 13a of the Framework Directive (2009/140/EC). ENISA and the EC received, as part of the fifth round of reporting from the NRAs, 138 reports about major outages/disruptions impacting electronic communications services that occurred in 2015.

From the 138 significant incidents reported to ENISA and the EC, 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:

- **Mobile internet most affected service:** In 2015 most incidents affected mobile internet (44% of all reported incidents). Mobile internet and mobile telephony were the predominant affected services in the previous years also, except for 2014 where fixed telephony was the most affected.
- **Mobile services outages have affected in average more users than other services:** Incidents affecting mobile Internet or mobile telephony affected most users (around 1.3 million users and 1.0 million users respectively per incident). On average 18% of national user base was affected by incidents on mobile internet services.
- **Emergency services are affected by incidents**: In 20 % of the incidents there were problems in reaching the 112 emergency services, a small decrease since the previous year.
- **Interconnections between providers are affected by incidents**: In more than 4 % of the incidents there were problems in interconnecting between providers, although a decrease compared with previous years. In most of the cases the impact by third parties is unknown.
- **Switches and routers most affected assets:** Overall, switches and routers were the network components most affected by incidents (13%), followed by mobile base stations (10%).
- **New services affected:** TV broadcasting / Cable TV Networks (13,7%) and SMS/MMS (13%), public email (5,8%), IPTV (5,1%), VOIP services (4,3%) were the most affected services among the new ones included from this year.

Causes of incidents:

- **System failures are the dominant root cause of incidents:** Most incidents were caused by system failures or technical failures (66,7 % of the incidents) as a root cause. This has been the dominant root cause for all the reporting years so far. System failures was also the most common root cause for all the main services when looking at them separately. In the system failures category, software bugs and hardware failures were the most common causes. The assets most often affected by system failures were switches and routers, and mobile base stations.
- **Third party failures continues to affect a part of the total number of incidents**: 15,2% off all incidents were caused by third party failures; although the percentage might not seem so big these are incidents completely out of the control of the provider, so very difficult to tackle. System failures followed by human errors (e.g. cable cuts and faulty software updates) were the most common cause category for third party failures also.

- **Human errors affected on average more user connections per incident:** In 2015 human errors was the root cause category involving most users affected, around 2.6 million user connections on average per incident. The second place was taken by system failures with 2.4 million user connections on average per incident.

- **Malicious actions are not focused on causing disruptions:** the total number of incidents caused by malicious actions dropped to 2.5% from higher previous values (9.6% in 2014). This may indicate that the malicious actions are not necessarily aiming at causing unavailability of services.

- **Malicious actions started causing long lasting incidents:** Incidents caused by malicious actions (e.g. DDoS), although we didn't have too many of them, had most impact in terms of duration, on average almost two days per incident.

- **Natural phenomena are causing the most long lasting incidents:** Incidents caused by natural phenomena (e.g. heavy winds), had most impact in terms of duration, on average almost four days per incident.

- **Hardware failures and software bugs are the most common initial causes for incidents:** 27% of all incidents had as an initial cause hardware failures and 21% were caused by software bugs.

- **Faulty software changes and overloads have most impact in terms of connections:** Incidents caused by human errors (particularly faulty software changes) and system failures (overloads) had most impact in terms of connections affected (12.6 mil).

- **Root causes per new services:** System failures is also the main root cause for all new services, with a percentage of 75,6% to 85,6% of the total incident reports that included at least one of the new services.

These patterns and trends need particular attention in the risk and vulnerability assessments carried out in the electronic communications sector. ENISA is permanently analysing the current threat environment and develops projects that address particular technical or more "political" topics related to the electronic communications sector.

Given thatseveral years have passed since the publication and implementation of the Framework Directive including Art. 13a, an impact evaluation of the new article was done last year, with the purpose of assessing the changes in outcome that can directly be attributed to the provision of Art. 13a, the effects caused by this particular set of obligations within the Telecom Package. The result can be found here. In 2015 a study was also carried out to analyse alternative indicators for measuring impact in electronic communications services. The non-exhaustive list of indicators can be found here.

Based on the annual summary reporting of previous years, 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.

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 EC 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

- ENISA's reports about the 2011, 2012, 2013, 2014 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- ENISA's study "Impact evaluation on the implementation of Article 13a incident reporting scheme within EU": https://www.enisa.europa.eu/publications/impact-evaluation-article13a
- 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 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

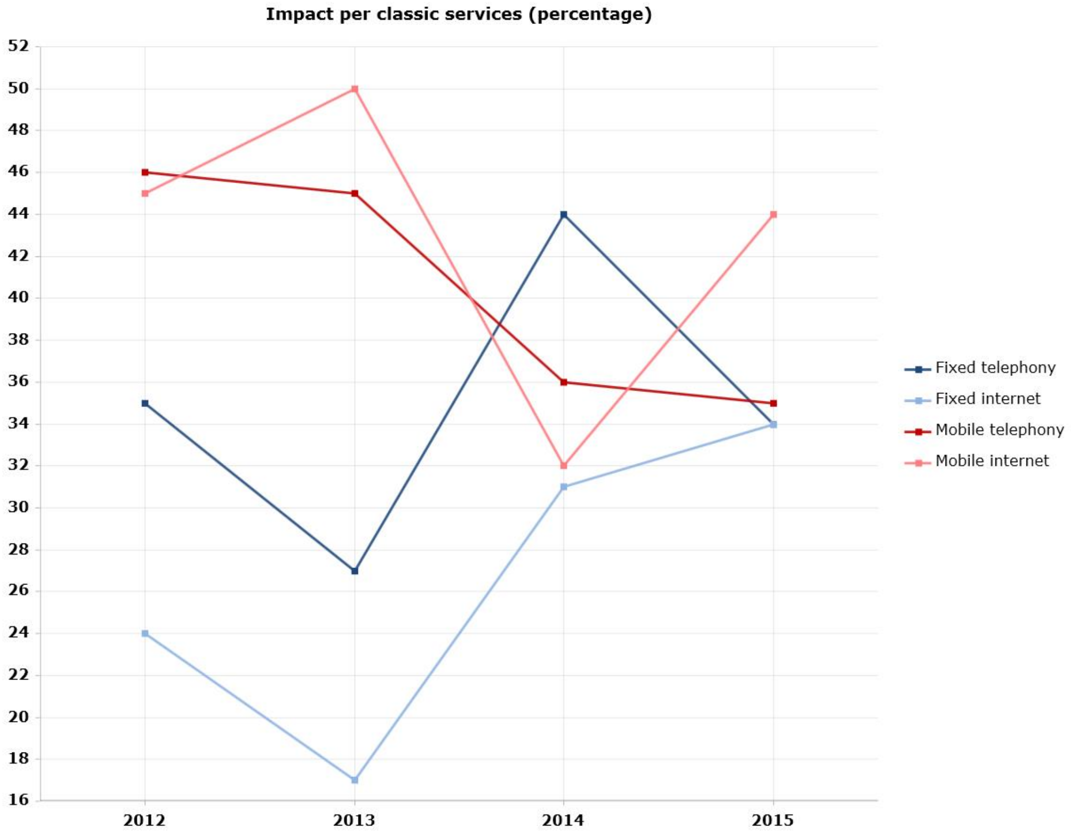
- Article 13a of the Framework directive of the EU regulatory framework for electronic communications: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0140
- The EU regulatory framework for electronic communications (incorporating the Framework Directive including Article 13a): https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf
- The NIS directive, that also contains incident notification provisions for essential (ESPs) and digital service providers (DSPs): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

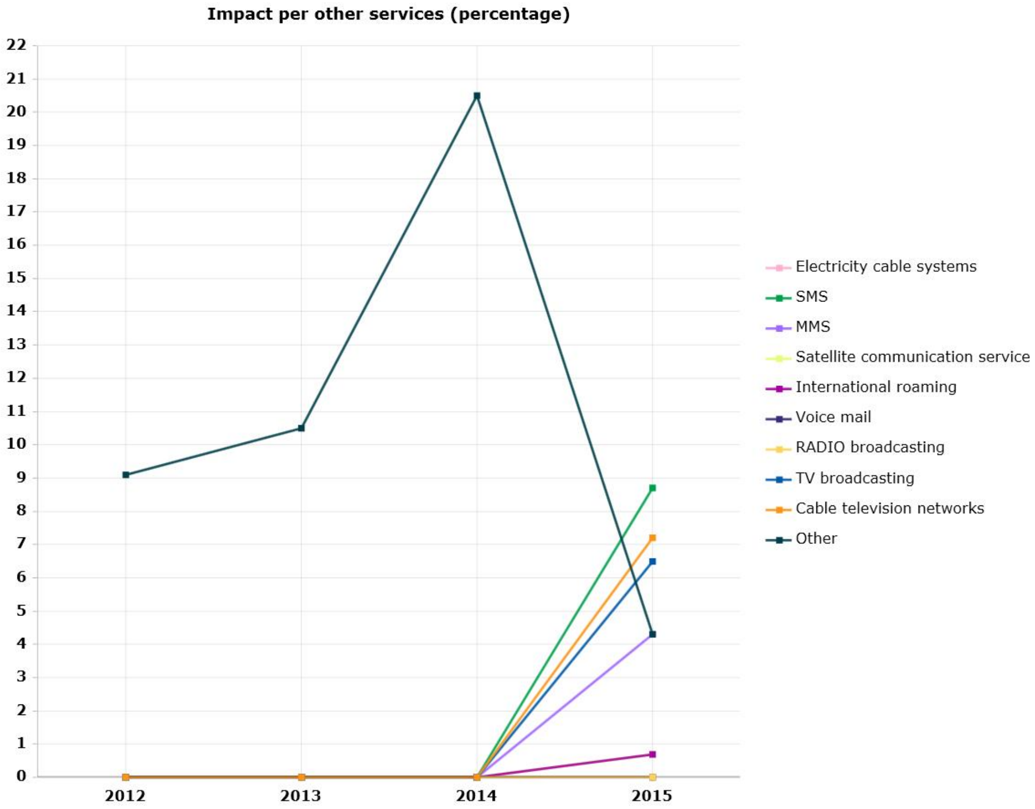
Annex

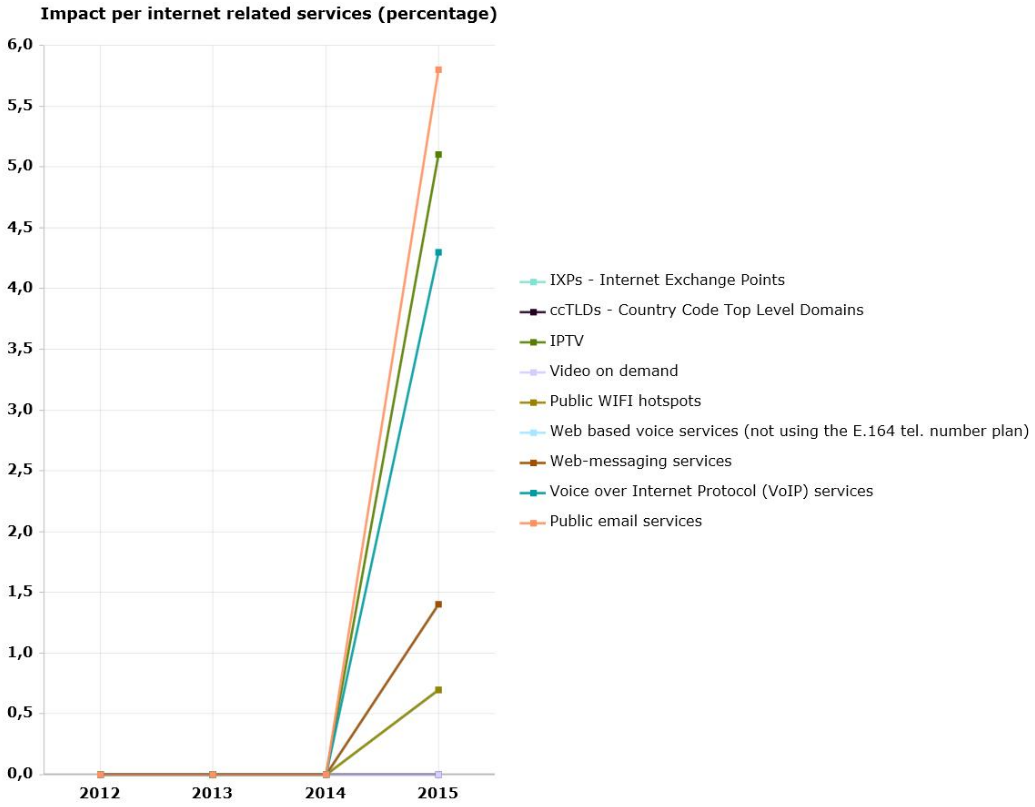
In this annex (A-D) we present graphs showing the situation between 2012 and 2014 based on the annual summary reporting by the NRAs to ENISA and the EC. The graphs provide a brief comparison betweeen the years, but conclusion should be drawn with care, as the threshold for the incidents in scope has 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: Impact of incidents

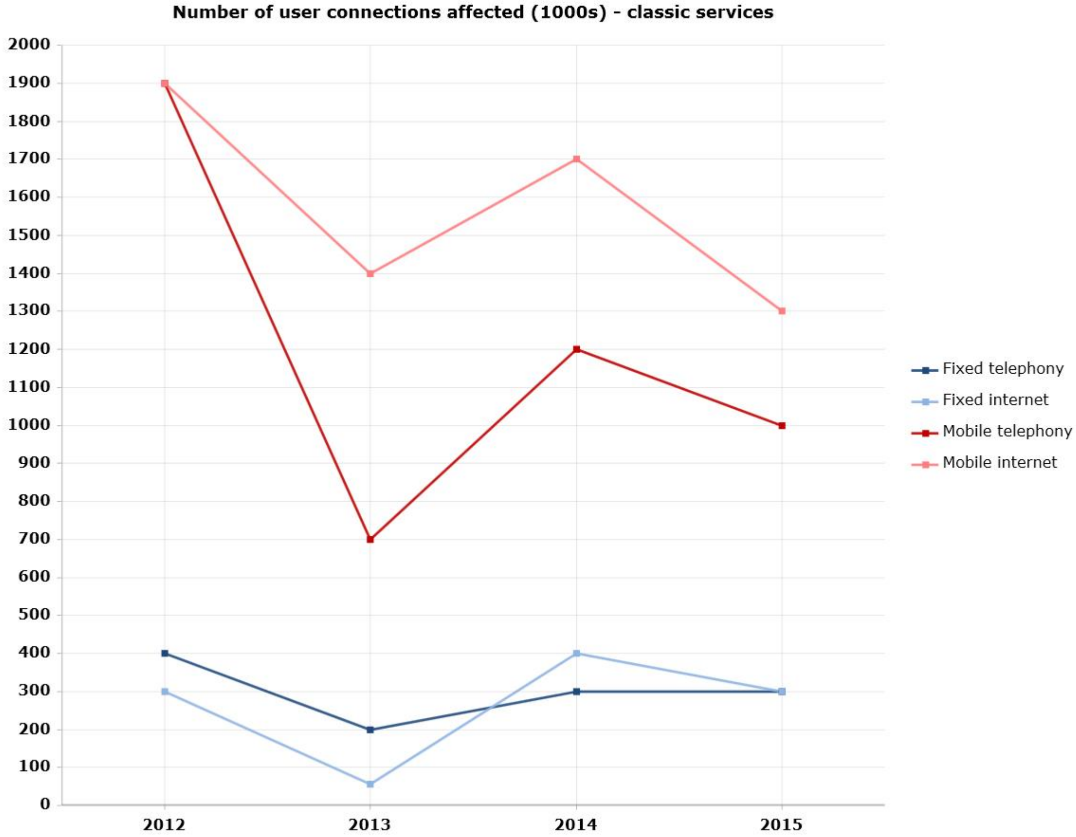
A.1 Impact per service

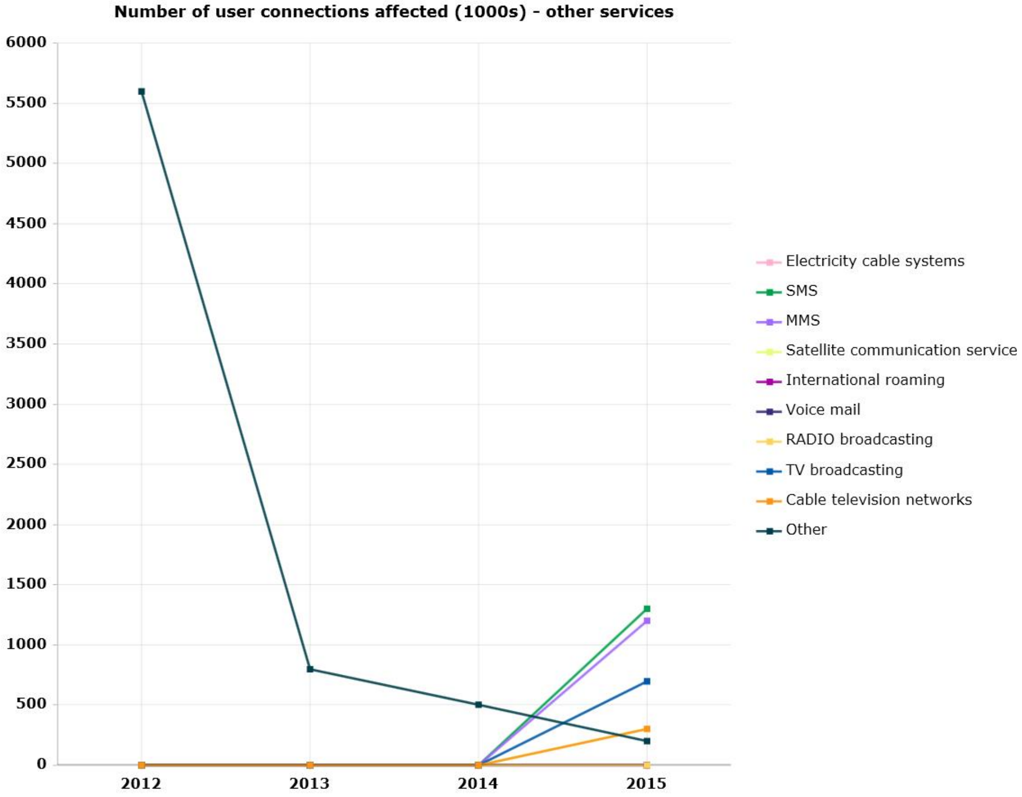


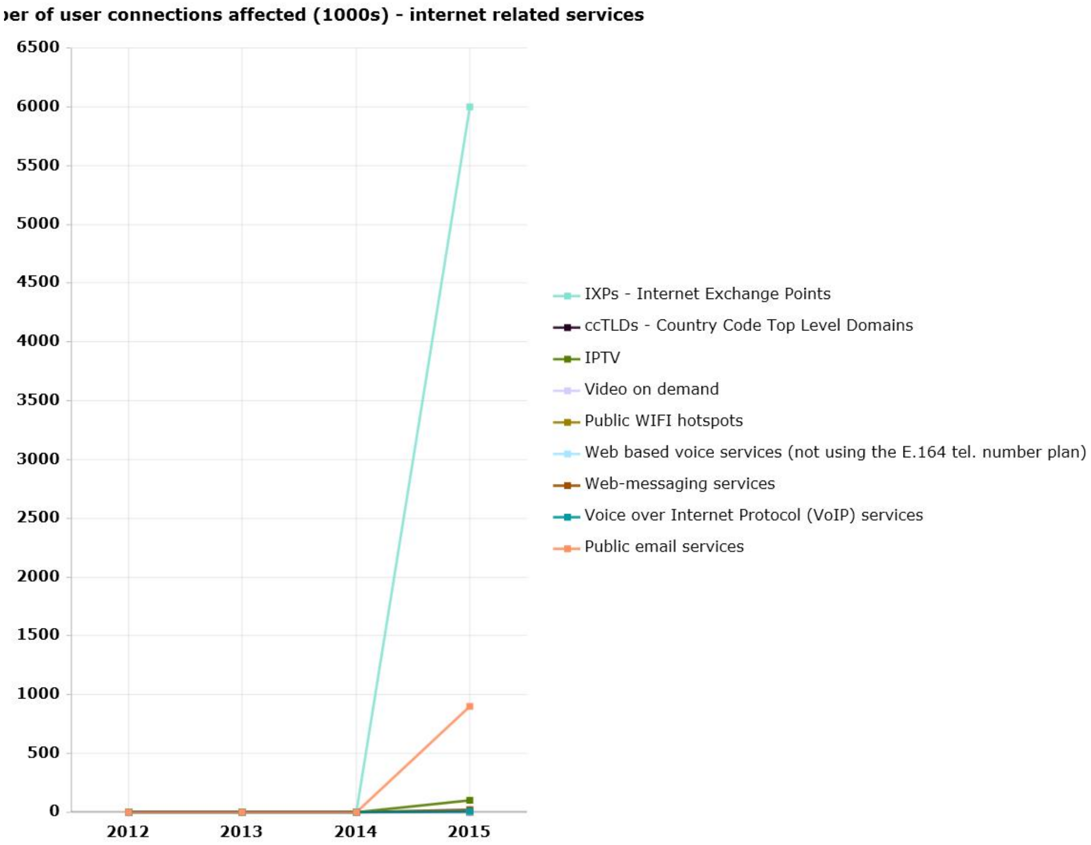

Impact per other services (percentage)
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
2012
2013
2014
2015
Electricity cable systems
SMS
MMS
Satellite communication service
International roaming
Voice mail
RADIO broadcasting
TV broadcasting
Cable television networks
Other


Impact per internet related services (percentage)
6,0
5,5
5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0,0
2012
2013
2014
2015
IXPs - Internet Exchange Points
ccTLDs - Country Code Top Level Domains
IPTV
Video on demand
Public WIFI hotspots
Web based voice services (not using the E.164 tel. number plan)
Web-messaging services
Voice over Internet Protocol (VoIP) services
Public email services

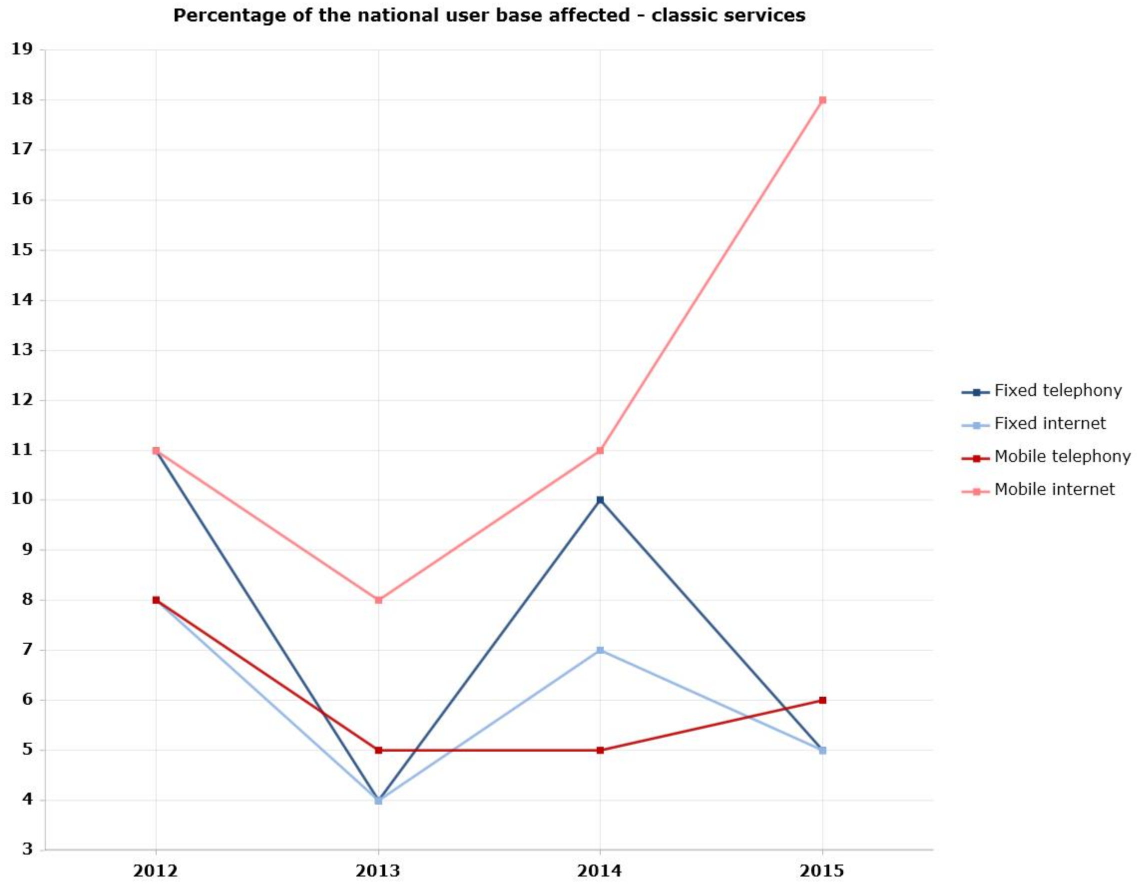
Number of user connections affected



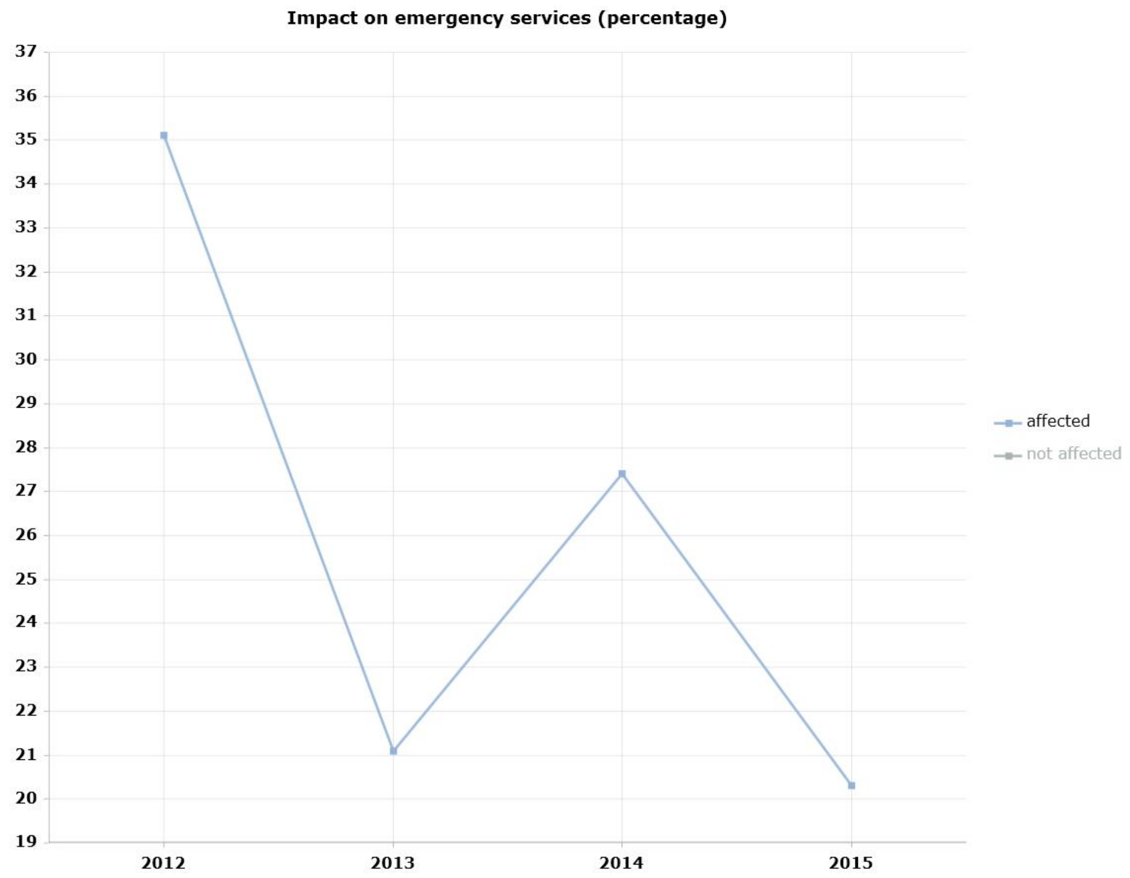



ber of user connections affected (1000s) - internet related services
6500
6000
5500
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
2012
2013
2014
2015
IXPs - Internet Exchange Points
ccTLDs - Country Code Top Level Domains
IPTV
Video on demand
Public WIFI hotspots
Web based voice services (not using the E.164 tel. number plan)
Web-messaging services
Voice over Internet Protocol (VoIP) services
Public email services

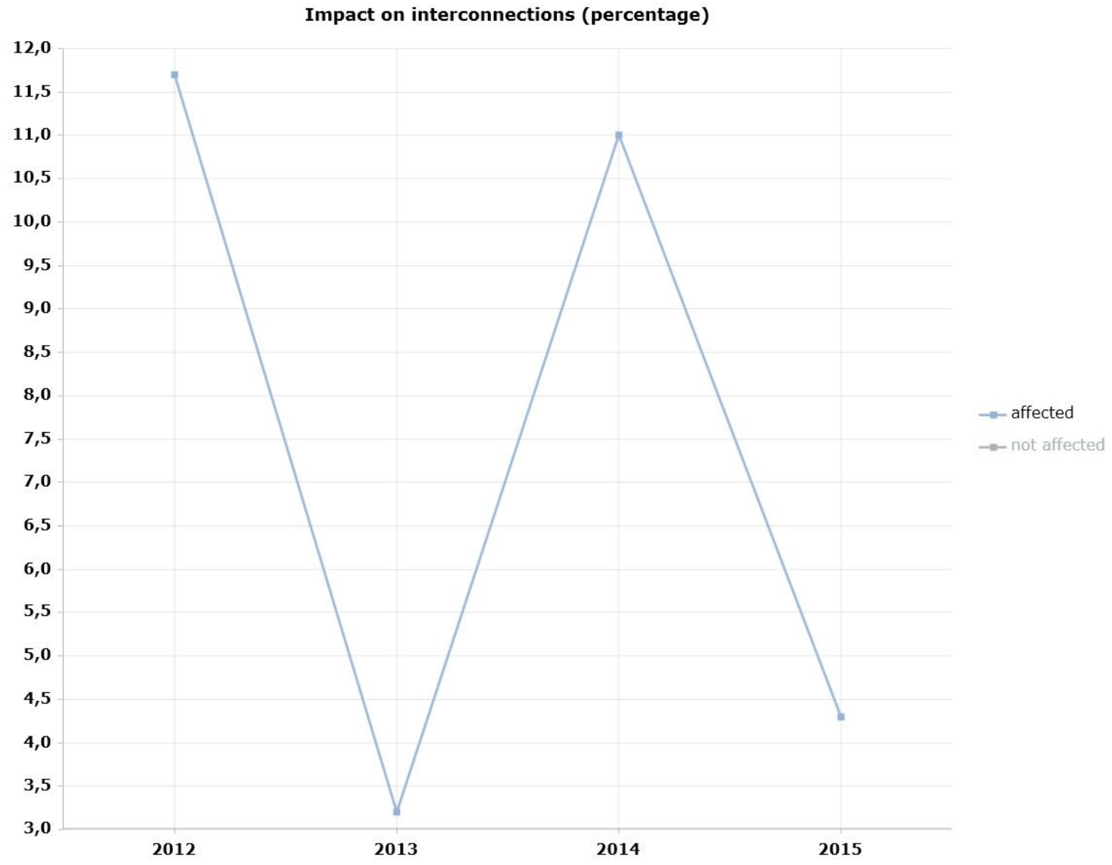
A.2 Percentage of the national user base affected



A.3 Impact on emergency services

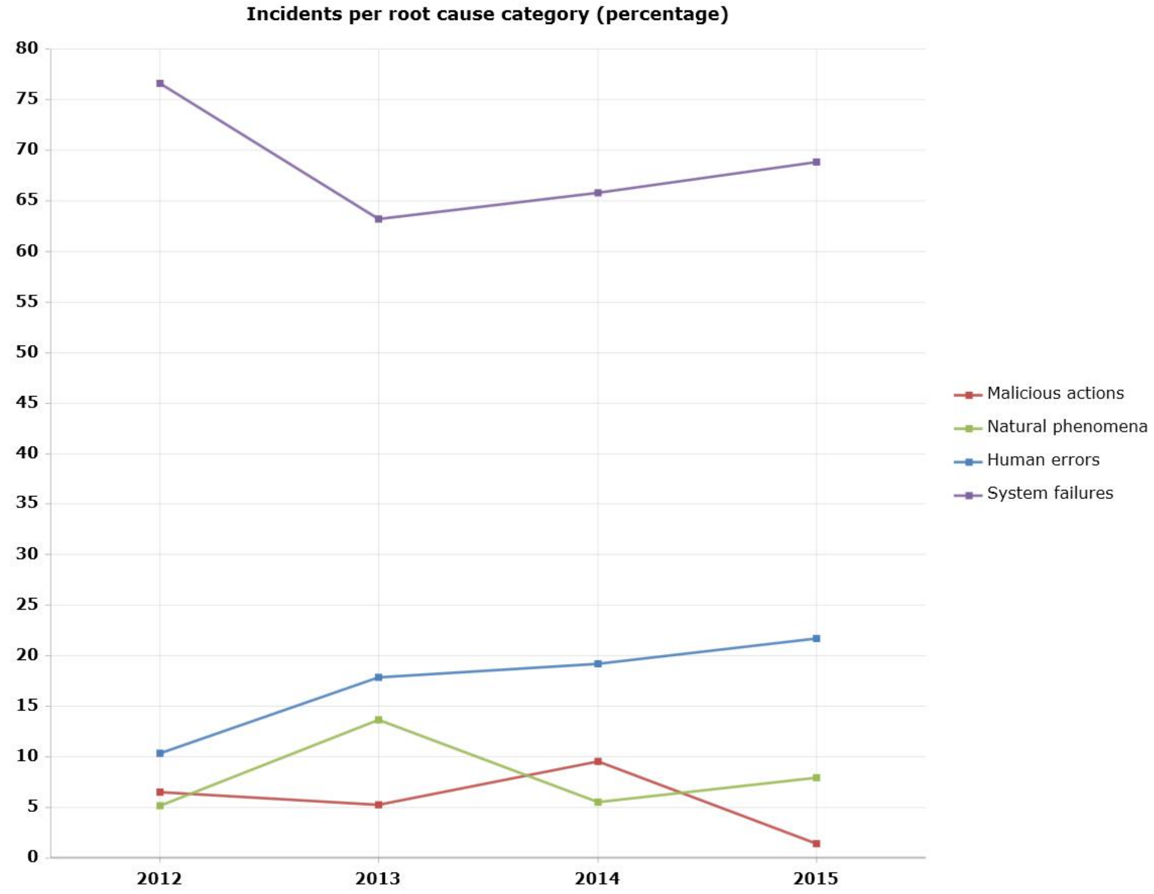


A.4 Impact on interconnections

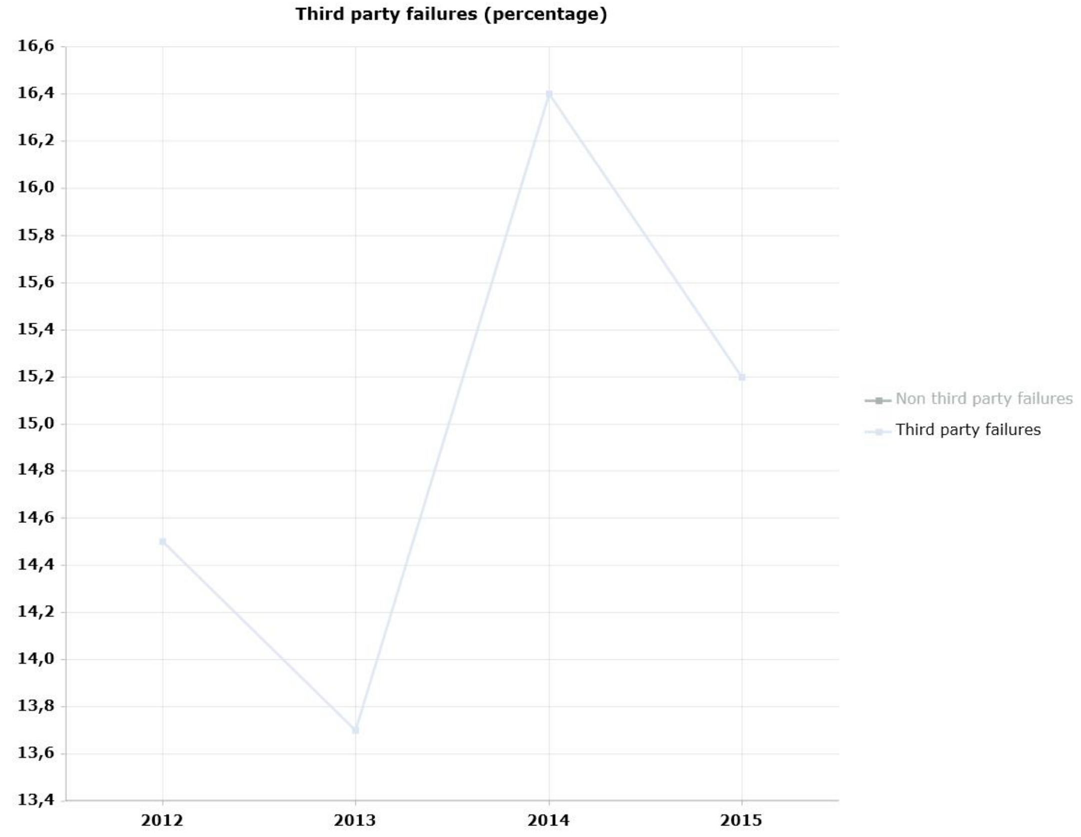


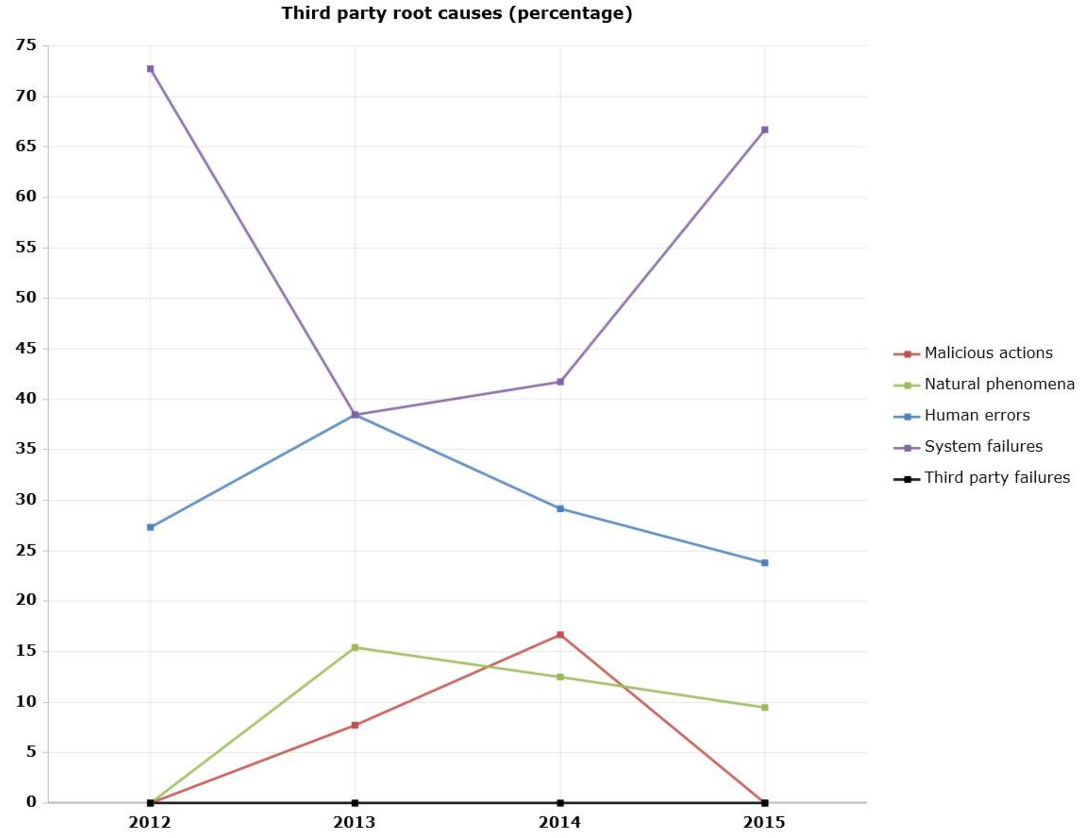
Annex B: Root cause categories

B.1 Incidents per root cause category (percentage)



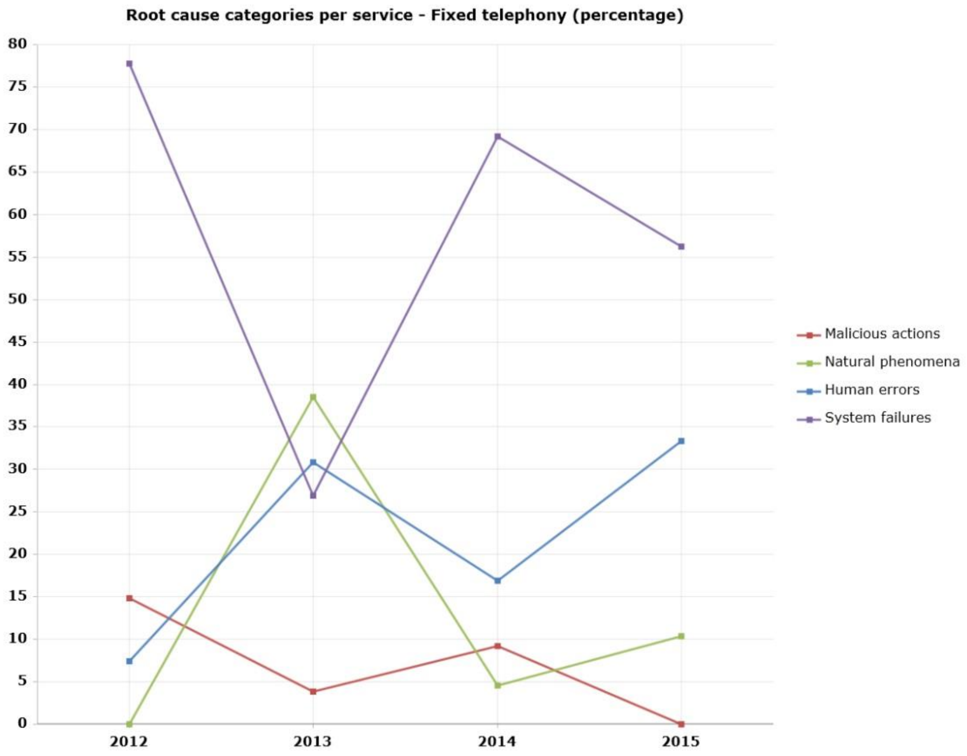
B.2 Third party failures (percentage)



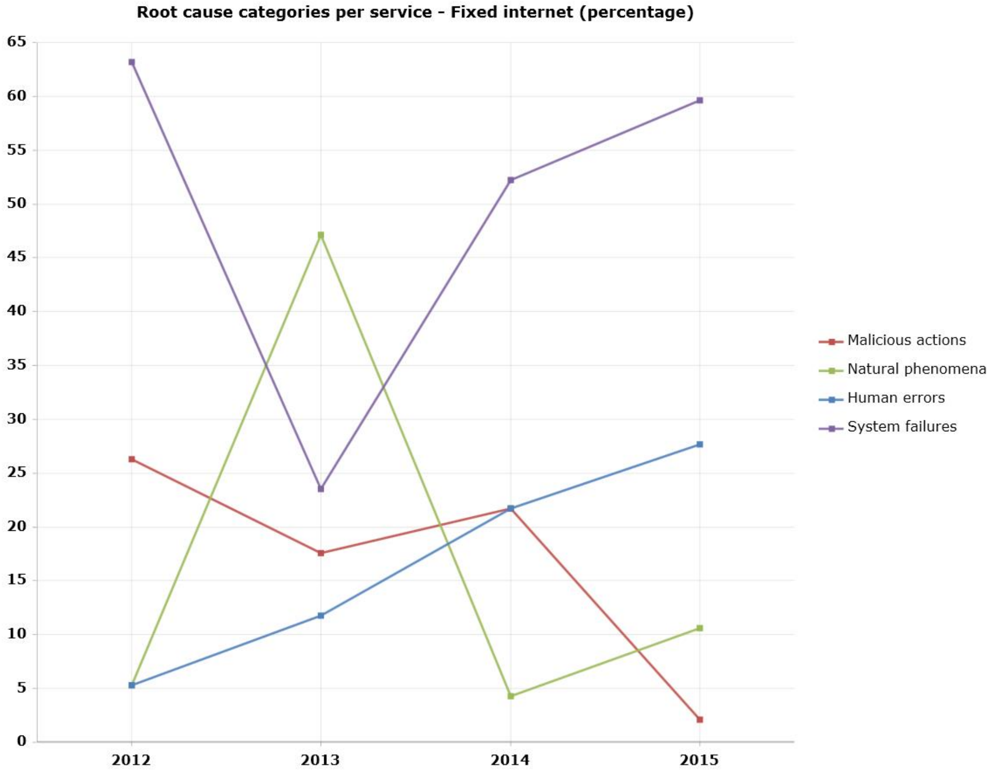


B.3 Root cause categories per service

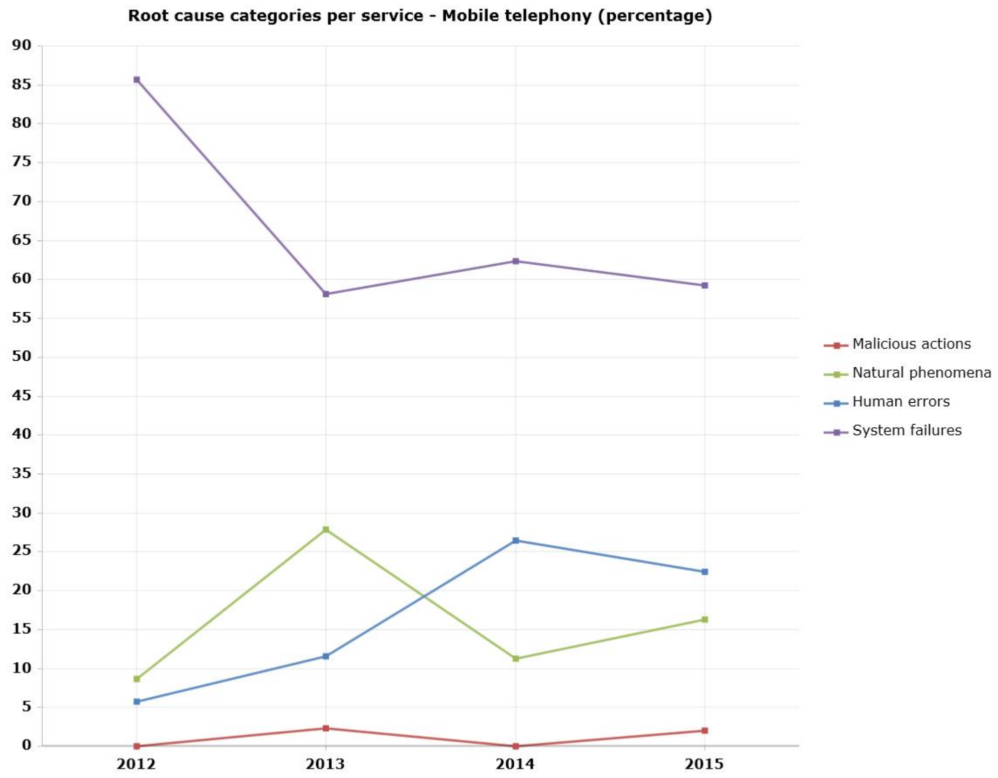
Fixed Telephony



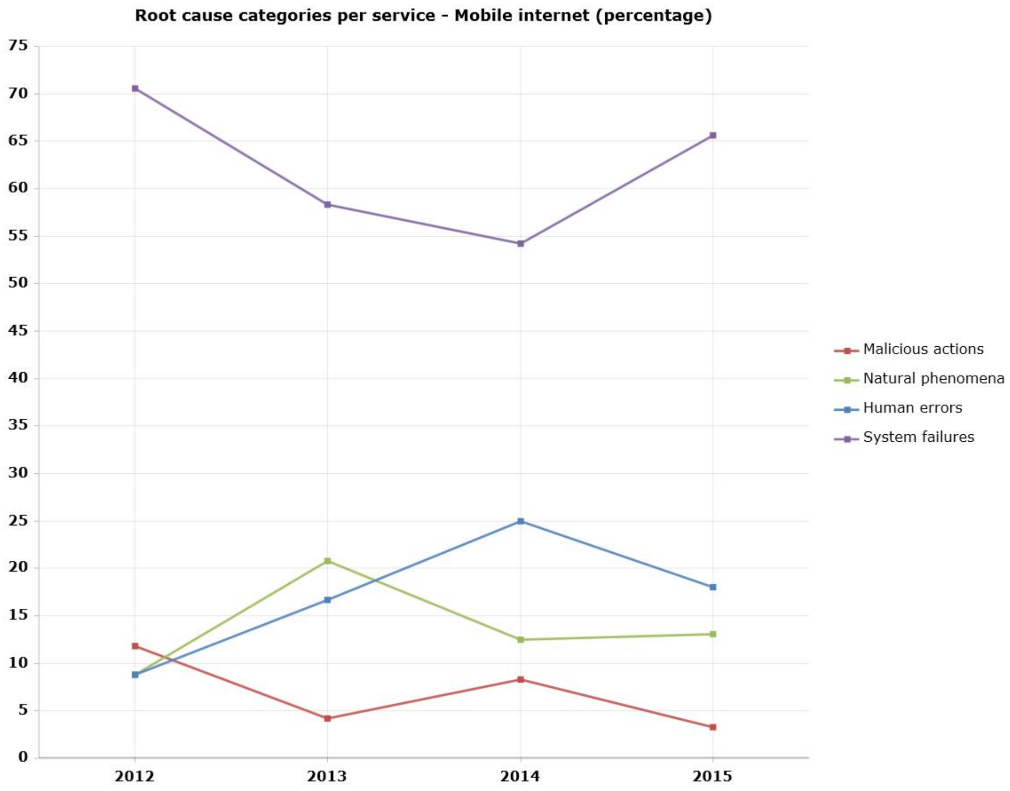
Fixed Internet



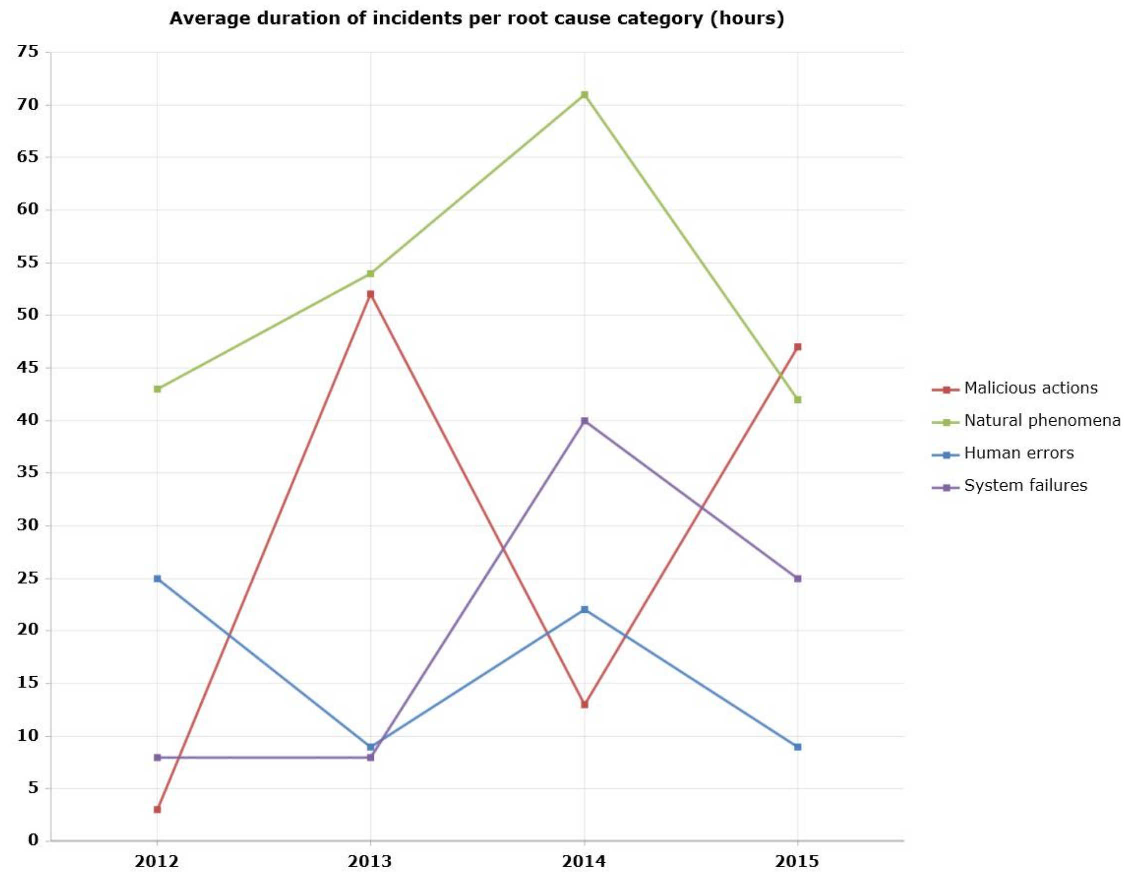
Mobile telephony



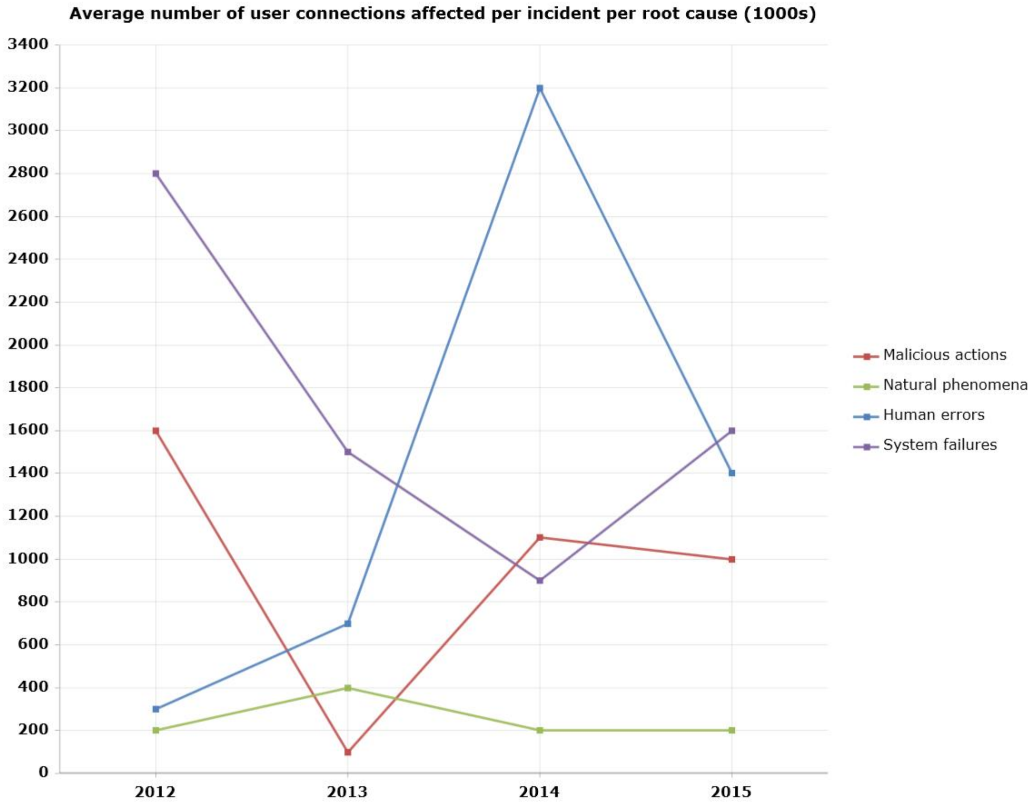
Mobile internet



B.4 Average duration of incidents per route cause category

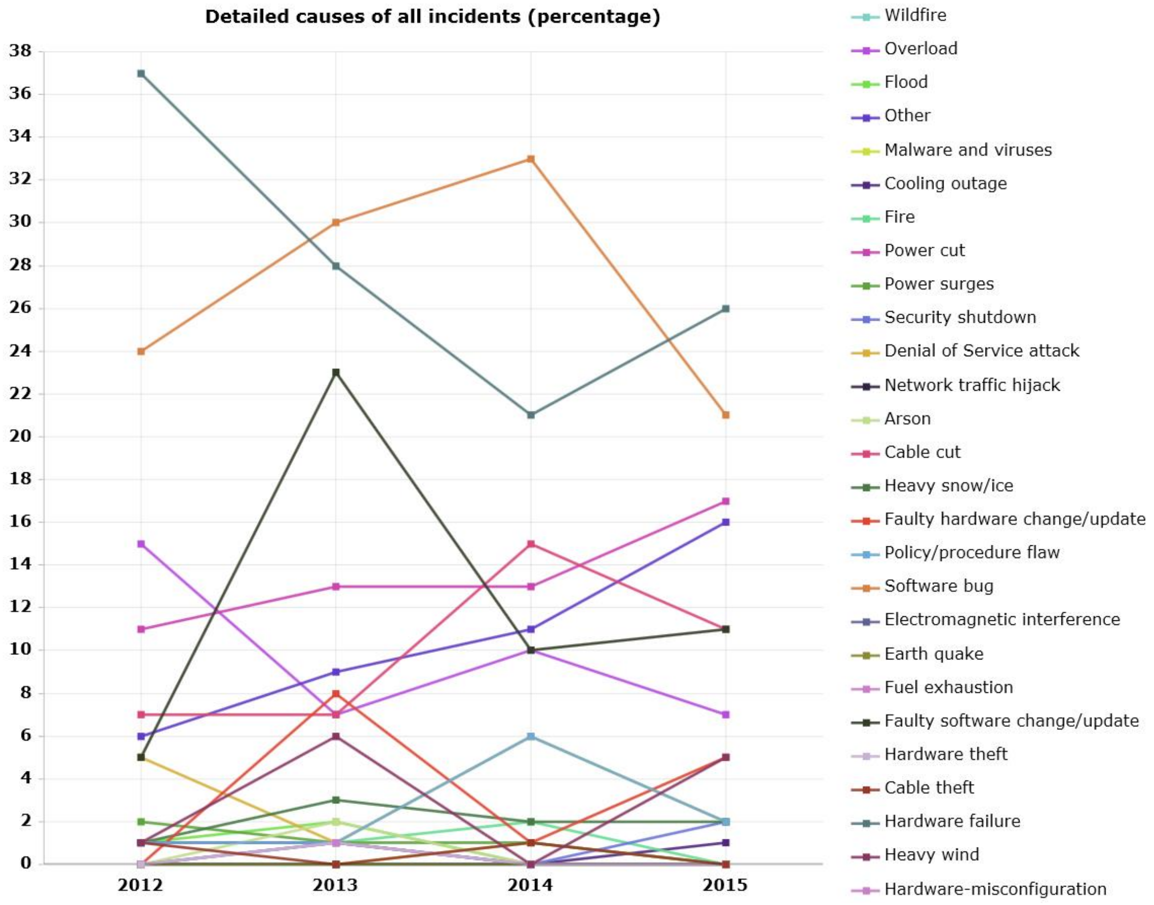


B.5 Average number of user connections affected per route cause category



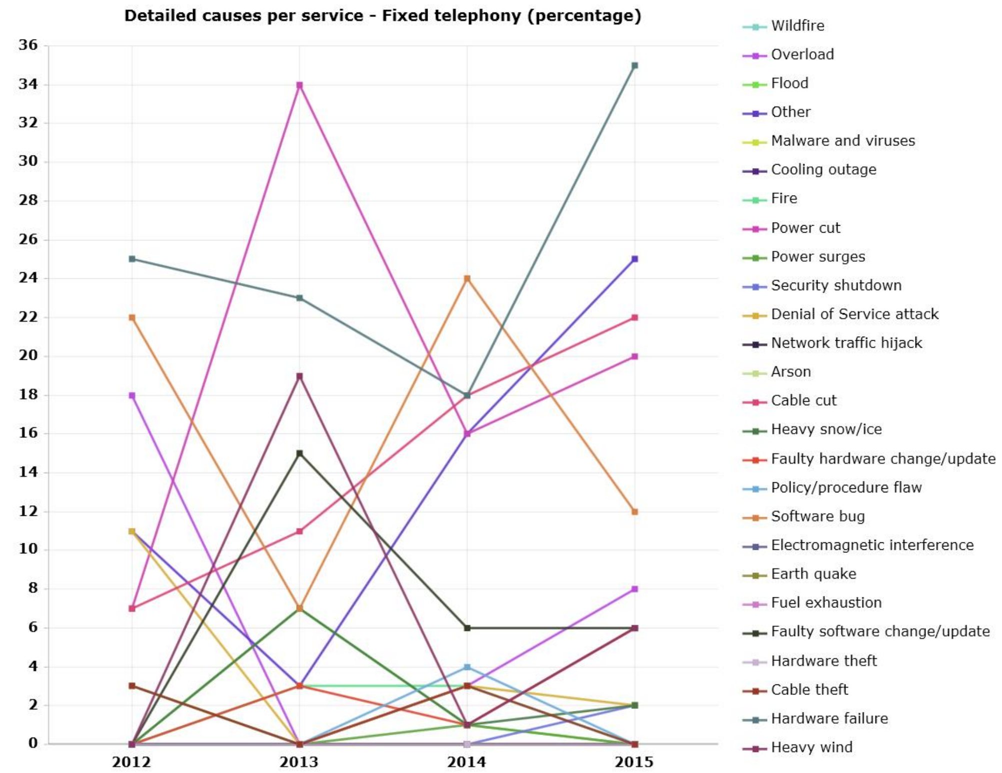
Annex C: Detailed causes

C.1 Detailed causes of all incidents

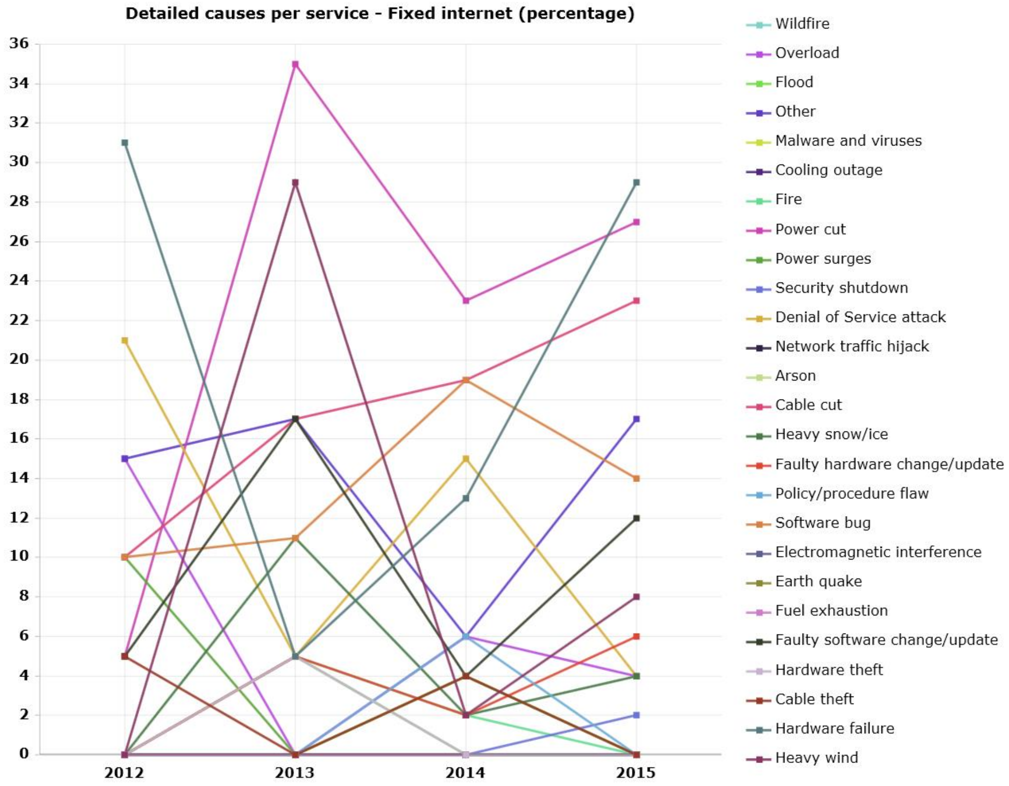


C.2 Detailed causes per service

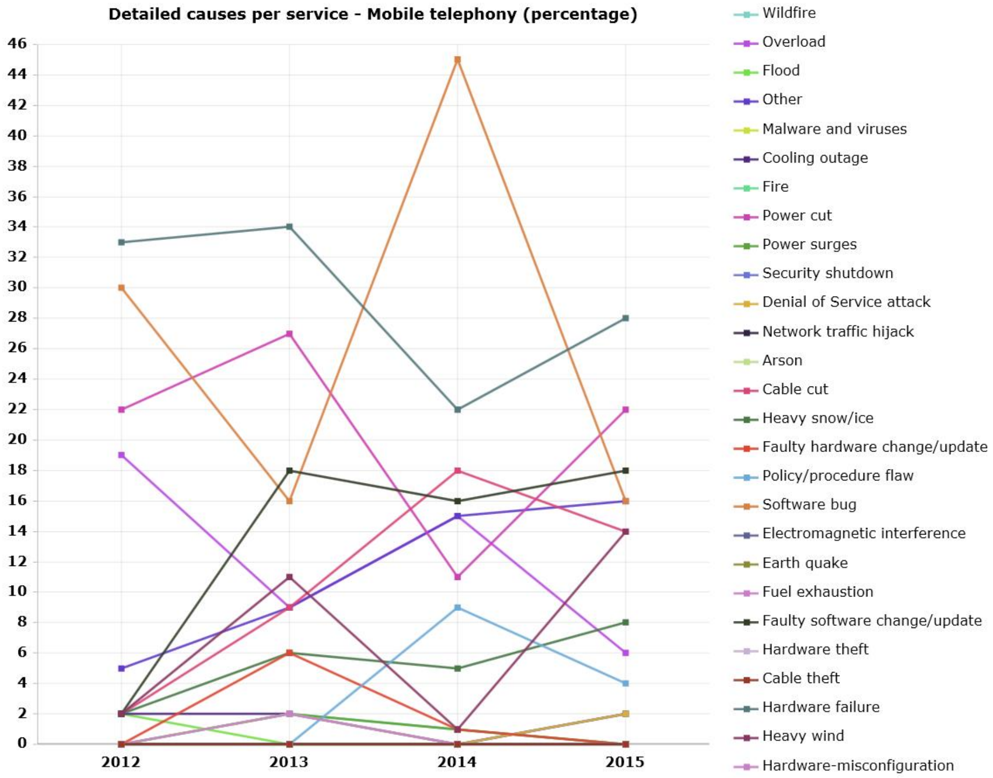
Fixed Telephony



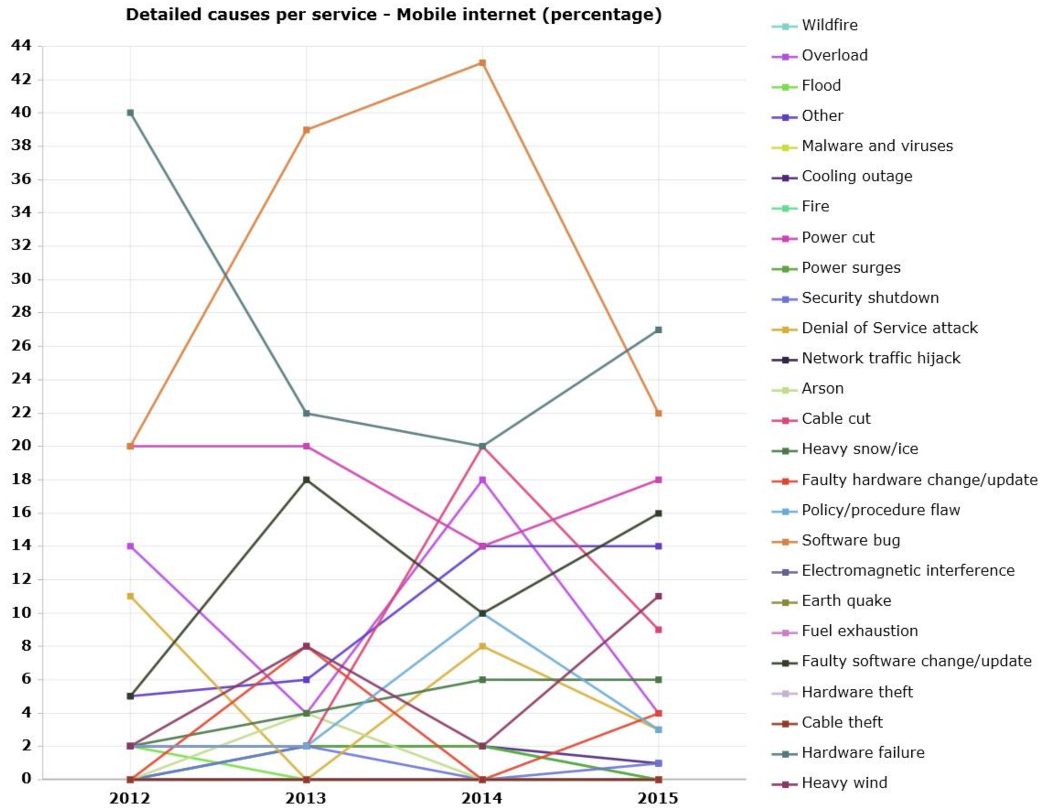
Fixed Internet



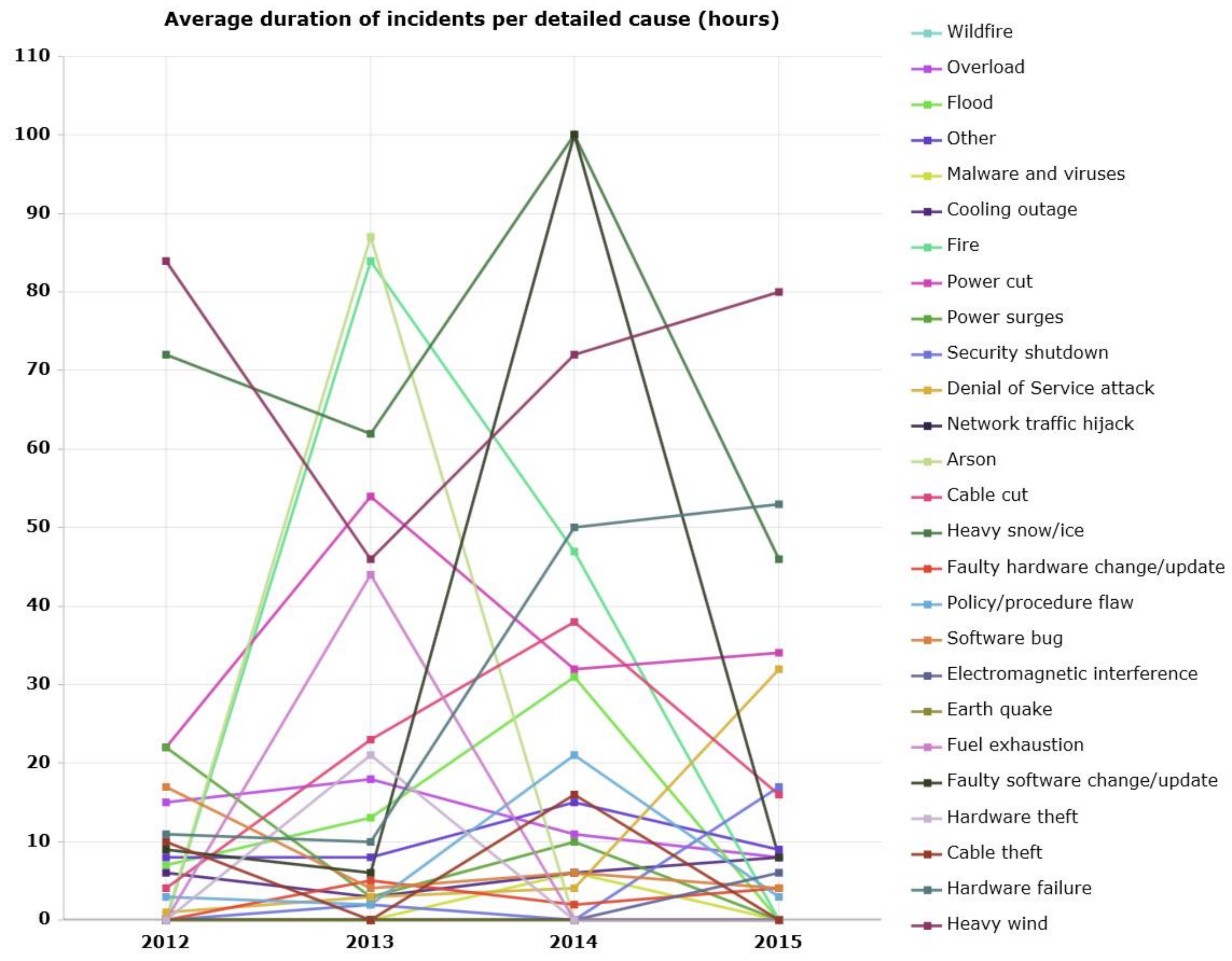
Mobile Telephony



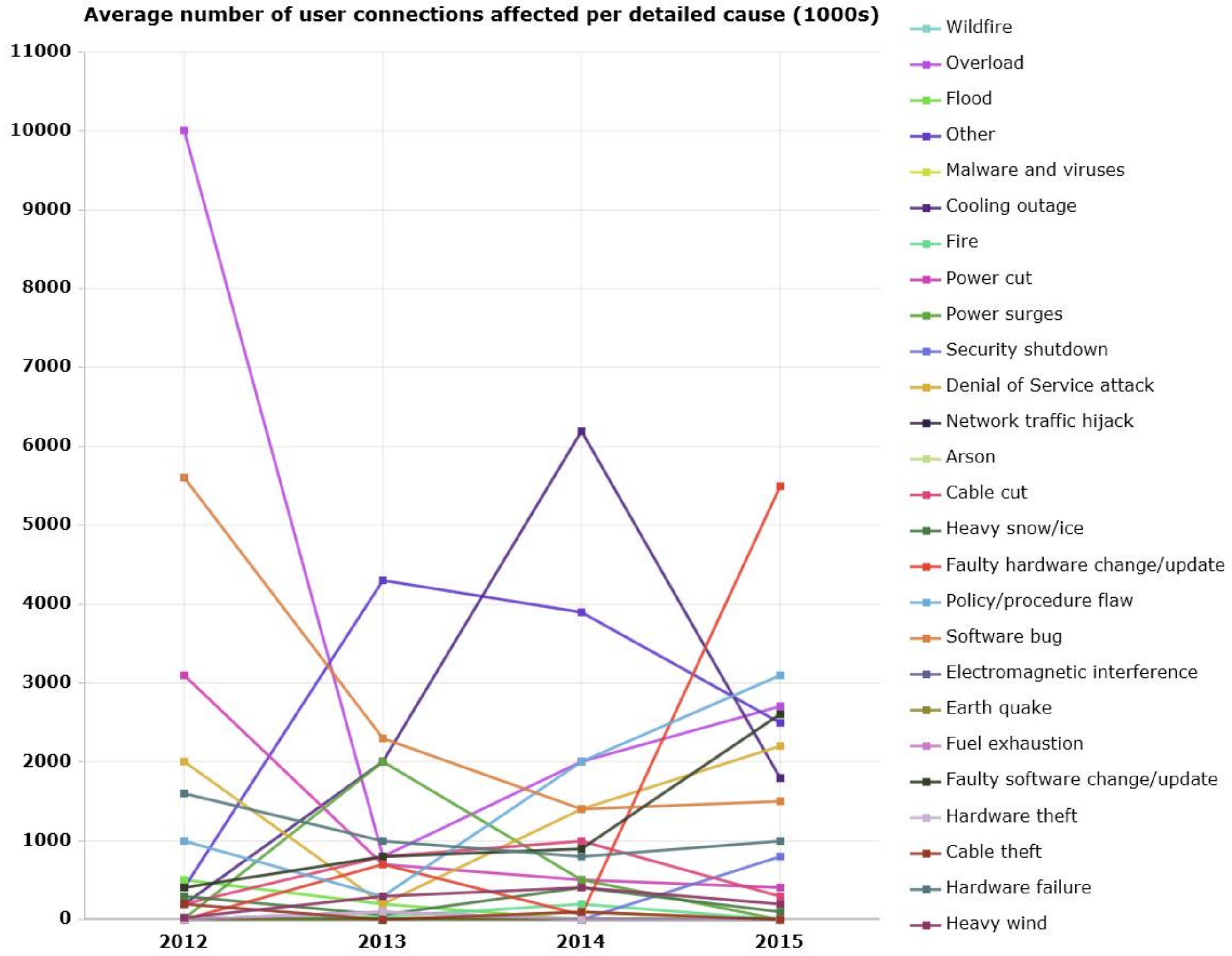
Mobile Internet



C.3 Average duration of incidents per detailed cause (hours)

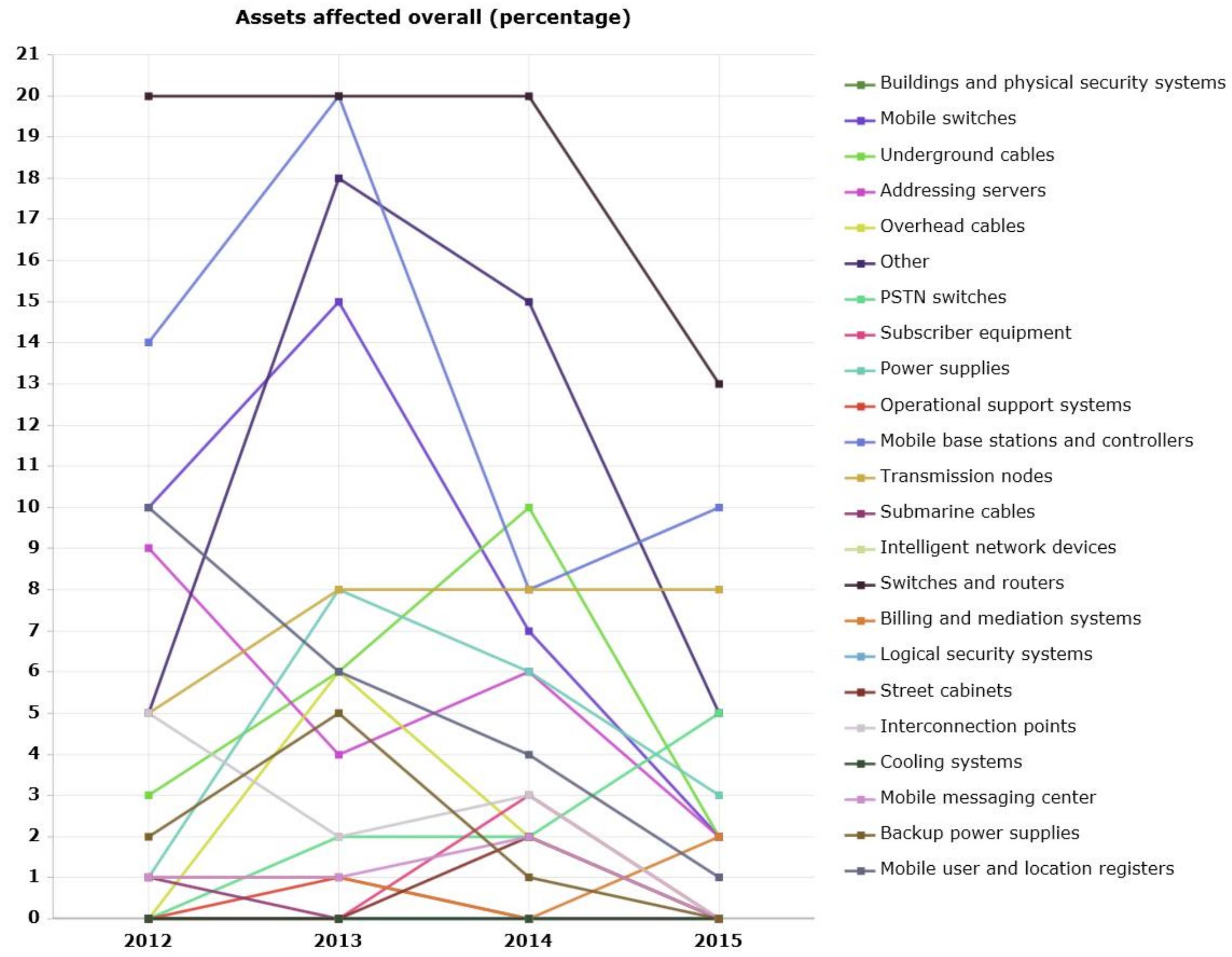


C.4 Average number of user connections affected per detailed cause (1000s)

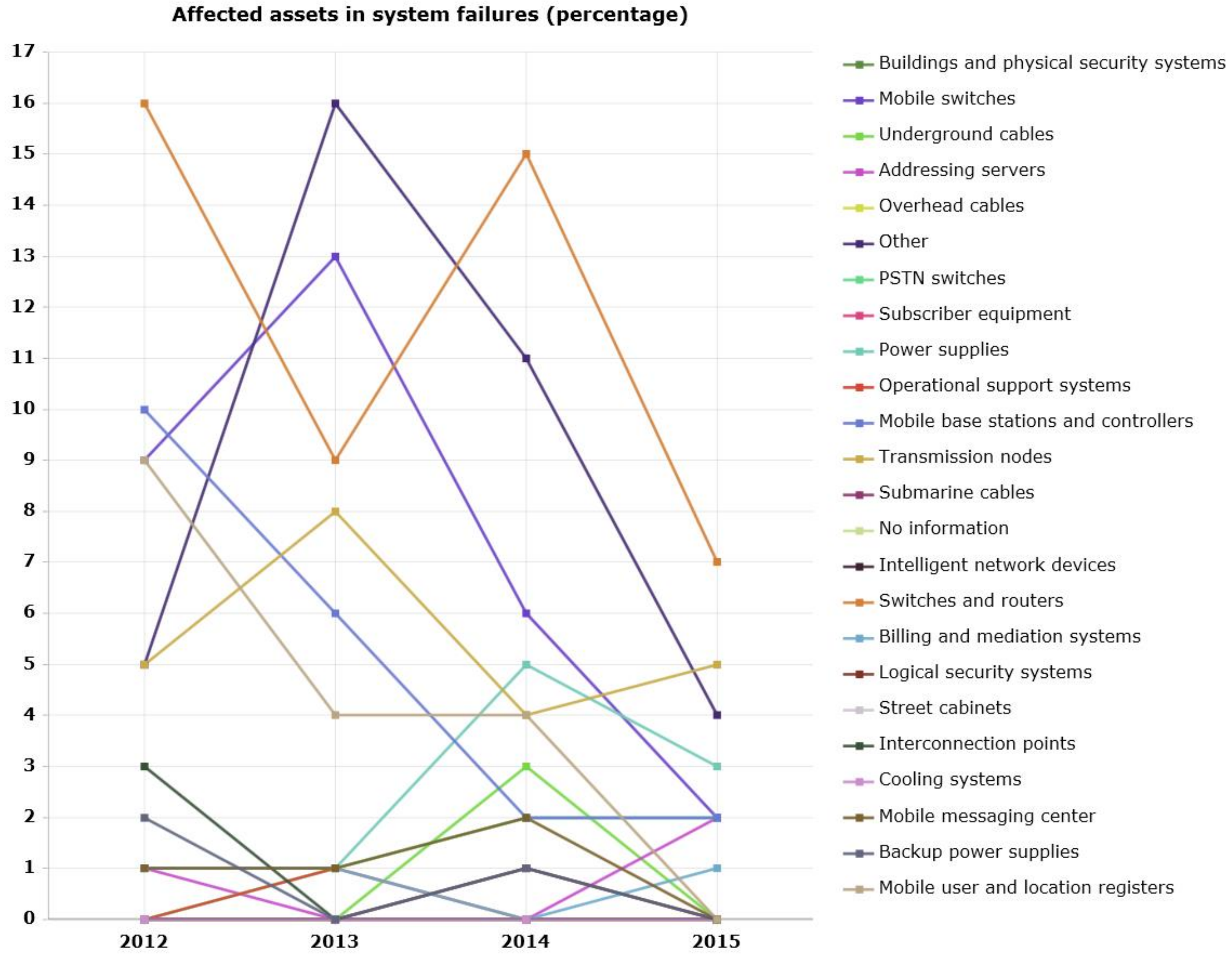


Annex D: Assets affected

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-16-001-EN-N

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

ISBN: 978-92-9204-176-2
doi: 10.2824/10420