enisa

European Network and Information Security Agency

Annual Incident Reports 2011

Analysis of the Article 13a incident reports of 2011

October 2012

About ENISA

The European Network and Information Security Agency (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

Dr. Marnix Dekker, Christoffer Karsberg

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 working group of experts from national regulatory authorities and ministries from across Europe.

PTS (SE), Ministry of Economic Affairs (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT, ADAE (GR), Ministry of Defence (DK), CPNI (UK), RTR (AT), ANCOM (RO), EA "ECNIS" (BG), CCED (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO, CTO (CZ), CERT LT (LT), MFSR(SK), ILR (LU), APEK (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), PT (NO).

Executive summary

For the first time in the EU, in spring 2012 national reports about security incidents were reported to ENISA and the European commission, under Article 13a of the Framework Directive (2009/140/EC) which is a new article in the EU legal framework for electronic communications. In this document we analyse the 51 incident reports of severe outages of electronic communication networks or services.

We summarize the key conclusions that can be drawn from the incident reports. Details can be found in the body of this document.

- 11 countries reported 51 significant incidents and 9 countries reported no significant incidents but this is probably due to the fact that these countries had implemented national reporting schemes towards the end of 2011. The number of users in these 20 countries was 166 million. We estimate that the number of incidents that will be reported over this year (2012) will increase by a factor of 10 because most countries now have mature implementation of the incident reporting process.
- Most reported incidents affected mobile telephony or mobile internet (around 60% of the incidents).
- Incidents affecting mobile telephony or mobile internet affected most users (around 300.000 users). This is consistent with the high penetration rate of mobile telephony and internet.
- Most incidents were caused by root causes in the categories Hardware/software failure and Third party failure.
- Incidents with root causes in the category Natural phenomena (storm, floods, et cetera) lasted 45 hours on average.
- Natural phenomena like storms, floods and heavy snow have a big impact on the power supply of providers. Often these power cuts last several hours.
- The reported incidents show there is a strong dependency on power supply, of both mobile and fixed communication services. It is well known that battery capacity of 3G base stations is limited to a few hours, and this means that lasting power cuts cause communication outages.
- Hardware/software failures are the most frequent cause of mobile communication outages, and this percentage is notably higher than for fixed telephony or fixed internet. This could be the result of higher complexity (more dependencies in the more modern networks like 3G), less redundancy, or simply due to the fact that the more modern networks use hardware and software that is less mature and less reliable.

ENISA, the National Regulatory Authorities (NRAs) and the EC have implemented the first incident reporting almost like a pilot, aware of the fact that implementation across the EU was still not complete. This has produced some crucial insights that would have been difficult to get otherwise – they are summarized in an epilogue.

As part of the activities of the Article 13a Working Group, ENISA, together with the NRAs of the different EU member states will discuss about specific types of incidents, and where needed initiate a discussion on technical guidance for NRAs and providers about preventing these incidents.

ENISA will publish a similar overview and analysis, yearly, following subsequent rounds of annual summary reporting by the NRAs in the EU member states. The next report will be published in spring 2013, and will summarize and analyse the incidents that occurred in 2012.

Table of contents

1 Introduction

For the first time in the EU, in spring 2012 national reports about security incidents were reported to ENISA and the European Commission, under Article 13a of the Framework Directive (2009/140/EC), a new article introduced in the 2009 reform of the EU legal framework for electronic communications. In this document ENISA analyses the received 51 incident reports of severe outages of electronic communication networks or services. We refer to the Executive Summary for a summary of the analysis and the conclusions.

This document is structured as follows. In Section 2 and Section 3 we briefly summarize Article 13a and we summarize the details of the technical implementation of Article 13a, as agreed in the Article 13a WG by the different NRAs of the EU member states. In Section 4 we describe step-by-step how this year the incident reporting (about the 2011 incidents) has been carried out. In Section 5 we analyse the incidents which were reported, and we conclude this paper with some general conclusions (Section 6) which follow from the analysis of the incidents. For the interested reader, as an epilogue, we raise some issues about the process of annual summary reporting itself. These issues are being discussed in the Article 13a Working group.

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. We do not make any references here to specific countries or specific providers. The incidents will be discussed in more detail in the Article 13a WG.

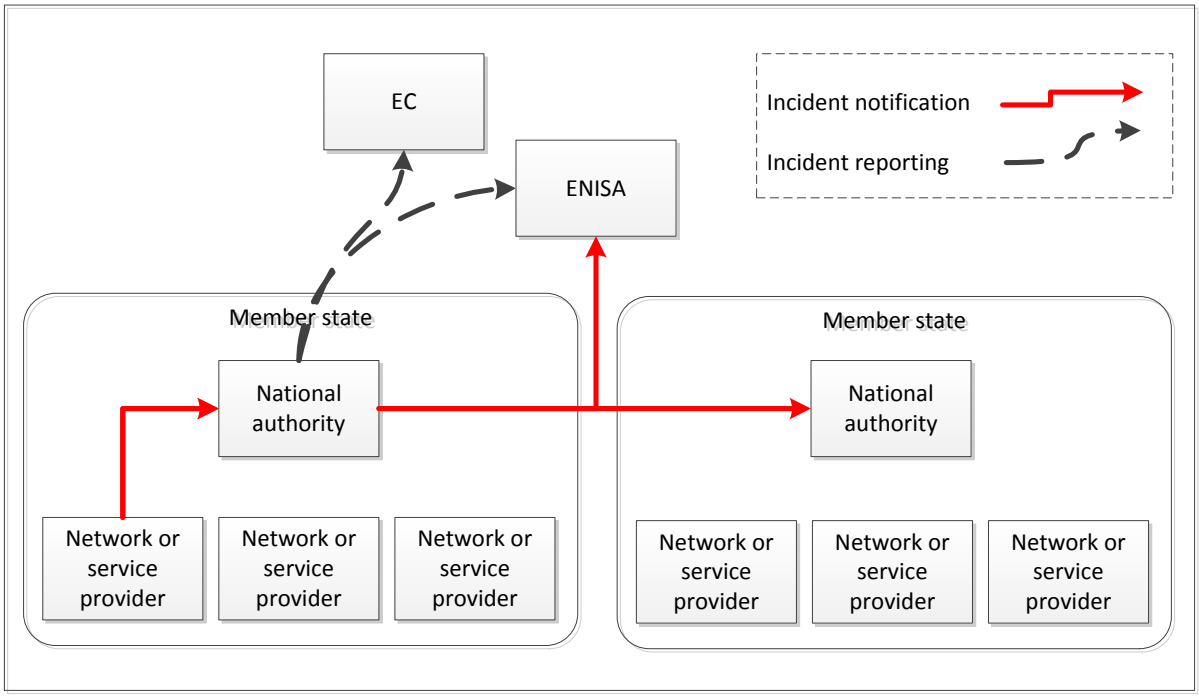
2 Article 13a of the Framework directive: *'Security and Integrity'*

The reform of the EU legal framework for electronic communications, which was adopted in 2009 and came into effect in May 2011, adds Article 13a to the Framework directive. Article 13a addresses security and integrity[1] of public electronic communication networks and services. The legislation concerns national regulatory authorities (NRAs) and providers of public electronic communication networks and services (providers).

Article 13a states:

- Providers of public electronic communication networks and services should take measures to guarantee security and integrity of their networks.
- Providers must report to competent national authorities about significant breaches of security or integrity.
- 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 (EC) about the incidents.

The main incident reporting flows are shown in the diagram below. This document analyses the incidents that have been reported to ENISA and the EC (the black dashed arrow).



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

3 Article 13a Working Group

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 working group of representatives of NRAs, the Article 13a Working Group, reached agreement on two non-binding technical documents providing guidance to the NRAs in the EU member states:

- Technical Guideline for Incident Reporting and
- Technical Guideline for Minimum Security Measures.

The Article 13a working group continues to meet several times a year to discuss the implementation of Article 13a, and to share knowledge and exchange views about addressing incidents. The current version of the technical guidelines (version 1.0) is now being updated (to version 2.0).

3.1 Technical Guideline Incident Reporting Version 1.0

For the sake of reference we summarize the Technical Guideline on Incident Reporting Version 1.0.

3.1.1 Services and incidents in scope

It was agreed with the NRAs to report only about incidents involving outages of services[2]. The services in scope for annual summary reporting to ENISA and the EC are as follows:

- fixed telephony services,
- fixed internet services,
- mobile telephony services,
- mobile internet services,
- message services
- e-mail services

In the remainder of this document we ignore e-mail, because only a few NRAs reported incidents regarding email, and because the total number of users (the basis for the reporting threshold) is often unknown to the NRA. We also merge messaging and mobile telephony for the sake of brevity.

3.1.2 Incident reporting template

The reporting template has the following parameters:

- Services impacted (selection)
- Number of users (percentage)
- Duration (hours)
- Root cause category (see below)
- Emergency calls or interconnections impacted
- Details about the incident

[2] *This does not mean that these are the only incidents that should be considered significant. To give an example: A cable cut of a redundant submarine cable or a security breach at a provider could well be considered significant by an NRA, but if this incident did not cause an outage it would be out of scope.*

- Actions taken to mitigate
- Lessons learnt

It is important to note that the number of users, a percentage, is the percentage of the national user base of a service, not the percentage of the providers' customers[3].

3.1.3 Thresholds for annual summary reporting

The thresholds for annual summary reporting to ENISA and the EC are as follows.

1. **Number of users affected:** The incident impacts more than 15% of the users of the service.
2. **Duration of the incident:** The incident has impact for more than 8 hours.
3. **Geographic spread/region:** The incident has impact in a specific, vulnerable, region, for instance an incident affecting an entire island or a large region with scarce population.
4. **Emergency calls:** The incident has impact on the reachability of emergency call centres (112).
5. **Number of users affected and duration of the incident:** The combination of number of users affected and duration of the incident is in the red area in the diagram below.
6. N**umber of users affected and geographical spread/region:** A service is unavailable for more than 10% of the users, all in a specific geographic area.
7. **Duration of the incident and geographical spread/region:** The service is unavailable in a specific geographic area for more than 4 hours.

	1h<…<2h	2h<…<4h	4h<…<6h	6h<…<8h	>8h
1%<…< 2% of users					
2%<…< 5% of users					
5%<…< 10% of users					
10%<…< 15% of users					
> 15% of users					

3.1.4 Root cause categories

In the incident reports we distinguish between five categories of root causes.

- **Natural phenomena** - For instance storms, floods, heavy snowfall, earthquakes, and so on.
- **Human errors** - Incidents that are caused by errors committed by employees of the provider.
- **Malicious attacks** - Incidents that are caused by an attack, a cyber-attack or a cable theft e.g.
- **Hardware/Software failures** – Incidents caused by a failure of hardware or software
- **Third party failures –** Incidents caused by a failure or incident at a third party.

[3] *For example, suppose a provider with 1 million customers suffers a full outage, and suppose that in that country 10 million people have mobile internet, then the number of users affected is reported as: 10%.*

4 Annual reporting over 2011

In this section we summarize how the annual reporting over 2011 was implemented.

In spring 2012 the European Commission agreed with the EU Member states (in meetings of the COCOM) to do the first round of annual summary reporting about the 2011 incidents. The decision included a recommendation to use the reporting template published by ENISA agreed in the Article 13a WG. Following the COCOM meeting, ENISA implemented the technical procedure by deploying a basic electronic form based on the Article 13a guideline for incident reporting.

In total, 29 countries participated in this process: all EU countries, and some of the EFTA and EU candidate countries. Eleven countries reported in total 51 significant incidents and 9 countries reported there were no incidents. The total number of users in these (20) countries was 166 million.

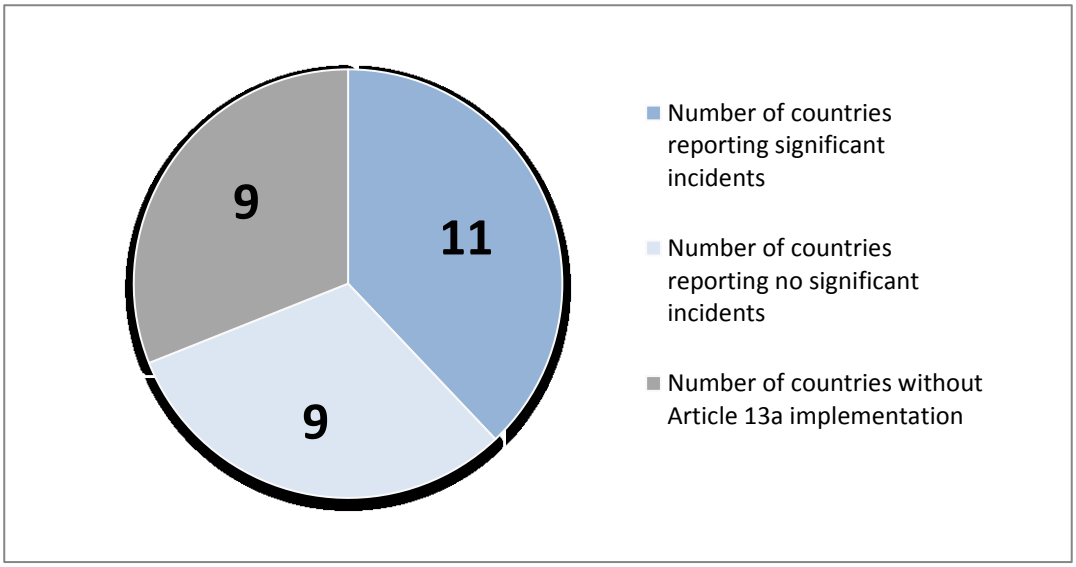


Figure 1: Countries involved in the annual summary reporting over 2011

Many countries implemented Article 13a late in 2011. This explains why so many countries (9) indicated they had not received reports about significant incidents. We estimate that the number of incidents that will be reported over this year (2012) will increase by a factor of 10.

5 Analysis of the Incidents

In this section we aggregate the 51 reported incidents and we analyse them. First we give some examples of incidents (in Section 5.1), then we analyse the impact per service (in Section 5.2), then we analyse the impact per root cause category (Section 5.3), and in Section 5.4 we look at detailed root causes.

We would like to stress that statistical conclusions based on these numbers should be drawn with care. The smaller incidents are not reported at an EU level and this means that the view is biased towards the larger incidents. Moreover many countries had set up incident reporting procedures only towards the end of 2011.

5.1 Examples of incidents

To provide an idea of the different incidents that were reported, we provide some anonymized examples in this section.

5.1.1 Big storm affecting power supply causing large scale outage (days, millions, natural disaster)

A severe storm hit several countries. The storm had a major impact on the power grid infrastructure and to a limited extent also on mobile network equipment (like mobile base stations). The prolonged power cuts eventually caused many mobile base stations to run out of power. As a result around a million users were without mobile communication services for 24 hours, and in some cases up to two weeks.

The dependency of mobile communication services on external power supply is a common theme in many incident reports. Mobile base stations have limited battery power (for 4 to 8 hour), which is enough for everyday power outages, but obviously doesn't help when there is a longer term power grid failure. This sequence of events (natural disaster, power cut, and outage) was frequently described in the incident reports.

5.1.2 Configuration error (hours, millions, configuration error)

An employee of a fixed telephony provider made a configuration error. The error prevented fixed telephony users to make outgoing international phone calls to Western European countries for 4 hours. The incident was resolved after a reconfiguration and a reboot.

5.1.3 Vandalism by former employee affected DSL (days, thousands, malicious attack)

A former employee of a provider deliberately set fire to a switching system, which was used for providing fixed internet service to around 10.000 subscribers. The incident was resolved by replacing the switch. Around 36 hours later the fixed internet service was working again.

5.1.4 Faulty software update affected mobile telephony (hours, thousands, software failure)

A provider applied a regular software update at a Home Location Register (HLR) which turned out to be faulty. The failure at the HLR impacted mobile telephony and internet services. The incident affected about half of the provider's customers and lasted around 8 hours.

5.1.5 Submarine cable cut from anchorage (hours, thousands, third party)

A ship's anchoring damaged one *of four submarine cables connecting two islands. Contingency plans were triggered quickly, which meant that only a smaller number of users were affected.*

5.2 Impact on services

In this section we look at how the incidents impacted the electronic communication services.

5.2.1 Incidents per service (percentage)

Figure 2 shows which percentage of incidents affected which services. Most incidents have an impact on two or more services (in fact the percentages in the chart add up to 175%).

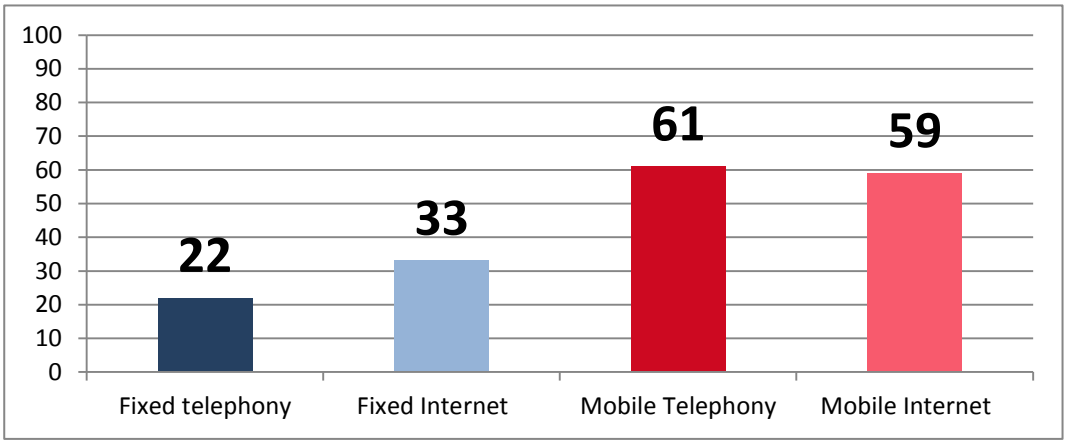


Figure 2: Incidents per service (percentage)

Most incidents (around 60%) affected mobile telephony or mobile internet. This would suggest that mobile services are more at risk of large-scale outages but we stress that the number of reported incidents is still rather small to support such conclusions.

5.2.2 Number of users affected per incident per service (1000s)

Figure 3 shows the average number of users affected, per incident, per service.

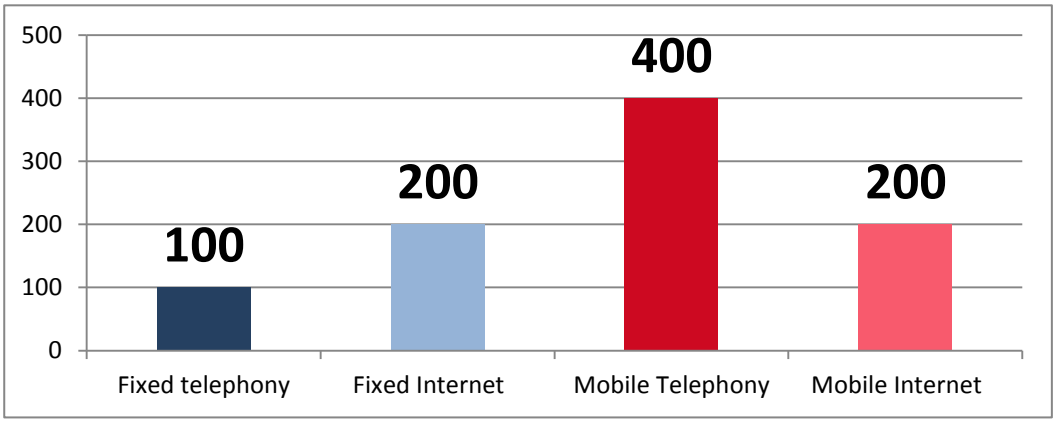


Figure 3: Average number of users affected per incident per service (1000s)

Incidents affecting the mobile telephony involve on average 400.000 users. This is the highest for all services. This is partly due to the fact that mobile telephony has a larger penetration (on average 110% of the population for mobile telephony, compared to 50% for fixed telephony). The next paragraph corrects for this factor.

5.2.3 Number of users affected per incident per service (percentage of national user base)

Figure 4 shows the average percentage of users affected per incident, per service.

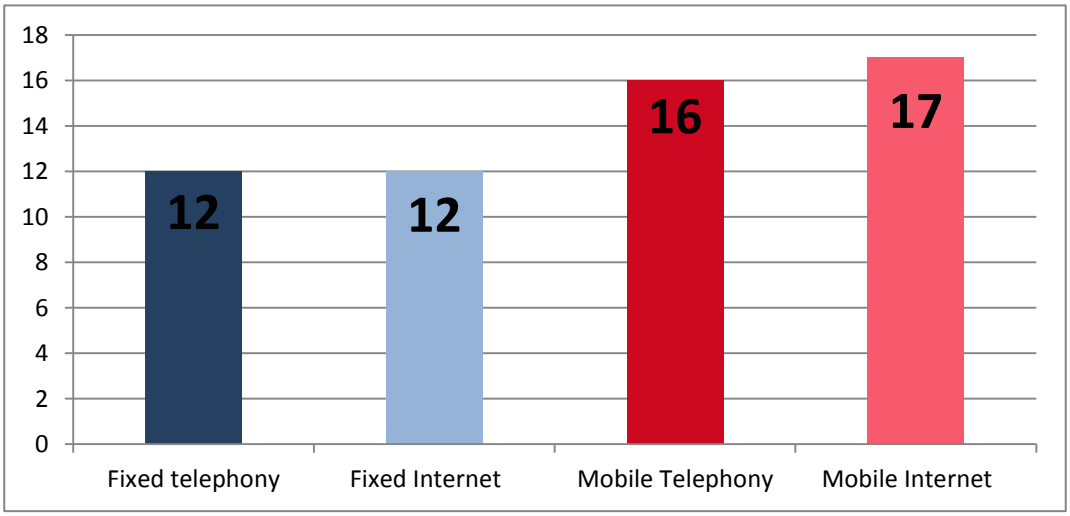


Figure 4: Average number of users affected per incident per service (percentage)

On average, incidents affecting mobile telephony or mobile internet affect 16-17% of the users. This is slightly more than the percentages for the fixed communication services. This would suggest that, not only mobile communication services (telephony, internet) may be more vulnerable, but also that a larger portion of the users is affected in the incidents that were reported.

5.2.4 Impact on emergency services and interconnections

In 33% of the incidents there was impact on emergency services - i.e. the possibility for users to contact emergency call-centres. In only 6% of the incidents there was impact on interconnections.

5.3 Root causes

In this section we look at the impact of incidents, per root cause category. We also split the incidents out in more detailed root causes to give a better view of common root causes.

5.3.1 Incidents per root cause category (percentage)

In Figure 5 we show the percentage of incidents per root cause category.

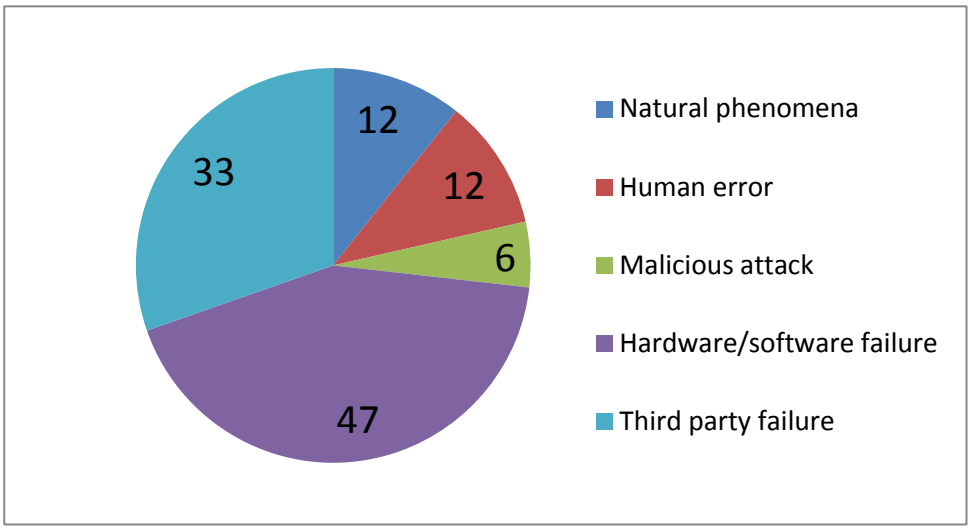


Figure 5: Incidents per root cause category

Most of the incident reports indicate that the root cause falls in the category 'Hardware/Software failure' (47 %) or 'Third Party failure' (33 %).

5.3.2 Average duration of incidents per root cause category (hours)

Figure 6 shows the average duration of the incidents per root case category.

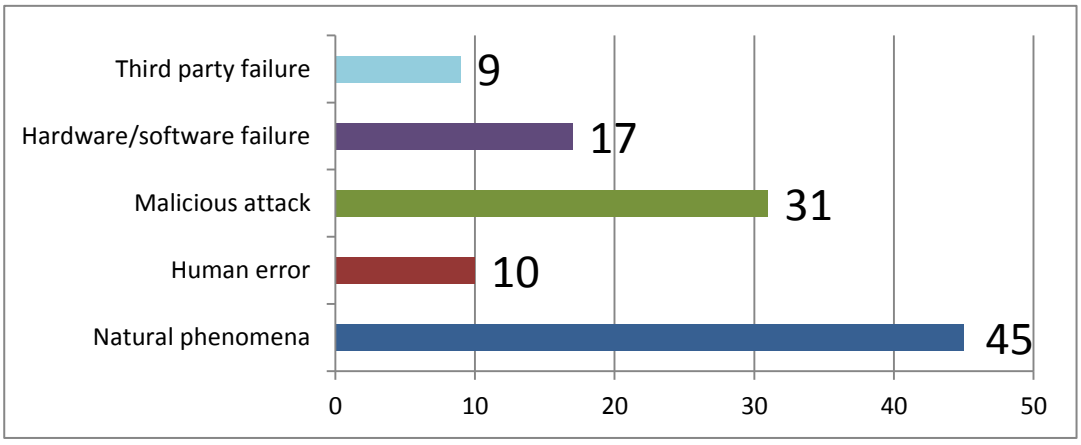


Figure 6: Average duration of incidents per root cause category (hours)

On average incidents caused by natural phenomena lasted longest (45 hours).

5.3.3 Root cause categories per service (percentage)

Figures 7, 8, 9, and 10 show the root cause categories of incidents split out per service.

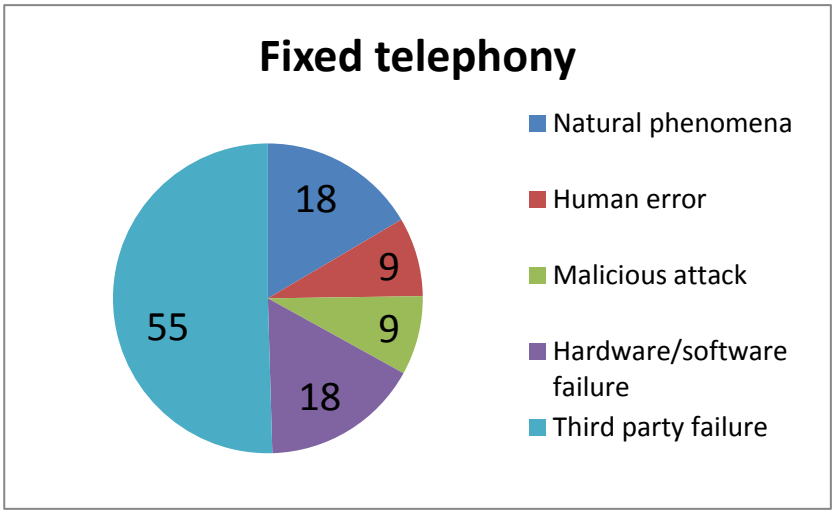


Figure 7: Root cause categories for fixed telephony (percentage)

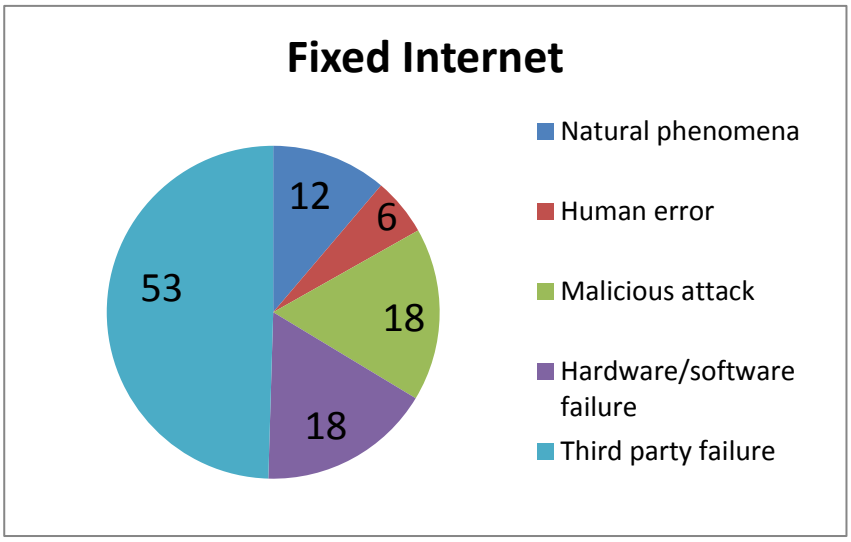


Figure 8: Root cause categories for fixed internet

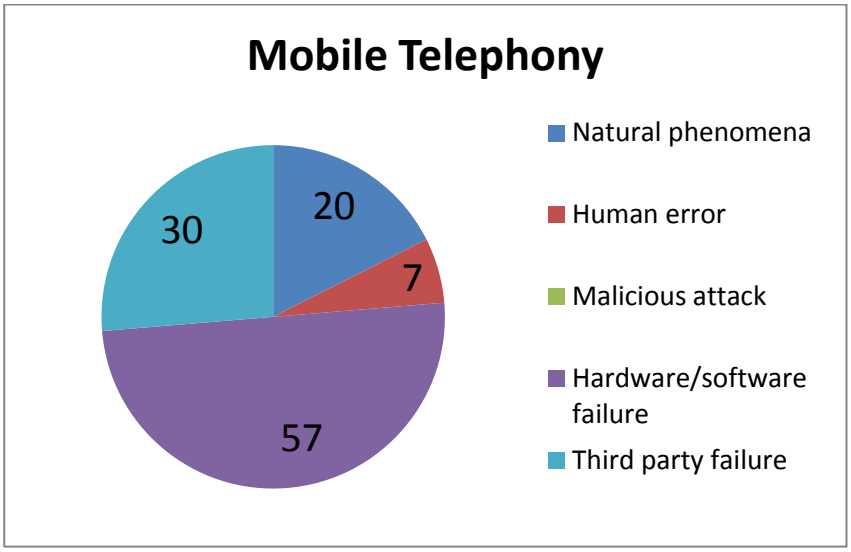


Figure 9: Root cause categories for mobile telephony

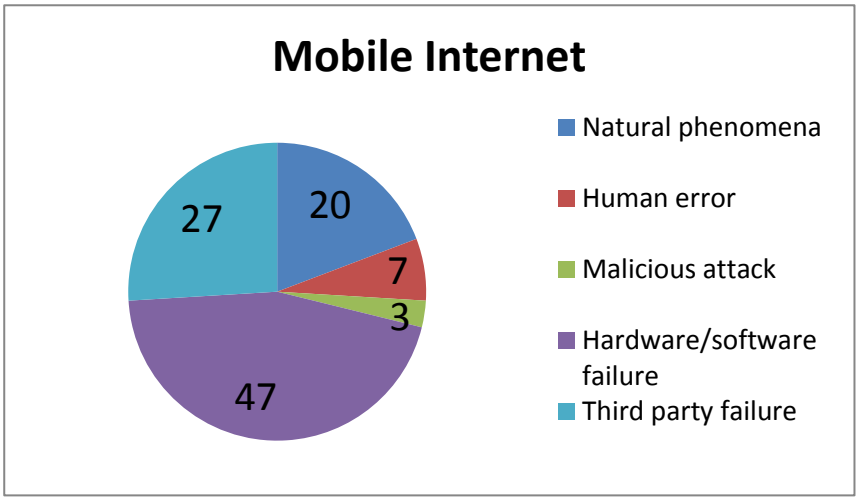


Figure 10: Root cause categories for mobile internet

5.4 Detailed root causes and secondary causes

In this section, instead of looking at the 5 root cause categories, we look at root causes and secondary causes triggering the incident. Based on the textual description in the incident reports, we have identified per incident one or two root causes that lead up to the incident. For example, when a storm leads to a power cut which leads to a network outage then for this incident *both* power cut and storm are counted as detailed root causes. Based on the textual descriptions in the 51 incident reports we identified 14 detailed (recurring) causes which lead up to the incidents.

5.4.1 Root causes and secondary causes (percentages)

Figure 11 shows the percentage of incidents with a certain detailed cause causing it.

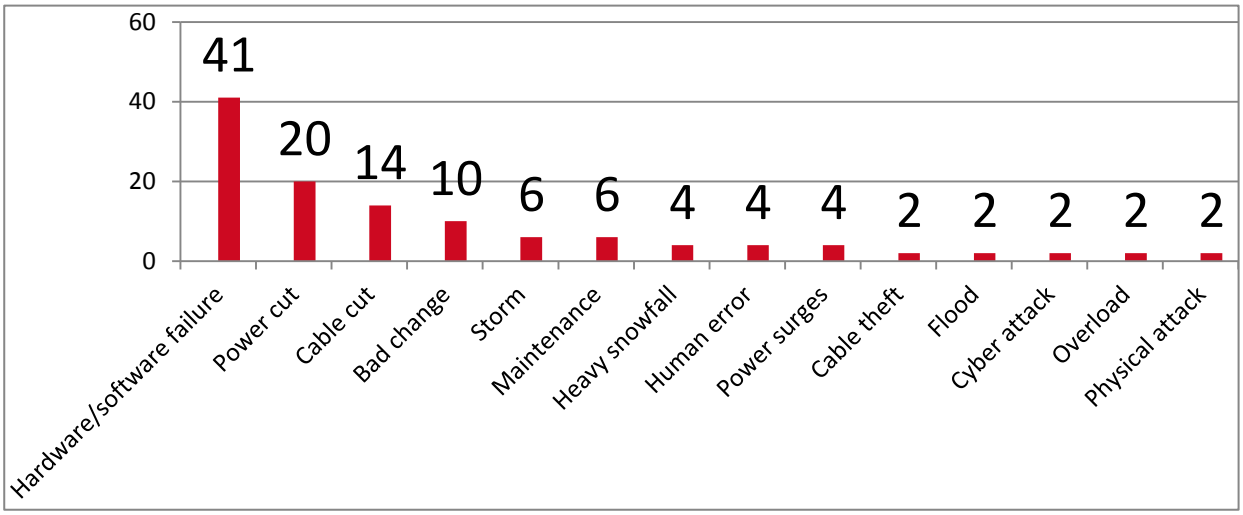


Figure 11: Detailed root causes and secondary causes (percentages)

5.4.2 Root causes and secondary causes (percentages per service)

Figure 12 shows the percentage of incidents per service by a particular cause.

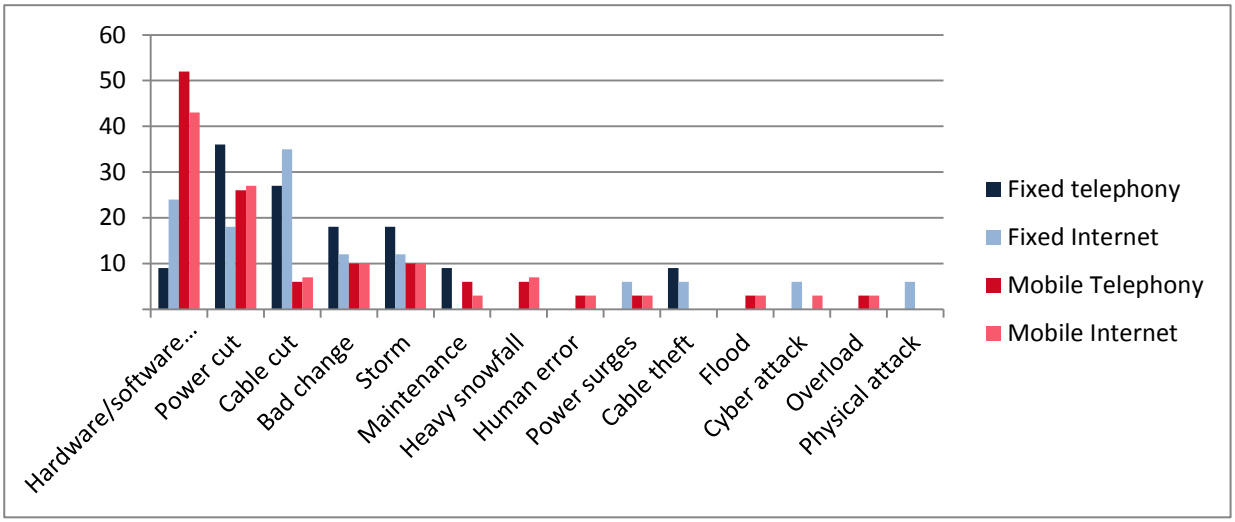


Figure 12: Detailed root causes and secondary causes (percentages per service)

5.4.3 Detailed root causes and secondary causes per service (percentages)

In Figure 13, 14, 15, 16 we show the detailed root causes and secondary causes, split out per service.

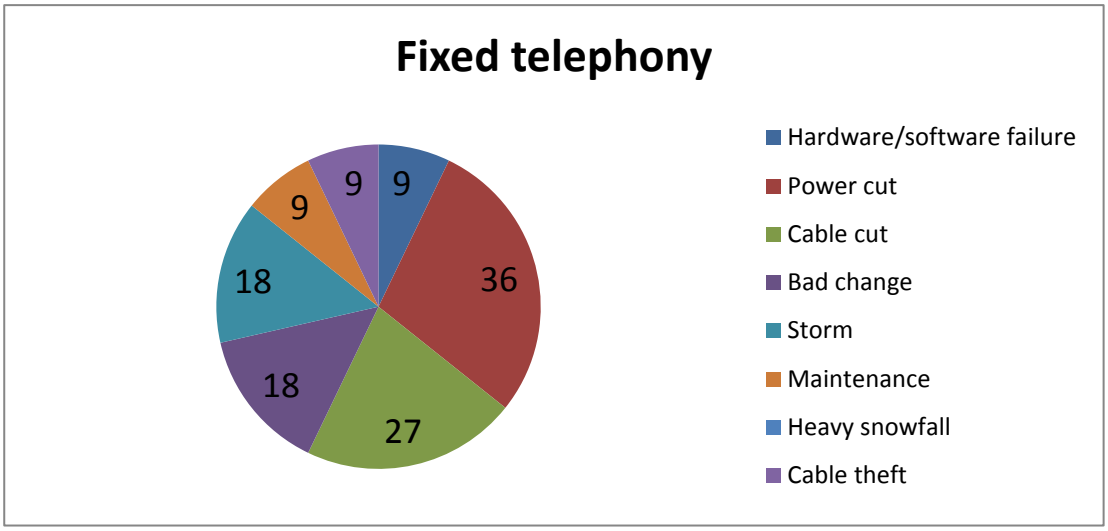


Figure 13: Detailed root causes and secondary causes for fixed telephony.

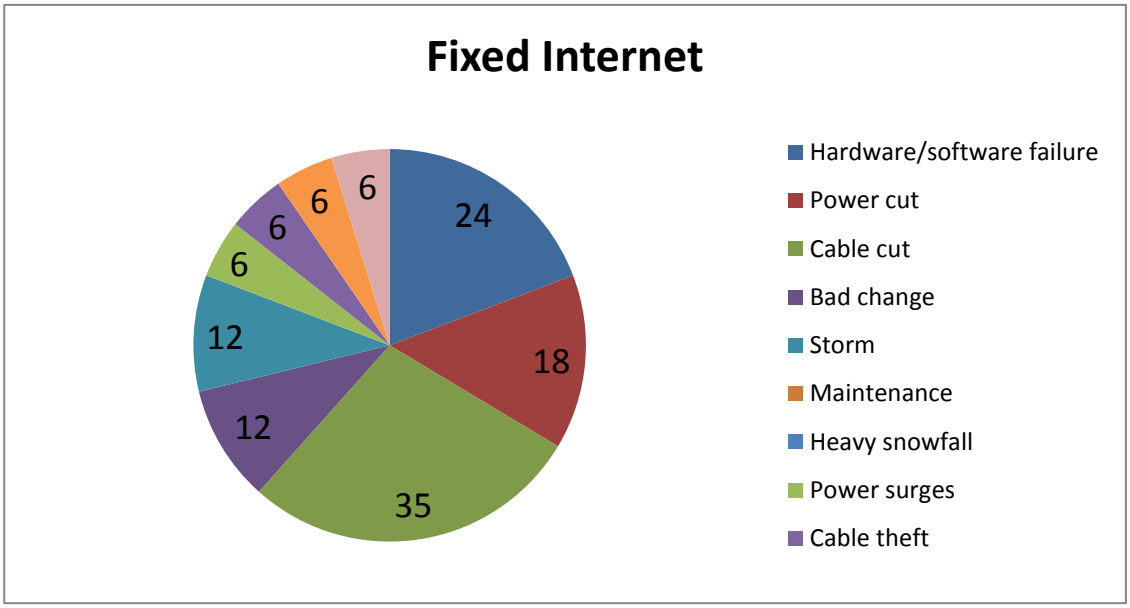


Figure 14: Detailed root causes and secondary causes for fixed internet.

For fixed internet most incidents are caused by cable cuts followed by Hardware or software failures.

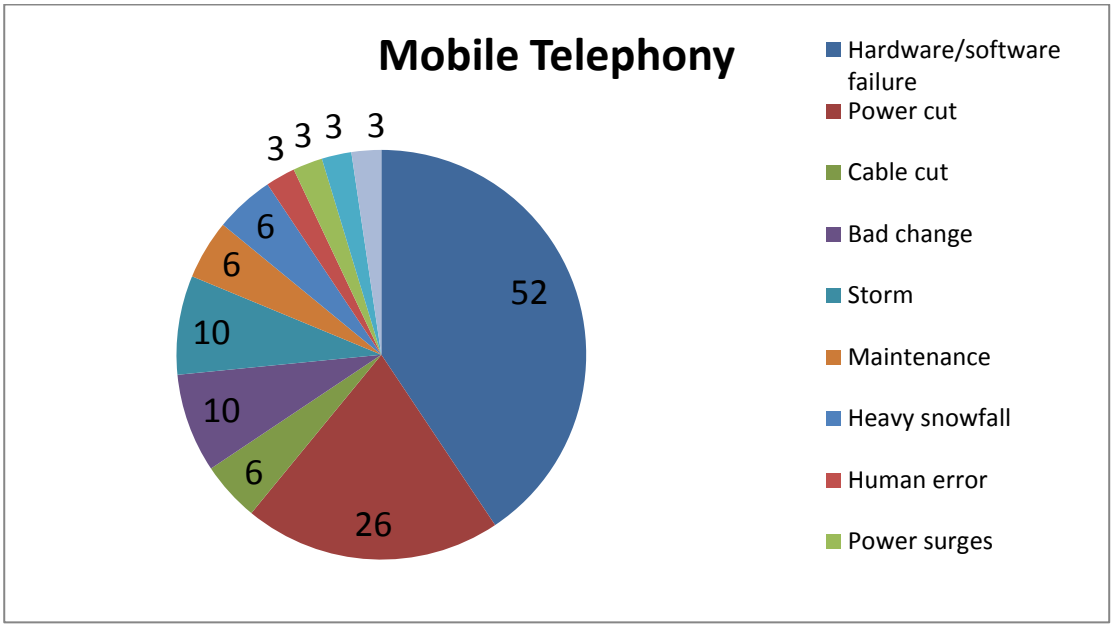


Figure 15: Detailed root causes and secondary causes for mobile telephony.

More than half of Mobile telephony incidents involve (as primary or secondary cause) a hardware or software failure.

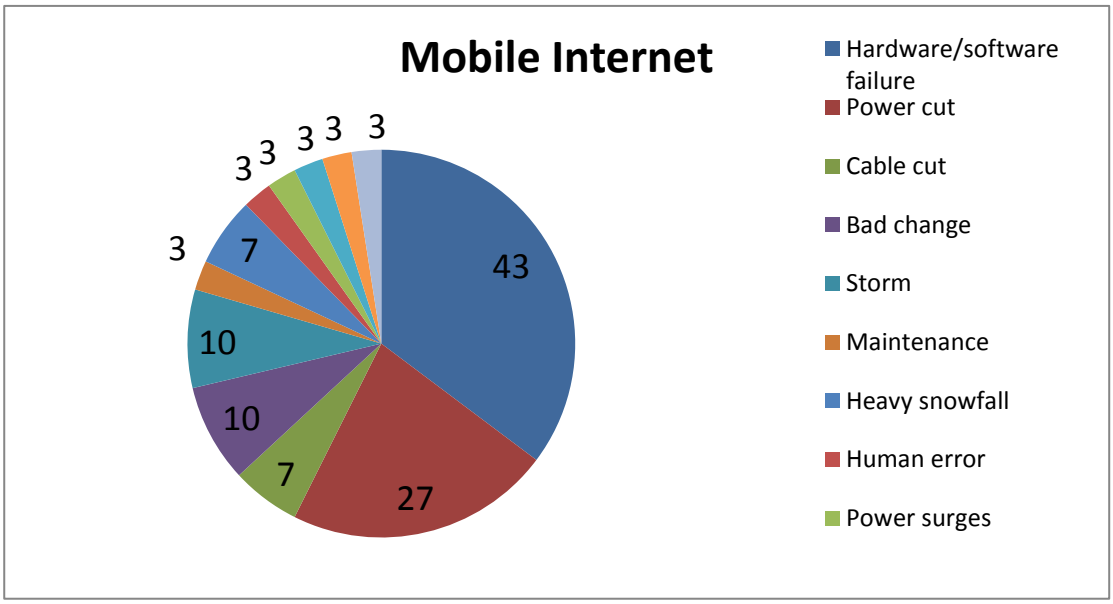


Figure 16: Detailed root causes and secondary causes for mobile internet.

6 Conclusions

In this document we summarized how the incident reporting scheme, mandated by Article 13a of the Framework Directive (2009/140/EC), was implemented across the EU and we analysed the incident reports ENISA and the EC received as part of the first round of reporting: 51 reports about major incidents that occurred in 2011.

From the 51 significant incidents reported to ENISA and the EC, we can draw the following conclusions.

- **Mobile networks most affected:** Most incidents affected mobile telephony or mobile internet (around 60% of the incidents).
- **Mobile network outages affect many users:** Incidents affecting mobile telephony or mobile internet affected most users (around 300.000 users). This is consistent with the high penetration rate of mobile telephony and mobile internet.
- **Hardware/software failures and third party failures are most common root causes:** Most incidents were caused by root causes in the categories Hardware/software failure and Third party failure.
- **Natural phenomena cause long lasting incidents:** Incidents with root causes in the category Natural phenomena (storms, floods, etc.) lasted 45 hours on average[4].
- **Bad weather disrupting power supply causing outages:** Natural phenomena like storms, floods and heavy snow have a big impact on the power supply of providers. Often these power cuts last several hours. In the incident reports we received, incidents caused by natural phenomena lasted 45 hours, on average.
- **Dependencies on the power supply sector:** Dependency on power supply from both mobile and fixed communication services is clear. It is well known that battery capacity of 3G base stations is limited to a few hours, and this means, inevitably that lasting power cuts cause communication outages.
- **Hardware and software failures hit mobile networks more than other services.** Hardware/software failures are the most frequent cause of mobile communication outages, and this percentage is notably higher than for fixed telephony or fixed internet. This could be the result of higher complexity (more dependencies in the more modern networks like 3G), less redundancy, or simply due to the fact that the more modern networks use hardware and software that is less mature and less reliable.

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

ENISA will publish a similar overview and analysis, yearly, following each round of annual summary reporting by the EU member states. The next report will be published in spring 2013, and will summarize and analyse the 2012 incidents.

We would like to take this opportunity to thank the NRAs, the European Member States and the European Commission for the fruitful collaboration, which has allowed for an efficient and rapid implementation of the incident reporting process.

[4] *IPCC (the International panel on climate change) expects extreme weather to have more impact and to be more frequent in the coming years.*

7 Epilogue

ENISA, the NRAs and the EC have implemented the first incident reporting almost like a pilot, fully aware of the fact that implementation across the EU was still not complete. This pilot has provided us with some crucial insights that would have been difficult to get otherwise. For the interested reader we list them here. Note that these issues are currently being discussed in the Article 13a WG.

- **Absolute thresholds:** Reporting on the basis on percentage of users instead of absolute numbers appears to make the reporting unbalanced. Large countries report few incidents, while small countries have to report many (smaller incidents). Absolute numbers for reporting should be introduced to make sure the burden of reporting is proportional to the size of the country and the resources of the NRA.
- **Simplification of thresholds:** Thresholds used in the first version of the incident reporting guideline were sometimes unclear and complicated. Not all NRAs applied all the thresholds. To align the reporting across the EU we are simplifying and reducing the number of thresholds.
- **Impact on networks:** The incident reporting template only mentions the type of service that was affected, for example mobile telephony. But it could be very useful to understand which type of network was affected. This could, for example, show if 2G networks are more resilient in the face of power cuts than 3G networks. The template should allow for additional fields that describe which network is impacted.
- **Use of the reporting template:** While most of the NRAs used, as recommended by the EC, the incident reporting template of the Article 13a WG, some member states did not used this template. In most of these cases vital information was missing from the incident reports, and for this reason these incidents could not be included in the overall analysis. To allow for the incident reports to be included in an overall analysis, NRAs should use the same reporting template.
- **Generic root causes:** Many incident reports mentioned Hardware/software failure or Third party failure as the root cause category. Both categories are quite generic. For example, a power cut which is a frequent cause of outages, would be reported as third-party failure, just like it was a software update by a third party vendor, or the interruption of a network connection managed by a third party. It would be good to use more detailed root causes for the incident reporting.
- **Sequence of events:** In a number of incident reports there was a common pattern in how the incident started. For example, often there was severe weather and then a power cut, followed by the failure or depletion of backup power, causing outage. It would be useful to allow NRAs to report about such chains of events in the incident reporting template. This would also reduce conflicting situations where incidents may be perceived has having one out of two possible root causes, for instance a storm affecting power supply (third party or natural disaster?).
- **Mapping to security measures:** Preventing incidents is the main goal of Article 13a, but there is currently no clear mapping from the incident reports to the security measures (mandated by Article 13a). Incident reporting should include a pointer to the security measures that could have (or should have) prevented the incident. This would allow NRAs (nationally) and the Article 13a WG (on an EU level) to better understand how to prevent future incidents.

8 References

8.1 Related ENISA papers

- The Article 13a WG technical guidelines on incident reporting and on minimum security measures: https://resilience.enisa.europa.eu/article-13
- ENISA's whitepaper 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:
- For the interested reader, ENISA's 2009 paper on incident reporting shows an overview of the situation in the EU 3 years ago

8.2 EU Legislation

- Article 13a of the Framework directive of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf
- The electronic communications regulatory framework (incorporating the telecom reform): http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf
- An overview of the main elements of the 2009 reform: http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu