Resilient e-Communications Networks

September 08

# Stock Taking of Member States' Policies and Regulations related to Resilience of public eCommunications Networks

enisa European Network and Information Security Agency

# Acknowledgements

## About ENISA

This report was conducted by CyTRAP Labs GmbH on behalf of ENISA. It is part of ENISA Multi-annual Thematic Program One (MTP 1[1] ), Resilience of Public eCommunications Networks. With this Program the Agency, among others, intends to take stock of Member States (MS) regulatory and policy environments related to the resilience of public eCommunications Networks.

The stock taking aims at identifying at national level all relevant authorities (stakeholders) and focuses on their tasks, existing policy initiatives and regulatory provisions, exchange of information between authorities and providers, national risk management processes, and preparedness and recovery measures.

The exercise was conducted during summer and involved relevant authorities from EU Member States and EFTA countries. The methodology part of the report fully explains the way the stock taking was done.

The report presents the policies and regulations of 21 Member States and 2 EFTA Countries that finally took part in the exercise. The findings of the report will be the basis for further analysis and discussion among relevant Member States authorities.

Stakeholders could use the findings of the stock taking to identify common approaches, confirm the appropriateness of their measures and activities, and be inspired by the initiatives of other stakeholders from other Member States.

Several people contributed to the success of this report. ENISA's Management Board, Permanent Stakeholders Group, and National Liaison Officers helped us to identify relevant authorities and contacts within Member States. In close co-operation with these high qualified experts ENISA developed a good and well accepted questionnaire that was used as a basis for the stock taking.

Despite the difficult period that the stock taking was planned and executed all experts demonstrated significant interest and commitment. Almost all Member States' representatives participated in the interviews. The interviews actually last more than they were initially planned. Given the tough deadlines of this study the experts had to validate the national reports only within days. The role of our contractor to organise the interviews, prepare the draft national reports, get them validated by experts and finalise this report on time was crucial. We thank them all for their availability, commitment and professionalism.

[1] *More information about MTP 1 can be found under: http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf.*

We hope that this report will evolve in the future by covering more countries. Our intention is to keep it up to date so as it could constitute a good basis for future policy analysis and development.

## Contact details

More information on this report or ENISA's activities on the resilience of public eCommunications Networks can be obtained by

Dr. Vangelis Ouzounis
Senior Expert, Network Security Policies
Technical Department
ENISA
Email: resilience@enisa.europa.eu, Web: http://www.enisa.europa.eu/resilience

## 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 an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated 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 educational and information purposes only. 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.

## Table of contents

# Summary

The Stock Taking of Member States' Policies and Regulations related to Resilience of public eCommunications Networks is part of ENISA's Work Programme 2008[2].

It aims at identifying at national level all relevant authorities (stakeholders) and focuses on their tasks, existing policy initiatives and regulatory provisions, exchange of information between authorities and providers, national risk management processes, and preparedness and recovery measures.

The intention of the study and accordingly of the report is not to assess how well a country is doing or benchmarking Member States against each other. Far from it, instead it focuses on giving an accurate picture of the country's current situation. In turn, the issue is to provide an inventory that outlines the laws and regulations in place and, most importantly, how countries have managed to put the regulation into practice. This includes recommendations, best practice and other measures countries may have chosen to implement to improve resilience of their public e-communications networks.

The report presents 23 different national strategies and approaches that are being used to facilitate, support and strengthen efforts to improve dependability and resilience of public e-communication networks. There is a significant variety in the deployed strategies, policies, approaches and regulatory provisions. Despite these differences, there are certain commonalities that could be highlighted at this stage:

- Develop a national strategy, a solid policy and/or regulatory environment and concrete preparedness measures; define clear roles and responsibilities of involved public agencies; encourage intra- agency collaboration and information sharing,
- Encourage voluntary collaboration between public and private stakeholders and support the development of commonly agreed best practices and guidelines by capitalising on the know-how of experts from both industry and public authorities,
- Focus on how well things are working in practice and foster continuous learning by developing the appropriate mechanisms (e.g. exercises, audits, onsite visits, ..)
- React promptly on reported incidents and analyse them within a trusted group of experts from public and private stakeholders
- Achieving better dependability and resilience of public e-communication networks is a journey not a destination, hence having started yesterday taking many small but frequent steps is more effective than failing to shore up resources now

We do hope that Member States' authorities and other institutional stakeholders could use this inventory of policies, strategies, mechanisms, and measures to identify common approaches, confirm the appropriateness of their measures and activities, and be inspired by the initiatives of other Member States.

[2] *ENISA Work Programme - MTP 1.1. More details about MTP 1.1. can be found in Appendix 1 of this report.*

Hopefully this report will evolve in the future by covering more countries. Our intention is to keep it up to date so as it could constitute a good basis for future policy analysis and development.

Meanwhile ENISA will continue its efforts in this area by analysing the findings of the stock taking. The results of this analysis will be presented at the end of the year.

# Introduction

This report provides the reader with the results of the stock taking conducted about resilience and dependability of public e-communication networks across EU Member States in the frame of ENISAs Multi-annual Thematic Programme 1 - Work Package 1[3].

Before going in-depth into the findings country by country, the approach and methodology used for realising the interviews and producing the reports are explained. Each of the following country reports is based on a phone interview made with governmental experts from regulatory and critical infrastructure bodies in each Member State using a conference call and a survey instrument for interviewing[4]. Each country report follows the structure as outlined below:

- An introduction with information about date and duration of interview, interview participants and authorities concerned;
- A summary of the responses provided by experts, question-by-question;
- References regarding relevant legislation and regulations – these references could be labelled SE 1, HU 1 – labels are again used in the text to allow the reader to find the original document interviewees referred to;
- Additional references pertaining to materials or reports;
- Additional links: URLs of relevant institutions and other important sources

The report ends up with some appendices that provide more information about the study's focus (ENISA research program Appendix 1), the survey instrument used (Appendix 2), the templates provided to countries to receive important information and references (see Appendices 3 and 4).

In short, the reports provide readers a concise overview about the approaches chosen by the Member States towards the resilience of public e-communication networks. Some countries were forced to address dependability and reliability issues of their telecommunications infrastructure through actual crisis (e.g., storms or floodings). Besides such sometimes disastrous events, however, a group of countries use field exercises to test how well things work under difficult conditions. To illustrate, exercises that go beyond the paper-and-pencil approach might play out a field scenario in a region of the country. During the exercise, operators, regulators and government experts have the opportunity to see how certain measures might work or fail to deliver the dependability and resilience levels for public e-communications networks.

Reading each country report allows to draw conclusions while focusing on: a) the practical measures that are used in several countries; and b) the strategies, tools or approaches that can be adapted and transferred to another country.

[3] *See Appendix 1 – project description ENISA – for details.*

[4] *See Appendix 2 for the questionnaire.*

The above will be highly beneficial by allowing Member States to benefit from each other's experience while adapting solutions to their unique political, social and economic circumstances.

# Methodology

This section of the report describes the methodology used for collecting, treating and reporting data.

## Questionnaire development

Initially ENISA had developed a set of questions for the stock taking exercise. This set of questions was shared with Member States during a workshop in Brussels 2008-03-21. Member States also discussed with ENISA the questions and made recommendations for changes.

ENISA incorporated the Member States' suggestions and comments. In turn, it mailed out a revised version of the questionnaire to Member States for feedback and input. Based on the feedback received changes were made to the questionnaire. One of the challenges was to keep questions detailed enough, while assuring that the instrument would not become too long for a telephone interview.

During the workshop held on 2008-06-13 in Brussels, Member States were again given the opportunity to address the questionnaire's content and its focus. During one of the sessions it also became apparent that various terms required refinement. This would then help in assuring that participants were using the same term to mean the same thing. Also, a glossary was given with the questionnaire to make sure, all stakeholders operate on the same understanding[5].

For instance, resilience may mean robustness for some people. In turn, resilience or robustness must be achieved in order to arrive at a level of dependability and reliability (sometimes also called availability) of public e-communication networks that is acceptable to a Member State.

## Preparatory action taken for interview

### *Selection of the sample*

The interviews were targeting different stakeholders in the EU Member States as well as representatives from EFTA members. The interview phase for the stock taking was foreseen from mid- July until the end of August 2008.

Sample selection used the steps as outlined below. First, the contractor was provided with a list of members of the ENISA Management Board as well as the National Liaison Officer from each Member State and affiliated countries. ENISA initiated the first contact with these parties via e-mail, inviting them to participate in the stock taking about resilience of public e-communication networks. ENISA also asked Management Board Members and

[5] *See Glossary in Appendix 2*

National Liaison Officers to confirm the interview participants as identified by ENISA. In addition, recipients of this e-mail were also invited to name additional experts for the interview if they though this would be helpful.

Countries were given a week to respond and, thereafter, the contractor contacted the individuals directly asking for their availability. One challenge was that July and August are when most Europeans take summer vacations. Although vacationing times differ between Northern and Southern Europe (i.e. Southern part is more likely to take holidays in August), it is more difficult to get hold of people during those months than, for instance, during spring. Because of the requirements of the contract and ENISA's work program as approved by its Management Board, the timeframe set for the study required a start in July.

During the Brussels workshop Member States suggested that carrying out one interview with every participating country was the most effective approach. This approach would help to gather all the important facts and insights pertaining to a country's resilience efforts in an effective way. Answering the questions listed in the survey instrument as drafted by the Member States required regulatory, policy/legal and technical expertise about public e-communications networks. In an ideal case, the interview would be done with two to three experts with in depth knowledge about these domains. The experts chosen for the exercise had to be highly knowledgeable regarding the latest technical and regulatory developments and represent more than one authority/ agency. In turn, such an knowledgeable group of participants would be able to adequately present and describe regulatory, technical and other efforts that had and were being undertaken to improve the resilience of public e-communication networks in their respective country Member State[6].

In most cases it took several e-mails before the contractor was able to get the final list of participants. In some cases, it took six to twelve weeks until the experts chosen by the Member State were finally ready to participate in the phone interview. In some instances, it was simply impossible to get access to these experts and in other the experts who had originally committed to an interview, did not come through.

After a few e-mails and possibly phone calls, we usually found a time convenient to all experts representing the Member State. Quite often, one of the stakeholders in a Member State acted as coordinator for the interview. This was very helpful for further interaction. In a few cases, the Member State decided to provide us with different experts than originally suggested to the contractor CyTRAP Labs.

CyTRAP Labs as the contractor did interview all those experts who were accessible for an interview. The final decision about who was to participate and how (e.g., directly in the

[6] *In some countries the individuals recommended by the Management Board Member or Liasion Officer were those that were then participating in the interviews. In other cases, the people recommended had left their positions or felt themselves not qualified to participate.*
*In some instance, the Management Board member was able to help us connect to other parties that were both qualified and authorized to respond. Sometimes CyTRAP Labs as the contractor had to use other means to find the experts needed. In a couple of cases the Ministry invervened and provided us with individuals that it felt were qualified and authorized.*

interview or just by helping to provide written answers) was the Member States' decision to make and they did[7].

### Scheduling of interviews

In the following we present in a tabular overview the timeline of contacts between ENISA and the contractor on one side and the stakeholders in the Member States on the other.

| | |
|---|---|
| Week 27 - beginning July 2008 | Email by ENISA to MB members and NLOs with names of pre-selected stakeholders |
| Week 28 – July 2008 | Email by Contractor asking for availability for interviewing, 2 convenient time slots and telephone numbers. |
| Week 30 – July 2008 | Phone calls by Contractor to stakeholders who had not reacted to emails |
| Week 32 – August 2008 | Reminder email by Contractor to all stakeholders where a date and time for interview was not agreed |
| Week 33 – August 2008 | Reminder email by Contractor to stakeholders where a date had been promised but was not agreed yet (numerous exchanges with several countries) |
| Week 35 – August 2008 | Email by ENISA to all stakeholders where a date and time for interview was not agreed |
| Week 36 – 37 September 2008 | Individual contacts between contractor and stakeholders to further try to achieve an interview. |

**Exhibit 1: Scheduling of interviews**

While scheduling of interviews besides dealing with the fact of people being on holidays was generally not too difficult. However, it required extensive efforts to get the group of experts required to conduct the interview in about five cases. Numerous phone calls and e-mails were required. Here, time spent was way beyond what the contractor had budgeted for.

### *Interview participants*

Who are the experts that participated in the interview? Respondents with vastly different skill sets, experience and responsibilities were part of this stock taking exercise. For instance, in some Member States all interviewees came from the same ministry or authority. Nonetheless, the interviewees brought legal, engineering and policy know-how to the table. In other cases, CERT, cyber-crime, critical infrastructure, defence and privacy experts were part of the interview[8].

[7] *In very rare instances, a Member State did not want to participate in the study. Some countries refused an interview but were, fortunately, willing to write their responses to the questionnaire and support us in other ways.*

[8] *Details about the interviewees and their organisational affiliation are given at the beginning of each country report.*

**Twenty one (21) Member States** participated in this study. The countries included were:

- Belgium
- Bulgaria
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Latvia
- Lithuania
- Luxembourg
- Netherlands
- Poland
- Portugal
- Slovenia
- Spain
- Sweden
- United Kingdom

In addition, **two EFTA member countries** participated in the stock taking exercise as well:

- Norway
- Switzerland

Of these, three countries – Bulgaria, Poland and Estonia– chose to participate by not giving us an interview. Instead, these Member States wrote their answers and submitted these to us. In turn, completing the final draft report required several iterations between Member State and the contractor.

***The conference call system***

The technology used to carry out interviews with the participants was a commercial system that ENISA uses made available to the contractor. This system offers various features but for simplicity's sake we chose the conference calling feature only. The more sophisticated aspects of the system require that the moderator logs into the system on the web. He or she can then invite people beforehand to participate in a conference call. The invited parties receive an e-mail that provides them with a hyperlink for accepting or rejecting the invitation.

Just before the meeting, invited conference call participants can click another hyperlink that makes the system call their phone number. Unfortunately, several of these e-mails sent out by the system to conference call participants got labelled as spam and never reached the intended parties.

Once we had identified this problem we decided to:

- log-on via the web-based interface to moderate the conference call a few minutes before the call was scheduled, take the time to
- enter each participant's number, and
- ask the system to call these numbers to start conference call.

This way the 'spam filter challenge' was eliminated. In turn, once we had agreed with the parties regarding the time and date, we sent them an e-mail in ASCII format to avoid the spam filter problem. In this e-mail, time and date were confirmed.

One to two days before the actual interview, we sent participants a short reminder. Not in a single case did any of the parties involved in one of these interviews miss the time of day or date. Hence, conference calls happened on the time agreed and scheduled without any exception. In turn, not one interview had to be re-scheduled or cancelled due to absences or people being on a mission.

In many cases, country participants chose to gather in one room to participate using a speaker phone. In other cases, we connected several participants in different locations using the conference system. Overall, the conference call system made things quite easy and except for a few disconnects that could not be explained, things went without a hitch.

### *Providing written responses*

Once the time and date was agreed regarding the interview, some Member States chose to submit written responses as well. Some MS submitted these answers before and others after the interview. Again, countries felt that this procedure would make it easier to collect advice and answers from various experts beforehand. In turn, more accurate answers could then be provided.

It was also believed that this would cut down the time for the interview. The responses received in several cases did help speed things along but, as the section below explains, it did not save time. However, it allowed participants to go into more depth and breath regarding the resilience issues to be addressed. In other instances, one or two participants in one country chose to prepare for the interview by writing down their answers. In these cases, we got some of these responses and ideas afterwards.

In all cases where we received written responses, these were included usually in full in the country report. Thereafter, notes taken during the interview were then entered as well. Finally, during the review process of the draft reports most countries added additional information and edited or fine-tuned answers to make sure that it was accurate and correct as it pertained to the particular Member States.

## Interview

As mentioned above, the interview was conducted using a conference calling system. Usually, the person interviewing the respondents from the participating Member State called participants including an officer from ENISA (participating in the interview in silent mode). In most cases there was more than one person participating in the interview as the country reports indicate. In some instances, one person was participating with others nearby, in the room but not on the phone or else several people where connected in from different locations.

### *Interviewing Phase 1*

Due to the matters covered in the interview, the sample selected for interviewing and the approach chosen, validating the questionnaire and interview methodology was not an option before the interviewing started. However, during Phase 1, several measures were taken that allowed changes if needed.

A couple of interviews - Lithuania and Portugal – were conducted in late July by both senior experts from CyTRAP Labs. These interviews were considered to be trials that would allow to fine-tune the interviewing process if necessary. That way we could make sure that both researchers had the opportunity to listen in and see how the other was conducting the interview. As well, sharing the experience and, in turn, assure inter-rater reliability was checked this way. The latter can be assured to a certain degree if interviewers use the same strategies and probing methods when interviewing participants. This approach allowed us to learn from mistakes and improve our procedure.

We conducted the interview with Switzerland on site. This allowed surveying the participants about the interview process. It gave interviewees a chance to provide feedback regarding procedures after the interview process was completed. Important was to see if the approach used was most helpful for people whose first language might not be English. Particularly during this interview, it became obvious that some additional structuring of the information collected was required. Hence, we developed two templates, namely: a) institutional information (agencies involved in resilience and dependability issues); and b) reference and resources list (e.g., what are the important laws, regulations, checklists and so forth).

### *Providing templates*

Based on these recommendations during phase 1 of the interviewing phase of this study, subsequent participants were provided with two templates before the actual interview. Both templates can be found in Appendix 3 and Appendix 4 respectively. On the *first* template, we asked Member States to list the persons that participated in the interview. Each participant was asked some background (e.g., education) and job-related (e.g., job title and responsibilities) information. In most cases, this information is provided about each interview participant in each country report[9].

In some cases, experts from different agencies may have contributed to filling in the questionnaire. However, some of these were not participating in the actual interview. In other cases, when the Member State reviewed the draft report it asked an expert for additional input or information. He or she may have added valuable information. Hence, some countries listed the experts participating in the interview itself as well as those that contributed with expertise or reviewing the draft report only. Member States decided whom they wanted listed. The template also helps collecting information about the agencies involved in dependability and resilience matters regarding public e-communications networks. One list includes the agencies represented by experts in the interview. Another section dealt with agencies that might work in the area of resilience but did not participate in this study[10].

*Template 2* guides countries through the format needed to provide the relevant references and links to laws, regulatory texts and recommendation including but not limited to best practice. Countries wanted to have this information included. However, to make it easier to put together such a list they wanted a template with some examples regarding format. All countries that participated in the stock taking exercise have filled out these templates.

### *Interviewing Phase 2*

Countries participating in Phase 2 were sent Template 1 (Appendix 3) and Template 2 (Appendix 4) at least three working days before the actual interview. Some chose to ship back the templates filled in before the interview. Others chose to do it after completion of the interview. During this phase, each senior researcher conducted several interviews individually. Again to assure consistency, all interviews were written up immediately after they had taken place and exchanged among the interviewers. Frequent telephone de-briefings about the interview process and experience made took place between the interviewers.

### *Interviewing Phase 3*

These set of interviews had to be scheduled right up into the second half of September due to reasons such as vacations, lost e-mails, Member States deciding to change participating experts compared to the initial ones chosen and so forth.

### *Time required*

Most of the interviews took between one and two hours, sometimes a bit more, sometimes a bit less.

[9] *The rational for this information was that a group of lawyers may answer questions slightly differently than a group of signalling engineers. As well, getting an idea regarding job responsibilities may also suggest why certain answers were provided in a certain way putting emphasis on certain things.*

[10] *This was done to provide readers of this report with a quick overview for each country regarding the organization and structure pertaining to the resilience efforts undertaken for e-communication networks.*

The written answers provided beforehand helped to streamline the interview and, therefore, saved time. In general, this was true but it made it also easier for the researchers to dig deeper and ask the experts for clarifications. For instance, whilst the written response may have indicated that a law was in place as well as a regulation, the interview might have revealed that the administering of the regulation was most interesting. For instance, a written regulation about quality of service is applied differently in various countries due to cultural factors, policy preferences as well as political realities. Reading the country reports will reveal interesting pieces of information to readers and allow them to draw their own conclusions.

The very long interviews were often due to many insights shared and this is also reflected in the extensive reference lists countries provided for this inventory. Without countries help regarding listing the appropriate legal texts and sharing with us recommendations and explaining amendments to law approved to increase resilience, the country reports would be far less interesting.

## Writing country reports

Each country report follows the structure as outlined below:

- An introduction with information about date and duration of interview, interview participants and authorities concerned;
- The responses provided by experts, question-by-question;
- References regarding relevant legislation and regulations – these references could be labelled SE 1, HU 1 – labels are again used in the text to allow the reader to find the original document interviewees referred to (laws list which articles are particularly relevant to dependability and resilience of public e-communciation networks);
- Additional references pertaining to materials or reports; and
- Additional links: URLs of relevant institutions and other important sources

Below we discuss the procedures we went through to develop the final country reports as printed in this document.

## Data collection and preparation for analysis

After concluding the interview the researchers analysed the following sources:

- reviewing the notes taken during the interview;
- completing and revising interview notes;
- screening the written answers to the questionnaire by the interviewed Member State;
- collecting information from references as provided by Member States (e.g., laws and regulations); and
- using additional resources from URLs provided by Member States (e.g., CPNI in the UK has an extensive collection of material for public consumption).

## Preparing the draft country report

Based on the information provided above, a draft country report was written. This included the written responses Member States may have submitted previously, as well as the notes taken during the interview. In addition, comments made during the interview were supplemented with footnotes and other material from resources referred to by the experts and cited in the reference list.

Throughout the document, researchers put in questions and comments asking the interviewed parties for more information, clarifications and/or additional details. For example, for an answer such as "General audits are conducted regularly" the following comment was made:

"Could you please specify if these audits are focusing on resilience issues in particular? If yes, how is such an audit conducted (on site, reviewing documents, etc.). How will audit findings be used? Any changes resulting thereof? If so will you follow up and how will this be done please? Thank you for your help"

## Sending draft report for approval to Member States

Thereafter, we sent the draft report to Member States, meaning:

- the persons directly participating in the interview as well as to the
- ENISA Management Board member and the
- ENISA National Liaison Officer for information.

Member States were free to consult about the draft with other experts within the government before providing feedback to the researchers. Generally, one person – the interview coordinator – collected all comments and e-mailed back one document containing all changes and comments to the contractor CyTRAP Labs.

Some countries provided specific examples as requested by us in case clarifications seemed necessary (see end of previous section). Others simply ignored a comment, or provided the necessary illustration including pointing out which article was relevant to the issue. In turn, the regulation did then provide the specific information regarding how the law would be administered and enforced if this was necessary.

## Receiving back the approved report

The feedback received was extremely useful for finalising the country reports. Some Member States were quicker in responding than others; some chose to add a lot of more material to what had already been contributed. In other cases, countries were surprised by the fact that certain materials declared as confidential during the interview, were found on a public websites for citizens to view and comment on.

Once we received the feedback, Member States' changes and additions were integrated into the report. It needs to be underlined that while editing the reports, we refrained from changing or editing texts the Member States had written and wanted it in that way. Nevertheless, the message that countries wanted to get across is clear. Where things seemed too complex or difficult, we took the liberty to adjust things slightly.

## Submitting final draft of report

After the above changes were made all country reports were put together into one report which was submitted to ENISA. The latter than sent the complete report to all Member States including ENISA Management Board members for informational purposes as well as receiving feedback

## Workshop November 12 - 13

The report will be discussed during this workshop organized by ENISA and held in Brussels.

## Country reports

### *Caveat*

We acknowledge each country experts' willingness to provide us with feedback and pointing out errors in their country's report as well as adding additional insights. All mistakes and omissions are, however, our own.

### *Differences between reports*

As the reports indicate they are not all of the same length and depth. Various reasons may account for this as outlined above.

Interesting might also be to see how a country has managed to make things work in practice and if fire drills or exercises have been used to test and see what might work as intended and what might fail.

A careful reader may also conclude that some country reports point out recent developments, shortcomings and other practical measures undertaken to advance resilience and dependability of telecommunications networks. In other cases, the report is more general if not abstract.

As importantly, the reports show that every country has excelled in at least one area. This in itself might provide other Member States with ideas and opportunities that could benefit their own efforts.

# National Report of Belgium

## Introduction

### Interview

Date and Duration 27 August 2008 1 hour and 55 minutes.

| Interviewee | Mr Luc Beirens | Mr Miguel De Bruycker | Mr Rudi Smet |
|---|---|---|---|
| Authority | Federal judicial police<br>Federal Computer Crime Unit FCCU | Belgian Army | BIPT |
| Position title | Chief Superindentent<br>Head of Federal Computer Crime Unit | Major | Senior engineering advisor |
| Education/ Training | Master criminology<br>Master information technology | MIT | M.Sc Eng. |
| Task and Responsibilities | Investigating cyber crime incidents<br>Partner in the governemental platform BeNIS | Cyber Defense CIRC Manager<br>Partner in the governmental platform BeNIS | Network Security<br>Partner in the governmental Platform BeNIS |
| If applicable, rel.ship to ENISA | N/A | N/A | Board Substitute Member – NLO |

Interview with (continued)

| Interviewee | Ms Martine Ducobu | Mr Marc Mattheussens | Mr Dirk Leroy |
|---|---|---|---|
| Authority | BIPT | Federal Public Service for ICT | Federal Public Service Economy |
| Position title | Senior Advisor | Attaché | Attaché |
| Education/ Training | Master in Political Sc. and international rel. | Msc Personnel Management<br>Msc Public Administration | Engineer |
| Task and Responsibilities | Information security policy<br>Partner in the governmental Platform<br>BeNIS | Prevention advisor<br>Information security analyst<br>Secretary BeNIS | Electronic signature – Information Society<br>Partner in the governmental platform BeNIS |

| | | | |
|---|---|---|---|
| If applicable, rel.ship to ENISA | Not directly | N/A | N/A |

**Authorities involved with Network Resilience**

| Authority | FeDICT<br>Federal Public service for ICT | BIPT – Belgian Institute for Post and Telecommunication | Federal Public Service Economy |
|---|---|---|---|
| Main Tasks | Administration for enterprises and simplification, in charge of eGovernment strategy<br>Chairman of the Belgian coordination and dialogue platform of network security | Regulatory tasks in the liberalised telecommunications markets.<br>Supreme authority in specific technical fields such as the electromagnetic spectrum or the numbering space. | Information to enterprises<br>Create the conditions for a competitive, sustainable and balanced functioning of the goods and services market in Belgium |
| Reports to | Minister of Enterprises and Administrative Simplification | Minister of Enterprises and Administrative Simplification | Minister of Enterprises and Administrative Simplification |
| Year established | 2001 | 1991 | 2002 |
| URL | http://fedict.be | http://www.bipt.be/Home.aspx?levelID=1&lang=fr | http://economie.fgov.be |

### Authorities involved but not part of the interview

| Authority | DGCC- ADCC<br>General Direction of Crisis Centre | BELNET CERT |
|---|---|---|
| Main Tasks | Hot standby for federal government 24*7*365<br>It can permanently pick up, analyze and send useful informations to political and responsible authorities.<br>Act as national and international point of contact<br>Planning and coordination of public order.<br>Protection of national and international institutions and security of officials under threat.<br>Coordination of emergency planning<br>Infrastructure offered for crisis management<br>Commission for National Defense matters ( CPND-CNVV)<br>Governmental telecommunications network ( REGETEL)<br>(= the directorate within the Crisis Centre involved with network resilience) | To provide information to the BELNET community and help it to handle computer and network security incidents<br>ELNET CERT is focused on BELNET's customers (Belgian universities, public administrations, high schools and research centres connected to BELNET's network) |
| Reports to | Ministers of Defence and of Home Affairs | Minister of SME's, Self employed workers, Agriculture and Scientific Policy |
| Year established | 1988 | 2004 |
| URL | http://www.ibz.fgov.be/code/fr/loc/crise.shtml | http://cert.belnet.be |

## Scope and governance

Belgium's infrastructure is owned in part by Belgacom (the incumbent operator) and Telenet (the largest cable operator). Those two operators own about 90% of the infrastructure. There are 157 service operators that provide internet access and telecom services (status on 26/09/2008).

### Question 1 : The authorities

In Belgium, two authorities are responsible for matters of resilience of public e-communications networks: a) The Belgian Institute for Postal Services and

Telecommunications (BIPT)[11], set up in 1991; and The Mixed Committee for Telecommunications (Comixtelec)[12], set up in 1957.

The Minister of Enterprises and Administrative Simplification is the overseeing authority of BIPT. The former, together with the Ministry of Defence shares responsibility and has oversight of Comixtelec.

One staff member of BIPT participates in meetings at Comixtelec and is the information linking pin for BIPT with Comixtelec. The cooperation is above all dedicated to coordination matters between the two authorities. Cooperation is the mode of functioning between the various authorities and organisations at different levels in Belgium[13].

A recent royal decree deals with cooperation agreements between federal state and regions and communities (see BE 3 in reference list). Art 106 of the law on electronic communications (BE 1) prescribes the cooperation Comixtelec and telecommunication operators as regards matters of civil defence. It addresses prevention, service continuity, definition of priority services, and so on. In the recent past, the practical collaboration has been limited for various reasons.

**Question 2 : The mandate of the authorities**

The Belgian Institute for Postal Services and Telecommunications (BIPT) is the supervising authority for all public electronic communications networks and services.

The main competencies of the Mixed Committee for telecommunications (Comixtelec) include the supervision of crisis planning in public electronic communications. Comixtelec groups the Ministry of Defense and the national regulator, and is the main authority regarding resilience of public e-communications networks. Currently, its mandate and mission are under review.

The Federal Public Service Economy has in its organisation chart a direction for telecommunication and information society; this direction is not staffed yet.

The Telecom operators act on a minimum of level of resilience. A regulation following Art 114 of the law on electronic communications (BE 1) on obligations regarding security measures and resilience of communication networks is still missing and no practical – non-regulated- solutions are in place.

The Belgian Network of Information Security (BeNIS) is a Dialogue Platform that has been created by Federal Ministers Council on 30/09/2005. This group has written a White Paper (BE 8).

[11] *In Dutch BIPT – Belgisch Instituut voor postdiensten en telecommunicatie; in French IBPT – Institut Belge des service postaux et des télécommunications*

[12] *Gemengde Commissie voor telecommunicatie - Commission Mixte de Télécommunication*

[13] *In the ICT Regulation Tool Kit, Belgium is described as a system where "regulatory bodies are established as corporate bodies"*

BIPT, the FPS Economy, the Ministry of Defense and FeDICT, work together in different advisory groups.

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

The electronic communications act stipulates that operators should take all necessary measures to assure continuity of its service offering (see BE 1 in reference list). The measures to be implemented by the historical operator (incumbent operator – Belgacom) under the universal service provision have been defined (see BE 5). Their application to other operators is currently being prepared. In order to facilitate this implementation, BIPT has established an inventory based on a survey among operators which started in February 2007 and is still going on (see also Q 7).

The operators were quite reluctant to cooperate in this survey and to provide information. Here as well, a regulation following article 106 of the electronic communication law (BE 1) that would stipulate that operators have to respond to such requests for information would help efforts regarding resilience. Currently, BIPT has no mandate to request that type of sensitive information.

In case of national crisis the National crisis coordination centre gathers all the preparation, planification and coordination of the civilian and military assets missions (BE 6). Comixtelec (BE 8) with its constituents BIPT and the military would be one of the advisors providing the National crisis coordination centrer with information about the e-communication networks in case of a national crisis.

The BeNIS platform has developed a white paper on information security policy based on a number of projects. This white paper has been forwarded to a coordination committee on security (BE 7). One of its recommendations is to establish a national CERT. This CERT could be run as an independent department (BE 7). The White Paper is seen as a Guideline for the government to put the necessary budgets and human resources in place to help in particular further improve network dependability and resilience in Belgium.

As regards future strategies, a working group (under the BeNIS platform) of representatives of different federal public services is discussing the ongoing critical issues for the ICT-sector and proposing possible measures to be put in place. Contacts will be held with different parties from the different sectors to come to sector specific emergency planning: ISPs, IAP, operators, data centres, Government and manufacturers.

**Question 4 : Initiatives between providers and public authorities**

The act on electronic communications (art 114-115) (BE 1 in reference list) imposes a series of obligations regarding security on operators. Besides, Article 115 defines the priority categories of restoration in case of infrastructure disruption. Moreover, the authorities imposed additional measures on the historical operator through flexible protocols, notably regarding the warning and information process. The security measures imposed on the historical operator are financed by the operator. There is a dedicated budget for these measures, specified in a contract – a so called contract of management - between the historical operator and the Belgian State.

The Minister of Public Enterprise and Administrative Simplification is currently negotiating on the security measures to be implemented with the incumbent Belgacom. BIPT takes part in the negotiations and acts as technical advisor.

Following a recent incident where 80,000 people were off-line for 8 hours as consequence of a cable cut by a contractor, a review was undertaken. The five largest operators ( by turn-over) hold 80% of the market are: Belgacom (fixed), Telenet (fixed), Belgacom Mobile (mobile), Mobistar (mobile), Base (mobile).

Concerning initiatives among providers, Belgium is currently preparing a regulatory framework regarding the means of cooperation between providers. These will be integrated into a national CSIRT/CERT. The latter still requires first, approval and, second, subsequently allocating the necessary budgetary resources must be secured before anything can be done.

Initiatives known at the time are:

- Meetings of a group of operators with AGORIA which is the Belgian private business sector organization where most operators are member. IBPT takes part in such meetings.
- BELTUG is the Belgian Telecommunication User Association. Its membership comprises 200 very large users mainly from the private sector. Some public administrations are also members of BELTUG.
- The Consultative Committee on Telecommunications brings together telco operators, trade unions, and other stakeholders. BIPT runs the secretariat of this Committee.

## Tasks

### Question 5 : Typical task

Among the typical tasks of the authorities in Belgium are the following:

- BIPT holds regularly consultations with the sector by means of questionnaires published on its website.
- Information exchanges happen into the framework of the agreements between the historical operator and the civil and military authorities.
- In order to enforce regulations, additional competences have been assigned to the national regulator regarding the coordination of the network security policy.
- A decision about carrying out audits has to be made yet.

Currently, BIPT is neither able to perform any kind of onsite checks nor carry out supervising tasks. Such work is restricted to the exchanging of written questions to the operator and receiving an answer. In part this is most certainly due to lack of human capital available to perform these important tasks.

### Question 6: Exchange of information between providers and public authorities

Exchange of information regarding the resilience of the networks takes place in the framework of the agreements between the historical operator and the civil and military authorities. Other than that, information exchange is limited as operators resist due to claiming that it is proprietary information. Only incidents which become publicly known are reported to BIPT. For the reporting, no standard formats or maximum delays in time are given.

Among measures taken to close the information gap, operators are contacted by BIPT, sometimes on site visits are made and it is controlled whether an operator found remedy for the incident. Nevertheless, as pointed out under Q 5, in practice, it is difficult for BIPT to perform these tasks.

### Question 7 : Handling of security incidents

When there is a breach of network integrity or dependability, operators have an obligation to inform the regulator and consumers about this incident (Art 114 of Law 13.06.2005 BE 1). A regulation following this law outlining exactly how this may work in practice is still missing. In the current setting, any kind of information can be disclosed at the request of BIPT and the Mixed Committee for telecommunications (Comixtelec).

Since 2003, working groups on network and information security are dealing with the issues. It is expected that the future national CERT might be ask to assess regulatory compliance in the area of incident reporting. How this will work in practice is still unclear.

Possible Changes: While BIPT has the mandate to regulate, it has so far not undertaken any steps to address with public telecom operators and service providers what information must be disclosed, to whom and under which conditions. For instance, based on the survey BIPT initiated in 2007 (some operators refused to respond so far – see Q 3), mutually acceptable and workable procedures should be developed that facilitate information gathering and response work undertaken by operators.

### Question 8 : Audits related to resilience

Audits of providers related to resilience are not done at this point. BIPT claims that limited resources neither allow doing any audits nor assessments today. Similarly, because operators are not required to provide information about incidents to the regulator, enforcement is more theoretical than practical.

Possible Changes: Similarly to other countries, Belgium might establish a working group between operators (i.e. infrastructure owners) and the regulator. The group may subsequently develop best practices that are thereafter followed by all operators. In turn, the regulator could assessments to see if these best practices are being followed and where improvements might be needed. Information collected through assessments and shared by the regulator, with group members, may further facilitate practical steps that can be undertaken to improve resilience of public e-communication networks in Belgium.

### Question 9 : Enforcement actions

The general conditions provide for the following penalties: fines and/or the withdrawal of the right to operate a network or services. The management contract between the historical operator and the state provides for universal service provision, service assurance and continuity.

However, because of the limited information exchange between infrastructure operators and the regulator, it is unclear how Belgium enforces these laws in telco sector. As well, how such enforcement efforts have helped in improving resilience and dependability of public e-communication networks is not very well known (i.e. not documented).

## Risk Management and preparedness measures

### Question 10 : The national risk management process

A national risk management process for Belgium is not yet in place. However, there are national crisis management centres, particular web pages, reference lists and similar provisions addressing the resilience of public e-communication networks.

The Belgian Defence Ministry has done risk management exercises; these were not shared with other authorities due to lack of communication. In order to improve sharing of information, the Belgian Defence Ministry permitted BeNIS to share information with other agencies and stakeholders.

The CERT system of the Ministry of Defence has been presented and it was explained how the exercise was planned, executed and what was learned from it. However, due to lack of interest there was no follow-up[14].

Currently, everybody is waiting for the decision on the national CERT. Besides the CERT it would be important to have an agency that would be in control in an eventual crisis and would coordinate efforts and resources amongst different actors in case of a national crisis. But so far, the government has other issues to address first.

As a reaction to the White Paper (BE 7), BeNIS has been asked during 2008 for an estimation of cost for all the measures asked for in the White Paper.

Possible Changes: While a national CERT is an important step, most countries have decided to move on several fronts taking small steps to improve resilience. Here Belgium has to begin to improve its regulatory work regarding resilience and public e-communication networks. Starting on the journey today by taking small steps might be more feasible than waiting to get government approval and budget for a giant leap forward.

[14] *Information was available to stakeholders but not any stakeholder group made a request to get and share more detailed information with BeNIS.*

### Question 11 : The preparedness and recovery measures

The measures addressed in the question are provided for by the Act on Electronic Communications and are applicable to all the public operators (Art 115 see BE 1 in reference list). It provides for priority restoration for priority users such as the blue light services (emergency, police, and rescue). But it is not defined how it is supposed to be restored in case of a disaster such as flooding in some part of the country. Moreover, the historical operator shall respect the measures provided for in specific agreements existing between the civil and military authorities. As an example, the National Coordination and Crisis Centre as well as the province governors can have recourse to a priority treatment of the telecommunications services. Moreover, the emergency services can use some private networks. In practice the crisis coordination management is agreed but there are no rules or conventions allowing the center to take charge and decide.

As regards the governmental telecommunications network (REGETEL BE 9), hot lines enable the user to have recourse to the communication means thanks to an independent routing to the REGETEL servers when the local telecommunications infrastructure is faulty. Independent routings are also provided for through other civil and military networks.

### Question 12 : Incident response capabilities

Belgian Defence Ministry has launched in 2007 a Computer Incident Response Capability (CIRC). This system works 24/7; is has been set up in collaboration with NATO. While BIPT communicates with CIRC, this link is not used to exchange incident information. Neither do other agencies have a formal link to CIRC.

The Police maintains a national/ federal collaboration network on computer crime in the framework of the G8 network. There are also contact points with Interpol.

BelNET, the national ISP for the academia and public authorities operates a CSIRT for its customers. BelNET operates also the BNIX. The e-security platform has difficulty to respond fast enough. No procedures are in place and all are waiting for the national CERT.

Possible Changes: As the above illustrates, most important is finding of better means to collaborate and facilitate rapid and formalized ways of information exchange in Belgium. Hence, the laudable efforts by CIRC can be strengthened by fostering collaboration with other agencies. For instance, with the help of agreements, following best practice for information sharing and incident reporting amongst participants will all help in making collaboration between various groups for the benefit of Belgian society more effective.

### Question 13 : Good practice on resilience

A repository on good practice is not in place at this time.

### Question 14 : Guidelines for procurement

Guidelines for procurement are not in place at this time.

## References

**BIPT** BIPT telecom regulator, status, http://www.ibpt.be/ShowDoc.aspx?objectID=948&lang=fr.

**BE 1** Loi du 13 juin 2005 relative aux communications électroniques (Law on electronic communications) Moniteur Belge. 13 June 2005 (– not available in English).
Available: http://www.ibpt.be/ShowDoc.aspx?objectID=951&lang=fr, released on 20 june.
Last Access: September 15, 2008.
Particularly relevant are articles: 106; 107; 113; 114 ; 115.

**BE 2** Arrêté royal relatif à la notification des services et des réseaux de communications électroniques (Royal Decree 23 march 2007 about notification of services and telecommunications networks : Page 16336 (explanations) and page 16343 - not available in English).
Available:
http://www.bipt.be/ShowDoc.aspx?levelID=204&objectID=2272&lang=fr.
Last Access: September 15, 2008.

**BE 3** Accord de cooperation entre l' Etat et les Communautés (About cooperation agreement between federal state and regions and communities – not available in English).
Available: http://www.ibpt.be/ShowDoc.aspx?objectID=2063&lang=fr.
Last Access: September 15, 2008.

**BE 4** National authorities involved in network and information security: ENISA Belgium country page.
Available: http://www.enisa.europa.eu/doc/pdf/Country_Pages/Belgium.pdf.
Last Access: September 15, 2008.

**BE 5** see **B1** Loi 13.06.2005 (Quality of the Universal Service.Tecnical conditions / Law 13.06.2005).
Last Access: September 15, 2008.
Particularly relevant are articles: 68 to 104
Report of BIPT Council :
http://www.ibpt.be/ShowDoc.aspx?objectID=2806&lang=fr.

**BE 6** Arrêté royal du 31 janvier 2003 Arrêté royal portant fixation du plan d'urgence pour les événements et situations de crise nécessitant une coordination ou une gestion à l'échelon national. (general management of crisis situations).
Available:
http://www.kwgc.be/legislation/arrete_royal_du_31_janvier_2.php.
Last Access: September 15, 2008.

**BE 7** Livre Blanc élaboré par la plate-forme de concertation sur la sécurité de l' information. " Pour une politique nationale de sécurité de l' information " (White paper written down by the dialogue platform on information security " For a national policy regarding information security – not publicly available)

This paper was developed by the dialogue platform – initiated by the Federal Ministers Council on 30/09/2005. The dialogue platform included the following groups and experts:

- Commission for privacy protection,
- National Authority on security,

- General Intelligence and security service,
- Security of state (sûreté de l’ Etat),
- BIPT (telecom regulator),
- FCCU (Federal Computer Crime Unit),
- Control and mediation (Ministry of Economy),
- FeDICT (Federal ICT);
- Cross-Bank on social security,
- Crisis center.

**BE 8** Royal Decree related to CoMixtelec.

**BE 9** REGETEL - governmental and crisis networks, http://www.regetel.be/BIENVENUE.htm, (not available in English).

**Additional Resources**

**BE 10** Towards a Belgian strategy on information security – by private associations and academia – September 2008.
Available:
http://www.lsec.be/upload_directories/documents/TowardsaBelgianStrategyonInformationSecurity_BISI_080908.pdf.
Last Access: September 15, 2008.

**Additional Links**

Contrat de gestion : regarding missions imposed on Belgacom by Law:
http://www.ejustice.fgov.be/cgi_loi/loi_a.pl.

# National Report of Bulgaria

## Introduction

The Bulgarian stakeholders preferred to answer in writing. Several exchanges between the Bulgarian authorities and the contractor took place, and the Bulgarian authorities confirmed that "nothing can be added for the moment" (email dating 11/08/2008)

Exchanges in writing to place with:

| Interviewee | Mr Vasil GRANCHAROV | Mr Todor DRAGISTONOV |
|---|---|---|
| Authority | State Agency for Information Technology and Communications (SAITC)<br>Crisis Management and Defence and Mobilization Preparation Directorate | State Agency for Information Technology and Communications (SAITC) |

| Authority | SAITC - Information Technology and Communications |
|---|---|
| Reports to | Government |
| Year established | 2007 |
| URL | http://www.daits.government.bg / |

### Preliminary remarks

The notion "resilience" (of networks) has been consistently imposed by ENISA in recent times. However, Bulgaria has transposed Regulatory Framework 2002 where the phrase "network integrity" is used. So, our answers will be based on the assumption that "resilience" is (almost) equivalent to "network integrity" and we will give information on the latter. And since we think that "… other essential eCommunications networks …" is not concrete enough we will talk about public eCommunications networks.

## Scope and governance

### Question 1 : The authorities

In Bulgaria, three authorities are responsible for issues related to resilience of public eCommunications networks:

- The Council of Ministers
- State Agency for Information Technology and Communications (SAITC)
- Communications Regulation Commission

The Council of Ministers and the SAITC deal with policy development and legislative matters, the Communications Regulation Commission deals with regulation.

**Question 2 : The mandate of the authorities**

In accordance with the Electronic Communications Act (May 2007), state governance of electronic communications is carried out by the Council of Ministers and the State Agency for Information Technology and Communications[15]. The Council of Ministers, at the proposal of the Chairperson of the State Agency for Information Technology and Communications, adopts the Electronic Communications Policy.

The Communications Regulation Commission[16] performs functions on regulation and control of the provision of electronic communications.

In their activities the Council of Ministers, the State Agency for Information Technology and Communications and the Communications Regulation Commission adhere to one of the goals of the Electronic Communications Act - creation of conditions ensuring maintenance of the integrity and security of public electronic communications networks. Direct obligations related to network integrity are imposed on the undertakings - whether operating with general authorization or rights of use. The authorities work closely together.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

Regulatory issues are dealt with in the secondary legislation in Bulgaria which includes ordinances. There are about twenty ordinances stemming from the Electronic Communications Act. As laid out in the ordinances, requirements on the undertakings with respect to "network integrity" are imposed only in terms of interconnection.

Concerning future strategy, it was explained that the Telecommunication Sector Policy (updated in 2004) has no provisions regarding network integrity. Obviously, that is an issue that should be included in the next update.

**Question 4 : Initiatives between providers and public authorities**

Initiatives between providers and public authorities are very common. The Electronic Communications Act was posted for public consultation and the relevant comments of all stakeholders have been taken into account. But again, "network integrity" has not been a special issue.

Exchanges between providers and public authorities concern different topics, and their outcome varies.

There is no information whether similar initiatives take place among providers in Bulgaria.

[15] *See Chapter 3 Section 3 of LAW ON ELECTRONIC COMMUNICATIONS May 10, 2007*
[16] *See Chapter 4 Section 1 of LAW ON ELECTRONIC COMMUNICATIONS May 10, 2007*

## Tasks

### Question 5 : Typical task

The Bulgarian authorities do always hold public consultations with providers when reviewing existing or developing new regulations, guidelines or recommendation. They also exchange information with providers. These exchanges take place regularly to pursue providers' obligations, and occasionally upon request by the authorities. Audits are not carried out; enforcement of regulation is taking place.

### Question 6 : Exchange of information between providers and public authorities

Providers in Bulgaria do not exchange information with the authorities regarding the resilience of their network.

### Question 7 : Handling of security incidents

Security incidents are not reported.

### Question 8 : Audits related to resilience

While no audits are taking place, providers are subject to normal control by the Commissions Regulation Commission with the purpose of assessing regulatory compliance. These controls are exercised by authorised employees of the CRC administration following an annual plan or after notifications of violations.

### Question 9 : Enforcement actions

Enforcement actions use penalties as a means. The penalties include fines or property sanctions for every specific violation.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

A national risk management process is not yet in place in Bulgaria.

### Question 11 : The preparedness and recovery measures

There are no specific preparedness and recovery measures related to network integrity in place. Preparedness and recovery measures in place are provided for crisis situations affecting national security. Exercises and trainings are organised.

### Question 12 : Incident response capabilities

Crisis management centres operate when the national security is threatened. A Bulgarian governmental CERT is in the process of establishment. Therefore, cooperation among those centres is still non-existent. Past incidents are probably collected, within individual institutions.

**Question 13 : Good practice on resilience**

There is no repository of good practices regarding resilience issues in Bulgaria.

**Question 14 : Guidelines for procurement**

As regards public procurement, the requirements follow those transposed from EU Directive 99/5. They do not specifically refer to resilience issues.

## References

**Law on Electronic Communicatio**n - May 10, 2007, Bulgarian text (Law on Electronic Communications) May 10, 2007.
Available: http://www.daits.government.bg.
Last Access: August 15, 2008).
Non-binding English Version http://daits.government.bg.
Particularly relevant are: Chapter 3 Section 3 and Chapter 4 Section 1.

# National Report of Cyprus

## Introduction

### Interview

Date and Duration: 6 August 9-10 h = 1 hour.

| | |
|---|---|
| Interviewee | Mr Antonis Antoniades |
| Authority | OCECPR - Office of the Commissioner of Electronic Communications and Postal Regulation |
| Position title | Senior Officer |
| Task Responsibilities | responsible for many matters among others for network security |

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | OCECPR - Office of the Commissioner of Electronic Communications and Postal Regulation |
| Main Tasks | Regulation, policy implementation, advice on policy development |
| Reports to | Council of Ministers (not subjected to a ministry)<br>The Commissioner and Deputy Commissioner are appointed by the Council of Ministers.<br>The Commissioner reports to the President of the Republic of Cyprus. |
| Year established | 2004 |
| URL | URL: http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&tt=ocecpr&lang=gr (under construction)<br>Greek version available. English version under construction |

## Scope and governance

### Question 1 : The authorities

The regulator responsible for issues related to resilience of eCommunication networks in Cyprus is OCECPR - Office of the Commissioner of Electronic Communications and Postal Regulation.

OCECPR advise the Ministry for Communication and Work (responsible for electronic communications) and the Ministry for Finance (responsible for information society in general) on policy development, implement policies, and cooperate with providers.

OCECPR also collect information on best practice with other stakeholders such as other authorities, operators and service providers, consumer organisations, other organisations involved in network security issues and academia.

**Question 2 : The mandate of the authorities**

The mandate of OCECPR embraces advising the ministers, enforce regulations if necessary, cooperate with other authorities, and implement policies. The mandate is described in Part 3 and Part 5 of 'The Regulation of Electronic Communications and Postal Services' Law of 2004 (see OCECPR 1 in reference list).

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

Currently, the provisions concerning the resilience of eCommunication networks are very general. They are inscribed in the licenses which are handed out to the providers.

Very soon, Sept – Oct 2008, there will be a detailed document on the policies of the various ministries. The conclusions of this report will be transposed into 'secondary legislation'. The document will be published in the Official Journal of Cyprus and on the OCECPR web site as well (in Greek) (see OCECPR 2 in reference list). This document describes also the strategies of Cyprus in the domain of resilience of public eCommunications networks for the future. As the document is under decision-making currently, details about its content are not yet public. The documentation of the secondary legislation will undergo public consultation. However, it will cover all issues relevant for information security and network resilience. It will give guidelines for providers and define how audits will be done.

According to article 98 of the Law 112(I)/2204, on a voluntary basis, a lot of provisions which are expected to be regulated by the new regulations are already put in place by the main providers. These measures cover, among others, the physical protection of networks for external and internal threads, the implementation of information security management systems, the implementation of the ISO27001 (ISMS), access management, risk management, business continuity plans, malware protection, etc. The overall regulation of all issues under one umbrella needs still to be done.

**Question 4 : Initiatives between providers and public authorities**

The matter of initiatives between operators and the state (regulator) regarding resilience issues are currently investigated (see OCECPR 3 in reference list). The authority is aware that some operators do have a business continuity plan in place, and provide network protection for customers and other users. Regarding initiatives between providers, all operators work more or less together. There are altogether 44 providers in Cyprus with 4 public eCommunications providers. They are encouraged by OCECPR to cooperate. The cooperation is mainly focused on exchange of information.

## Tasks

### Question 5 : Typical tasks

Among the typical tasks of OCECPR are the following:

- Public consultation with providers to review existing and develop new regulations,
- Exchange of information with providers upon request; no regular exchange with the providers is taking place; and
- Enforcement of regulations.

### Question 6 : Exchange of information between providers and public authorities

Upon request of OCECPR, the providers do exchange all kind of information with OCECPR. In particular, information on security policy issues, information on business continuity plans and Information on locations with high infrastructures density are exchanged if requested. The exchange of information on preparedness measures can be enforced by OCECPR. As regards information on geographical, topological and technical network structures, it is an obligation for the operators to inform about it regularly. The information collected in these exchanges is used to propose new policies, to enforce regulation, to audit, to provide information to other bodies, e.g. EU.

### Question 7 : Handling of security incidents

In Cyprus, there is no specific obligation to report security incidents in place. Security incidents are only reported upon request. The reporting duties will change considerably once the secondary legislation (see above) will be implemented (see OCECPR 2 in reference list). Usually, the information is treated confidentially. The operator who has given the information may request that the information is treated as confidential. However, the Commissioner (Head of the OCECPR) might declare the non-confidentiality of given information.

### Question 8 : Audits related to resilience

OCECPR carries out so-called high-level audits. During these audits OCECPR verifies that the operators are fulfilling the requirements in general. OCECPR may request appropriate reporting and information by the operators to verify compliance with existing obligations. Currently there are no regulations in place to deal with audits or details thereof.

### Question 9 : Enforcement actions

Enforcement actions in case of non-compliance with the regulations consist in penalties and other administrative measures. The end of the enforcement actions scale might be the suspension of a license.

It has happened once that a license was suspended but not for security reasons. The secondary legislation, currently under decision, foresees more detailed provisions for administrative measures.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

No national risk management process regarding resilience of eCommunications networks is in place in Cyprus. The national risk management process of the government does not cover all providers and operators of public or other essential communication networks but only areas which are not in the focus of the present study (defence, civil security, etc).

Currently, a project of the authority is dealing with risk management in order to develop a national risk management process for eCommunications networks. Individual operators and providers have developed a risk management process on their own.

### Question 11 : The preparedness and recovery measures

A series of measures are in place and a minimum set of obligations for preparedness and recovery measures exists in Cyprus. These measures are updated through monitoring and in open communication with the stakeholders.

### Question 12 : Incident response capabilities

Cyprus does not have a national CERT. A CY CERT is under discussion. This CERT would consist of two parts:

- the current academic CERT and
- a CERT for 'all the rest'

To establish the CERT, OCECPR are working closely with ENISA. The result of this collaboration will be a final paper on the creation of a national CERT that will be submitted to the Cyprus government. Apart from ENISA, OCECPR will also cooperate with FIRST network. Currently, national sets will provide basic core services only (reactive and proactive). Past incidents are not analysed.

### Question 13 : Good practice on resilience

Information on best practice on the resilience of eCommunications networks is collected but there is no repository in place.

### Question 14 : Guidelines for procurement

Specific guidelines for procurement of public sector eCommunication networks are not yet in place.

## References

**OCECPR–1** Ο περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 (The regulation of electronic communications and postal services law of 2004).
Available:
http://www.ocecpr.org.cy/nqcontent.cfm?a_id=1053&tt=ocecpr&lang=gr.
Last Access: September 25, 2008.
Non-binding English version,
http://www.ocecpr.org.cy/media/documents/Legislation/GE_Law_OCECPR_EN_N-112-I-04_31-4-04.doc.

**OCECPR–2** Αντιμετώπιση Κινδύνων στα Δημόσια Δίκτυα Ηλεκτρονικών Επικοινωνιών – Επανάκαμψη μετά από καταστροφή και Επιχειρησιακή Συνέχεια Ασφάλεια Υποδομών – Προστασία Πληροφοριών (Disaster recovery and business continuity).
Available:
http://www.ocecpr.org.cy/nqcontent.cfm?a_id=668&tt=ocecpr&lang=gr.
Last Access: October 3, 2008.

### Additional Resources

**OCECPR – 3** Information not publicly available.

### Additional Links

Additional publications from OCECPR in English can be found on its Greek website using: http://www.ocecpr.org.cy/

# *National Report of Cyprus*

# National Report of Denmark

## Introduction

### Interview

Date and Duration - 18 August 2008 – 1 hr 10 min.

| | |
|---|---|
| Interviewee | Thomas Kristmar |
| Authority | National IT and Telecom Agency – NITA |
| Position title | Senior Adviser |
| Education/Training | |
| Task Responsibilities | Security Division |
| If applicable, rel. ship to ENISA | None |

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | Ministry for Science Technology and Innovation --- National IT and Telecom Agency – NITA |
| Main Tasks | Regulations, guidance, and policy development for the ministry |
| Reports to | Ministry of Science Technology and Innovation |
| Year established | NITA has been created a long time ago as an agency for the regulation of coastal matters and grew into a telecom regulatory agency with the wider deployment of telecom and e-communications networks |
| URL | http://www.itst.dk/ |

### Authorities involved but not part of the interview

The Danish Preparedness Act Part 2, Art 4 (see DPA in the reference list) gives the Ministry of Defence the guidance to manage national rescue preparedness.

The Danish Emergency Management Agency (DEMA) – reporting to the Ministry of Defence - manages the National Rescue Preparedness Corps. The latter supervises the national and municipal rescue preparedness. It advises authorities on matters of preparedness.

Art 24 of the Danish Preparedness Act (see DPA) states, "Within their respective fields of administration, individual ministers shall plan for the maintenance and continuation of society's functions in the event of accidents and disasters, including actions of war, and in order to provide support to the defence forces".

The Department of Defence coordinates the planning in relationship to civil emergency planning.

## Scope and governance

### Question 1 : The authorities

The authority responsible for issues related to public networks for e-communication in Denmark is the National IT and Telecom Agency (NITA). NITA communicates to the public during a crisis regarding availability of public e-communication networks.

It is responsible for providing the communication capacity. Each ministry is responsible for making sure that in case of disaster, its communication facilities work. On its web site, NITA describes its role regarding security of networks (http://en.itst.dk/it-security/emergency-planning) as follows

> *"In the Executive Order on Emergency Preparedness in the Telecommunications Sector, powers in this area have been delegated, to a wide extent, to the National IT and Telecom Agency. The Agency may lay down detailed rules on emergency planning in the IT and telecommunications sector, including physical protection of infrastructure and restrictions on traffic for parties other than selected users*."

The most important – and unique – role of NITA is to prioritise traffic in case of a disaster. NITA is:

> ***"…** coordinating and prioritising the varying demands of the emergency authorities for vital electronic communications in an emergency situation".*

### Question 2 : The mandate of the authorities

NITA has a general mandate for IT matters and IT security. Its mandate is based on a Parliamentary Act[17].

NITA deals with the societal communication preparedness in various areas; for example, it operates a prioritised scheme for the fixed telephone network. This scheme does not exist for mobile telephony.

In 2005, the government published a policy, stating that more cooperation between different agencies and operators was needed[18] and that cooperation on preparedness within energy, IT, telecom, transport, health should be encouraged. A coordination body has been set up in which NITA holds the chair currently and exchanges with other public agencies and authorities (from energy, IT, telecom, transport, health) on all matters of information security. The Council meets four to six times during the year. If required, the parties exchange information more frequently.

[17] *The Parliamentary Act is not available in English See: Bekendtgørelse om ændringer i ministeriernes forretningsområde-* https://www.retsinformation.dk/Forms/R0710.aspx?id=45863).

[18] See *http://forsvaret.dk/NR/rdonlyres/F43B7906-C47C-4198-8358-5017A107000F/0/regeringenBeredskab5.pdf*

### Question 3 : Regulatory issues of resilience of public and other essential e-communications networks

The predominant provision related to resilience of public communication networks follows the Danish version of the ISO 27002 standard called DS 484. It is a standard which must be followed by all ministries. Moreover, DS 484 gives guidance on how each ministry must protect its information security.

Two regulations that deal with resilience of e-communication networks and telecommunication preparedness were issued in May 2008. Both regulations also address the matter of prioritising network communication (See NITA 1 and NITA 2), and acts supplementing the legal base are in progress.

Currently government organisations are reaching out to industry by using their buying power. A public contract on telecommunications concluded with a provider includes an obligation that the contractor must adhere to the IT Security standard ISO 27007, that is DS 484. That way, Denmark hopes that awareness regarding resilience of public services improves across society.

### Question 4 : Initiatives between providers and public authorities

An information exchange has been set up between NITA, telecom operators and key customers (from health, defence, energy, etc.) in the form of the BERIT forum (BERedskabsforum for IT og tele) network. The network meets several times a year and discusses issues such as dependencies of the infrastructures, matters of availability or future strategies. However, it does not necessarily address best practice issues or come up with recommendations that are, in turn, then becoming best practices to be followed by infrastructure operators and service providers.

There are similar initiatives among providers. They hold regular meetings. However, NITA does not take part in these meetings. The meetings focus on information exchange. However, regarding spam, the operators have set up a self-regulation initiative. The group runs a web site on Spam (see Additional Links section).

## Tasks

### Question 5 : Typical tasks

NITA holds public consultations with stakeholders, and exchanges information with providers; it does not carry out audits, but NITA carries out supervision mainly by contacting providers in formal writing and inform them officially of their responsibilities that they are obliged to confirm that they comply with.

### Question 6 : Exchange of information between providers and public authorities

The process of exchanging information with providers is currently under review. Within the BERIT network, information exchange takes place regularly.

In specific questions, NITA can write to the operators and ask for clarifications. Operators are obliged by law to answer. The timeframe given to respond is determined on a case by case basis. It was pointed out that NITA does get the information it needs to fulfil its tasks as stipulated by the law. NITA uses information it collects for confidential discussions with operators. Such data are also used to determine if current procedures are adequate.

In summary, NITA monitors the issues of network resilience and leaves it to the operators to organise the preparedness and have the correct procedures in place.

### Question 7 : Handling of security incidents

Providers do not report security incidents on a voluntary basis. Upon request by NITA, operators are obliged to report a security incident (see Question 6, information request).

### Question 8 : Audits related to resilience

NITA does not carry out audits. Accordingly, it is ministries responsibility making sure they follow DS 484 and thus making sure that their operator meets their resilience requirements.

### Question 9 : Enforcement actions

In order to enforce regulations, NITA puts a fine on the operator. It does not happen often in the security domain. Mr Kristmar cannot remember one single case where a fine was given.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

Overall, there is no national risk management process in place. There is one mentioned in the DS 484, which regards only the risk management of government institutions. It is foreseen that a risk management process for operators will be obligatory.

### Question 11 : The preparedness and recovery measures

The preparedness and recovery measures for the communication networks are in the responsibility of the different ministries following the Danish version – DS 484 – of the information security standards ISO 27002. Most ministries have measures in place and can communicate in crises. For example, dedicated telephone lines are determined, which must be available and accessible all the time.

In this process, NITA has a strong role in emergency prioritising actions and respective decisions on priorities. For example, if an operator cannot meet the demands, NITA will prioritise.

Every second year, a national emergency exercise is taking place, where each ministry is feeding in with tasks, scenarios etc. An evaluation of the exercise is taking place for improving preparedness and recovery measures.

**Question 12 : Incident response capabilities**

Denmark does not have a national CERT. A recent report recommends the setting up of a national CERT and currently, this plan is under political discussion. Uni-C DK as well as the Danish IT Centre for Education and Research carry out Sector-CERT activities. The latter is a national organization under the Danish Ministry of Education.

In case of an emergency, a national management body is set up among the key ministries (e.g., Cabinet Office, Health, Justice and Defence). NITA coordinates the measures and provisions which need to be carried out within the frame of the e-communications networks.

As far as international cooperation is concerned, UNI-C belongs to the trusted introducers in the frame of CSIRTS. It is also a member of FIRST.

Past incidents are analysed if NITA becomes aware of them and asks the operators to provide information. NITA might be informed by a ministry or by any other organisation about an incident. The purpose of the post-investigation is threefold:

- to verify if the operator has handled correctly the regulation,
- whether the response was adequate, and
- whether further actions are necessary.

**Question 13 : Good practice on resilience**

There is no repository of good practice related to resilience of e-communications networks.

**Question 14 : Guidelines for procurement**

NITA follows EU legislation here. Currently, in each procurement contract with a provider, an obligation is included that the contractor must adhere to the IT Security standard ISO 27007, i.e. DS 484. However, there is no specific requirement stipulating that procurement needs to address reliability and dependability of e-communication networks.

## References

| | |
|---|---|
| **DPA** | LBK nr 137 af 01/03/2004 Gældende (Beredskabsloven) [Danish Preparedness Act, LBK n° 137 of 1/03/2004 (in force)].<br>Available: https://www.retsinformation.dk/Forms/R0710.aspx?id=6365.<br>Last access: 25 August 2008.<br>Non-binding English version<br>http://www.beredskabsstyrelsen.dk/uk/danish_preparedness_act.htm#Part_2.<br>Particularly relevant are articles: 4, 24. |
| **NITA 1** | Bekendtgørelse om sikring af offentlige telenet og teletjenester (Law pertaining to security of public telecommunication infrastructure and services) BEK nr 421 af 21/05/2008 Gældende (available in Danish only).<br>Available https://www.retsinformation.dk/Forms/R0710.aspx?id=117087.<br>Last Access: 28 August 2008.<br>Particularly relevant are articles: § 2. |
| **NITA 2** | Bekendtgørelse om teleberedskab (Law on electronic communication) BEK nr 370 af 21/05/2008 Gældende (available in Danish only).<br>Available https://www.retsinformation.dk/Forms/R0710.aspx?id=117086.<br>Last Access: 28 August 2008.<br>Particularly relevant are articles: § 3 , section 1,2 and 3. |

### Additional Resources

| | |
|---|---|
| **NITA 3** | Emergency planning in the IT and telecommunications sector is part of the emergency preparedness planning of the civil sector.<br>Available http://en.itst.dk/it-security/emergency-planning.<br>Last Access: 1 September 2008. |

### Additional links

| | |
|---|---|
| ***DEMA*** | Danish Emergency Management Agency, http://www.brs.dk/uk/. |
| **GISF** | Government Information Security Forum http://en.itst.dk/it-security/standard-for-information-security. |
| **SPAM** | Web site run by providers http://www.isp-sikkerhedsforum.dk/. |
| **Uni-C DK** | CERT in educational field https://www.cert.dk/. |

# National Report of Estonia

## Introduction

### Interview

There was no interview on the telephone conducted with Estonia. Only written answers were received by.

| | | |
|---|---|---|
| Interviewee | Mr Oliver GAILAN | Mr Toomas VIIRA |
| Authority | ETSA – Estonian Technical Surveillance Authority | Estonian Informatics Centre |
| Position title | Head of Electronic Communication Service Department | Information Security Manager |
| Education/Training Degree | | |
| Task Responsibilities | *In field on electronic communication*:<br>- planning, coordination and management of the use of radio frequency bands<br>- exercising the surveillance over the use of frequency bands,<br>- developing of requirements for apparatuses;<br>- supervision over requirements for electronic communications services and networks;<br>- management of Estonian Numbering Plan resources.<br>*Safety supervision over*:<br>- mining operations<br>- explosive substances and blasting<br>- pressure equipment<br>- lifts and cableway installations;<br>- machinery (including cranes);<br>- gas equipment, gas operations and gas installations;<br>- electrical plants, electrical works and electrical installations, electromagnetic compatibility;<br>- handling of dangerous chemicals.<br>*In field of railway regulation*:<br>- supervision over safety and efficiency | - responsible for information security in Estonian Informatics Centre<br>- responsible for the coordination of IT security issues in Estonian Public Sector organizations<br>- development and coordination of development and implementation of Information Systems Three Level Baseline Protection System in Estonian Public Sector<br>coordination and implementation of the development of state registers, computer networks and data communication, standardisation, IT public procurement, monitoring Estonian IT situation, operating CERT-EE etc. |
| If applicable relationship to ENISA | | National Liaison Officer for Estonia. |

**Authorities involved with Network Resilience**

| Authority | ETSA – Estonian Technical Surveillance Authority | RIA – Estonian Informatics Centre |
|---|---|---|
| Main Tasks | conducts national safety surveillance, market regulation and development in a variety of fields | coordination and implementation of the development of state registers, computer networks and data communication, standardisation, IT public procurement, monitoring Estonian IT situation, operating CERT-EE etc. |
| $Reports to | Ministry of Economic Affairs and Communications | Ministry of Economic Affairs and Communications |
| Year established | 2008 | 2003 |
| URL | www.tja.ee | www.ria.ee |

**Authorities involved but not writing a questionnaire response**

| Authority | Ministry for Economic Affairs and Communications | CERT EE | Estonian Ministry of Defence | Estonian Ministry of Interior |
|---|---|---|---|---|
| Main Tasks | Liberalisation, universal service | management of security incidents in .ee computer networks<br>national contact point for international co-operation in the field of IT security. | | to assure the internal security of the state (…)<br>to regulate the crisis management and rescue works |
| Reports to | | | | |
| Year established | | 2006 | | |
| URL | www.mkm.ee | www.cert.ee | www.mod.gov.ee | www.siseministeerium.ee. |

## Scope and governance

### Question 1 : The authorities

There are several authorities which are responsible for issues related to resilience of public communications networks. Estonian Technical Surveillance Authority (ETSA) and Ministry of Economic Affairs and Communications are general regulatory authorities in the field of electronic communication. CERT Estonia is responsible for coordination and handling of incident in .ee networks. Every network or service provider is responsible for their own network resilience issues. Also, every organization is responsible for their own internal networks.

Other authorities playing a role in the domain are the Estonian Informatics Centre which is a subdivision of the Ministry of Economic Affairs and Communications, the Estonian Ministry of Defence as well as the Estonian Ministry of Interior.

**Question 2 : The mandate of the authorities**

The Ministry of Economic Affairs and Communications is formulating policies and is acting as a body of legislation. In particular it is responsible for the general ICT coordination – more precisely the Department of State Information Systems. The tasks of the department include the coordination of state IT-policy actions and development plans in the field of state administrative information systems (IS):

- state IT budgets,
- IT legislation,
- coordination of IT projects,
- IT audits,
- standardisation,
- IT procurement procedures,
- and international cooperation in the field of state IS.

There are also IT councils of ministries and IT councils of counties. In addition, there is the Estonian Informatics Council, which is a government committee of experts and the implementing body in the general coordination of state information policy. The Estonian Informatics Centre, which is a subdivision of the ministry, is responsible for:

- the coordination and implementation of the development of state registers,
- computer networks and data communication,
- standardisation,
- IT public procurement,
- monitoring Estonian IT situation,
- development of Information Systems Security standard and coordination of standard implementation in public sector
- etc.

ETSA's task is supervision over the provision of electronic communications services, according to Electronic Communications Act (EE 8).

The Computer Emergency Response Team of Estonia (CERT EE), established in 2006, is an organisation responsible for the management of security incidents in .ee computer networks. Its task is to assist Estonian internet users in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats. CERT Estonia deals with security incidents that occur in Estonian networks, are started there, or have been notified by citizens or institutions either in Estonia or abroad.

CERT Estonia offers the following services: Incident handling – receiving incident reports, assigning priorities to incidents according to their severity level, performing incident analysis, responding to incidents, giving assistance in incident response, coordinating incident response activities. Giving information and issuing warnings – informing users about attacks, viruses, worms, Trojans occurring in .ee networks and notifying about vulnerabilities discovered in the most widely used systems and applications in Estonia. Warnings are mainly issued in cases of attacks with higher level of severity, extremely widespread viruses, and highly severe vulnerabilities.

The Estonian Ministry of Defence manages and controls the Estonian Cyber Security Policy development and implementation.

The Estonian Ministry of Interior is responsible for activities related with CIP and CIIP issues. Under the governance of ministry is Police Board, which is also responsible for running „Cyber Police" department.

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

There are several laws and acts, which directly and/or indirectly regulate these issues. For instance, from Electronic Communications Act (EE 8) we have:

> *§ 101. Security requirement*
>
> (1) A communications undertaking must guarantee the security of a communications network and prevent third persons from accessing the data specified in subsection 102 (1) of this section without legal grounds.
> (2) If clear and present danger exists to the security of the communications network, the communications undertaking shall immediately inform the subscriber of such danger in a reasonable manner and, if elimination of the danger by the efforts of the undertaking is impossible, also of possible means to combat the threat and of any costs related thereto.

To illustrate, in the Regulation No. 140 of the Government of the Republic of 22 June 2006, „Technical requirements for the provision of communications services and technical requirements for the communications networks" are defined as follows:

> *§ 3 Requirements for the communications networks, quality of service and provision of communications services*
>
> (1) A communications undertaking shall plan, design, construct and maintain the communications network used for the provision of communications services in the following way:
>
> 1) The access to communications network and to the data forwarded and stored in it shall be restricted for unauthorized persons;
> 2) The communications services shall be minimally disturbed by interruptions of electricity supply, breakdown in the communications network, software viruses or other factors disturbing the network and service;

> 3) The communications undertakings shall choose the extent and methods of maintenance of network so, that the conditions provided by the contract and quality requirements are ensured**.**

Estonia has a large number of regulations and acts in place related to some degree to issues of resilience of public e-communications networks. In details these concern:

- Digital Signatures Act (DSA) entered into force on 15 December 2000. It gives the digital and handwritten signatures equal legal value and sets an obligation for all public institutions to accept digitally signed documents(EE 1)
- The Personal Data Protection Act (PDPA) protects the fundamental rights and freedoms of persons with respect to the processing of their personal data and in accordance with the right of individuals to obtain freely any information that is disseminated for public use. Since 2008 personal data is divided into two categories, namely "personal data" and “sensitive personal data” as the sub-class under special protection. For clarity purposes, the definition of “personal data” has been specified in the draft Act, stating that the protection of personal data shall extend to all forms of data, including audio and graphic data as well as biometric data. (EE 2)
- The Databases Act which has been taken over by Public Information Act since January 1, 2008 (EE 3)
- The Archives Act sets the principles for collecting, evaluating, archiving, preserving, accessing of archival documents and for the activities of archives. (EE 4)
- The State Secrets Act establishes the legal bases for the conduct of systematic and purposeful official statistical surveys (EE 5).
- The Official Statistics Act establishes legal grounds for the methodical and systematic regulation of state statistical observations (EE 6)
- The new Public Procurement Act of Estonia includes legal provisions enabling the further development of eProcurement (eAuctions, dynamic purchasing system, eCatalogues etc.) so as to give better opportunities for taking forward a fully electronic Procurement tendering process (EE 7)
- The Electronic Communications Act implements the EU Regulatory Framework for Electronic Communications. The purpose of this Act is to create the necessary conditions to promote the development of electronic communications networks and communications services while ensuring the protection of the interests of users of such services (EE 8)
- The Public Information Act (PIA) guarantees the free access public information. Act covers state and local agencies, legal persons in public law and private entities that are conducting public duties including educational, health care, social or other public services. Any person may make a request for information and the holder of information must respond within five working days. Requests for information are registered. Since January 1, 2008 the Act also regulates the field of former Databases Act (in force from 1997 to 2007). The Act sets out the general principles for the creation and maintenance of databases and monitoring of databases management. The Act also covers the provisions of the EU Directive 2003/98/EC on the re-use of public sector information (PSI). Estonia has thus notified full transposition of the PSI-directive. (EE 9)

- The Consumer Protection Act regulates the offering and sale, or marketing in any other manner, of goods or services to consumers by traders, determines the rights of consumers as the purchasers or users of goods or services, and provides for the organisation and supervision of consumer protection and liability for violations of this Act (EE 10)
- The Information Society Services Act entered into force on 1 May 2004. This Act implements EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. It establishes the requirements pertaining to information society service providers, organisation of supervision and liability in case of violation of the requirements (EE11)
- The National Broadcasting Act provides the legal status, objective, functions, financing, and organisation of management and activities of Estonian National Broadcasting (EE 12)
- The purpose of the Copyright Act is to ensure the consistent development of culture and protection of cultural achievements, the development of copyright-based industries and international trade, and to create favourable conditions for authors, performers, producers of phonograms, broadcasting organisations, producers of first fixations of films, makers of databases and other persons specified in this Act for the creation and use of works and other cultural achievements (EE 13)
- The State Liability Act provides the bases of and procedure for the protection and restoration of rights violated upon the exercise of powers of public authority and performance of other public duties and compensation for damage caused (state liability) (EE 15 )

As regards future strategies, the Cyber Security Strategy was adopted by the government on May 2008 and now we continue with several strategy related activities (see EE 14 in reference list). The Estonian Cybersecurity Strategy sets the priorities and activities in improving the security of country's cyberspace. The Cybersecurity Strategy concentrates on the following areas - the responsibilities of state and private organizations, vulnerability assessments of critical national information infrastructure, response system, domestic and international legal instruments, international cooperation as well as training and awareness raising issues.

### Question 4 : Initiatives between providers and public authorities

In Estonia, there are public-private partnerships in the field on incidents’ handling, in developing cyber security strategy, PKI infrastructure development and so forth. Between different providers are different ad-hoc workgroups and some initiatives e.g. Providers, who are connected to the Tallinn Internet Exchange have a cooperation agreement.

## Tasks

### Question 5 : Typical task

In general, ETSA has a supervisory responsibility, but as resilience issue is not yet much regulated (no clear requirements), supervision is quite limited. The Estonian authorities hold public consultation with providers to review existing or develop new regulations, guidelines or recommendations, and exchange information with providers. Audits will be regulated by a government decree, which validates obligatory IT audit for public sector organizations in the end of this year.

### Question 6 : Exchange of information between providers and public authorities

Information exchange between providers and public authorities is not required by ETSA. Information is not shared with ETSA. Other authorities exchange information with providers, which is needed for performing certain tasks according to the laws, regulations and agreements between different parties. Later on the collected information is used for development or changing strategies, policies, acts etc, - according to the needs and problems.

### Question 7 : Handling of security incidents

Handling of security incidents is not required by ETSA. Public sector organizations have obligation to report to CERT-EE. Private sector organizations are recommended to report to CERT-EE. Some kind of incidents is reported also to Estonian Technical Surveillance Authority. According to the laws (EE 9, EE2), information is disclosed according to the "need to know" principle.

### Question 8 : Audits related to resilience

Regular audits will start after the adoption of a governmental decree on Information Systems Security Standard implementation. Random audits or audits after an incident may be done by the National Audit Office of Estonia, Data Protection Inspectorate etc. According to ETSA, at the moment there is no regulation which would be demanding those audits. If service providers are auditing their networks, they are doing it voluntarily.

### Question 9 : Enforcement actions

Enforcement actions include official notices by the surveillance or audit authorities up to penalties.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

There is a general risk management process, which is implemented to ICT sector also. The Estonian Ministry of Interior is responsible for the general level risk management issues in Estonia. ETSA has no information about this.

### Question 11 : The preparedness and recovery measures

Risk analysis, business continuity plans, standard and security measures implementation are in place in Estonia. The Information Systems Security standard is updated every year. We organize also training for security experts, administrators, network administrators etc.

ETSA has a notion of some crisis-plans at government level, but does not have no detailed information about them.

### Question 12 : Incident response capabilities

CERT Estonia is the only incident response capability in Estonia. The CERT-EE has their own internal network or community, where certain topics are discussed. They also cooperate with other CERT teams worldwide and with other partners.

Possible Changes: Concerning analysis of past incidents, it was stated that "Always incidents analyses maybe done better and we can't say, that all incidents are properly analysed. It really depends on incident, on organization, their abilities to handle and analyse the incidents etc".

### Question 13 : Good practice on resilience

There is no official repository of good practices. Within the CERT community, different guidelines and/or good practices and according to the certain situation are given.

### Question 14 : Guidelines for procurement

Several guidelines for procurement are related to some degree to the resilience of public e-communications networks such as Public Procurement Act, IT procurement procedures, Estonian IT Interoperability Framework- version 2.0 or the Estonian IT Architecture.

## References

**EE 1** Digital Signatures Act- Approved on 8 March 2000, the Digital Signatures Act (DSA) entered into force on 15 December 2000. It gives the digital and handwritten signatures equal legal value and sets an obligation for all public institutions to accept digitally signed documents. See a more detailed overview at Public Key Infrastructure.

**EE 2** Personal Data Protection Act- The Personal Data Protection Act (PDPA) was passed by Parliament in June 1996 and entered into force on 19 July 1996. A new version entered into force in January 1, 2008 that has not been translated yet. The Act protects the fundamental rights and freedoms of persons with respect to the processing of their personal data and in accordance with the right of individuals to obtain freely any information that is disseminated for public use. Since 2008 personal data is divided into two categories, namely "personal data" and “sensitive personal data” as the sub-class under special protection. For clarity purposes, the definition of “personal data” has been specified in the draft Act, stating that the protection of personal data shall extend to all forms of data, including audio and graphic data as well as biometric data. Data protection is supervised by the Data Protection Inspectorate.

**EE 3** Databases Act - since January 1, 2008 the field of this Act was taken over by Public Information Act.

**EE 4** Archives Act - The Archives Act entered into force on May 1, 1998. The Act sets the principles for collecting, evaluating, archiving, preserving, accessing of archival documents and for the activities of archives.

**EE 5** State Secrets Act - This Act entered into force on February 28, 1999. This Act establishes the legal bases for the conduct of systematic and purposeful official statistical surveys.

**EE 6** Official Statistics Act - The Official Statistics Act took effect on July 17, 1997. This Act establishes legal grounds for the methodical and systematic regulation of state statistical observations.

**EE 7** Public Procurement Act - The new Public Procurement Act of Estonia came into force in May 2007, thus transposing the EU Directives on public procurement (2004/17/EC and 2004/18/EC). It includes legal provisions enabling the further development of eProcurement (eAuctions, dynamic purchasing system, eCatalogues etc.) so as to give better opportunities for taking forward a fully electronic Procurement tendering process.

**EE 8** Electronic Communications Act - The Electronic Communications Act was passed on 8 December 2004 and entered into force on 1 January 2005. It implements the EU Regulatory Framework for Electronic Communications. The purpose of this Act is to create the necessary conditions to promote the development of electronic communications networks and communications services while ensuring the protection of the interests of users of such services.

**EE 9** Public Information Act - The Public Information Act (PIA) was approved in November 2000 and took effect in January 2001. A new version entered into force in January 1, 2008 that has not been translated yet. The goal of the law is to guarantee the free access public information. Act covers state and local agencies, legal persons in public law and private entities that are conducting public duties including educational, health care, social or other public services.

Any person may make a request for information and the holder of information must respond within five working days. Requests for information are registered. Since January 1, 2008 the Act also regulates the field of former Databases Act (in force from 1997 to 2007). The Act sets out the general principles for the creation and maintenance of databases and monitoring of databases management. The Act also covers the provisions of the EU Directive 2003/98/EC on the re-use of public sector information (PSI). Estonia has thus notified full transposition of the PSI-directive.

**EE 10** Consumer Protection Act - This Act entered into force on 15 April 2004. This Acts regulates the offering and sale, or marketing in any other manner, of goods or services to consumers by traders, determines the rights of consumers as the purchasers or users of goods or services, and provides for the organisation and supervision of consumer protection and liability for violations of this Act.

**EE 11** Information Society Services Act - The Information Society Services Act entered into force on 1 May 2004. This Act implements EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. It establishes the requirements pertaining to information society service providers, organisation of supervision and liability in case of violation of the requirements.

**EE 12** National Broadcasting Act - The National Broadcasting Act entered into force on 1 June 2007. This Act provides the legal status, objective, functions, financing, and organisation of management and activities of Estonian National Broadcasting.

**EE 13** Copyright Act - This Act entered into force on 12 December 1992. The purpose of the Copyright Act is to ensure the consistent development of culture and protection of cultural achievements, the development of copyright-based industries and international trade, and to create favourable conditions for authors, performers, producers of phonograms, broadcasting organisations, producers of first fixations of films, makers of databases and other persons specified in this Act for the creation and use of works and other cultural achievements.

**EE14** Cyber security strategy - cyber security strategy committee - Ministry of Defence (2008). (Available: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf (36 pages) Last access: September 28, 2008).

In addition Information Systems Security Standard called ISKE – Information Systems Three Level Security Baseline System, which is obligatory for implementation in public sector organizations.

Here are the Acts translated by Estonian Legal Language Centre.

For some Acts eupractice's overview of Estonian legal framework offers a more detailed overview.

Legal Acts can also be searched for Electronic State Gazette (*Riigi Teataja* in Estonian). Currently only introduction is in English and the browsing has to be done in Estonian.

## Additional resources

Overview of Estonia's IT-development history – eupractice.eu country factsheet http://www.epractice.eu/document/3327.

## Additional links

Riso http://www.riso.ee

Ria http://www.ria.ee

Tehnilise Järelevalve Amet (Estonian Technical Surveillance Authority), http://www.tja.ee/

# National Report of Finland

## Introduction

### Interview

Date and Duration 2008-08-29 – 135 minutes.

| | |
|---|---|
| Interviewee | Mr Kari Ojala |
| Authority | Ministry of Communications |
| Position title | Communications Counsillor, Senior Advisor |
| Education/Training/ Degree | M.Sc. in Electronics<br>- telecommunications<br>- applied electronics<br>- medical electronics |
| Task and Responsibilities | Critical Infrastructure,<br>Preparedness |
| If applicable, rel.ship to ENISA | Mrs. Mari Herranen is our liaison officer to ENISA |

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | Ministry of Transport and Communications (MTC) |
| Main Tasks | -Communications policy and strategy<br>-Preparation of laws and statutes<br>-Granting of mobile and radio licences |
| Reports to | Parliament |
| URL for Agency or Authority | www.mintc.fi |
| Year established | 13 September 1892 |

### Authorities involved but not part of the interview

| Authority | The Finnish Communications Regulatory Authority (FICORA) | National Emergency Supply Agency (NESA) | National CERT (CERT-FI) | The Office of Data Protection Ombudsman | State Cabinet |
|---|---|---|---|---|---|
| Main Tasks | -Enforcement of communication laws<br>-Regulation<br>-Controlling communications and disturbances, and interference<br>-Granting frequency licenses<br>- CERT-FI operations | - security of supply i.e. preparedness, critical infrastructure<br>- maintain stockpiles<br>- promotion and coordination the readiness of authorities for exceptional circumstances<br>- promotion of preparedness in companies<br>- secure the technical INFRASTRUCTURE functioning<br>- secure the production of fundamental goods and services in CRISIS<br>- analysing the threats for security of supply and make protection plans<br>- cooperation with corresponding organisations in other countries | FICORA's CERT-FI group prevents, observes, and solves information security violations and gathers information on threats to information security. CERT-FI cooperates with national and international CERT actors and representatives of trade and industry. It is in contact with suppliers of equipment, networks, and software as well as with the police and other authorities.<br>CERT-FI provides special service for actors in CI in Finland. The special service includes 24/7 incident warning and solving, also via SMS and secured mobile public authority network VIRVE, personal advising, and focused product vulnerability warnings. | The protection of personal data, provide guidance and advice on all issues related to the processing of personal data and control the observance of the law. | Governing |
| Reports to | Ministry of Transport and Communications | Ministry of Employment and Economy | | Ministry of Justice | President, Parliament |
| URL | http://www.ficora.fi | http://www.nesa.fi | http://www.cert.fi | http://www.tietosuoja.fi/1560.htm | http://www.valtioneuvosto.fi/etusivu/en.jsp |
| Year agency or authority was established | 1988 | 1993 (1924) | | | |

## Scope and governance

The country's strategy regarding information society and e-communciation networks is outlined in its strategy – YETTS - approved by government resolution in late November 2006 (see FI 10) which will be renewed within couple of years.

The report defines the term preparedness[19] as follows:

> *All measures implemented to guarantee that tasks can be carried out with minimal disruption in all security situations. These measures include, among other things, contingency planning, advance preparations and preparedness exercises.*

Additionally there is a strategy for information security.

**Question 1 : The authorities**

Finland has liberalised its communications in the years 1987...1994. In 1940's we had over 800 telecom operators while today's number is 185 including 43 service operators. Today three operators, namely TelisaSonera, Elisa and DNA[20] account for 90% or more of market share as far as  telecom infrastructure markets are concerned[21].

The authorities responsible for issues related to resilience of public and other essential e-communication networks are the following:

- Ministry of Transport and Communications (MTC) (laws, statutes and gives licenses to operate mobile telecom services)
- Ministry of Interior
- The Office of Data Protection Ombudsman
- Ministry of Finance
- Ministry of Education
- FICORA (The Finnish Communications Regulatory Authority) – also administers radio frequency licenses
- NESA (National Emergency Supply Agency) and NESC (National Emergency Supply Council
- The National CERT-FI

The only authorities who can give norms for telecommunications are MTC and Ficora.

**Question 2 : The mandate of the authorities**

MTC[22] has the responsibility for policy issues, preparing the legislation for transport and communications and granting licenses for mobile networks. MTC has cooperates closely with providers and may give recommendations.

[19] *See FI 10, p. 65*

[20] *DNA is a group of providers that formed this association in order to gain economies of scale and secure better supply contracts. In turn, DNA consists of several operators that run their business independently.*

[21] *For details see http://www.ficora.fi/en/index/viestintavirasto/lehdistotiedotteet/2008/P_9.html*

[22] *The Ministry of Transport and Communications has about 2-3 experts addressing resilience and usability as well as economic issues pertaining to network robustness and telecommunication in general.*

Ministry of Interior deals with the communications network for authorities, especially for emergency[23].

The Office of Data Protection Ombudsman provides guidance and advice on all issues related to the processing of personal data and controls the observance of the law.

Ministry of Finance gives recommendations for ICT in public authorities which are used also as guidelines in private sector.

Ministry of Education is in charge of preparation of the IPR (Intellectual Property Rights) legislation.

FICORA (The Finnish Communications Regulatory Authority) regulates the security and protection matters (among the others) at the teleoperators and electronic mass media, which constitute an important part of CII.

The National CERT-FI group provides special service for the Critical Infrastructure (CI) actors.

NESA[24] is the cross-administrative operative authority for the security of supply in Finland, under the auspices of the Ministry of Employment and the Economy. NESA serves to develop cooperation between the public and private sectors in the field of economic preparedness, in coordinating preparations within the public administration, and in developing and maintaining the security of supply.

NESC is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyze threats against the country's security of supply, to plan measures to control these threats, and to promote readiness planning in individual industrial sites. NESC members include representatives of ministries, government agencies, the private economy, and various industrial organizations. NESC has several planning bodies in the area of information infrastructure.

NESA and NESC analyze threats and risks that may affect the critical infrastructure. They formulate plans and guidelines for public authorities and businesses with respect to the management and control of such threats and risks.

MTC's Director General in Communications Department is the chair of Information Society Pool.

*In practice*: The telecom operator needs to get a license for mobile telecommunication networks from the MTC first. Thereafter, FICORA will assign the operator a radio frequency

*[23] Details can be found at http://www.everkot.fi/index.php?L=2*

*[24] The stakeholders [Critical Information Infrastructure (CII) actors] are members of a Public Private Partnership organization, NESC (National Emergency Supply Council), The security of supply organization in Finland consists of a government agency, National Emergency Supply Agency (NESA) and of a public private partnership organization, National Emergency Supply Council (NESC). NESA is also the secretariat in the Council.*

license. These two licenses must be secure first before one can begin to operate in the assigned spectrum.

FICORA focuses on administering the law and, if necessary, provides additional regulation to further clarify the law as regulated in Telecommunications Market Act (FI 1, especially articles 128 and 129). It can conduct audits (see Q 5) and take other steps to assure the control necessary in assuring compliance and the level of network dependability and resilience demanded.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

There are a few issues that can be mentioned here – not in any particular order [25], namely

a. Communication Market Act articles 90, 128 and 129 (see FI 1),
b. Act on the Protection of Privacy in Electronic Communications articles 19-23, 26-33 ( FI 2),
c. Radio Act (FI 3), Act on Communications Administration (FI 4),
d. Government Decree on Communications Administration (FI 5),
e. Preparedness Act (Renewal in Finnish Parliament) (FI 6) and
f. MTC's Code of Conduct for Preparedness (FI 7).

As far as electronic information and communication technologies (ICT) are concerned, again the strategy is quite specific, too, but the main mandatory issues come from Communications Market Act. The YETTS strategy (see FI 10) stipulates that:

> *the basic infrastructure for ICT systems must be sufficiently secure and safeguarded contain redundancies even in normal conditions. Otherwise, they will not survive in all security situations. Special attention must be paid to teleoperators' preparedness obligations, including relevant authority-teleoperator cooperation, data security in networks and services as well as to guaranteeing services to selected user groups (p. 46)*

**Question 4 : Initiatives between providers and public authorities**

MTC, FICORA and NESA/NESC have permanent and AdHoc working groups (WGs). Public-private partnership (PPP) has been instrumental for national preparedness in Finland for over 50 years (NESC).

As already mentioned in previous answers, FICORA's process in issuing technical regulations for telecom operators is very collaborative. This means the stakeholders are involved in the process from the very early phase. That is one example of the long PPP history Finland has. PPPs are an effective way for making sure that the most important

[25] *Under the section of Additional Resources in this document, an extensive list of detailed lower level regulations are provided including URLs to English translations wherever available.*

issues are regulated. In turn, this achieves better resilience and protection on public communication networks and services.

The private sector is involved in identifying and designating national critical infrastructures in the ICT sector in the NESC committees, particularly in NESC Information Society Sector, and in its Communications Networks Pool, Electronics Industry Pool, Information Technology Pool, and Mass Communications Pool. In the pools, the critical enterprises are chosen using the following criteria:

- important position or great market share in a critical field,
- production or service is indispensable or very important for national security of supply,
- service is regionally indispensable,
- central task or position in value network / value chain,
- one of few actors in a critical field,
- an important subcontractor for the preparedness and business continuity of a critical enterprise,
- strategic export production which makes critical import possible; and
- (un)controllability from Finland.

In the context of public private partnerships NESA may participate in some financing regarding e.g. EMP-shielding of very important equipment rooms of eCompanies. NESA's year budget for the support of ICT is appr. 8 M€.

The authorities stipulate what quality levels are to be achieved. However, it is left to the operators to choose technical and other means for getting there.

Several important resilience projects where undertaken this year. One example is a project to improve the spare capacity for emergency power supply with generators.

Possible Changes: NESA has the possibility to fund efforts of public interest that help improve preparedness and resilience of public e-communication networks. NESA's year budget for the support of ICT is approximately Euro 8 mio.

## Tasks

### Question 5 : Typical task

A detailed answer of the tasks of FICORA (the regulator) as well as NESA and NESC is given in Q 2.

- FICORA's decision 54 (spare energy, priorities, physical protection, etc.).
- IT Society Sector belongs to the NESC organisation. Under the IT Society Sector exists e.g. telecommunications and information technology pools. Their task is to monitor, study, plan, and prepare measures for improving security of supply in their own branches, in co-operation with companies.

Exchange of information is lively between providers and authorities. The main challenge for ICT in preparedness is to improve cooperation, agreements and regulations especially in IT sector. Common exercises with private sector are crucial, e.g. Tieto (Knowledge) 2007.

Preparedness auditing (resilience, technical audit) is done by MTC, FICORA together with NESA.

- FICORA does auditing approx. 10 providers per year.
- NESA does auditing 2 providers per year which is included in FICORA's number.
- Extra auditing is done by MTC.

FICORA enforces communications regulation. FICORA usually gives a deadline by which the operator must improve or show how the identified risks have been better managed in order to improve network resilience.

*Costs and resilience*: Cost-benefit analysis is an important part of any resilience work. Finland's operators can use the cost systems they prefer. Nevertheless, this still requires the operator to be able to show certain figures and be able to explain succinctly how they were arrived at. Information collected is then provided to the European Commission (see also page 80 for a cost approach regarding risk and resilience).

**Question 6 : Exchange of information between providers and public authorities**

The kind of information exchanged between operators and authority (ies) can be described as follows:

- failure reporting is mandatory according to article 21 in the Act on the Protection of Privacy in Electronic Communications (FI 2)[26],
- preparedness and security of supply reports are mandatory,
- FICORA's order 9 and recommendation 9 (see 9) in reference list specify what needs to be reported (see also FI 11 and FI 12 in reference list for link to forms that must be used to report what exactly – online form); and
- NESA/NESC exchange data with MINTC, FICORA and telecommunications companies regarding readiness of communication networks and services in Finland.

Information sharing has a central role in raising national preparedness (see NESC, NESA, FICORA, CERT-FI). Finland follows and prefers using principle-based standards[27].

Accordingly, FICORA's process in issuing technical regulations for telecom operators is very collaborative. As well, stakeholders are involved in the process from the very early phase. Information sharing among those groups is essential in order to foster resilience and

[26] *FICORA's order 9 provides additional regulation to further clarify the law on this matter.*

[27] *Principle-based standards or guidelines outline the objectives but leave it to the operator to decide how to fulfill or reach these. However, the operator must be able to demonstrate that best practice was being followed or else be able to justify not doing so, while achieving the objectives set regarding network resilience.*

protection on public communication networks and services taking into account business secrets in competition. However, naturally information sharing (even among those closed groups) can not be very detailed because of the nature of issues that are handled.

The focus of auditing is the dependability of communication networks including preparedness together with implementation level. NESA provides advice to undertakings during inspections to help telecommunications companies improve their preparedness in disruptive situations of all kind. That is done by discussions during inspections and by reports of inspections afterwards.

As well, FICORA has a large database that contains information about operators including but not limited to infrastructure density, structure, architecture and so forth.

Possible Changes: These days often FICORA may find out about disruption of services and so forth via the media. In turn, if the latter asks the regulator for information. FICORA then asks the operator to provide information. This includes giving reasons about the plans for minimizing the likelihood of such an event in the near future. If FICORA has an indication that something happened whilst not having been informed by the operator, it can do an unannounced audit at the corporation’s premises.

There is still room for improvement here within the next 24 months.

### Question 7 : Handling of security incidents

Security incidents are reported according to FICORA's order 9 [28]. The kind of information to be disclosed is specified in: a) Publicity Act (FI 8), b) Act on the Protection of Privacy in Electronic Communications (FI 2); and c) Act on Competition (FI 8).

Incidents can be reported to the CERT FI using an online form (see FI 11 for link to English form). Faults and disturbances in communication networks and services are reported to FICORA also online (see FI 12 for link to English form).

### Question 8 : Audits related to resilience

In part, answers to this are also provided in Q 5 and 6 of Finland’s Country Report. Regarding who performs the audit, NESA participates in inspections of readiness in telecommunications companies together with MINTC and FICORA every year.

MINTC, FICORA and NESA/NESC in co-ordination with each other perform inspections related to integrity and availability of public networks particularly in disruptive situations and exceptional conditions.

FICORA audits approx. 10 providers per year while NESA audits 2 providers per year together with FICORA. Extra auditing is done by MTC.

[28] *See Detailed orders 2) (Viestintävirasto 9 B/2004 M) in Additional reference list).*

**Question 9 : Enforcement actions**

FICORA has the possibility to impose fines according to the law. However, there rarely if ever is a need to consider such type of measure. Instead, cooperation and discussions have resulted in the improvements needed to achieve better dependability and resilience of public e-communication networks.

Finland is in the fortunate position to be able to report that no fines were issued due to resilience related matters again any of the infrastructure operators or service providers.

## Risk Management and preparedness measures

**Question 10 : The national risk management process**

In Finland, the focus is on preparedness, whereby dependability and resilience of e-communication networks is part of these efforts.

For instance, ministries' preparedness obligations include, but are not limited to, the special situations. Ministries have to prepare for all estimated risks and threats within their purview (see FI 10 p. 60).

The NESC pools use a 5 criteria indicator set, defined by NESA and NESC together, to assess annually the level of security of supply in all critical sectors (CI, CII and others). The indicators used are:

- capacity redundancy,
- availability redundancy,
- domestic controllability,
- security arrangements; and
- level of contingency planning.

The analysis is done by breaking down each infrastructure (and services) to components (typically tens of them), including supporting functions from other sectors.

In addition, NESA and NESC have used a linear risk analysis method for identifying the most critical areas in the interdependent infrastructures. This method gives higher risk value to those elements / areas on which many others depend. The mathematical method is well established and public (see page 80).

The method has been used to rank infrastructure risks on a national level. It has also been applied to a detailed analysis of ICT-infrastructure in order to rank the functions of CII by their criticality.

Telecom operators in Finland are obliged to notify FICORA about major faults and disturbances in communication networks and services. Based on that information and also information gathered from telecom operators by other means FICORA has made estimations on risk levels and has given regulations for telecom operators to reduce those risks (see FI 12 for the online report to report major faults).

Possible Changes: Critical infrastructures are coupled and their failures are interdependent in many ways. NESA staff under the leadership of Hannu Sivonen has developed a mathematical method for quantifying and ranking risks by taking the interdependencies of failures into account, even though exact statistics are not available. The method is the same as used by the Internet search engine Google when ranking page links. You find more details about this in page 80. Here, economic values are assigned to various risk such as when breaking down each infrastructure into its components including functions from other sectors[29].

### Question 11 : The preparedness and recovery measures

Preparedness and recovery measures are considered as «business as normal» kind of activities! Several, if not all, technical regulations by FICORA are aimed at mitigating risks.

The blue light organizations (e.g., police and the 112 number) use a Tetra-based network whereby mobiles using that network can also function similar to a walkie talkie. Operators have to decide themselves which services the need to prioritize do satisfy the market. Competitive markets means that operators' interests are served best if in case of problems full services are restored as quickly as possible. FICORA has also created a ranking system in their regulation 54/2008M (see Additional resources).

### Question 12 : Incident response capabilities

The most important incidents response capabilities in Finland are the owners and operators of the networks who bare the burden to response. FICORA and NESA give support to the operators facing an incident. FICORA has its own incident response capability CERT-FI. NESA participates in the working groups and finances CERT-FI activities from a Security of Supply Fund. Private companies and other organisations like universities have their own CERTs. Domestic cooperation is pretty well organised as is international one, too.

i. CERT-FI gives vulnerability alerts publicly and additionally directly to partners.
ii. CERT-FI publishes also on its web site analysis and statistics.

### Question 13 : Good practice on resilience

Until now we do not have a central register making information accessible as far as resilience is concerned. Many of the regulations given by FICORA are resilience targeted – the meaning of the regulation is to enhance resilience within a certain context, i.e. e-mail, Internet access, network maintenance and so forth.

Another kind of a set of best practices is the work done by Ministry of Finance under the umbrella called VAHTI. It has published several resilience related guidelines. Visit

[29] *You may received a copy of the spreadsheet that can be used to apply this exercise at your institution directly from Hannu Sivon through Nesa Fill out the online contact form here: http://www.nesa.fi/contact-us/.*

http://www.vm.fi/vm/en/01_main/index.jsp and enter VAHTI in the search box. Numerous guidelines will come up in English.

As far as information security is FICORA (the regulator) has a good website with lots of pertinent information. Another useful link for good practice on resilience issues and vulnerabilities is to be found on their web site. All here referred materials are publicly available.

### Question 14 : Guidelines for procurement

There is not a law that specifies the addressing of resilience and dependability when purchasing network hardware and so forth. Nonetheless, NESA has guidelines to support resilient facilities for preparedness.

As well, Finnish laws and regulations state the QoS (Quality of Service) of communications and FICORA has the power to demand it. References are as earlier mentioned Communications Market Act and FICORA’s orders.

## References

### Overall Regulation

**FI 1** Viestintämarkkinalaki (393/2003 Communication market act) [Online] (Available: http://www.finlex.fi/fi/laki/ajantasa/2003/20030393.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/2003/en20030393?search[type]=pika&search[pika]=communication*
Particularly relevant are articles: 90, 128 and 129.

**FI 2** Sähköisen viestinnän tietosuojalaki (516/2004 Act on the protection of privacy in electronic communications).
Available: http://www.finlex.fi/fi/laki/ajantasa/2004/20040516.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/2004/en20040516?search[type]=pika&search[pika]=communication*

Particularly relevant are articles: 19-23 and 26-33.

**FI 3** Laki radiotaajuuksista ja telelaitteista (1015/2001 Radio act) [Online] (Available: http://www.finlex.fi/fi/laki/ajantasa/2001/20011015. Last Access: September 18, 2008) Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/1988/en19880517?search[type]=pika&search[pika]=communication*

**FI 4** Laki viestintähallinnosta (625/2001 Act on communications administration).
Available: http://www.finlex.fi/fi/laki/ajantasa/2001/20010625.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/2001/en20010625?search[type]=pika&search[pika]=communication*

**FI 5** Valtioneuvoston asetus viestintähallinnosta (697/2001 Government decree on communications administration).
Available: http://www.finlex.fi/fi/laki/ajantasa/kumotut/2001/20010697.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/2001/en20010697?search[type]=pika&search[pika]=communication*

**FI 6** Valmiuslaki (Emergency Powers Act, 1080/1991) (Renewal in Finnish Parliament).
Available:
http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search%5Btype%5D=pika&search%5Bpika%5D=valmiuslaki#highlight2.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/1991/en19911080.

**FI 7** Valmiusohje (MTC's Code of Conduct for Preparedness) [Online] (Not available, classified).

**FI 8** Laki viranomaisten toiminnan julkisuudesta (0621/1999, Act on the Openness of

Government Activities).
Available: http://www.finlex.fi/fi/laki/ajantasa/1999/19990621.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/1999/en19990621?search%5Bteksti%5D=621%2F1999&search%5Btype%5D=meta.

**FI 9** Laki kilpailunrajoituksista (480/1992, Act on competition restrictions).
Available:
http://www.finlex.fi/fi/laki/ajantasa/1992/19920480?search%5Btype%5D=pika&search%5Bpika%5D=kilpailu.
Last Access: September 18, 2008.
Non-binding English text
http://www.finlex.fi/en/laki/kaannokset/1992/en19920480?search%5Bteksti%5D=480%2F1992&search%5Btype%5D=meta.

**FI 10** The strategy for securing the functions vital to society (government resolution 23.22.2006).
Available: http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf.
Last Access: September 18, 2008.
(PS. A new strategy is expected to be published by mid 2009).

**FI 11** Finnish Communications Authority -- CERT-FI incident report form.
Available English: http://www.ficora.fi/englanti/lomake/TIe.pdf.
Last Access: September 22, 2008.

**FI 12** Finnish Communications Authority -- Form for reporting fauls and disturbances in communications networks and services.
Available English: http://www.ficora.fi/englanti/lomake/TIe.pdf.
Last Access: September 22, 2008.

## Additional Resources

### Detailed Regulation

[YHTEISKUNNAN ELINTÄRKEIDEN TOIMINTOJEN TURVAAMINEN
- VIESTINTÄVIRASTON ANTAMIA SÄÄDÖKSIÄ JA MÄÄRÄYKSIÄ.]

*Source: FICORA, telecommunications orders*
*http://www.ficora.fi/index/saadokset/maaraykset/teletoiminta.html*

1) MÄÄRÄYS VIESTINTÄVERKKOJEN JA -PALVELUJEN VARMISTAMISESTA (Viestintävirasto 54/2008 M) (REGULATION ON PRIORITY RATING, REDUNDANCY, POWER SUPPLY AND PHYSICAL PROTECTION OF COMMUNICATIONS NETWORKS AND SERVICES)
Available:
http://www.ficora.fi/attachments/suomi_R_Y/5vB4GW4xt/Files/CurrentFile/Viestintavirasto542008M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/5wJbOLb5P/Files/CurrentFile/FICORA542008.pdf

SEKÄ PERUSTELUT JA SOVELTAMINEN (Justification and applying)
Available:
http://www.ficora.fi/attachments/suomi_M_Q/5vB4CgCnI/Files/CurrentFile/MPS54.pdf.
Last Access: September 18, 2008.

**Deatailed Orders [YKSITYISKOHTAISIA MÄÄRÄYKSIÄ:]**

***Communications in Networks***

2) MÄÄRÄYS TIETOTURVALOUKKAUSTEN SEKÄ VIKA- JA HÄIRIÖTILANTEIDEN ILMOITTAMISVELVOLLISUUDESTA YLEISESSÄ TELETOIMINNASSA (Viestintävirasto 9 B/2004 M) (REGULATION ON OBLIGATION TO REPORT INFORMATION SECURITY INCIDENTS AND FAULTS AND DISTURBANCES IN PUBLIC TELECOMMUNICATIONS).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858975217/Files/CurrentFile/Viestintavirasto09B2004M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489108198/Files/CurrentFile/FICORA09B2004M.pdf.

JA SUOSITUS SEN SOVELTAMISALASTA (Justification and applying).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1156442752261/Files/CurrentFile/SMS09B.pdf.
Last Access: September 18, 2008.

3) MÄÄRÄYS SÄHKÖPOSTIPALVELUJEN TIETOTURVASTA JA TOIMIVUUDESTA (Viestintävirasto 11/2004 M)
*Erityisesti pykälät 7§: haittaohjelmaliikenteen havaitseminen ja suodattaminen sekä 8§: muun haitallisen sähköpostiliikenteen havaitseminen ja suodattaminen.* (REGULATIO ON INFORMATION SECURITY AND FUNCTIONALITY OF E-MAIL SERVICES).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858975686/Files/CurrentFile/Viestintavirasto112004M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489108386/Files/CurrentFile/FICORA112004M.pdf.

JA SUOSITUS SEN SOVELTAMISALASTA (Justification and applying).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1156442753292/Files/CurrentFile/SMS11.pdf
Last Access: September 18, 2008.

4) INTERNET-YHTEYSPALVELUJEN TIETOTURVASTA JA TOIMIVUUDESTA (Viestintävirasto 13/2005 M)

*Erityisesti pykälät 6§: runkoverkon tietoturvallisuus sekä 8§: haitallisen liikenteen havaitseminen ja suodattaminen runkoverkossa.*
(REGULATION ON INFORMATION SECURITY AND FUNCTIONALITY OF INTERNET ACCESS SERVICES ).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858976108/Files/CurrentFile/Viestintavirasto132005M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489108776/Files/CurrentFile/FICORA132005M.pdf.

JA SUOSITUS SEN SOVELTAMISALASTA (Justification and applying).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1156442753495/Files/CurrentFile/SMS13.pdf
Last Access: September 18, 2008.

5) MÄÄRÄYS TELEYRITYSTEN TIETOTURVASTA (Viestintävirasto 47 B/2004 M) (REGULATION ON INFORMATION SECURITY OF TELECOMMUNICATIONS OPERATORS).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858986420/Files/CurrentFile/Viestintavirasto47B2004M.pdf
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489119589/Files/CurrentFile/FICORA47B2004M.pdf.

6) MÄÄRÄYS VIESTINTÄVERKKOJEN JA -PALVELUIDEN SUORITUSKYVYSTÄ (Viestintävirasto 29 D/2005 M) (REGULATION ON THE PERFORMANCE CAPACITY OF COMMUNICATIONS
NETWORKS AND COMMUNICATIONS SERVICES).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858980467/Files/CurrentFile/Viestintavirasto29D2005M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489110058/Files/CurrentFile/FICORA29D2005M.pdf

7) MÄÄRÄYS HÄTÄLIIKENTEEN OHJAUKSESTA JA VARMISTAMISESTA (Viestintävirasto 33 C/2006 M) *Erityisesti pykälä 6§ hätäliikenteen varmistaminen.* (REGULATION ON ROUTING AND ENSURING EMERGENCY TRAFFIC).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/5jTsnTU8u/Files/CurrentFile/Viestintavirasto33C2006M.pdf Last Access: September 18, 2008).
Non-binding English text
http://www.ficora.fi/attachments/englanti/5kbMwxzBC/Files/CurrentFile/FICORA33C2006M.pdf.

***Network Construction***

8a) MÄÄRÄYS KIINTEISTÖN SISÄISESTÄ YHTEISANTENNIVERKOSTA JA –JÄRJESTELMÄSTÄ **(**Viestintävirasto 21 E/2007 M) (Customer premises community aerial network and community aerial system).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/5qKajkgei/Files/CurrentFile/Viestintavirasto21E2007M.pdf.
Last Access: September 18, 2008 (available in Finnish and Swedish).

8b) JA SUOSITUS SOVELTAMISALASTA (Justification and applying).
Available:
http://www.ficora.fi/attachments/suomi_M_Q/5yC5S95jl/Files/CurrentFile/MPS21.pdf.
Last Access: September 18, 2008.

9a) MÄÄRÄYS KIINTEISTÖN SISÄJOHTOVERKOSTA (Viestintävirasto 25 E/2008 M) (Customer premises telephone networks).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/5uQ33dGiz/Files/CurrentFile/Viestintavirasto25E2008M.pdf.
Last Access: September 18, 2008 (available in Finnish and Swedish).

9b) JA SUOSITUS SEN SOVELTAMISALASTA (Justification and applying).
Available:
http://www.ficora.fi/attachments/suomi_M_Q/5wTMx8ORg/Files/CurrentFile/MPS25.pdf.
Last Access: September 18, 2008, Non-binding.

10) MÄÄRÄYS VIESTINTÄVERKKOJEN YHTEENLIITETTÄVYYDESTÄ, YHTEENTOIMIVUUDESTA JA MERKINANNOSTA (Viestintävirasto 28 F/2005 M) *Erityisesti pykälä 4 §: yhteydenmuodostus, yhteenliitettävyys ja yhteentoimivuus.* (ON INTERCONNECTIVITY, INTEROPERABILITY AND SIGNALLING IN COMMUNICATIONS NETWORKS).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858979014/Files/CurrentFile/Viestintavirasto28F2005M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489109854/Files/CurrentFile/FICORA28F2005M.pdf.

11) MÄÄRÄYS VIESTINTÄVERKON SÄHKÖISESTÄ SUOJAAMISESTA (Viestintävirasto 43 C/2004 M) (Electronic protection of a telephone network).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858985452/Files/CurrentFile/Viestintavirasto43C2004M.pdf.
Last Access: September 18, 2008 (available in Finnish and Swedish).

12) MÄÄRÄYS VIESTINTÄVERKON VERKONHALLINNASTA (Viestintävirasto 50 C/2007 M) (REGULATION ON MANAGEMENT OF COMMUNICATIONS NETWORKS).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/5rklMXZzx/Files/CurrentFile/Viestintavirasto50C2007M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/5rkkISOB0/Files/CurrentFile/FICORA50C2007M.pdf.

SEKÄ SUOSITUS SEN SOVELTAMISALASTA (Justification and applying).
Available:
http://www.ficora.fi/attachments/suomi_M_Q/5rklBtci5/Files/CurrentFile/MPS50.pdf.
Last Access: September 18, 2008.

13) MÄÄRÄYS VIESTINTÄVERKKOJEN JA -PALVELUJEN TEKNISESTÄ DOKUMENTOINNISTA (Viestintävirasto 41 C/2004 M) (REGULATION ON TECHNICAL DOCUMENTATION OF COMMUNICATIONS).
Available:
http://www.ficora.fi/attachments/suomi_R_Y/1158858985186/Files/CurrentFile/Viestintavirasto41C2004M.pdf.
Last Access: September 18, 2008.
Non-binding English text
http://www.ficora.fi/attachments/englanti/1156489112948/Files/CurrentFile/Ficora41C2004M.pdf.

**Additional Links**

Ministry of Transport and Communications (MTC), http://www.mintc.fi.

Ministry of Interior, http://www.intermin.fi.

The Office of Data Protection Ombudsman, http://www.tietosuoja.fi/.

Ministry of Finance, http://www.vm.fi.

Ministry of Education, http://www.minedu.fi/OPM/.

FICORA (The Finnish Communications Regulatory Authority), http://www.ficora.fi/.

NESA (National Emergency Supply Agency) and NESC (National Emergency Supply Council, http://www.nesa.fi/ and http://www.nesa.fi/organisation/national-board-of-economic-defence/.

The National CERT-FI, http://www.cert.fi.

## Appendix: EAPC / PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning in Zurich on 9-11 September 2004

Below is a presentation given at the Working group 3: Best Practices and Common Standards in CIP and CEP. It is included here with permission by the author[30] and Finnish government.

Among the principal functions of the National Emergency Supply Agency are financing and controlling critical emergency stockpiles and backup systems made for technical infrastructures in Finland as well as coordinating the ensuring of critical infrastructures and basic services in cooperation with private companies and state agencies.

### Calculating Compound Risk of Failure Based on Interdependencies of Critical Infrastructures

#### 1. This presentation

Critical infrastructures are coupled and their failures are interdependent in many ways. In this presentation we see a mathematical method of quantifying and ranking risks by taking the interdependencies of failures into account, even though exact statistics are not available. The method is the same as used by the Internet search engine Google when ranking page links. The central idea is to use the rough classification and the visually appealing four step colour code presented in the document *Interdependencies of Critical Communications Infrastructure by NATO Civil Communications Planning Committee, Group of Rapporteurs 23.2.2004* and to make calculations based on this and similar classifications. We at the National Emergency Supply Agency are collecting input data for this mathematical model, so the examples that we see are not final. During this workshop we have learned that a good practice needs to be well established. The method we are currently discussing is not finalised yet, but I would like to get your feedback. Do you feel that this idea, when matured, could be used in your countries, too?

#### 2. Why a mathematical model?

We use mathematical models all the time. Assessing the duration of a car trip based on the average speed and the distance to be travelled is one example. The high-tech products that surround us are based on physics and behind that, mathematics.

A mathematical model is a systematic and consistent way to use both the rough assessments of experts, and statistics, if they exist.  It helps us to see the total picture and reach agreement on the relative importance of different items. The structure of the model base, the computer program, allows us to delve deeper into the components of the most critical items.

[30] *Hannu Sivonen, Senior Researcher, National Emergency Supply Agency (contact info: hannu.sivonen@nesa.fi).*

The combined effects and risks caused by the complicated, multilevel interdependencies between tens or hundreds of items are impossible for a human being to assess. Here a computer would help.

A model can help find a new point of view regarding the risks to society and communicate this finding outside the circle of experts.

## 3. Starting point of calculation

The model is built as an Excel spreadsheet. The program which runs the model is about 1000 lines of Visual Basic code. The horizontal lines of the spreadsheet represent items to be explored. Now the program allows for 250 items. If needed, the program can be expanded.

An item is basically just a word or a concept to which we can attach properties like: the frequency, duration, and effect of failures as well as dependency of a failure on the failures of other items.

The input to the calculation is items with these properties. The model assumes a simplified linear behaviour of society: two days of interruption in a service is twice as harmful as one day of interruption.

## 4. Examples of items

One is free to choose any taxonomy of items. We use the list of critical infrastructures and basic services specified in the Finnish government decision on *The Goals of Security of Supply from May 2002 and the threats specified in the decision on Strategy of Securing the Vital Functions of Society* by the Finnish government in November 2003. The list below is a partial example of this taxonomy. Each item can be broken down to a more detailed level.

| TECHNICAL INFRASTRUCTURES | BASIC SERVICES AND SUPPLIES | THREATS |
|---|---|---|
| Energy supply<br>electricity<br>fuel<br>heating<br>Communications<br>fixed line telephone services<br>mobile telephone services<br>Internet-services<br>data communication services<br>security networks<br>Information systems | Agriculture<br>food industry<br>logistics of perishable goods<br>water supply<br>Transport logistics<br>Mass media<br>Health care<br>Financial services | Threats to data systems<br>Illegal immigration<br>Threats to food and health<br>Threats to environment<br>Economic threats<br>Crime and terrorism<br>Disasters<br>International tension<br>War and warlike situations<br>Food supply |

It is important to understand the difference between threats and the rest of items: threats come from outside the system of otherwise interdependent technical infrastructures and basic services. The model will first allocate all risks to the threats, because all failures depend on them, at least indirectly, but they don't depend on anything.

So, in order to see the relative risks involved in the infrastructures and basic services, the model has to be run again, and this time the threats eliminated.

## 5. Colour codes

| |
|---|
| ⬛ |
| 🟥 |
| 🟨 |
| 🟩 |
| |

The interdependencies between different infrastructures and basic services and threats are presented as a grid of coloured squares. The colour symbol BLACK means that a failure in the item in the vertical column is one of the primary causes of a failure in the item in the horizontal row (e.g. relative value of 1). RED means a secondary cause (relative value of 0.1), YELLOW a rare cause (relative value 0.01) and GREEN a possible cause (relative value 0.001). (WHITE: no dependency.) If there are 200 items, there will be 40 000 possible positions in the interdependency grid.

The mean time between failures in each infrastructure or service and occurrence of a threat are classified as BLACK (less than a year), RED (1-10 years), YELLOW (10-100 years), and GREEN (more than 100 years).

The durations of different failures are classified as =< 0.5 day, =< 1 day, =< 0.5 week, =< 1 week, > 1 week.

The direct effect of a one-day-long failure in each infrastructure or service is classified as BLACK (more than 1000 units), RED (100-1000 units), YELLOW (10-100 units), GREEN (1-10 units). The unit can be freely chosen. It can be 1000 €, loss of one human life, or an abstract disadvantage measurement unit.

## 6. Frequency and duration

| | **Mean Time Between Failure (Years)**<br>**(Colour Code)** | | | | |
|---|---|---|---|---|---|
| **Item** | **At most 0.5 day** | **0.5-1 day** | **at most 0.5 week** | **0.5-1 week** | **more than 1 week** |
| electricity | 🟥 | 🟨 | 🟨 | 🟩 | |
| Fuel | | 🟩 | | | |
| Heating | 🟨 | | 🟩 | | |

In this example we see that on the average, for each consumer, electricity fails for a short time once in 1-10 years. Longer interruptions are possible, especially in the countryside where electric lines go through forested areas and are exposed to storms. Fuel market and logistics function very reliably and there are alternative fuels available. The vulnerability of heating lies somewhere in between.

### 7. Effect

The model allows for the input of the direct effect of one day of failure in each item. The area of the effect may concern one city or one province or the whole country.

But in practice, because the calculation allocates the effect according to the combination on multilevel interdependencies, only the sum of direct effects is truly meaningful. This sum is redistributed over all items. So it suffices to put one large figure somewhere into the model to be redistributed. It could be e.g. the GDP of one day of the geographical area concerned.

| **Item** | **Direct Effect of Failure Units / Day (Colour Code)** |
|---|---|
| electricity | ■ |
| Fuel | |
| Heating | |

In this example we have put one black square, over 1000 units, for electricity to be redistributed over all items.

### 8. Interdependencies

| **Depending Item** | **Effective Item** | eletcricity | fuel | heating | telephone services |
|---|---|---|---|---|---|
| Agriculture | | ■ | 🟩 | | 🟥 |
| food industry | | ■ | 🟩 | 🟨 | 🟥 |
| logistics of perishable goods | | ■ | 🟩 | 🟨 | ■ |

| Depending<br>Item | Effective Item | eletcricity | fuel | heating | telephone services |
|---|---|---|---|---|---|
| water supply |  | ■ | 🟩 |  |  |

Here we see that an electricity failure is the primary cause of failure in agriculture, food industry, logistics of perishable goods, and water supply. Failure in fuel availability is only a possible cause. The availability of telephone service is much more important.

Internal causes of failure are frequent (such as technical failure and human error). So, usually there is a diagonal line of black squares in the interdependency grid representing high degree of dependency of items on themselves. If one wants to dig deeper into the internal causes, one has to break an item into its components. For calculations, the horizontal line of reasons is normalised to add up to 1.

The dependency of item A on item B does not mean the conditional probability of A failing when B has failed, but it is the relative share of responsibility of failures in A allocated to failures in B. Therefore we can calculate the combined effect e.g. of electricity by taking the direct effect of each item and multiplying it by its dependency on electricity and summing these up.

But this is the combined effect where only one level of dependencies is taken into account. So this calculation has to be repeated after putting the recently calculated combined effect into the place of direct effect in each item. By repeating this time and time again, we exhaust the total information in the dependency grid and thus take into account the multilevel chains of dependencies.

Fortunately this process ends and converges to certain inherent values of the interdependency grid.

## 9. Results supplied

The results of the calculation are, for each item:

- probability of at least one failure in a year (to give an indication of vulnerability),
- combined effect of failure of one day; and
- combined risk for one year.

The items are sorted by decreasing combined risk.

## 10.Interdependent items

| | CALCULATED OUTPUT | | |
|---|---|---|---|
| | Probability of at Least One Failure a Year | Combined Effect Units a Day | Combined Risk Units a Year |
| Item | % | | |
| data communication services | 86 | 713 | 1 102 |
| electricity | 20 | 2 735 | 507 |
| transport logistics | 87 | 128 | 333 |

Here we see that even though the combined effect of electricity is higher that that of data communication, the risk of data communication is higher because of a higher probability of failure.

This calculation has been run in such a way that the threats have been eliminated, as explained earlier in paragraph 4.

## 11.Threats

| | CALCULATED OUTPUT | | |
|---|---|---|---|
| | Probability of at Least One Failure per Year | Combined Effect Units / Day | Combined Risk Units / Year |
| Group of Items | % | | |
| Threats to data systems | 98 | 463 | 1 559 |
| Economic threats | 2 | 4 607 | 1 173 |
| Threats to environment | 4 | 246 | 70 |
| Crime and terrorism | 2 | 135 | 34 |

Similarly, the calculation of combined risks of threats can be run. The calculation takes into account the interdependencies between the critical infrastructures and basic services, in addition to their dependencies on the threats.

## 12.Status of the model in Finland

The program was technically tested in April 2004. The first pilot set of data concerning the logistics of daily perishable goods was gathered in May. The results of the model were credible and acceptable to the experts in that area.

Now, we are building a model which covers the technical infrastructures and basic services as well as the threats listed in the Finnish government decisions. The input assessments to the model are acquired by interviewing experts in the different areas. This round will last till the end of October 2004. After that we will concentrate on a few critical areas and break them up into their components.

This model reflects a principle adopted by the Finnish government: when the infrastructures and services are protected by appropriate technical solutions and a properly functioning organisation in normal times, this will also be a reliable basis for effective functioning in times of crisis. Thus the model is not a simulation model which alters itself when rare things happen, but a simple static model which facilitates resource allocation.

We, at the National Emergency Supply Agency in Finland, believe that this method brings us one step forward in understanding the interdependencies of infrastructures and basic services as well as the combined effect and risk created by these interdependencies. The mathematical model is a tool which facilitates discussion and the attainment of a common understanding of where the risks lie.

## 13.Summary

It is possible to take complicated interdependencies into account and thereby assess the combined risks in the infrastructure and basic service items as well as the threat items.

The mathematical model is a means of describing the behaviour of different items in society. It brings different fields of expertise onto a common platform. It is one step forward from intuitive assessment of combined risks. The method is no secret: It was discovered by the German mathematician Jacobi in 1846. The same idea is used by the Internet search engine Google when determining which link comes highest on the link list of search results and which comes next.

### The mathematical ideas and assumptions

The occurrence of failures in each infrastructure or service is a Poisson process where the mean time between failures is known or has been assessed. The Poisson process assumes that the occurrence of the next failure is independent on the previous one. The Poisson theory gives us the probabilities of a failure occurring 0, 1, 2, 3, … times a year in each of the duration categories.

The compound effects of failure of the infrastructures or services (or components thereof) are calculated using iterative matrix multiplications, the result of which converges to the dominant eigenvector of the dependency matrix.

The compound risk connected to the infrastructures or services is the stochastically expected value of the effect of failures. This is equal to the (effect * probability * duration) added over the different duration categories and 0,1,2,3,..,15 times of occurrences of failure a year (at 15 times of failures the probabilities are practically zero, so we stop there[31]).

[31] *To get a copy of this spreadsheet for use, please contact Mr. Hannu Sivonen through NESA. Fill out the online contact form here: http://www.nesa.fi/contact-us/*

*National Report of Finland*

# National Report of France

## Introduction

### Interview

Date and Duration 2008-09-02 – 130 minutes.

| | |
|---|---|
| Interviewee | Mr François CHOLLEY |
| Authority | Conseil général des technologies de l'information (CGTI) -Ministère de l'économie, de l'industrie et de l'emploi |
| Position title | Co chairman of innovation and enterprises section |
| Education/Training/ Degree | Engineer |
| Task and Responsibilities | Special adviser |
| If applicable, rel.ship to ENISA | |

**People involved in filling out the questionnaire and reviewing contents** (not part of interview itself)

| | | |
|---|---|---|
| Participant | Mr Michel BENEDITTINI | Mr Constant HARDY |
| Authority | Direction centrale de la sécurité des systèmes d'information (DCSSI) -<br>Secrétariat général de la défense nationale (SGDN)<br>Prime Minister | Service du Haut fonctionnaire de défense (HFD) -<br>Ministère de l'économie, de l'industrie et de l'emploi |
| Position title | Deputy director | Department manager |
| Education/Training/ Degree | Rear admiral | Engineer |
| Task and Responsibilities | Deputy director | Head of commissariat aux telecommunications de défense |
| If applicable, rel.ship to ENISA | DCSSI's director is a member of ENISA management board | |

**Authorities involved with Network Resilience**

| Authority | CGTI - Conseil général des technologies de l'information | DCSSI - Central Information Systems Security Division | HFDS - Haut Fonctionnaire de Défense et de sécurité |
|---|---|---|---|
| Main Tasks | amongst others these are: to enhance the Ministry's capacity to provide high level expertise, strategic studies and consultancy in a complex and rapidly evolving domain - namely, information and communication technology in all its fields of application | Contribute to interministerial definition and expression of governmental policy in terms of information systems security | Has the mission of protecting official secrets, supervising information system security and document classification and archiving rules, and applying defence and emergency plans within the Ministry. |
| Reports to | Minister of economy, industry and employment | General secretary for national defence (Prime Minister). | Minister of economy, industry and employment |
| URL for Agency or Authority | http://www.cgti.org<br>http://www.cgti.org/cgti/CGTI-presentation-anglais.pdf. (English Description) | http://www.ssi.gouv.fr<br>http://www.sgdn.gouv.fr<br>http://www.certa.ssi.gouv.fr | http://www.hfd.minefi.gouv.fr |
| Year established | December 13, 1996 | July 31, 2001 | Sept 2, 1993 |

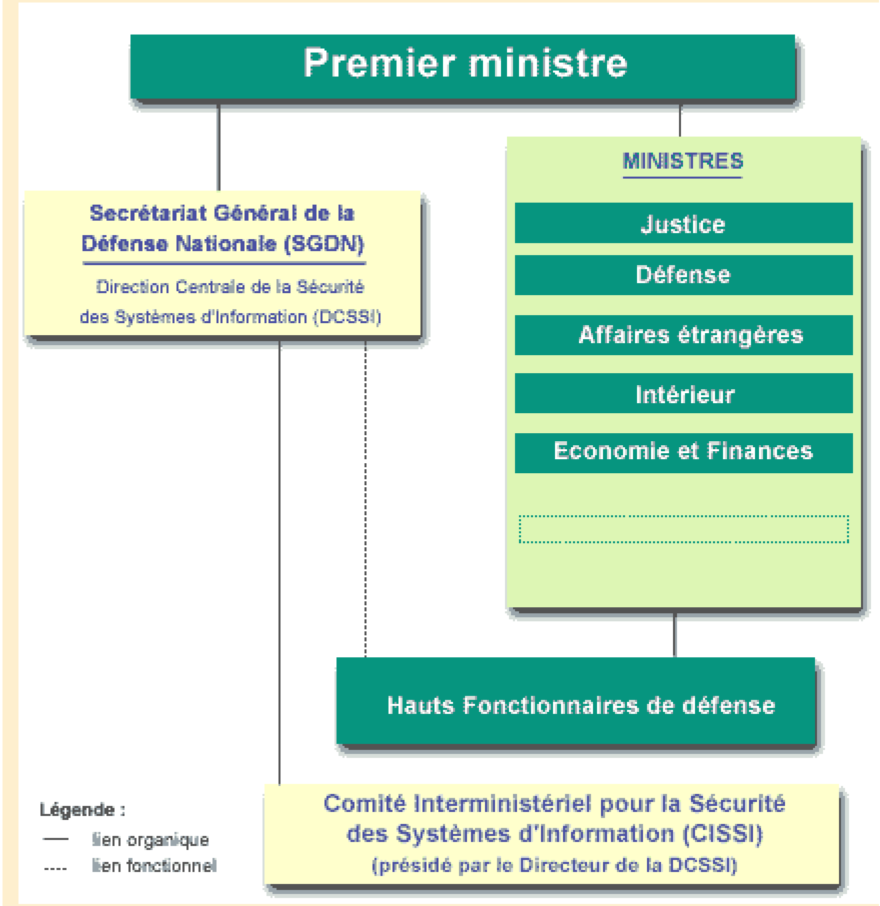
**Authorities involved with Network Resilience (not part of interview nor participating in filling out questionnaire)**

| Authority | Authority for telecommunication and postal regulation (ARCEP) |
|---|---|
| Main Tasks | One of ARCEP's main responsibilities is to ensure that competition can be effectively exercised on the 18 market segments—the so-called "relevant markets"—identified by the European Commission. |
| Reports to | |
| URL for Agency or Authority | http://www.arcep.fr/index.php?id=9&L=1 |
| Year established | 1996 and 2005 |

## About the organisation in France

DCSSI is under the authority of the Prime Minister, through the General Secretary for National Defence. It leads the work of the ministries in the area of security. There is a HFDS in every ministry, who is the DCSSI's point of contact within the ministry. This way, security efforts including resilience of e-communication networks can be coordinated across ministries using the DCSSI.

Organizing matters this way assures close collaboration, information exchange and a more coordinated approach across ministries when addressing dependability and resilience of public e-communication networks. The chart below illustrates how each ministrys HFDS division connects to the DCSSSI.


Premier ministre
Secrétariat Général de la Défense Nationale (SGDN)
Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)
MINISTRES
Justice
Défense
Affaires étrangères
Intérieur
Economie et Finances
Hauts Fonctionnaires de défense
Comité Interministériel pour la Sécurité des Systèmes d'Information (CISSI)
(présidé par le Directeur de la DCSSI)
Légende :
— lien organique
---- lien fonctionnel

Source: (http://www.ssi.gouv.fr/fr/dcssi/orgassi.html ).

In our understanding, resilience of communications networks has to cover both networks for public use (i.e private and individual users) and dedicated networks such as control networks of public utilities (water and power supply). Resilience of communications is part of a broader issue, i.e. resilience of critical infrastructures.

A distinction is made between: a) Infrastructure owners whereby France Telecom, the incumbent operator, owns between 80-90% of all the fixed lines networks. The remainder is owned mainly by the two new operators: Neuf-Cegetel and Free; and b) Service providers whereby France Telecom has about 50-60%, Free 25-30% and Neuf Telecom Cegetel 20-25% of market share.

France has three main mobile operators namely Orange (France Telecom) (44%), SFR-Neuf-Cegetel (34%) and Bouygues Télécom (17% of market share). France's mobile virtual network operators (MCNO) capture less than 5% of market share altogether.

France is considering auctioning a fourth mobile license to a new operator to challenge the country's existing trio: Orange (France Telecom), SFR and Bouygues Télécom. However, a recent finance ministry study also argues that mobile virtual network operators (MVNOs) can boost competition.

Currently Bouygues Télécom and KPN (see NL Country Report – Dutch incumbent) are talking about if the latter may be able to use Bouygues Télécom's network. This would enable the Dutch company to become a virtual mobile operator in France. The move could undermine the sale of a fourth licence and the arrival of an aggressive new domestic competitor in France.

As well, there are fibre optic cables along power lines owned by Électricité de France EDF. EDF rents out the use of its fibre optic capacity to network operators. However, France does not classify EDF as a telecom provider. Accordingly, EDF does not fall under the telecom regulatory regime. Nevertheless, the operators leasing this capacity fall under the telecom regulation. In turn, this means that EDFs network is being assessed/ audited indirectly.

As far as telecommunication networks are concerned, France has few critical infrastructure operators. There are two important points to consider here:

a) for the telephony and data transfer, the operators concerned will be those having more than 10% of the national users' market, and
b) for the internet, the conditions defining the critical infrastructure operators have not been set at this time.

Redundancy and resilience: State of the art levels of redundancy must be part of any network if one intends to have a resilient network. Hence, checking software and hardware architecture assures that the network infrastructure represents state of the art. Of particular interest is therefore, how an operator deals with redundancy (see also Q 5). In addition, it is essential to have guidelines and procedures to deal with outages or failures.

As well, matters of resilience go beyond telecommunication and include, for instance, power supply (electricity networks, batteries and backup generators). It goes without saying that telecommunications resilience is important not only for operators but also for other organizations that depend on the service running properly to deliver their product.

Enforcement of matters pertaining to resilience is handled at the state level.

## Scope and governance

### Question 1 : The authorities

In the French organisational structure, every Ministry is responsible for issues related to resilience of networks in its field of responsibility. This part of a ministry's work is coordinated from the Prime Minister's Office. The organisational structure is based on a governmental decree (FR 2) that gives every Ministry the responsibility regarding the resilience of critical infrastructure in the Ministry's respective area (Interior, Justice, Defence, Food, Electronic communication, Industry, Space and research, Finance, Water, Health, Transportation, Energy) (see FR 1 to FR 4). This organisation applies to national networks.

The Ministry of Economy, Industry and Employment – Haut Fonctionnaire de Défense (HFD) (see RF 11) are in the process of defining which of communication networks run by operators can be considered public/strategic and must, therefore, be resilient (work in progress).

Possible Changes: France does intend to deal with service providers as well as operators of infrastructure. Investigation will be at the basic level to allow France to make sure that resilience is assured at infrastructure as well as service level. It was highlighted that many severe issues and disasters have their root in software problems and not the physical infrastructure per se. Hence, software architecture and hardware architecture require careful assessment to assure dependability and resilience of public e-communication networks.

Finally, dependable power supply and resilience of e-communication networks is highly interdependent. Hence, HFD addresses this as part of its mandate within the ministry (see also Feb. 2006 decree – FR 11 in reference list).

### Question 2 : The mandate of the authorities

Every Ministry has to analyze the risks and to establish appropriate national guidelines for the activities that are considered as essential for the stability of the country. It also approves the security plan submitted by critical infrastructure operators among which are communications network and service operators. The general policy is determined by the Prime Minister. The French Authority for Telecommunication and Postal Regulation (ARCEP – see FR 9 in reference list) is the regulatory authority. It surveys the quality of the public telecommunication networks which covers reliability. But it does not have a mandate for resilience issues. DCSSI surveys the security of information systems.

### Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks

ARCEP's main focus is not on dependability and resilience but, instead on innovation, pricing, regulatory compliance and so forth. France Telecom, the incumbent and universal service provided can be fined by ARCEP if its service does not function properly such as due to a blackout in a region of the country. Investigation regarding such an incident will be done by the Ministry of Economy, Industry and Employment - HFD group (Commissariat aux Télécommunications de Défense) since this would be identified as a matter of national security.

In general, guidelines are written by the DCSSI and must be implemented by the HFD of the different ministries. These guidelines are made available to private companies.

**Question 4 : Initiatives between providers and public authorities**

A permanent working group among the public authorities and the telecommunication operators called "Commission interministérielle de coordination des réseaux et services de télécommunications pour la défense et la sécurité publique" (CICREST) discusses the evolution of the legal framework (see FR 11).

There is also a working group between operators called Fédération Française des Télécommunications et des Communications Électroniques (FFTelecom) that has a working group called Commission Sécurité[32] (see Additional Links).

Both FFTelecom as well as CICREST are channels that can be used to develop and/or discuss best practices or guidelines. This is a way to find consensus on what the HFD intends to do regarding network resilience and security.

<u>Possible Changes:</u> These bodies and their findings also help for a better understanding between the le Secrétariat général de la défense nationale (Secretariat-General for National Defence) (SGDN) and communication operators why and how resilience and dependability of public e-communication networks is a strategic issue.

These dialogues are particularly important, because in competitive markets, trade-offs regarding cost-benefits such as, prices, dependability, risks, innovation and resilience must be made. It will also influence the possibilities of various approaches to be implemented and administered.

Regarding market deregulation and dependability as well as resilience of public e-communications networks two points should be stressed:

1) market deregulation and competition address demand, pricing and supply,
2) achieving highly dependable networks and satisfactory resilience is attained through structure and investment enforced by administrative constraints.

Accordingly, one cannot claim that market deregulation and competition by themselves will improve resilience. Unless the necessary steps are taken from a regulatory perspective[33], efforts undertaken by market participants could be unsatisfactory.

[32] *It had its most recent meeting on May 18, 2008, addressing issues also pertaining to its work with CICREST see http://www.fftelecom.org/docs/prive/CR-securite20081905.pdf*

[33] *Here the regulator can set the parameters of what is expected. The government procurement process is one mechanism whereby market pressure can be put upon operators and infrastructure owners. In turn, as a large*

Competition and price pressure may prevent market participants from being able to invest in resilience unless this is required by regulation.

## Tasks

### Question 5 : Typical tasks

Public consultation with providers to review existing or develop new regulations, guidelines or recommendations is done. However, these consultations do not take place in the area of resilience. Enforcement of regulation is not part of the legal mandate of the agencies. Nevertheless, resilience issues are discussed as part of CICREST's mandate.

As far as auditing is concerned and as pointed out in our answer to Q 2, audits can be part of the activities necessary to establish overall security. When a major basic outage occurs, CGTI will do the investigation. For instance, a severe case occurred in 2007 where during a few hours there was no phone service at all. This triggered

1) an investigation to find out why it had happened and how this could be avoided in the future, as well as,
2) a change in specifications to subsequently assure better redundancy with improved architecture of the e-communication network (see also Q 14).

Possible Changes – Security Master Plan: Each ministry's HFD has to ask the critical infrastructure operator in the ministry's domain to submit a security master plan. There might be a possible conflict of interest amongst master plans across ministries. In this case, such conflicts will have to be discussed with the SGDN to find a consensus across ministries. Operators were informed about the general guidelines and given six months to submit their general operator's plan to the concerned minister. After two years they have to submit their separate protection plan for every point of vital importance to the local authority responsible of the area where such a point is located (see FR 2).

The 2007 case described above (the only recent one regarding resilience) happened in part due to a software glitch/error and lack of redundancy. The results from this investigation will flow into the new procurement guidelines that should be published in 2009 (see Q 14).

### Question 6 : Exchange of information between providers and public authorities

Every operator or provider designated (in progress) has to submit a masterplan for security (based on decree – see FR 3) within two years once general guidelines have been published. The national security guidelines in the telecommunication field have been approved and will be sent to operators by the end of 2008. The information collected this way is under control of each ministry. It is used to check whether the operator or provider

*customer, public agencies and institutions can demand that certain dependability and resilience parameters are addressed and taken care of when tendering for and supplying telecommunication systems and services as part of a infrastructure or telecom service contract (see also Q5, Q9 and Q14).*

is compliant with national security guidelines (confidential not published). Once the operators have submitted their security master plan, the HFD follows up to verify if the plan has been implemented properly and satisfactorily.

Possible Changes: Before the 2006 decree (FR 2 updated in 2008 with FR 3) was issued, HFD had no possibility to get certain information from providers. Based on this regulation, however, the HFD in each ministry has begun to ask operators to provide the security masterplan. The work is still in progress. By 2010 these masterplans will have been a) submitted and, most importantly, b) implemented.

In turn, HFD will have the necessary data and can, if necessary, change regulation accordingly. The security masterplan, as to be submitted by each operator in the future, allows addressing risk management issues. Specifically, this will be useful for evaluating how the operator tries to address which risk using what measures to reduce the likelihood of network failure.

**Question 7 : Handling of security incidents**

Every major outage must be immediately reported to the operational centre for inter-ministerial crisis management in the Ministry of the Interior (see section Additional Links for URL). There is a definition of what constitutes a major or minor failure in the telecommunication network (as stated in the Directive Nationale de Sécurité, Secteur d'activité d'importance vitale "Communications électroniques, audiovisual et information", not made public, defence confidential).

In addition, telecommunications networks are overseen by the centre of defence telecommunications (commissariat aux télécommunications de défense) of the ministry in charge of the industry. Information systems security breaches are examined by the French Computer Emergency Response Team (CERTA), part of the Centre opérationnel en sécurité des systèmes d'information (COSSI - Information Technology Security Operational Center (ITSOC)).

Submitting of information is mandatory and confidential. Nevertheless, as is the case in other Member States, sometimes media is first in report a public incident, and the HFDs may learn about it through the media first or via complaints launched by consumers.

**Question 8 : Audits related to resilience**

Audits on the resilience master plan do not take place. The operators, and above all the historical incumbent are very active in the area of resilience and their work is appreciated. CGTI and HFD are familiar with their procedures and networks. 'Trust' and 'prove' play an important role here.

Newer or small communication operators may be under more cost pressure than more established ones. In turn, this might affect or at least influence their risk management to some degree. France's state authorities are aware of this and, therefore, keep careful watch regarding resilience and dependability of these networks.

Possible Changes: As mentioned in Q5, security master plans must be submitted by critical infrastructure operators. In turn, once submitted HFD will have to assess through an audit how well the operators have implemented the plan. A third party may conduct part of such an audit.

**Question 9 : Enforcement actions**

An operator may be prosecuted in case of neglect to establish a compliant security master plan (see FR 2, Code de la défense, art. L1332-7).

*ARCEP has powers to sanction operators not fulfilling their obligations. It may remove their frequency and numbering resources and, in an emergency, take conservatory measures. (see FR 9)*

The 2007 breakdown (see Q 5) was a commercial issue between the customer and the telecom supplier (see service level agreement - SLA). It did result in penalties as the SLA stipulated financial consequences.

It is important here that based on this major incident, the procurement guidelines (see Q 14) will also address how SLA's should take into consideration and define what is meant by resilience (e.g., is a 100% outage acceptable? If not, what redundancy is needed and how much will this cost?). Again, changing the procurement process accordingly will create a market demand that will require infrastructure operators to satisfy this customer need or else loose market share.

In turn, the recommendations (see Q 14) will trigger the implementation of certain procedures and recommendations if operators want to continue being the supplier of certain services to the state.

## Risk Management and preparedness measures

**Question 10 : The national risk management process**

While there is no national risk management process per se, each Ministry is tasked with doing a risk assessment regarding network resilience and information security by using a specific method prescribed by the SGDN. Most ministries and government agencies use EBIOS (Expression of Needs and Identification of Security Objectives) (see FR 8).

Other approaches exist, such as the MEthode Harmonisée d'Analyse de RIsque (MEHARI) offered by CLUSIF (Club de la Sécurité de l'Information Français) (see FR 10). Both approaches lead more or less to the same results.

All knowledge and results are centralised at the Secretariat-General for National Defence (SGDN) (see Additional Resources for mission and URL).

In 2007, a report on the resilience of communications networks was submitted to the National Council of Homeland Security chaired by France's President (see FR 13 in reference list).

The Ministry of the Interior manages national crises, while the operational end is with Le centre opérationnel de gestion interministérielle des crises[34].

### Question 11 : The preparedness and recovery measures

There two levels how France approaches this challenges, first the national level and second the local level. Every master security plan submitted by an operator within the next two years will have to address both two levels in detail.

France has not yet conducted national exercises addressing the resilience of telecommunication networks. However, France conducts such exercises regularly as far as the security of information systems and data are concerned. Most exercises are organized by the prefecture together with the HFD group of the ministry.

### Question 12 : Incident response capabilities

For communication networks breakdown, incident response depends on the very nature of the failure and must take in account that networks are geographical. Nevertheless, for security breaches, cooperation between CERT's, software vendors and so on is used.

Past records show that a major outage in the public communications networks occurs every two to three years. Most likely it will be a software-related problem that triggered an incident. All major failures require submission of a special report and later investigations.

### Question 13 : Good practice on resilience

Good practices with respect to resilience are known by the technical experts and correspond to the "state of the art" in engineering. Examples are EBIOS and MEHARI (see FR 8 and 10) for risk analysis.

While there are no incentives given to providers to deploy good practices, they are doing it. This is generally sufficient and works in practice. But France intends to check to make sure that critical infrastructures, such as communication infrastructures are really protected against all kind of threats.

DCSSI has a kind of a repository that contains lots of information about guidelines, standards and so forth (http://www.ssi.gouv.fr/fr/index.html).

*[34] The Inter-Ministerial Crisis Management Centre (Le centre opérationnel de gestion interministérielle des crises) is located within the Ministry of the Interior in Paris. This centre provides the Minister of the Interior with a reinforced central inter-ministerial crisis management capability for internal crises. This allows for operations involving police, Gendarmerie and civil security forces in the event of a major crisis. It will also benefit from associating all the ministries concerned by the crisis (such as health or telecommunication) in the same building.*

## Question 14 : Guidelines for procurement

Currently, a working group is writing a new set of quality clauses to improve the level of availability, security, and resilience of communications services for public procurement.

As pointed out in Q5, the 2007 incident resulted in recommendations and specifications that will be part of the service level agreement (SLA) for new contracts between the government and telecom providers.

The recommendations culminating from analysing the 2007 incident were passed on to the working group that is developing new procurement guidelines. These procurement guidelines will become available in 2009.

## References

**FR 1** Conseils des ministres Sécurité des activités d'importance vitale (press release of the Prime minister about the enhancement of the protection of critical activities - not available in English) (2006-02-22).
Available: http://www.archives.premier-ministre.gouv.fr/villepin/acteurs/gouvernement/conseils_ministres_35/conseil_ministres_22_fevrier_791/securite_activites_importance_vitale_55388.html
Last Access: September 17, 2008.

**FR 2** Code de la défense - Section 1: Dispositions générales Article R1332 (Defence code- From Section 1: Disposition general Article R1332 –1 to Article 1332-42 not available in English) (2008-08-06 version).
(Available: http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006574323&idSectionTA=LEGISCTA000006182854&cidTexte=LEGITEXT000006071307&dateTexte=20080721.
Last Access: September 17, 2008.
décret n° 2006-212 du 23 février 2006 relatif à la sécurité des infrastructures d'importance vitale.
Available: http://www.legifrance.gouv.fr/rechTexte.do?reprise=true&page=1.

**FR 3** Décrets, arrêtés, circulaires TEXTES GÉNÉRAUX PREMIER MINISTRE, Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs NOR : PRMX0609332A (2006-06-04) *JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE* Texte 1 sur 62.
(Available: http://www.legifrance.gouv.fr/jopdf//jopdf/2006/0604/joe_20060604_0129_0001.pdf)
Last Access: September 17, 2008)

**FR 4** Décrets, arrêtés, circulaires TEXTES GÉNÉRAUX PREMIER MINISTRE - Arrêté du 3 juin 2008 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs NOR : PRMD0813724A (2008-07-05) *JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE* Texte 6 sur 140.
Available: http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20080705&numTexte=6&pageDebut=10823&pageFin=10823.

**FR 5** Le Livre blanc sur la défense et la sécurité nationale (The French White Paper on defence and national security) (2008-06-17).
Available: http://www.premier-ministre.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/.
Last Access: September 17, 2008.
Non-binding English text, http://www.premier-ministre.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/ressources_888/translated_documents_890/.

**FR 6** Défense et Sécurité nationale LE LIVRE BLANC (The French White Paper on defence and national security) (Chapters 1-6) (pp. 1-124).
Available: http://www.premier-ministre.gouv.fr/IMG/pdf/livre_blanc_tome1_partie2.pdf.

Last Access: September 17, 2008.
Particularly relevant are the following:

- on page 64 : " ... *La résilience suppose aussi d'organiser la coopération entre l'État et les collectivités territoriales, pour la complémentarité des moyens, et entre l'État et les entreprises privées dans les secteurs stratégiques (..., communication, ...).*"
- on page 53 (Attaques informatiques majeures)
- on page 96 : "... *Elle proposera aussi que la Commission impose aux opérateurs des règles de durcissement des réseaux et des procédures destinées à en accroître très fortement la résilience.*"

**FR 7** éfense et Sécurité nationale LE LIVRE BLANC (The French White Paper on defence and national security) (Chapters 7-18) (pp. 125-350).
Available: http://www.premier-ministre.gouv.fr/IMG/pdf/livre_blanc_tome1_partie2.pdf).
Last Access: September 17, 2008.
Particularly relevant are the following:
on page 182 : "*Des dispositions réglementaires seront également prises pour que les opérateurs de communications électroniques mettent en œuvre les mesures techniques et d'organisation nécessaires à la protection de leurs réseaux contre les pannes et les attaques les plus graves. À ce titre, le réseau Internet devra être considéré comme une infrastructure vitale et un effort important devra être mené pour améliorer sa résilience*."

**FR 8** EBIOS - Expression des besoins et identification des objectifs de sécurité (Expression of Needs and Identification of Security Objectives).
Available: http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html.
Last Access: September 17, 2008.
English version http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html.

**FR 9** TELECOMMUNICATIONS REGULATION AND THE CREATION OF A SECTOR AUTHORITY - ARCEP'S MISSIONS AND ASSIGNMENTS - sanction powers.
Available: http://www.arcep.fr/index.php?id=13&L=1#11131.
Last Access: September 17, 2008.

**FR 10** MEthode Harmonisée d'Analyse de RIsque (MEHARI) 2007 - CLUSIF (Club de la Sécurité de l'Information Français).
Available: https://www.clusif.asso.fr/fr/production/mehari/mehari.asp.
Last Access: September 17, 2008.
English Version https://www.clusif.asso.fr/en/production/mehari/.

**FR 11** Commissariat aux télécommunications de défense : defence telecommunication centerfull.
Available: page 60, http://www.hfd.minefi.gouv.fr/rap_hfds2007.pdf.
Last Access: September 17, 2008.

**FR 12** Décret no 2000-759 du 1er août 2000 modifiant le décret no 93-1036 du 2 septembre 1993 relatif à l'organisation des télécommunications en matière de défense, NOR : ECOI0020060D (2006-08-01) *Journal officiel du 6 août 2000* Texte 1-1 sur 774.
Available:
http://www2.equipement.gouv.fr/bulletinofficiel/fiches/Bo200015/A0150006.htm
Last Access: September 17, 2008.

**FR 13** rapport sur la résilience des réseaux de télécommunication [Report on resilience

of communications networks for the le Secrétariat général de la défense nationale (Secretariat-General for National Defence)] (2207). (not publicly available)

**Additional Resources**

Information Systems Security special purpose server - Methods to achieve information systems security provides public access to several risk management and information security assessment instruments for free download such as:

- EBIOS (Expression des besoins et identification des objectifs de sécurité),
- PSSI (Information Systems Security Policy) and TDBSSI (Information Systems Security Trend Chart)

Available: http://www.ssi.gouv.fr/en/confidence/methods.html.
Last Access: September 17, 2008.

Le Secrétariat général de la défense nationale (Secretariat-General for National Defence) (SGDN) http://www.sgdn.gouv.fr/rubrique.php?id_rubrique=16.
Reporting to the Prime Minister and working in close liaison with the President of the Republic's office, the SGDN assists the Head of Government in fulfilling his/her responsibilities in matters of national defence and security.

Le serveur thématique sur la sécurité des systèmes d'information http://www.ssi.gouv.fr/fr/index.html. French government website dedicated to information system security.

Le centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (governmental center of expertise of computer attacks processing and answers) (CERTA) http://www.certa.ssi.gouv.fr/.

The CERTA is the privileged contact for security incidents.

**Additional Links**

French Computer Emergency Response Team (RENATER CERT), http://www.renater.fr/spip.php?rubrique19.

Fédération Française des Télécommunications et des Communications Électroniques (FFTelecom)
http://www.fftelecom.org/la-s%C3%A9curit%C3%A9.

Le centre opérationnel de gestion interministérielle des crises (The Inter-Ministerial Crisis Management Centre)
http://www.interieur.gouv.fr/sections/a_l_interieur/defense_et_securite_civiles/gestion-risques/cogic.

# National Report of Germany

## Introduction

### Interview

Date and Duration 28 August 2.5 hours.

| Interviewee | Mr Rainer WYPHOL | Mr Jörn-Uwe HEYDER |
|---|---|---|
| Authority | BNetzA – Bundesnetzagentur | BSI - Bundesamt für Sicherheit in der Informationstechnik |
| Position /Title | Senior Expert | Senior Expert |
| Education/Training | Engineer | Mathematician |
| Task Responsibilities | - Security in telecommunication networks, including international affairs<br>- Data protection of postal and telecommunication services | - International relations, including international network security affairs<br>- Coordination of BSI's EU activities |
| Relation with ENISA if applicable | | NLO and alternate MB member |

### Authorities involved with Network Resilience

| | | |
|---|---|---|
| Authority | BNetzA – Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway) | BSI - Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) |
| Main Tasks | The central task of BNetzA is to provide for compliance with the Telecommunications Act (TKG), the Postal Act (PostG) and the Energy Act (EnWG) and their ordinances having the force of law. | BSI is the central IT security service provider for the German government and in a wider sense for the whole German society. |
| Reports to | Bundesministerium für Wirtschaft und Technologie (BMWi, Federal Ministry of Economics and Technology) | Bundesministerium des Innern (BMI, Federal Ministry of the Interior) |
| Year established | 1998 as "Regulation Authority for Telecommunication and Post" | 1991 |
| URL | www.bundesnetzagentur.de | www.bsi.bund.de |

### Authorities involved but not part of the interview

| Authority | BMWi - Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology) | BMI - Bundesministerium des Innern (Federal Ministry of the Interior) |
|---|---|---|
| Main Tasks[35] | Development and reviewing of regulatory acts in telecommunication (and postal) policies | National IT strategy and IT security, communication infrastructures of the federal government and administration |
| Reports to | Government | Government |
| URL | www.bmwi.bund.de | www.bmi.bund.de |

## Scope and governance

### Question 1 : The authorities

Four authorities[36] in Germany deal mainly with matters of resilience of public and other essential e-communication networks. These are:

- BMWi - Bundesministerium für Wirtschaft und Technologie (Federal Ministry of Economics and Technology)
- BMI - Bundesministerium des Innern (Federal Ministry of the Interior)
- BNetzA – Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway)
- BSI - Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)

BMWi is responsible for telecommunications and postal policy. It pursues a competition-oriented telecommunications policy in order to ensure the provision of telecommunications services that meet the needs of users.

BNetzA is the national regulatory authority for all public networks in Germany. For the purpose of implementing the aims of regulation, the Agency has effective procedures and

[35] *Here only tasks related to the topics of the questionnaire are listed*

[36] *In a wider understanding of resilience of public and other essential e-communication networks, several other ministries and governmental agencies have a role to play. These are under the responsibility of the BMI, the Bundesverwaltungsamt/ Bundesstelle für Informationstechnik (BVA/ BIT, Federal Administration Office/ Federal Office for Information Technology, www.bit.bund.de) and the Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS, Federal Agency for Digital Radio of Security Authorities and Organisations, www.bdbos.bund.de); under the responsibility of the Bundesministerium der Finanzen (BMF, Federal Ministry of Finance, www.bmf.bund.de) the Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT, Centre for Information Processing and Information Technology, www.zivit.de); under the responsibility of the Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS, Federal Ministry of Transport, Building and Urban Affairs, www.bmvbs.bund.de/) the Deutscher Wetterdienst (DWD, German Weather Service, www.dwd.de).*

instruments at its disposal including also rights of information and investigation as well as the right to impose graded sanctions.
BMI is responsible for IT policy development. Its IT policy aims at and coordinates introducing and usage of information technology in administration and society while – at the same time – ensuring an appropriate level of IT security.

BSI is the national information security authority. On an operational level it is responsible for governmental networks. In a cooperative sense it is also responsible for public networks usage as it's recommendations are applied for all governmental and public networks.

**Question 2 : The mandate of the authorities**

The regulatory mandate of Bundesnetzagentur is based on the Telecommunications Act (TKG, see DE 1) and on the Post and Telecommunications Safeguarding Law (see DE 2). BNetzA deals with every network that is related to the telecommunications act.

BNetzA is a separate higher federal authority within the scope of business of BMWi and is the national regulatory authority.

The BNetzA's task is to provide, by liberalisation and deregulation, for the further development of the electricity, gas, telecommunications, postal and railway infrastructure markets. For the purpose of implementing the aims of regulation, the Agency has effective procedures and instruments at its disposal including also rights of information and investigation as well as the right to impose graded sanctions.

Moreover, it acts as the root certification authority as provided for by the Electronic Signatures Act.

BNetzA plays an active and important role in the field of e-communications on the European and international level[37].

BMWi is amongst others responsible for telecommunications and postal policy. It pursues a competition-oriented telecommunications policy in order to ensure the provision of telecommunications services that meet the needs of users. The competitive telecommunications policy is based on the 1996 Telecommunications Act which was

[37] *Most important at European level is the Agency's work for the European Commission. This involves meeting its reporting requirements and working in the Communications Committee (COCOM).*
*To facilitate the regulation of electronic communications networks and services, the Agency is a member of both the Independent Regulators Group (IRG, http://irgis.icp.pt/site/en/) and the European Regulators Group (ERG, www.erg.eu.int).*
*The specialist departments provide input for the European and international frequency coordination organisations such as the European Conference of Postal and Telecommunications Administrations (CEPT, in particular for the Electronic Communications Committee, ECC) and ITU Radio communications (ITU R) as well as the European and international organisations addressing technical cooperation such as the European Telecommunications Standards Institute (ETSI) and telecommunications standardisation (ITU T). The Agency is also involved in the ITU's Telecommunication Development Sector (ITU D).*

amended to meet European requirements. The amendments came into effect on 26 June 2004.

BMWi is bearing the main responsibility for developing and reviewing the regulatory acts in this field - especially the Telecommunications Act (Telekommunikationsgesetz, TKG, see DE 1) and the Post and Telecommunications Safeguarding Law (Post- und Telekommunikationssicherstellungsgesetz, PTSG, see DE 2).

The telecommunications security policy containing emergency calls, data protection, secure infrastructure and contingency planning as well as lawful interception is dealt with in part 7 of the TKG.

BSI is mainly defined as a technical support authority for information security. It is the central IT security service provider for the German government and in a wider sense for the whole German society. Apart from the federal government and administration it advises manufacturers, distributors and users of IT as well as providers in terms of IT security. BSI promotes IT security and especially the protection of essential infrastructures by several means. It is technically responsible for the security and the coordination of operations of the governmental wide area networks (WAN) and services.

Regarding the governmental WANs BMI and BSI – together with assigned providers from the private sector – are bearing the full responsibility for operation and security. Towards providers of public communication networks BMI and BSI are following a cooperative and advisory approach.

BMI is amongst others responsible for the national IT strategy, IT security and communication infrastructures of the federal government and administration. Its IT policy aims at and coordinates introducing and usage of information technology in administration and society while – at the same time – ensuring an appropriate level of IT security. Essential parts are the "National Plan for Information Infrastructure Protection" (NPSI) (see DE 6 in reference list) adopted by the Federal Government in 2005, the "eGovernment Strategy" and the "Federal IT-Steering Strategy". Within the frame of the latter, the Office of the Federal Government Commissioner for Information Technology has been established on 1 January 2008.

Other ministries and agencies play a role in the domain of network and information security[38].

[38] *These are in detail mentioned in note 34. Their respective tasks are:*
*BVA/BIT is a central IT service provider for the federal administration. As a shared service centre for information technology it is covering the whole life cycle of IT products and services. It is intended that BIT will take on the organisational responsibility for governmental WANs.*
*BDBOS' mandate is to set up, operate and ensure the operability of a digital voice and data communication system for the police forces and other authorities with security functions.*
*BMF supervises ZIVIT, the central IT service provider of the federal fiscal administration and an important shared service centre for IT within the federal administration. It is responsible for specialised networks, e.g. in the tax or customs field, and for more than 300 specialised IT procedures.*

The cooperation among ministries and agencies is variegated and takes place on different levels and in different activities.

On national level BNetzA cooperates with BMI/BSI regarding security of telecommunications providers. On international level the agency is – itself and on behalf of BMWi – a member of various European and international organisations.

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

Several laws, regulations, guidelines and other provisions regarding the resilience of public and other e-communication networks are in place in Germany.

The Telecommunications Act (DE 1 in reference list). According to §109 of the Telecommunications Act (Telekommunikationsgesetz, TKG) any person operating telecommunication systems serving to provide publicly available telecommunication services shall make appropriate technical arrangements or take other measures in order to protect telecommunications and data processing systems operated for such purposes against any faults which would result in considerable harm to telecommunications networks, and against external attacks and the effects of natural disasters. This includes the obligation to nominate a security commissioner (security liaison officer) and to submit a security concept to the BNetzA which entails BCM (business continuity management) and BCP (business continuity planning).

BNetzA has issued a guideline for drawing up a security concept considering several provisions including IT security (DE 5 in reference list). All the areas mentioned in the question are covered. The agency also gives direct advice on the phone concerning questions relating to security and resilience of networks. BNetzA has a controlling function and may inspect the facilities of the telecommunication (systems) providers according to §115 of the act. The TKG distinguishes between service providers and persons (companies) operating telecommunication systems serving to provide publicly available telecommunication services – the latter ones shall be named “operators” in this context for ease of reading.

The Post and Telecommunications Safeguarding Law (see DE 2 in reference list) stipulates among other things that in times of crisis, natural disasters or in the event of a war, the P&T services for governmental authorities, the economy, the defence forces and vital services for the public have to be uphold. Private companies obliged to comply with this law can claim reimbursement from the government to make the necessary provisions.

The Electromagnetic Compatibility Act -EMVG (see DE 3) (in accordance with directive 2004/108/EG) engages BNetzA as stipulated in part 2, §14 especially in regard to

*BMVBS supervises DWD, which has a much broader mandate than observing and forecasting the weather. It is the central IT service provider of the federal administration for transport, building and urban affairs including the operation of specialised networks and procedures.*

resilience/safety of public telecommunications networks. It says, the Regulatory Authority shall be authorised where electromagnetic incompatibility occurs, to implement all the measures necessary to analyse why it occurred. The regulator can also initiate corrective action in cooperation with the parties concerned. Special measures may be imposed for the use of apparatus or to take all the measures necessary to prevent the use of such apparatus in order to remove existing or foreseeable electromagnetic incompatibility at a particular location and/or protect public telecommunications networks or radio transmitting or receiving equipment used for safety and security purposes. The EMVG is under full responsibility of BNetzA and can only be enforced by the Agency.

The Directive on the Verification Procedure of the Limitation of Electromagnetic Fields - BEMFV (DE 4) imposes limitations on electromagnetic fields emissions. Whenever a new mobile phone base station goes into service BNetzA has to ensure that the limits set by the directive are being met. Mobile phone (network) antennas do require a "location certificate" issued by BNetzA. Moreover BNetzA runs a database on the location of mobile phone base stations, which can be used to ensure redundancy.

Finally, there are a number of legal provisions pertaining to risk management in the field of commercial and financial law covering also ICT security risks, such as § 91 of the German Stock Corporation Act (Aktiengesetz, AktG, see DE 10), § 25a of the Banking Act (Kreditwesengesetz, KrWG, see DE 11) or § 33 of the Securities Trading Law (Wertpapierhandelsgesetz, WpHG, see DE 12). Likewise, obligations arising under foreign jurisdictions (e.g. the Sarbanes Oxley Act in the US) or from international agreements such as Basel II may have an indirect effect on companies' information and network security efforts.

Governmental strategies in Germany regarding resilience of eCommunication networks embrace the NPSI and CIP[39] Implementation Plan (see DE 6 and DE 7). The German "National Plan for Information Infrastructure Protection" (NPSI) became effective in July 2005. It is a superordinate strategy for IT security which focuses on:

- Prevention: Protecting information infrastructure adequately
- Preparedness: Responding effectively to IT security incidents
- Sustainability: Enhancing German competence in IT security

For the practical implementation of this national plan two additional plans have been worked out, an Implementation Plan for the Federal Administration and the CIP Implementation Plan.

The latter one was developed in cooperation with the private sector and put into force in 2007. It contains essential requirements in the field of prevention, which are largely implemented. The CIP Implementation Plan is focused on improving the preparedness and recovery measures of critical infrastructures in case of IT incidents. The working groups in

[39] *CIP = Critical Infrastructure Protection*

line with this plan are dealing with different topics [40]related to incidents, e.g. early warning on IT incidents, exercises, IT guidelines and best practices. Their aim is to create the basis for detecting incidents as early as possible and for coordinating combined reaction within a joint IT crisis management.

The working groups are supported by BSI not only in form of technical input regarding incident handling but also by hosting the function of a central office.

For more information on CIP in Germany see also: DE 8 and DE 9. Among Technical Standards related to resilience of public and other essential e-communications networks are IT-Grundschutz (DE 13), the ISi Series (DE 14), and the Technical Guideline Secure WLAN (DE 15).

*BSI has developed and maintains BSI Standards 100-1, -2, -3 (100-4 is available in draft version) in combination with the IT-Grundschutz catalogues (DE 13). This is a comprehensive reference work defining and presenting the IT-Grundschutz approach, an IT security management method, performing ISO 27001 in detail. The BSI Standards contain recommendations on methods, processes, procedures, approaches and measures relating to information security. The IT-Grundschutz method is on the one hand general enough to be applied to a large variety of possible IT operators, but on the other hand specific enough to be applied also to providers, what has happened actually several times so far and has been declared by corresponding certificates. BSI recommends the implementation of IT-Grundschutz for all kinds of providers.*

Moreover, BSI is developing an Internet security series (ISi Series, BSI-Reihe zur Internetsicherheit, DE 14). The primary objective is to contribute to an appropriate and consistently high minimum security level in the Internet. Focus of the ISi Series lies on providing secure connection to the Internet for users as well as those who provide services via Internet. The ISi Series expands on the IT-Grundschutz catalogues by proposing a basic architecture, which can be adapted – with the aid of various options – to meet individual needs.

It is intended to extend the series with chapters focussing on the core Internet infrastructure like routing or the Domain Name System (DNS) and therefore to address providers directly – but only on the basis of recommendations or guidelines.

The Technical Guideline Secure WLAN (Technische Richtlinie Sicheres WLAN, TR-S-WLAN) has been developed by BSI and gives recommendations to planners, purchasers, operators and users of WLAN systems on their secure implementation (DE 15). The focus lies on the user's view but it addresses also explicitly the operators of large WLANs and hot spots as providers of public telecommunication services in the sense of the TKG.

The overall approach of the German government in the field of ICT security in the future is governed by the above mentioned - National Plan for Information Infrastructure Protection

[40] *Four working groups have been established in 2007 and 2008 and are dedicated to the following topics 'emergency and crisis exercises', 'crisis response and management', 'national and international cooperation' and 'maintenance of critical infrastructure service'.*

(NPSI, see DE 6). Under the NPSI, the German government is going to continue the cooperative approach towards providers, in particular the implementation of the CIP Implementation Plan, as the process has just begun. The cooperation within the established working groups should be intensified in order to create an atmosphere of trust which enables all participants to lead an open discussion on possible weaknesses and actual incidents and to find appropriate solutions jointly. The working groups should improve the cross-sector collaboration, sector-wide collaboration as well as the collaboration between government and operators of critical infrastructures.
Apart from the CIP Implementation Plan German authorities are currently holding discussions with Internet service providers in order to find effective ways to improve Internet security. These discussions are informal.

In the future, BMWi and its agency BNetzA will be in charge for all measures pertaining to the regulation of the telecommunication markets.

**Question 4 : Initiatives between providers and public authorities**

BNetzA is organising (or participating in) the following cooperation:

- Facility sharing: Operators of telecommunication network services may (and do) opt to co-locate their technical equipment in order to safe costs and /or to compliment their respective technical equipment/facilities. There is a co-location data base hosted by BNetzA with relevant information on safety, security, resilience and redundancy.
- Mobile phone infrastructure: Local authorities and mobile phone network operators have an agreement on the installation (location) of new mobile phone base stations. Each side can make suggestions. The providers need the consent of local authorities for new installations.
- Consumer and health issues: Non compulsory agreement between federal authorities and mobile phone network operators on an expert report compiled once a year taking special account of the electromagnetic emissions. Source of information for the public: IZMF, the information centre relating to mobile phones. [see IZMF in the reference list]

This topical cooperation take place in working groups. The cooperation between providers and public authorities in the context of the CIP Implementation plan bases on several working groups and the exchange of information with the assistance of BSI.

The WG of the CIP Implementation Plan focuses on IT crisis management and exercises with special interest in the information flow before, during and after IT incidents. Several providers participate in these working groups on their own costs. The required basic studies and the activities of the central office are financed by BSI.

Besides CIP issues BSI initiates non-regular meetings with providers in order to find effective ways for improving Internet security. Initiatives between providers are the following:

The German Association for IT, Telecommunications and New Media (BITKOM) has established a working group on security management for their members (see BITKOM 1a). Apart from security and risk management further issues - like liability, return of security investment, certification and awareness raising - are considered. Within this WG there is a special subgroup for network operators concentrating on the protection of important infrastructures, legal interception, emergency calls and regulation (see BITKOM 1b). Both groups are focussing on political, not on technical aspects. Public authorities are not involved directly.

The association of the German Internet industry, eco, runs the largest German data exchange node, DE-CIX (Deutscher Commercial Internet Exchange), covering about 80 percent of national and 35 percent of international Internet traffic. Robustness and redundancy are main design principles of DE-CIX, so that it contributes decisively to the resilience of the German part of the Internet. The corresponding working group comprising the DE-CIX-involved providers is dealing regularly with resilience issues (see eco 1a). Apart from that eco has established a working group on data centres, where availability issues like resilience are discussed on a regular basis (see eco 1b).

## Tasks

### Question 5 : Typical task

BNetzA's tasks[41] pertaining to the resilience of e-communication networks are the following:

- auditing operators regarding their security concepts, business continuity management and planning in accordance with § 109 TKG
- auditing operators' facilities and premises in accordance with §§ 109 and 115 TKG
- advising providers and operators on organisational and technical regulatory requirements
- supervising operators with regard to incidents
- enforcing regulation in accordance with the relevant acts (measure of last resort)
- developing and maintaining corresponding guidelines
- hosting data bases with relevant information on safety, resilience and redundancy
- fulfilling obligations related to the EMC Act (safety, health and redundancy aspects)

BMWi's task with regard to network resilience:

- developing and maintaining regulatory acts after consulting all relevant stakeholders
- supervising the national regulatory authority, BNetzA
- establishing and facilitating cooperation in the field of network resilience
- exchanging information on national and international level

[41] *Many other tasks are carried out by BNetzA in relation to the area of telecommunication an telecommunication markets.*

- cooperating with international organisations and authorities

BSI's tasks[42] in the network resilience field can be summarized as follows:

- developing technical and organisational standards, recommendations, guidelines and good practices in cooperation with relevant stakeholders
- establishing cooperation between providers (as operators of critical information infrastructures) and the German government in accordance with the CIP Implementation Plan
- planning, supervising and auditing security and operations of governmental WANs
- running the national IT crisis response and situation centres as well as the governmental CERT
- certifying institutions in accordance with ISO 27001 on the basis of IT-Grundschutz including the training and certification of appropriate auditors from the private sector
- certifying products in accordance with Common Criteria and ITSec

BMI's tasks regarding network resilience:

- developing IT and IT security strategies for the federal administration on a political level
- supervising the technical authorities BSI, BVA/BIT, BDBOS
- running the national crises management centre
- establishing and facilitating cooperation in the field of IT security

**Question 6 : Exchange of information between providers and public authorities**

All operators of (physical) telecommunications services are obliged to nominate a security liaison officer and to submit a security concept to the BNetzA (DE 1 - § 109). The required security concept contains information on security policies, business continuity plans, preparedness measures, on geographical, topological and technical network structures, locations with high infrastructure density, and operators of (physical) e-communication services have to provide this information when commencing service. Changes to the service(s)/ technology/equipment etc. provided and changes in address or ownership of the company have to be communicated in writing to BNetzA. In case corrections of the security concept are requested by the agency the concept has to be resubmitted by the company.

As regards the use of information, BNetzA establishes on the basis of information received whether the company complies with the requirements. Should the requirements not be met all necessary steps have to be taken by the company to remedy the situation. In most cases the companies co-operate and comply. BNetzA has a controlling function and may inspect the facilities of the telecommunication systems operators. The upcoming CIP Implementation Plan foresees an information exchange between providers and authorities

[42] *Many other tasks are carried out by BSI regarding the area of information security.*

on resilience. Especially information on incidents should be exchanged. The conditions of this exchange are still in negotiation.

All exchanged information will be used to establish an appropriate, joint IT crisis management and to improve the common IT security level. Besides CIP issues BSI initiates non-regular meetings with providers in order to find effective ways for improving Internet security.

## Question 7 : Handling of security incidents

If the regulator gets to know about an incident (media reports or similar) the telecommunication systems operator is obliged to report and has to disclose the circumstances which led to the incident (if he is able to do this). The providers do usually not report minor incidents.

Quite often, the authority learns via the media about an incident or is informed by another provider. A report line exists where citizens can call the BNetzA to report an incident. Other channels of how the agency learns about incidents are not available for public information.

If the regulator gets to know about a major incident the company is obliged to fully disclose the circumstances leading to the incident. In cases of criminal intent leading to prosecution the competency / power of audit of the regulator may be overruled and has to wait for the outcome of the jurisdictional proceedings.

In the upcoming CIP Implementation Plan an information exchange between providers and authorities on security incidents is intended. Within the CIP Implementation Plan information on security incidents should be disclosed to authorities under strict confidentiality conditions and on a voluntary basis. Here a modus operandi might have to be found what should be reported.

## Question 8 : Audits related to resilience

Audits related to resilience take place in Germany and these are performed by BNetzA – the regulatory authority under the TKG. In general two types of audits can be distinguished:

Audit at a distance: All operators have to submit a security concept, non-compliances have to be remedied by the companies. When a new company is set up, the agency is in continuous exchange with this company until all obligations and requirements regarding the security concept are fulfilled. That way, the agency is well aware of the security set-up of the operators and providers.

In-situ audit: The large operators are visited on a regular basis, the smaller ones every couple of years. In case of non-compliance, refusal of co-operation, incidents – all of which are exceptional – a visit is foreseen.

These in situ audits are carried out the following way: Two officers of BNetzA go to check the security concept of a company and the remedies taken, to discuss the concepts such as business continuity planning or emergency recovery measures, and to inspect facilities and premises.  A report is made which is sent as hard copy – via post – to the agency and the files of the audit are kept non-accessible and secure in the agency.

Providers intending to obtain an ISO 27001 certificate on the basis of IT-Grundschutz have to initiate a corresponding audit by BSI-trained and -certified auditors from the private sector.

Private-sector providers of governmental networks are audited on resilience and other issues in order to guarantee all basic objectives of IT security: confidentiality, integrity and availability of the handled governmental data. Apart from this overall aim the audits' purpose is to assess compliance with internal rules and requirements for governmental networks and to detect possible weaknesses before attackers do. The audits are conducted by BSI itself regularly and additionally occasion-depending.

### Question 9 : Enforcement actions

Providers and operators acknowledge that it is in their best interest to avoid negative publicity through enforcement actions. Therefore the policy of BNetzA is to solve the problem with providers and not impose penalties. However, if enforcement actions have to be initiated, remedy is always the first choice. The operator is first asked to comply with the existing regulation(s). In the case of non-compliance the company is granted enough time to come up with a solution.

BNetzA may choose to inspect the provisions / corrective actions taken by the operator at site. As a measure of last resort a penalty may be levelled and in the most extreme case(s) the service(s) of the provider terminated. As an example the penalty for not supplying a security concept is € 100 000. It was underlined that during the last 12 months, no problems regarding resilience became apparent that would have forced the agency to impose fines.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

The NPSI can be considered as the beginning of a national risk management process. Harmonizing risk assessment and a risk model based on defining threats, vulnerabilities and impacts are discussed in the framework of the NPSI (DE 6). The working groups of the CIP Implementation Plan are focusing on IT crisis management. In turn, they aim at setting up a procedure for regular and crisis communication. One WG addresses the maintenance of critical services.

As regards to governmental networks, a comprehensive risk management process is established – in accordance with internal provisions and including governmental incident response capabilities as well as those of assigned providers.

## Question 11 : The preparedness and recovery measures

The PTSG (DE 2) stipulates among other things that in times of crisis, natural disasters or in the event of a war, the postal and telecom services for governmental authorities, the economy, the defence forces and vital services for the public have to be uphold. Critical services are defined and priorities established.

The Emergency Call Directive which is currently under the responsibility of Deutsche Telekom is under review and will change. BNetzA will become responsible for this directive/administering it within 112 measures.

BSI operates the national IT crises response and IT situation centre as well as the CERT for the federal government (see answer to question no. 12).

For the governmental networks BSI has enforced numerous preparedness and recovery measures following especially the IT-Grundschutz approach and requirements for a higher protection level, e.g.:

1) business continuity conceptions for incident handling supported by extensive tests
2) redundancy of IT infrastructure
3) redundancy of electric supply infrastructure
4) business continuity exercises

It is clear that IT security is a process, so that the taken measures have to be checked regularly regarding their correctness, completeness, effectiveness and efficiency. This is achieved by both adapting the recommended guidelines (like IT-Grundschutz) as well as re-tailoring the measures to be taken in order to protect the concrete entities. Exercises and trainings are components of this process.

## Question 12 : Incident response capabilities

BSI operates an IT crisis response centre with a standing 8/7 IT situation centre and a 24/7 on-call duty for German IT security. It analyses the current IT security situation in Germany and is the focal point for a coordinated national response to IT security crises. In those cases it directly assists the national crisis management of the BMI. In addition, it is responsible for the coordination of crisis management in governmental ICT networks. All these processes are supported by CERT-Bund, as the federal governmental CERT, and additional personnel of BSI's technical sections is deployed situation-depending.

The IT crisis response centre is currently creating a network of contact and cooperation with the critical national infrastructures (under the NPSI and its CIP Implementation Plan – see also DE 6). It is via CERT-Bund in touch with the CERT-Verbund, the organisation of German CERTs including commercial and academic CERTs. There are close connections to the European Governmental CERT Group (EGC) and it is in loose contact with other European and international CERTs.

Post-investigations take place if an incident triggers certain reaction measures and a formal after-action review is performed.

Additionally, the CIP Implementation Plan envisages the systematically joint analysis of IT crises by government and industry to improve IT security. This process is in course of establishment.

**Question 13 : Good practice on resilience**

BNetzA has developed a guideline for the compilation of a security concept (see DE 5 in reference list)

There is no dedicated web page, but in the various areas of the BNetzA web site, many interesting information related to good practice can be found. In general, BNetzA refers to IT Grundschutz; providers can use it on a voluntary base (see DE 13).

BSI standards 100-1, -2, and -3 (BSI standard 100-4 "Business Continuity Management" is available in draft version) in combination with the IT-Grundschutz catalogues are a comprehensive repository for establishing an appropriate level of IT security including network resilience. They are designed for all organisations operating complex ICT infrastructures, including providers of public and/ or other essential eCommunication networks.

The CIP Implementation Plan contains high level recommendations which can be considered as "good practice".

At the moment BSI is working out the following repositories which are intended to be made publicly available:

- high-availability compendium including consideration of network availability
- an extensive requirement catalogue for network security, which addresses all network architects and is already applied for government-internal purposes.

With regard to incentives, the situation in Germany is the following: BSI offers an ISO 27001 certification scheme on the basis of IT-Grundschutz (BSI Standards 100-1, -2, -3) that has been developed in cooperation with the private sector. It is designed as an incentive for all institutions – including providers – which are willing to or have to demonstrate a certain level of IT security, e.g. towards customers, insurance companies or authorities. Precondition for obtaining such a certificate is the necessary audit being conducted by BSI-trained and -certified auditors from the private sector. The awarding of several ISO 27001 certificates on the basis of IT-Grundschutz to different providers demonstrates that Grundschutz is actually also applicable to this kind of IT infrastructure operators.

Moreover, BSI strengthens this incentive by recommending customers, which are searching for an appropriate provider, to pay attention that providers have implemented IT-Grundschutz.

Apart from these government-driven incentives especially market forces have to be considered as incentive. Providers of telecommunication networks might be forced into contractual agreements by major clients to ensure a high level of safety and security including resilience (see presentation by France Telecom, 1st resilience workshop back in March 2008).

### Question 14 : Guidelines for procurement

The CIP Implementation Plan recommends to apply certified products for critical processes.

Moreover, BSI has developed the procurement guide "*Leitfaden für die Auswahl von IT-Sicherheitssystemen für sensible Infrastrukturen, deren Schutz im nationalen Sicherheitsinteresse liegt",* that shall only be applied for the handling of classified data, so that providers for governmental networks will be affected, but not those operating public networks. Currently the procurement guide is not publicly available.

The security concepts to be developed by the operators and to be presented to BNetzA do not contain any details with respect to procurement.

## References

**DE 1** Telekommunikationsgesetz (TKG), Telecommunications Act.
Available: http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf.
Particulary relevant is section 7, especially §§ 109 and 115.

**DE 2** Post- und Telekommunikationssicherstellungsgesetz (PTSG), The Post and Telecommunications Safeguarding Law.
Available: http://www.gesetze-im-internet.de/bundesrecht/ptsg/gesamt.pdf.

**DE 3** Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG), Electromagnetic Compatibility Act (EMC-Act).
Available: http://bundesrecht.juris.de/bundesrecht/emvbg/gesamt.pdf.

**DE 4** Verordnung über das Nachweisverfahren zur Begrenzung elektromagnetischer Felder (BEMFV), Directive on the Verification Procedure of the Limitation of Electromagnetic Fields. Available:
http://www.bundesnetzagentur.de/enid/Elektromagnetische_Felder__EMF__/Standortverfahren_BEMFV_i5.html.

**DE 5** Leitfaden zur Erstellung eines Sicherheitskonzeptes gemäß § 109, Abs. 3 TKG, Guideline for the compilation of a security concept according to § 109, para. 3 TKG.
Available: http://www.bundesnetzagentur.de/media/archive/4552.pdf.

**DE 6** Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), National Plan for Information Infrastructure Protection.
Available in English:
http://www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf.
Last Access: September 15, 2008.

**DE 7** Umsetzungsplan KRITIS, CIP Implementation.
Available:
http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2007/Kritis,templateId=raw,property=publicationFile.pdf/Kritis.pdf.
Last Access: September 15, 2008.

**DE 8** Leitfaden *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement*, Protecting Critical Infrastructures –Risk and Crisis Management (A guide for companies and government authorities).
Available in English:
http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfaden__Schutz__kritischer__Infrastrukturen__en,templateId=raw,property=publicationFile.pdf/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf.
Last Access: September 15, 2008.

**DE 9** Weitere Informationen zum Schutz Kritischer Infrastrukturen in Deutschland, further information on CIP in Germany.
Available:http://www.bsi.bund.de/fachthem/kritis/index.htm.
Last Access: September 15, 2008.

**DE 10** Aktiengesetz (AktG), Stock Corporation Act.
Available: http://www.gesetze-im-internet.de/bundesrecht/aktg/gesamt.pdf.
Last Access: September 15, 2008.
Particulary relevant is § 91 (2).

**DE 11** Kreditwesengesetz (KWG), Banking Act.
Available: http://www.gesetze-im-internet.de/bundesrecht/kredwg/gesamt.pdf.
Last Access: September 15, 2008.
Particulary relevant is § 25a.

**DE 12** Wertpapierhandelsgesetz (WpHG), Securities Trading Law.
Available: http://www.gesetze-im-internet.de/bundesrecht/wphg/gesamt.pdf.
Last Access: September 15, 2008.
Particulary relevant is § 33.

**DE 13** IT-Sicherheitsmanagement und IT-Grundschutz, BSI-Standards 100-1, -2, -3, -4 und IT-Grundschutz-Kataloge, IT Security Management and IT-Grundschutz, BSI Standards 100-1, -2, -3, -4 and IT-Grundschutz catalogues.
Available: http://www.bsi.bund.de/english/publications/bsi_standards/index.htm and http://www.bsi.bund.de/gshb/index.htm.
Last Access: September 15, 2008.

**DE 14** BSI-Reihe zur Internetsicherheit (ISi-Reihe, im Aufbau befindlich), BSI Internet security series (ISi Series, under construction).
Available: http://www.isi-reihe.de/.
Last Access: September 15, 2008.

**DE 15** Technische Richtlinie Sicheres WLAN (TR-S-WLAN), Technical Guideline Secure WLAN.
Available: http://www.bsi.bund.de/literat/tr/trwlan/index.htm. The guideline itself is available as a printed version only.
Last Access: September 15, 2008.

**IZMF** Allgemeine Verbraucher- und Gesundheitsinformationen zum Thema Mobilfunk, General information for the public on consumer and health issues regarding mobile radio.
Available: http://www.izmf.de/html/de/index.html.

**BITKOM 1a** BITKOM Arbeitskreis Sicherheitsmanagement, BITKOM working group on security management.
Available: http://www.bitkom.org/de/themen_gremien/18173.aspx.
Last Access: September 15, 2008.

**BITKOM 1b** BITKOM Fachausschuss Netzbetreiber, BITKOM subgroup for network operators.
Available: http://www.bitkom.org/DE/THEMEN_GREMIEN/44123.ASPX.
Last Access: September 15, 2008.

**eco 1a** eco Arbeitskreis DE-CIX, eco working group on DE-CIX.
Available: http://www.eco.de/arbeitskreise/de-cix.htm.
Last Access: September 15, 2008.

**eco 1b** eco Arbeitskreis Datacenter, eco working group on data centres.

Available: http://www.eco.de/arbeitskreise/datacenter.htm.
Last Access: September 15, 2008.

## Additional Information

**Federal Network Agency,** http://www.bundesnetzagentur.de/.

**Federal Office for Information Security,** http://www.bsi.bund.de/.

# National Report of Greece

## Introduction

### Interview

Date and Duration 5 September 2008 2 hrs and 15 minutes.

| | |
|---|---|
| Interviewee | Dr George Drossos |
| Authority | Ministry of Transport and Communications |
| Position title | Radiocommunications Expert |
| Education/Training/ Degree | BEng, MSc, MBA, PhD Engineering |
| Task and Responsibilities | Spectrum management, standardization, EMC |
| If applicable, rel.ship to ENISA | National Liaison Officer ENISA |

**People who provided input but did not participate in interview[43]**

| Interviewee | Dr George Roussopoulos | Dr Panagiotis Trakadas | Sofia Fragoulopoulou |
|---|---|---|---|
| Authority | Hellenic Data Protection Authority (HDPA) | Hellenic Authority for the Information and Communication Security and Privacy (ADAE) | National Regulatory Authority (EETT) |
| Position title | Auditor | Engineer | Engineer |
| Education/Training/ Degree | | | |
| Task and Responsibilities | | | |
| If applicable, rel.ship to ENISA | | | |

*[43] These agencies were sent the questionnaire by the ministry and filled in the answers (Greek or English). Responses were returned to the ministry. We interviewed the ministry representative. Some agencies that were sent the survey by the ministry chose not to respond. We experienced some delay getting names for the individuals who were actually responsible for answering the questionnaire. At the beginning some of the material was submitted without identifying an individual.*

## Authorities involved with network resilience

| Authority | Hellenic Data Protection Authority (HDPA) | Hellenic Authority for the Information and Communication Security and Privacy (ADAE) | National Regulatory Authority (EETT) |
|---|---|---|---|
| Main Tasks | Supervisory Authority in the field of data protection, incl. data and network security | Law Enforcement in the ICT, on network security and integrity | Supervises and regulates the telecommunications as well as the postal services market. |
| Reports to | Parliament | Parliament | Parliament |
| URL for Agency or Authority | www.dpa.gr | www.adae.gr | www.eett.gr |
| Year established | 1997 | 2003 | 1992 |

## Authorities involved with network resilience – not asked to respond

| Authority | National Intelligence Service (EYP) |
|---|---|
| Main Tasks | EYP's mission – always within the framework of the Constitution and legislation – is the quest for collection, processing and disclosure of intelligence to all competent authorities.<br>In addition, in 2008 EYP was defined as the national authority for dealing with electronic attacks. |
| Reports to | Ministry of Interior,<br>Ministry of National Defence |
| URL for Agency or Authority | www.nis.gr |
| Year established | 1924 |

The incumbent telecom provider is Hellenic Telecoms Organization SA (OTE). It is the provider used for the Universal Service Provision. Currently OTE owns more than 90% of the telecom infrastructure in Greece.

Other companies are starting to build their own infrastructure networks. The aim is to connect two million households with optical fibre networks by 2013. Hence, private firms besides OTE are investing in physical infrastructure and building fibre optic networks in urban areas (MTC 1).

The authorities deal with operators and infrastructure owners. Public e-communication networks are defined in Electronic Communications law 3431/2006 (EETT 1) in accordance with the relevant EU Directive.

HDPA and ADAE, as well as National Regulatory Authority (EETT), collaborate with other authorities and Ministries and report to the Greek President of Parliament and the Parliament – once a year with an activity report… In contrast to other Member States, they do not report to a ministry.

## Scope and governance

### Question 1 : The authorities

In Greece, the following authorities are the ones dealing with issues related to the resilience of public e-communication networks:

- The Ministry of Transport and Communications (MTC)
- The National Regulatory Authority (EETT)
- The Hellenic Data Protection Authority (HDPA)
- The Hellenic Authority for the Information and Communication Security and Privacy (ADAE)

EETT, HDPA and ADAE are independent authorities that report to parliament. At the end of the year, all the actions and activities conducted are submitted to the president of the Parliament, the relevant ministers and the Greek parliament. These agencies are subject to parliamentary examination in ways and procedures that follow current parliamentary rules.

EETT bases its mandate on the Electronic Communications law 3431/2006 (EETT 1), According to this law, the operators shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations. According to the law, EETT proposes to the Ministry of Transport and Communications and the Ministry of Interior, the issuing of a Ministerial Decision, regarding measures that are considered necessary. EETT monitors the implementation of the Ministerial Decision.

According to Electronic Communications law 3431/2006, the Ministry of Transport and Communications is responsible for planning the security policy of public electronic communications networks and services, together with the other Ministers in cases of sharing competences.

### Question 2 : The mandate of the authorities

As far as EETT is concerned, the Electronic Communications law 3431/2006 (see EETT 1) stipulates that the agency has the responsibility of consulting with the operators. Such consultation shall involve measures that operators take in order to ensure the integrity of their networks and the availability of their services in extreme situations. As well, based on such consultations EETT is then proposing the issuing of a Ministerial Decision, regarding these measures that were developed with the help of such consultation with operators. As outlined in Q 1, EETT will then be responsible for monitoring the implementation of these measures by the operators.

The Hellenic Data Protection Authority (HDPA) is responsible for security of data processing and of the information and communication infrastructure used for this data processing (see HPDA 1, Art 10). There is no specific provision for the resilience of e-communication networks, but the HDPA is responsible as far as personal data processing is in place. Each case is considered separately as the level of security must be appropriate to the risks presented by processing and the nature of the data subject to processing.

HDPA may offer instructions and issue regulations involving the level of security of data and of the computer and information infrastructure, the security measures that are required for each category and processing of data as well as the use of privacy enhancing technologies (see HPDA 1, Art 10 and 19. 1.k).

The Hellenic Authority for the Information and Communication Security and Privacy (ADAE) is responsible for the protection of the secrecy of mailing, free correspondence of communication as well as the security of networks and communications (see ADAE 1, Art 1). The concept of privacy encompasses the control of observing and regulating the terms and processes of waving of privacy protection as foreseen by the law.

Possible Changes: What is common to both authorities is that they are both data processors. No formal obligations or procedures exist for collaboration; it takes place on a case by case basis. However, the supervising Ministries can require cooperation.

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

According to the " Regulation on General Authorizations " (EETT 2 Decision no 390/3/21-6-06):

*(…Any person that operates under a General Authorization regime and provides Electronic Communication Networks or/and Services to the public is under obligation to take reasonable measures during the design, installation and operation of the network or other equipment used, directly or through third persons, with regard to the provision of any service under a General Authorization regime and the conclusion of any contract with a third natural party or legal entity which pertains to the provision of the above services so as to ensure the following:*

*i. The security, integrity and maintenance of the functions of the Electronic Communication Networks used or/and controlled by the said person, as well as the security, integrity and maintenance of the functions of any other Electronic Communication Network operating under a General Authorization regime to the degree that it is within the control of the said person. Especially any persons operating Public Telephone Networks at fixed locations are under obligation to take all necessary measures in order to ensure the integrity of the network and, if a disastrous failure takes place or in a Force Majeure incident, the availability of the Public Telephone Network and Public Telephone Services at fixed locations.*

*…)*

The Hellenic Authority for the Information and Communication Security and Privacy has issued a regulation concerning six decisions ensuring privacy in the following areas (see ADAE 2)

- Mobile Telecommunication Services
- Fixed Telecommunication Services
- Wireless Telecommunication Services
- Internet Communications, Services and Applications
- Internet Applications and Internet Users
- Internet Telecommunication Infrastructures

This regulation concerns all telecommunication providers of mobile, fixed and wireless networks, providing telecommunication services. It also concerns all the public and private bodies related with Internet telecommunication services, and especially:

(a) internet access providers (fixed and mobile telecommunications providers, Internet Service Providers etc.);
(b) internet service providers; and
(c) value added internet service providers

As said, ADAE is responsible for the implementation and application of security policies to protect the privacy of communications. These six decisions above constitute the minimum measures in order to minimize the number and type of attacks that are related directly or indirectly with the privacy of communications. This way, the electronic communication is made resilient to threats and attacks against privacy of communication

As regards the future, the Ministry of Transport and Communications has devised a strategy for the years 2008 to 2013 (MTC 1). The strategy is a plan that will enable Greece to benefit from, develop and form modern trends in the digital era, ripping the greatest possible benefit for development, social cohesion and quality of life of citizens.

<u>Possible Change</u>: Via the convergence of networks and services, which will be achieved with the development of next generation access networks, we wish to:

- reinforce entrepreneurship,
- create new markets, new investments, and new jobs, and
- improve everyday life of each citizen, regardless of which part of the country he lives in.

The cost for realising the above objectives is estimated to be about 3 billion Euros. These will be covered by national and Community resources, with Public – Private Partnerships playing an important role. The essential policies that need to be developed are:

A) Infrastructure development with the creation of next generation networks. Infrastructure development constitutes the most expensive part of our strategy from the cost point of view. In the next 5 years we aspire to reach optical fibres in at least 2 million homes and make broadband connections available to each and every part of Greece. The total cost is estimated at approximately 2,5 billion Euros.

B) Introduction and development of new technologies in citizens' everyday lives.

The objective is to provide citizens with the opportunity to know and become familiar with new technologies and therefore understand the practical benefits. We present our citizens with pilot actions bringing new technologies closer to them. Through these pilot actions, we will:

- reinforce ADSL home connections for public transportation users
- subsidise terminal equipment for the visually impaired
- subsidise public and corporate websites to comply with "Guidelines for Accessibility to the context of the World Wide Web".
- encourage a high definition pilot TV programme through Hellas Sat.
- set up a Ministry Portal for e-art.
- arrange special events to show the potential of digital technology to all age groups (e-park).
- reinforce the National Digital Security pilot programme.

Finally, EETT is in the process of developing a proposal to the Ministries (as it is required by the Law) regarding network integrity measures that should be adopted by the providers (see also Q 5 – EETT).

### Question 4 : Initiatives between providers and public authorities

The HDPA has organised a consultation with major Greek Internet service providers to discuss the problems caused to their service by spam emails. As a result the HDPA is preparing a recommendation. Notice that spam may cause problems to the availability and functionality of their services (and especially the email service).

ADAE has organized a conference in 2005 dealing with the general principles of national strategy for the privacy and security of networks and information. The aim of this conference was to establish a continuous forum for discussing security and e-communication networks. Similar conferences were held in 2007 and 2008.

As far as EETT is concerned, there are no such initiatives between providers and public authorities.

Possible Changes: Similar initiatives among providers are not known. ADAE's conference findings are so far shared with those attending only.

## Tasks

### Question 5 : Typical task

HDPA issues regulations pertaining to special technical and detailed matters to which the data protection law refers (see HPDA 1 Art 10 and Art 19.1.j)

As far as audits are concerned, HDPA shall proceed ex officio or following up a complaint and do audits, in the framework of which the technological infrastructure and other means, automated or not, supporting the processing of data are reviewed (see HDPA 1 Art 19.1.j)

ADAE carries out regular audits or after a complaint. The audits are mainly dedicated to compliance with the above six decisions.  As pointed out earlier ADAE, undertakes audits ex officio or following complaints to service providers of electronic communications. The last audit took place in September 2008. It concerned a mobile telephony service provider. The audit investigated the application of the access procedure to the information systems that maintain customers' data.

ADAE follows a written procedure for the audits.  The procedure has been approved by ADAE Council. The audits involve the physical examination of the service provider's infrastructure (systems, data bases, archives, files). In cases where the laws are not followed, ADAE asks the service provider to supply clarifications and ADAE has the right to perfmorm a second audit and impose administrative sanctions, such as warnings or fines.

As outlined in Q3, EETT is in the process of developing a proposal to the Ministries (as it is required by the Law), regarding network integrity measures that should be adopted by the providers. For this purpose EETT has distributed a survey to providers regarding security and integrity measures they already adopted. Once, analyses of these data are complete a public consultation with providers with be held before finalising the proposal to be submitted to the ministry.

### Question 6 : Exchange of information between providers and public authorities

All personal data processors, including e-communications providers, must submit to **HDPA** a notification for processes where they intend to use personal data. In the context of the notification, e-communication providers are obliged to inform HDPA about the basic characteristics of the system and the safety measures taken for the protection of data processing. Providers must submit their information security policies and recovery plans. The HDPA uses these documents to decide on the level of protection of data processing, mainly when an audit is carried out.

After a serious incident in the mobile telephony sector, Greece has improved its procedures. ADAE receives information from service providers. There is an obligation to inform ADAE. Security policy which is applied is closely linked to the six decisions described above. At end of each year, each service provider must submit an annual report with the data relating to the security of e-communication and the protection of communication privacy.  At minimum should contain the following:

- all incidents that threaten the security of the provider and the protection of privacy and any injuries that the provider and the users experienced due to this occurrence must  be included, and
- all the measures taken for the recovery of the above incidents.

Also, providers must submit a report annually of all the calls at the European Emergency Number 112. The information collected is used:

a) as a point of reference for future audits
b) for the drawing of conclusions as far as the application of the legislation by the service providers,

c) for the annual report, and
d) in order to evaluate whether the current legislation needs modifications or updating.

Possible Changes: There is not a formalised procedure at the moment for the exchange of information between the providers and EETT. However, the providers have the obligation to provide EETT with any information that may be asked regarding the above mentioned subjects. The distributed questionnaires, mentioned in question 5 contained some of the above mentioned subjects (information security policies, business continuity plans, preparedness measures, information on geographical, topological and technical network structures, locations with high infrastructure density, etc.).

**Question 7 : Handling of security incidents**

Providers don’t have an obligation at the moment to report such incidents. In the case of such an incident, and depending on its severity, EETT demands from the providers data related to the incident.

In the data protection area, providers are not obliged by law to report such incidents to HDPA. This may be done after a question from the authority following a person’s complaint.

However, if the authorities ask questions, the operators are obliged to answer.

In addition to the annual reports (Q 6), ADAE requires to be informed and to inform subscribers in case of danger, breach of civil protection and communication privacy. The operators must provide data about how they took the necessary steps to reduce the risk for having this occur again.

In case of breaching privacy or special danger, the operator is obliged to inform the authority and subscribers

Possible Changes: A practical definition for what a critical incident might represent looking at security, resilience and privacy is not readily available. Also, since providers do not have an obligation to report network failures or resilience issues, it is difficult to see how data obtained about incidents can be used for analytical purposes. As well, analysing findings and developing recommendations from the data reports obtained may not be representative of the real situation.

**Question 8 : Audits related to resilience**

Providers are audited on Data Protection issues. However, there are neither assessments nor audits pertaining to resilience and dependability of e-communication networks.

ADAE undertakes over 60 audits per year, most of them after complaints. The audits aim to examine the service providers' conformance to the legislation.

ADAE undertakes audits ex officio or following complaints to service providers of electronic communications. The last audit took place in September 2008 to a service provider of mobile telephony. The audit concerned the application of the access procedure to the information systems that maintain customers' data.

ADAE follows a written procedure for the audits. The procedure has been approved by ADAE Council. The audits involve the physical examination of the service provider's infrastructure (systems, data bases, archives, files). In cases where the laws are not followed, ADAE asks the service provider to supply clarifications and ADAE has the right to perform a second audit and impose administrative sanctions, such as warnings or fines.

EETT states that providers are not audited regarding the resilience and dependability of their networks

**Question 9 : Enforcement actions**

In case that the providers do not comply with the electronic communications law (EETT 1) or the Regulation on General Authorizations (EETT2), EETT has the authority to address them a recommendation, impose a fine or revoke the provider’s general license.

The HDPA may impose administrative sanctions (warnings, fines up to the amount of about 150.000 €, revocation of permits) for the violations of Data Protection Legislation.

ADAE has the right to issue a decision in the case of breach of law in relation to the privacy of communications, sanctions can be either a recommendation for compliance or a fine 15,000 euros – 1.5 million euros (see ADAE 1, Article 11) It can also impose imprisonment of one year, fine 15,000 to 60,000 euros to anyone who breaches the privacy of communication (see ADAE 1, Article 10). Heavier fines are foreseen in case the person who breaches the communication privacy is a member of staff of a firm in the telecom business. Recently ADAE imposed the following fines: 115.000 euros (in 2006) and 83.960.000 euros (in 2007) In addition there are fines for ADAE staff that make public information and data that are available to them due to their position.

Possible Changes: It is not clear if the fines were issued based on resilience or other issues. As well, how the imposed administrative penalties were used to develop better benchmarks or best practices together with infrastructure owners appears non-existent for all practical purposes.

## Risk Management and preparedness measures

**Question 10 : The national risk management process**

In a data protection perspective a national risk management process is not applicable.

In a new legislation regarding ADAE domain (ADAE 3, Art 13), there is a provision for the development of a national plan for the security of communications in order to protect the infrastructure and the means of electronic communications

Possible Changes: The preparation for this national plan has not yet started since the law came in force by July 10. The plan will include the targets, the general principles and directions, the appropriate standards, the identified dangers, the obligations for the information of the public, the sanctions, and in general the rules for the security of communications for the public sector and the providers of networks and/or electronic communication services.

Responsible for the preparation of the plan is a Special Ministerial Committee. The Minister of Transport and Communications will decide the persons that will make up this committee.

**Question 11 : The preparedness and recovery measures**

In a data protection perspective preparedness and recovery measures are not applicable.

Possible Changes: It is unclear how the agencies collaborate to improve Greece's effectiveness in its level of preparedness and in case of resilience, such as restoring priority communication. Training preparedness and recovery measures and testing their effectiveness with exercises do not appear to happen at this time.

**Question 12 : Incident response capabilities**

In a data protection perspective, incidents response capabilities are not applicable.

In a recent law (EYP 1) concerning the National Intelligence Service, EYP is defined as the national authority for dealing with electronic attacks and it caters for the prevention and the static and dynamic treatment of electronic attacks against communication networks, information storing facilities and information systems.

Possible Changes: Time will tell the situation will change thanks to the National Authority of Dealing with Electronic Attacks whose mission is still evolving.

**Question 13 : Good practice on resilience**

Not known

**Question 14 : Guidelines for procurement**

It is not of our knowledge whether there exist such guidelines regarding the public eCommunications networks.

## References

**EETT 1** Law 3431/2006 FEK A' 13/3-2-2006 "Περὶ Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις" (English title: About Electronic Communications and other provisions – not available in English).
Available
http://www.eett.gr/nopencms/opencms/EETT/Electronic_Communications/GreekLaw/Laws/.

**EETT 2** EETT Decision no 390/3 FEK B' 748/21-6-2006 "Κανονισμός Γενικών Αδειών" (English title: Regulation on General Authorizations - not available in English).
Available http://www.eett.gr.
Last Access: 16 September 2008.

**HDPA 1** Law 2472/1997 FEK A' 47/27-02-2003 "Προστασία του ατόμου από την επεξεργασία δεδομένου προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις" (English title : Protection of individuals from processing of personal data with the amendments incorporated – not available in English).
Available
http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#tp.
Last Access: 12 September 2008.
Particularly relevant are articles: Articles 10, 19.

**ADAE 1** Law 3115/2003 FEK A' 47/27-02-2003 "Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών" (English title: Authority for the Information and Communication Security and Privacy).
Available: http://www.adae.gr/adae/nomoi.html?langid=el.
Last Access: 12 September 2008.
Particularly relevant are articles: Articles 1, 10, 11.

**ADAE 2** The following decisions have been issued by the Hellenic Authority for the Information and Communication Security and Privacy (ADAE) and published in FEK B' 87/26-01-2005 and FEK B' 88/26-01-2005:

1. Mobile Telecommunication Services Privacy Assurance Regulation (Decision 629a)
2. Fixed Telecommunication Services Privacy Assurance Regulation (Decision 630a)
3. Wireless Telecommunication Services Privacy Assurance Regulation (Decision 631a)
4. Internet Communications, Services and Applications Privacy Assurance Regulation (Decision 632a)
5. Internet Applications and Internet Users Privacy Assurance Regulation (Decision 633a)
6. Internet Telecommunication Infrastructures Privacy Assurance Regulation (Decision 634a)

Available: http://www.adae.gr/adae/regulations.html?langid=el.
Last Access: September 12, 2008.
English non-binding version
http://www.adae.gr/adae/regulations.html?langid=en

**ADAE 3** Law 3674/2008 FEK A’ 136/10-07-2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (English title: Reinforcement of the legal framework for the protection of the telephone communication privacy - not available in English).
Available: http://nomothesia.ependyseis.gr/eu-law/getFile/%CE%9D+3674+2008.pdf?bodyId=1000833.
Last access:29 August 2008.
Particularly relevant are articles: Articles 3, 8, 13.

**EYP 1** Law 3649/2008 FEK A’ 39/03-03-2008 Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις (English title: “National Intelligence Service and other provisions”) concerns the National Intelligence Service and its appointment as the National Authority for Encountering Electronic Attacks – not available in English.
Available: http://www.nis.gr/portal/page/portal/NIS/LegalFrame).
Last access: September 15, 2008.

**Additional References:**

**MTC 1** Εθνική στρατηγική στον Τομέα των Ηλεκτρονικών Επικοινωνιών για την περίοδο 2008 – 2013, Strategy of the Ministry of Transport and Communications on Electronic Communications and New Technologies 2008-2013 (http://www.strategyforum.gr/en/links.html).

# National Report of Hungary

## Introduction

### Interview

Date and Duration 22 August 2008 – 1 hr 45 min.

| Interviewee | Mr Miklos BALAS | Mr Csaba SANDOR | Dr Ferenc SUBA |
|---|---|---|---|
| Authority | NHH - NCAH[44] | Secretariat for IT and eGovernment | CERT Hungary |
| Position Title | Technical Advisor | Senior advisor in Hungarian Prime Minister's Office | Chairman of the Board, CERT Hungary |
| Education Training | Technical University, Budapest (telecommunications engineer, engineer-economist) | Eötvös József University, Budapest | Ruprecht-Karls Universitaet, Heidelberg, Magister Artium (English, History)<br>Eötvös Loránd University, Budapest, Iuris Doctor<br>Bar Exam<br>Stock Exchange Exam<br>Senior Civil Servant Exam |
| Responsibilities | Emergency systems | IT; eGovernment; civil protection, cyber protection, defence | Strategic Management of CERT Hungary, International Representation of Hungary in NIS (ENISA, FIRST, EGC IWWN) |
| Relation with ENISA (if applicable) | | | Vice Chair ENISA Management Board |

### Authorities involved with Network Resilience

| Authority | NHH – NCAH National Communication Authority | Secretariat for IT and eGovernment at the Prime Minister's Office in Hungary | CERT Hungary |
|---|---|---|---|
| Reports to | Formally independent; related to Ministry of Energy, Transportation and Communication | Prime Minister | Prime Minister's Office |

[44] *NCAH is the acronym for NHH in English*

| | | | |
|---|---|---|---|
| Year established | Legal predecessor 1991, recent reorganization 2003 | Recently, 2008 | 2004 |
| URL | http://www.nhh.hu/index.php | | http://www.cert-hungary.hu/ |

## Scope and governance

### Question 1 : The authorities

In Hungary, the following three authorities are primarily involved in issues related to the resilience of public e-communication networks:

- NHH – NCAH – National Communication Authority - regulator
- Secretariat for IT and eGovernment - at the Prime Minister's Office in Hungary
- CERT Hungary

Their main tasks in relation to the topics of the questionnaire are the following:

NHH – NCAH is running the early warning system in cooperation with service providers. Two systems are in place: the early warning system involving several service providers and a reporting system where service providers provide information.

Service providers assigned by Ministerial Decree 24/2004 (VIII.16.) (see HR 8) are required to take part in the defence tasks , maintain duty services which report to NHH-NCAH's duty service any event on a daily basis (24/24) which significantly influence their network or services (Ministerial Decree No. 27/2004. (X. 6.) (see HR 9)). The information collected is reported to the Government (to the Ministry). The types of significantly influencing events are:

a) Act of God and accident related to dangerous materials which causes significant disturbance in the work of the network or supply of services.
b) Nuclear accident causing damage of network, fall out or limitation of services.
c) Lack of energy supply causing fall out or limitation of services.
d) Great expansion fires causing fall out or limitation of services.
e) Human, animal or plant epidemics (quarantine) endangering or hindering the provision of services.
f) Faults of electronic communications transmission networks (cables, optical, microwave, radio and satellite connections) causing significant fall out of services.
g) Such faults of electronic communications networks (without mobile telephone networks) which influence at least one thousand user or subscriber, or cause fall out of services of several settlements.
h) Such fault of speech service of mobile networks, which causes the stop of service of one BSC's (= Basic Station Controller's) or wider territory for longer than one hour (daytime), or two hours (by night) – out of the planned service breaks, - and faults affecting the MSCs (= Mobile Switching Centres).

i) Such faults of electronic communications networks, which cause great or significant fall out of services of networks satisfying demands of governmental, administrative, national security or defence networks, and other non-civil systems.
j) Stoppage of public radio and TV broadcasting on the back-bone network longer than five minutes.
k) Stoppage of country-wide commercial radio and TV stations longer than five minutes.
l) Fall out of AM microwave programme distribution network longer than five minutes within the official running time.
m) Such disturbances of information processing and transmission systems, which causes significant damage in availability of the system, or in intimacy, authenticity, integrity, or availability of the stored or transmitted data.
n) Electronic attacks and unauthorized and presumably intentional activities against information systems.
o) Strike significantly influencing the trade and threat by public danger at service providing organisations.
p) Significant fall out of trade of postal services.
q) Act of terrorism and threat by execution of act of terrorism against the network of service provider.
r) Unusual events which are not listed in points a) to q), but judged important.

This Ministerial Decree No.27/2004 (see HR 9) prescribes in detail the system of reporting:

- The service provider's on-duty staff must report to NHH-NCAH about the above listed important events immediately, or every day, if the event's duration is longer.
- On-duty staff of the NHH-NCAH must report to the ministry and the leaders of NHH-NCAH once every week or daily if the event's duration is longer.
- Based on a cooperation agreement, the NHH-NCAH informs the nationwide authority organizations, the organizations of specialized communications networks (closed users group networks), and organizations having network management, and if needed other ministries.
- In a crisis situation, both NHH-NCAH's and the service providers' duty services report daily, or by the frequency prescribed during the execution of the task. The Decree also details the obligatory information content of the reports.

The ministry or NHH-NCAH informs the public in press release about those unusual events which significantly influence the communications and postal sector as whole. The service provider gives information to the public about those unusual events which significantly influence its information or electronic communications network.

The Secretariat for IT and eGovernment (at Prime Minister's Office) deals with policy making in the domain. It is also running, maintaining and regulating the IT systems of the government. The secretariat maintains and runs the emergency communication networks, and oversees CERT Hungary.

On a strategic level, the State Secretary for IT and eGovernment has the responsibility for all strategies in the area of telecommunication and Internet. Currently, the Secretariat is working on the development of a critical infrastructure strategy. The Hungarian Greenbook on national CIP evolved under the direct responsibility of the Prime Minister's Office (see HR 11)

The CERT Hungary is active in the following fields: incident handling, think-tank, international and national co-operation, awareness raising. It deals with information security of public communication networks. It handles network security incidents. It acts as think tank for the government and represents Hungary on the international level with respect to matters of network and information security. CERT Hungary is running an awareness raising web site (www.biztonsagosinternet.hu), organises trainings for schoolchildren, and will carry out, from next year on, a Safer Internet project dealing with child protection.

CERT Hungary has two working groups in place:

- WG 1 is dealing with NIS issues and security incidents in banks – financial sector
- WG 2 is dealing with CIIP issues among energy and telecommunication providers.

**Question 2 : The mandate of the authorities**

The mandate of NHH-NCAH is to give guidance to the service providers, to enforce execution of laws and prescriptions. The legal basis of the mandate is the Electronic Communication law (see HR6 in reference list).

The law (HR 6) does not make many direct references to information security and resilience in particular. Nevertheless, there are many mentions of information security in other laws (e.g., see HR 8, HR 9 in reference list).

The Secretariat for IT and eGovernment is governed by the Electronic Communication law (see HR 6). Its terms of operation are defined in the terms of operations of the Prime Ministers Office. Several Government decrees, and a recent Government decree on central electronic government services in particular (see Dec 1), lay down the mandate of the secretariat.

CERT Hungary acts on behalf of the national telecom agency (NHH-NCAH). Its legal mandate is laid down in a decree on service systems in the IT and electronic communication (and postal) sectors (see HR 9 in reference list). CERT Hungary has a mandate from the Prime Minister's Office to act as government agency in the area of network and information security. Within the legal provisions regarding the early warning system, the authority has the possibility to outsource services to non-profit organisations. As CERT Hungary is run by a foundation, it fulfils the conditions to obtain governmental mandates. It also has a mandate to represent Hungary internationally in the area of network and information security.

The authorities cooperate on several levels intensely, as for example:

- Involvement of CERT Hungary with the national early warning system.
- Weekly reports made available to all authorities.
- Interdependencies through the integration of telecom and energy providers into a detailed disaster plan.
- An intergovernmental working group chaired by PM on national policies regarding cyber-crime.

In general, all authorities participate in the working groups which are set up on the different information security domains.

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

The Electronic Communications Law (HR 6) foresees a number of decrees (e.g., HR8, HR 9 and which other) on the tasks of the telecommunication market players.

Several guidelines and other provisions for security incidents exist:

- A list of national agencies to help ministries in emergency situations is part of the early warning system.
- The working groups on security incidents in banks and on CIIP issues among energy and telecommunication providers are building  up scenarios.
- In the eGovernment domain, guidelines have been adopted following ISO 15408 and ISO 27002 standards. Hungarian municipalities use a combination of both standards.

All main telecommunication providers have established business continuity plans and emergency recovery plans which are used in incidents. NHH – NCAH maintain continuous contact with the main telecommunication providers and is well informed.

Possible Changes: Not many national guidelines address directly the public e-communication networks. One reason for this is that most of the guidelines applied in this domain are developed by the industry.

With respect to future strategies, two legal acts are under preparation: about overall IT security and about eGovernment. In both, a section will deal with the resilience of e-communication networks. The future CERT strategy is closely linked to these legal acts.

The Hungarian Green Book on national CIP has been accepted by a government resolution (see HR 11). It gives guidelines on CII structures based on sectoral schemes and addressing different industrial players. The CIIP strategy should be achieved by the end of 2009. Currently a consultation process is held between government and industrial players. This process will finish by mid of 2009. The regulatory concept should be ready by end of 2009.

### Question 4 : Initiatives between providers and public authorities

As the working groups mentioned above demonstrate, many initiatives among providers and authorities are going on. In general, there is exchange of information within the early warning system. Many working groups are in place, the ones in the banking sector and on energy and telecoms operate in the form of Public-Private Partnership (PPP). The CIIP consultation process is a good example of an initiative between providers and authorities.

Not much is known about initiatives among providers. In general, it can be said that the cooperation among providers is not very intensive, unless the state and public authorities initiate and promote the cooperation.

## Tasks

### Question 5 : Typical tasks

The three authorities are involved in the typical tasks listed in the questionnaire in varying degree.

NHH - NCAH holds public consultations on several topics regarding telecom regulations but not on guidelines and recommendations. Daily contacts exist between the security services of NHH-NCAH and the security services of the leading providers, and that way regular exchange of information is ensured. Within its mandate NHH-NCAH does audits. But only audits of the accounting of the main telecom players take place on a regular basis. Audits will be carried out if a problem has been reported or on a case by case basis in case of complains. Within its mandate NHH-NCAH also has the right to use enforcement but it has never been used. The market players cooperate on a voluntary basis.

The Secretariat for IT and eGovernment organise public forums and similar events for service providers involving the regulator, and other governmental eServices and networks. Regular interaction with service providers is fixed in the respective contracts; most often, government organisations are in daily contacts with their providers. Contractual obligations are supervised by the Department of Security. Enforcement is task of NHH-NCAH.

A further task of the secretariat is the responsibility for several non-public networks and government services which are different from the public networks.

In the frame of the early warning system, CERT Hungary holds regularly consultations with the largest telecom providers, energy providers and banks. CERT Hungary cannot directly use enforcement; in case of need NHH-NCAH is informed of a provider who does not cooperate, for example. It can also refer to the liability clauses for ISP of Act No. 108. of the year 2001 on e-Commerce.

Other typical tasks of CERT Hungary include security incidents handling, international representation, think tank for government (preparation of regulation and strategies) and awareness raising.

Audits are not conducted as far as dependability and resilience of e-communications networks are concerned.

**Question 6 : Exchange of information between providers and public authorities**

NHH-NCAH keeps contact with providers on information security policies. In the area of information on geographical and topological network structures there is a problem. The network databases of the different providers differ and are not compatible. Therefore, a large amount of data and information is collected and available but it can not be assessed in a structured way.

Information provision is mandatory for the main players and they do. Recently, one company complained that it was not part of the main players as it is not obliged to report. As regards the exchange of information on incidents, a decree (see HR 9, and Question 1) states that network incidents must be reported and gives the structure for incident reporting, and specifications about critical incidents. Accordingly, the report must address the following topics:

- nature of the incident,
- persons injured if any,
- financial damage,
- measures taken to rectify the situation,
- expected time for recovery,
- the number of subscribers affected, etc.

The CERT Hungary uses the Traffic Light Protocol (TLP), which was developed by the Centre for Critical Infrastructure Protection (CCIP) New Zealand[45]. Incident information that is sensitive (but unclassified) is labelled using the TLP (see HR 12a for more information). Here, the the originator signals how widely one wants this information to be circulated beyond the immediate recipient, if at all. Moreover, the incident handling activity uses the Response Tracker for Incident Response (RTIR) protocol[46] (see HR 12b).

CERT Hungary shares this kind of information with other government offices. NHH-NCAH releases information to the press too. In crises, the rules of the Hungarian crisis management system prescribe what kind of information is shared with the crisis emergency group. The latter in turn prepares these data and information to allow

[45] *The Traffic Light Protocol (TLP) was created in order to encourage greater sharing of information. Information sharing is important for helping mitigate the spread of electronic attacks, improving protection through sharing best practices, and building trust between players in this field. In order to encourage the sharing of sensitive (but unclassified) information, however, the originator needs to signal how widely they want their information to be circulated beyond the immediate recipient, if at all.*

[46] *RT is an enterprise-grade ticketing system which allows for the checking of the status of various tasks including such as, when the tasks were requested, who requested the tasks and why, when the tasks were completed and prioritizing. It was developed by the people at http://bestpractical.com and is the leading open-source issue tracking system. Best Practical has also created RT for Incident Response (RTIR), which is* "an Open Source incident handling system designed with the needs of CERT teams and other incident-response teams in mind.*" (see HR 12b in reference list)*

decisions to be made by the appropriate government authorities such as cabinet. CERT Hungary is using the information to organise and coordinate protective actions.

Possible Changes: What is currently still lacking are exercises whereby certain scenarios regarding e-communication networks such as a storm or power failure are played out in an exercise.

As well, how incidents are being reported regarding vulnerabilities or reliability of networks (e.g. redundancy issues, failure of service) online or using different channels still needs some discussion. The TLP is one step in the right direction.

**Question 7 : Handling of security incidents**

In general, reporting of security incidents to the public at large is obligatory for the assigned telecom providers in Hungary. The number of users of a service affected is the most important criteria whether a public announcement is made or not. The size and number of affected networks is the criteria whether the information is published by the authority or by the telecom provider. Parallel information can happen (see HR 9, and Question 1).

For example, some years ago, a cable cut in a network had happened. The authority and the telecom provider informed the public jointly by explaining what had happened, why no telephone connections were possible.

For about the last five years, NHH-NCAH has also started to publish information material to the public at large about potential problems that might happen within the communication networks, how to avoid and what to do in case of an incident. The covered topics (17.09.2008) are:

- subscribers' contract;
- fidelity contract;
- internet;
- internet telephony – Voice of IP (VoIP);
- cable TV;
- carrier selection;
- spam;
- number portability;
- telephone;

This is all part of "Tantusz" – the public tariff-comparison programme of NHH-NCAH) (see HR 13 in reference list). The above relates to Quality of Service (QoS) provisions that EU Member States provide online to increase the market transparency while reducing information asymmetry between consumers and operators.

CERT Hungary is sharing information on cyber security incidents with relevant organisations at the national and international level and it is sharing information in the working groups.

Incidents dealt with in the working groups are treated confidential. No communications are made to the outside. For example, there were massive incidents (phishing attacks) in 2006 against the 7 biggest banks in Hungary; the problem was communicated by the individual banks to their customers separately but not published in the media or by CERT Hungary.

### Question 8 : Audits related to resilience

NHH-NCAH audits the accounting systems of the main telecom providers. These are executed by accredited professional auditors. Currently, there are two auditing companies in Hungary which are accredited to do these audits. These audits take place yearly, and NHH-NCAH checks the results.

However, NHH-NCAH does not initiate audits that focus on network and software architecture or other issues related to resilience of e-communication networks.

CERT Hungary offers audits, penetration tests, etc. as a value added-service for payment.

Possible Changes: There are neither formal assessments nor review procedures including audits focusing on reliability, dependability, contingency and recovery plans for infrastructure owners today.

### Question 9 : Enforcement actions

NHH-NCAH has a legal mandate to use enforcement actions. Up to now enforcement has never been made in the field of security, as a case has not happened yet. The penalties to enforce regulations could include ordering a company to resolve a problem, imposing a fine to a company or to the manager of a company, increasing the fine if a problem persists.

The Secretariat for IT and eGovernment does not have a mandate to penalise. However, contractual penalties can be applied when included in the contracts with the eGovernment service providers.

In general, it was stated that the providers comply always with regulations, requirements, etc. A real problem has never happened so far.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

It was stated that an overall risk management process regarding resilience of public e-communication networks would not be possible and could not work.

In Hungary, a risk management plan is obligatory for all assigned companies active in the IT sector. Also, a risk management process has been established for all eGovernment areas. Here, all activities are subject to certification according to the eGovernment Guidelines of Information Security based on ISO standards (e.g. ISO 15408 and ISO 27002, and mixture). Certification will take place as of next year.

Hungary does not have a national risk management process.

**Question 11 : The preparedness and recovery measures**

In order to keep the preparedness and recovery measures to mitigate risks up to date, regular big national exercises are held with all players in the telecom sector.
Such a big exercise takes place at least every third year.

Smaller dedicated exercises are carried out regularly in-between. These exercises might cover, for example, the interdependencies between telecommunication and energy, oil, gas etc. In every sector, specific scenarios for recovery measures have been developed.

The public telecommunication sector in Hungary does not have formal priority services. Only some informal prioritisation guidelines exist. All assigned telecom providers are obliged to have emergency recovery and business continuity plans. These are controlled by NHH-NCAH visiting providers on site.

As a recent flood in Hungary has shown, all big providers ensure basic services in their domain in real incidents without posing any problems.

Possible Changes: Exercises will be carried out in the near future to determine possible areas of improvement regarding network resilience. Online communication might be expanded informing the public about these exercises, their intent and findings that will again result in changes for improving public e-communication network resilience.

**Question 12 : Incident response capabilities**

There are three CERTs in Hungary:

- The national CERT – CERT Hungary
- An academic network – NIIF CSIRT
- An ISP CERT (private sector) which is operated by the Computer Science Institute of the Hungarian Academy of Sciences - Hun CERT

The national CERT Hungary is the national coordination point and coordinates all actions against attacks.

At the international level, CERT Hungary cooperates with various networks, associations and with centres in other countries such as:

- FIRST (Forum of Incident Response and Security Teams)
- Trusted Introducer, TF-CSIRT (Task Force Computer Security Incident Response Teams)
- IWWN (International Watch and Warning Network)
- European Government CERT Group

Past incidents are always analysed in the framework of the working groups. The analyses are also useful for the exercises at large scale. Within the IWWN, exercises reflect the 2007 incident in Estonia.

### Question 13 : Good practice on resilience

Good practices have been worked out in the form of recommendations by the NHH-NCAH and the service providers regarding business continuity and recovery measures. The eGovernment guidelines on information security (based on ISO 15408 and ISO 27002 standards) are considered good practice.

Possible Changes: Good practice recommendations by NHH-NCAH do not exist in organized and written form. While they were mentioned in negotiations with service providers, in future, a more systematic collection and sharing with providers could further improve resilience of e-communication networks.

### Question 14 : Guidelines for procurement

The government procurement guidelines contain a requirement on virus protection. Resilience and dependability of public e-communication networks are not addressed in the procurement guidelines.

## References

This reference list provides those acts, governmental and ministerial decrees' which are related to the resilience of public eCommunications networks and points out their particularly relevant articles.

**HR 1** Act XX. of 1949., "1949. évi XX. Törvény A Magyar Köztársaság Alkotmánya" (Hungarian Constitution – available in English).
Available:
http://net.jogtar.hu/jr/gen/getdoc2.cgi?dbnum=1&docid=94900020.TV.
Last Access: September 25, 2008.
English non-binding version, http://www.servat.unibe.ch/icl/hu00000_.html and http://www.mkab.hu/en/enpage5.htm.
Particularly relevant are articles: 35.§ (1) i), 59.§ (1)

**HR 2** Act LXXIV. of 1999. "1999. évi LXXIV. Törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről" (Direction, organization of defence against catastrophes, and defence against grave accidents concerning dangerous materials – Act on Crisis Management).
Available: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99900074.TV.
Last Access: September 25, 2008.
English non-binding version - only Section 4 of the Act (paragraphs 3, 4, and 30 to 43), http://www.mkeh.gov.hu/Konyvtar?Search=1&topic_id=29&page=3 (near to bottom of the page).
The full law deals with crisis management and its organization, concentration, (mainly on dangerous materials). Particularly relevant are articles: 5.§ a) and e), 14.§ d) and e), 46.§. to 48.§.

**HR 3** Act CV of 2004 "2004. évi törvény a honvédelemről és a Magyar Honvédségről" (National defence and Hungarian Army) (updates 02.07.2007).
Available: http://www.hm.gov.hu/files/9/3857/2004._evi_cv._torveny.pdf and http://www.hm.gov.hu/files/9/3857/2004_cv_mod.pdf.
Last Access: September 25, 2008.
Particularly relevant are articles: 34.§. and 36.§. h), 43.§. (1) and (2).

**HR 4** Act CVIII. of 2001. "2001. évi CVIII. Törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről" (Certain issues of electronic commerce services and on information society services).
Available: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0100108.TV.
Last Access: September 25, 2008.
Particularly relevant are articles: 4.§. (3), 13.§.

**HR 5** Act XXXV of 2001 "2001. évi XXXV. Törvény az elektronikus aláírásról" (Electronic signature)
Available: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0100035.TV.
Last Access: September 25, 2008.
English non-binding version http://www.nhh.hu/dokumentum.php?cid=10623.
Particularly relevant are articles: 5) Act XXXV. of 2001. on "Electronic signature"

**HR 6** Act C of 2003 "2003. évi C. törvény az elektronikus hírközlésről" (Electronic communication law).
Available: http://www.nhh.hu/dokumentum.php?cid=9177.
Last Access: September 25, 2008.
English non-binding version http://www.nhh.hu/dokumentum.php?cid=10617.
Particularly relevant are articles: 4.§. (1) g), 5.§. (1) n) and o), 10.§. b) and l), 33.§, 34.§, 86.§.(1) c) and d), 92. §, 145.§, 156.§, 182.§. (2) b) and (4) a), l) and t).

**HR 7** Governmental Decree 100/2004. (IV.27.) "100/2004. (IV. 27.) Korm. rendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról" (Preparation system in electronic communications emergency and crisis situation, tasks of governmental organizations and supply of the conditions of their action).
Available: http://www.nhh.hu/dokumentum.php?cid=13011.
Last Access: September 25, 2008.
English non-binding version
http://www.nhh.hu/dokumentum.php?cid=10618.The full decree is important from the point of view of the topic.

**HR 8** Ministerial Decree 24/2004. (VIII.16.) "24/2004. (VIII. 16.) IHM rendelet a védelmi feladatokban részt vevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról" (Assignment of electronic telecommunications and postal service providers taking part in the defence tasks, and determination of their preparations tasks).
Available: http://www.nhh.hu/dokumentum.php?cid=8208.
Last Access: September 25, 2008. The full decree is important from the point of view of the topic.

**HR 9** Ministerial Decree No. 27/2004. (X. 6.) "27/2004. (X. 6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről" (Establishment, operation and sphere of authority of duty service systems in the IT and electronic communications and postal sector, their reporting and service connection obligations of the assigned providers).
Available: http://www.nhh.hu/dokumentum.php?cid=8207.
Last Access: September 25, 2008.
English non-binding version http://www.nhh.hu/dokumentum.php?cid=10863.
The full decree is important from the point of view of the topic.

**HR 10** Governmental Decree 182/2007. (VII.10.) "182/2007. (VII. 10.) Korm. rendelet a központi elektronikus szolgáltató rendszerről" (Central electronic service system).
Available: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0700182.KOR.
Last Access: September 25, 2008.
Particularly relevant is: Supplement No.4. „Information security regulations"

**HR 11** Governmental resolution 2080/2008. "Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. Kormány határozat" (Governmental resolution on the National Critical Infrastructure Protection Program) (Hungarian

Greenbook on national CIP) (Not publicly available).

**HR 12a** Traffic Light Protocol (TLP)– information labelling tool for sharing information about IT security.
Available: http://www.ccip.govt.nz/incidents/tlp.html.
Last Access: September 25, 2008.

**HR 12b** RTIR - incident handling tool, short description in English.
Available: http://bestpractical.com/rtir/comparison.html or see the slides here http://www.terena.org/activities/eurocamp/november07/slides/RT-Authen-Federation.pdf.
Last Access: September 25, 2008.

**HR 13** "Fogyasztói tájékoztatók" (Information for consumers).
Available:
http://www.nhh.hu/index.php?id=hir&cid=1882&mid=1344&lang=hu.
Last Access: September 25, 2008.

### Additional resources

The Hungarian National Platform for Disaster Reduction,
http://www.preventionweb.net/english/hyogo/national/v.php?id=77&pid:23

### Additional links

**CERT Hungary** (National CERT), http://www.cert-hungary.hu/, http://www.kiiv.hu (CIIP website operated by CERT Hungary.

**NIIF CSIRT** (Academic CERT), http://www.niif.hu/en/csirt.

**Hun CERT** (Private Sector CERT),
http://www.cert.hu/index.php?option=com_content&task=view&id=343&Itemid=31

# National Report of Ireland

## Introduction

In view of the lack of confidentiality of the data in the stock taking procedure, both interview partners underlined before the interview that 'conscious of the lack of confidentiality, they would give rather generic answers'.

### Interview

Date and Duration - 8 August 2008 – 50 minutes.

| Interviewee | Mr Aidan RYAN | Dr Paul CONWAY |
|---|---|---|
| Authority | Communications Sector - Department of Communications, Energy and Natural Resources (Ministry) | ComReg - Commission for communication regulations |
| Position title | Telecommunications Advisor | Officer |
| Education/training | Chartered Engineer, lawyer | Ph.D - Electronic Engineering |
| Task Responsibilities | Oversight of emergency planning for telecommunications networks | Compliance mechanisms |
| If applicable, relationship to ENISA | Management Board Member | |

### Authorities involved with Network Resilience

| Authority | **Communications Sector** | **ComReg** – Commission for communication regulations |
|---|---|---|
| Main Tasks | Promotion of investment in state of the art infrastructures,<br>Provision of a supportive legislative and regulatory environment<br>Development of a leading edge research and development reputation in the information , communications and digital technologies | Promote competition<br>Contribute to the development of the internal market<br>Promote the interests of users within the European Community |
| Reports to | Department of Communications, Energy and Natural Resources (Ministry) | An independent body under the aegis of Department of Communications |
| Year established | | 2002 |
| URL | http://www.dcenr.gov.ie | http://www.comreg.ie / |

## Scope and governance

### Question 1 : The authorities

Two authorities are responsible for issues related to resilience of public e-communications networks in Ireland:

The Communications Sector of Department of Communications, Energy and Natural Resources is responsible within the topics covered by the questionnaire for:

- preparation of legislation
- transposition of EU legislation
- the "Structured exercises" (see below) in the telecommunications area.

ComReg - Commission for Communication Regulation - is the regulator for the electronic communications (telecommunications, radio communications and broadcasting) and postal sectors. ComReg regulates the operators including their compliance with obligations of network security and integrity. ComReg describes its responsibilities and tasks on the Web

> *ComReg is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications and broadcasting transmission) and the postal sector.*

### Question 2 : The mandate of the authorities

The Ministry is in charge of the general legal framework. The legislative activities embrace specific legislation from the EU as well as domestic driven legislation including primary and secondary legislation. ComReg monitors compliance with the various legislative instruments and the General Authorisation (ComReg document – 03/89 General Authorisation) which requires operators to ensure the security of public networks.

ComReg is in charge of the day-to-day implementation based on the framework given by the Ministry. The mandate of ComReg is set out in the Communications Regulation Act of 2002 (see ComReg 1).

### Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks

In Ireland, the General Authorisation which public operators must adhere to requires the operator to take all measures necessary to ensure the security of Public Electronic Communications Networks against unauthorised access (see ComReg 2) according to EC Directive 97/66/EC of 15 December 1997.

In view of the fast changes in the telecommunication industries, legislation is technology neutral in general. It sets out principles; the interpretation of these principles is done by industries themselves.

The Ministry has prepared documents on the planning of telecommunications networks from an emergency perspective for use by Government Departments. These include guidelines for designing and deploying resilience. These guidelines are not available on the web site.

As regards future strategies concerning the resilience of communication networks, Ireland is participating in the drafting of the new EU Framework Directive in the area of security issues. Currently, they wait until the wording of the revised EU framework Directive is decided. A review of approach will take place following the implementation of the new framework.

**Question 4 : Initiatives between providers and public authorities**

Providers and public authorities work closely together on issues of resilience of public e-communication networks. The Communications Sector, ComReg and major operators come together on a regular basis. They have formed working groups on different levels, such as CEO level or technical level.

In these working groups, so called "Structured Exercises" are discussed, designed and done. For example, the working group dealing with technical issues, designs and stress tests for networks, addresses these issues in desktop exercises[47]. Such a meeting might take place during a whole day and the participants are 'locked' in rooms in a dedicated facility for stress tests. The results of such exercises are reported back to the CEO working group to draw conclusions, recommendations etc.

Representatives of public emergency services as well as industry engage in these exercises. The structured exercises form the basis of cooperation, information exchange, trust building between public authorities, industry and other stakeholders in the e-communications area of Ireland. All relationships take place in a consensual model of cooperation. All players are participating.

The providers have also a very good working relationship among each other. Operators run their own business continuity plans. In Ireland, formal cooperation agreements among the operators or among operators and public authorities do not exist.

The e-communication community (operators, public administration, and other key stakeholders) in Ireland is quite small; the key individuals know each other quite well, and all work in a collaborative manner. This approach is under review and will be revisited following the implementation of the new framework.

[47] *Just to explain in more detail, one can distinguish between a desktop exercise or a field emergency simulation. A desktop exercise is conducted using a scenario involving the responding to a situation where all relevant stakeholders need to work together to see how things might work out. In principle, the lessons learned can then be used to be tested in a field exercise or simulation.*

## Tasks

### Question 5 : Typical tasks

Both authorities are engaged in the typical tasks outline in the questionnaire. Public consultations with all providers about regulations, guidelines or recommendations are held.

Audits are carried out but in a non-formal way. For example, based on the results of the structured exercises, gap analyses are carried out which are then brought into the CEO working group for further discussion and consideration.

Operators' compliance to their obligations will be demonstrated as above. If deemed necessary ComReg can take enforcement action, directing compliance with the obligations. ComReg has two more tasks, which are typical:

a. The assessment and coordination of actions after an operator has notified ComReg about an incident.
b. The transposition of high-level obligations and requirements into operational exercises

It was underlined that for making the consensual model work, it is important to maintain good contacts with the individuals in the various organisations and to know well with whom to deal on which matters. Both authorities consider the networking as an ongoing task.

Possible Changes: Exchange of information between providers and authorities could be more formalised. As well, the information exchange regarding technical issues should be more detailed than is the case today. This will be reviewed following the implementation of the new framework.

### Question 6 : Exchange of information between providers and public authorities

In the frame of the consensual model, the key stakeholders know each other and providers share information with authorities easily. As the administration for resilience issues is a small one, public authorities need to share information with providers and engage in good exchange to enhance information level.

Information is exchanged on all topics addressed here, i.e. information security policies, business continuity plans, preparedness measures, information on geographical, topological and technical network structures, locations with high infrastructure density. In addition, information is exchanged about new technologies that have been rolled out. Within the cooperative model, information sharing, whereby formal requests are unnecessary is the norm. However, appropriate legislative requirements for information sharing are in place.

As regards the use of the information collected, ComReg holds a large stock of information. ComReg analyses the information appropriately according to various criteria.

In the frame of the consensual model, the key stakeholders know each other and providers share information with authorities easily.

### Question 7 : Handling of security incidents

Providers in Ireland report security incidents. The reporting is structured as follows:

- an initial report about the incidents,
- a progress report, and
- after damages from the incident are resolved, a closure report issued.

The Communication Sector follows this reporting procedure quite closely but increased formalisation of this is going to be considered. In general, the reporting is confidential. However, if the incident happened in the public domain, for example if a network was off, it could be made public by ComReg.

### Question 8 : Audits related to resilience

The Irish system does not foresee formal audit procedures for providers. Moreover, there is no need for formal audits.

However, information that could also result from audits becomes available through the "Structured Exercises" (see above). Given the size of the administration, it would be difficult to carry out audits. Through the continuous information flow, a lot of information is shared. In addition, the operators themselves are interested to demonstrate the efficiency and the effectiveness regarding security and integrity of the networks.

If audits were needed, ComReg would have the capability to conduct such audits. It was pointed out that audits are relevant. They will be done were necessary and appropriate at the discretion of ComReg.

### Question 9 : Enforcement actions

Enforcement actions belong to the day-to-day activities of ComReg. It has considerable power to enforce compliance. The respective directives impose obligations regarding civil and criminal offences.

Recent cases of enforcement did not concern network integrity and security. In any case, the operators are interested to avoid (negative) publicity due to enforcement actions. In general, enforcement actions are not really an issue in Ireland.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

Ireland does not have a national risk management process. Instead, Ireland has structured emergency planning implemented. A task force appointed by the Government is dealing with emergency planning. Mr Aidan Ryan is a member of the task force and reports on communications issues.

The working groups in the Structured Exercises are also dealing with risk management, emergency planning and related topics. For example, the CEO group discuss emergency scenarios.

The operators have their own risk management planning in place. They bring their knowledge about it into the structured exercises.

### Question 11 : The preparedness and recovery measures

Preparedness and recovery measures are topics at all levels of the structured exercises. Gap and SWOT analyses are carried out. Points for actions are brought forward to management level of structured exercises. Management then decides what resources and support for appropriate solutions must be provided.

In order to keep the information – elaborated in structured exercises – up-to-date independent experts from outside are appointed to assess, oversee and comment the measures.

### Question 12 : Incident response capabilities

Among the incident response capabilities in Ireland, there is a Robust Telecommunication Centre regarding the resilience of telecommunication facilities, equipped with adequate resources and experts.

There is also a publicly funded, educational CERT run by HEAnet (see HEAnet), Ireland's Education and Research Network.

In cases of normal routine, the numerous relationships with and among key operators permit to take appropriate decisions and actions should it be necessary.

An annual report about emergency planning is prepared by the Department of Defence and forwarded to Government.

### Question 13 : Good practice on resilience

In Ireland, no repository of good practices on the resilience of public e-communication networks exists. Each operator is obliged to follow good practice, and operators and stakeholders are engaging in good practice. Though not formalised, a good practice repository among various stakeholders in the sector exists.

### Question 14 : Guidelines for procurement

There are no official guidelines dealing with procurement. Service provision is considered a matter of the private sector, and the principles for it are in the legislation. All players aim at putting the best equipment in place.

## References

| | |
|---|---|
| **ComReg 1** | Communications Regulations Act 2002 - Number 20 of 2002.<br>Available http://www.irishstatutebook.ie/2002/en/act/pub/0020/index.html.<br>Last access: August 28, 2008. |
| **ComReg 2** | General Authorisation - Pursuant to Regulation 8 of the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations, 2003 (S.I. No. 306 of 2003) Conditions for the provision of Electronic Communications Networks and Services Document No: 03/81 Date: 25 July,2003.<br>Available http://www.comreg.ie/_fileupload/publications/ComReg0381.pdf.<br>Last access: September 30, 2008. |

### Additional Resources

none

### Additional Links

**HEAnet** - CERT run by HEAnet,
http://www.heanet.ie/services/services.php?serID=1&subID=6.

# National Report of Latvia

## Introduction

### Interview

Date and Duration - 1 September 2008 - 55 minutes.

| | |
|---|---|
| Interviewee | Mr Janis Graudins |
| Authority | Department of Communications, Ministry of Transport |
| Position title | Deputy Director |
| Education/Training/ Degree | Business |
| Task and Responsibilities | Responsible for International issues, broadband developments issues |
| If applicable, rel.ship to ENISA | National Liaison Officer ENISA |

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | Ministry or Transport |
| Main Tasks | Provides telecom regulation, develops regulation and policy |
| Reports to | The Cabinet of Ministers |
| URL for Agency or Authority | www.sam.gov.lv |
| Year established | 1990 |

### Authorities involved but not part of the interview

None.

## Scope and governance

### Question 1 : The authorities

Resilience policy of Latvia is still in the development stage. The authority responsible for issues pertaining to resilience and policy development is The Ministry of Transport. However, its work on dependability and resilience of e-communication networks has just begun.

The Ministry of Transport is the only authority responsible for any matters pertaining to dependability and resilience of e-communication networks. It will begin implementing matters pertaining to resilience from 2009 onwards. So far, the activities of the ministry were focused on broadband development and implementing EU regulation. In turn, resilience was not part of these activities.

The ministry does not yet have a budget earmarked for dependability and resilience of e-communication networks issues. Therefore, it cannot contract experts or hire staff.

**Question 2 : The mandate of the authorities**

The mandate of the Ministry of Transport stems from the Electronic Communication Law (see LV 1). The Ministry has developed regulations, policies and ways to encourage cooperation with providers. Nevertheless, resilience has not been at the core of these activities.

Possible changes: With the help of a budget and the necessary staff, more efforts can be put into the dependability and resilience of e-communication networks.

At least two to three full-time staff are required to do these issues some justice. Latvia hopes that by the beginning of 2009 activities will start. Nevertheless, unless there is a budget for such work in place by early 2009, activities cannot start. Accordingly, if there is no budget for work in the area of dependability and resilience of e-communication networks by 2009, there will not be any activities we can undertake during 2010. Of course, EU regulations pertaining to network dependability and resilience will be quite helpful for convincing the Council of Ministers to allocate the resources required.

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

The regulations regarding resilience of the public e-communication networks in Latvia are laid down in the Electronic Communications Law (see LV 1) in Chapter 4, Sections 19 and 21. The relevant paragraphs are the following:

*"Section 19. Duties of Electronic Communications Merchants*

*(1) Electronic communications merchants have the following duties, to:*
*(……)*
*16) perform technical and organisational measures in relation to the security of the electronic communications network for the protection of the user data thereof, as well as in the case of a threat to a specific electronic communications network to inform users regarding the risks of using the electronic communications network and the accessible means of legal protection for the reduction of such risks; and*
*17) inform users regarding the possibility of installing a content filter, which restricts access of such material in which is propagandised cruel behaviour, violence, erotica and pornography, and which creates a threat to the mental development of children, as well as ensure the installation of content filters if the subscriber and the electronic communications merchant have mutually agreed regarding them.*
*(…… )*
*(2) In addition to those referred to in Paragraph one of this Section, a public telephone network operator has the following duties:*
*(……)*
*2) to ensure for the end-users of its network access to operator assistance services, telephone directory services and comprehensive telephone directory services;*
*(……)*

*Section 21. Mutual Relations between Electronic Communications Merchants*

*The mutual rights, duties and liabilities between electronic communications merchants shall be determined by a contract."*

Communication networks are in the portfolio of the Ministry only since 5 years, initially with an information and communication technologies department. The department on information and communication technologies has been moved to the Ministry of Special Issues under e-government. Their focus is e-government services and not resilience of networks. The future strategies will include policy development in the field, staffing and launching all activities necessary.

### Question 4 : Initiatives between providers and public authorities

As far as known there are no initiatives regarding resilience between providers and public authorities in Latvia.

## Tasks

### Question 5 : Typical task

In Latvia, there are neither measures in place nor the staff necessary to audit or check compliance. For instance, auditing if operators and providers administer the law according to the letter as well as the spirit is, therefore, not possible. We do not follow-up to check if things work according to plan.

### Question 6 : Exchange of information between providers and public authorities

Working groups or forums for exchanging information with providers do not yet exist in Latvia.

### Question 7 : Handling of security incidents

Providers in Latvia do not report security incidents. Latvia has an independent public utility regulator the Latvian Public Utilities Commission (PUC). It checks providers and operators as far as tariffs and accessibility is concerned. However, the regulator does not with incidents pertaining to dependability and resilience of public e-communication networks (see LV 2).

A document on how to report does not exist for the operator as there are no requirements on reporting stated in the telecommunication law (see LV 1). In case of incidents, operators act accordingly but do not report to the authorities. Therefore, the authority may not hear about an incident.

### Question 8 : Audits related to resilience

Latvia does not conduct audits focusing on dependability and resilience of e-communications networks issues.

### Question 9 : Enforcement actions

Currently there is not much enforcement pertaining to dependability and resilience of e-communications networks issues. Neither is there much enforcement on how operators meet their security and dependability obligations for all practical purposes.

Possible Changes: In order to implement enforcement actions, Latvia needs to introduce specific regulation pertaining to enforcement and resilience in particular. This regulation would then specify under what conditions penalties or fines may apply in case of non-compliance with the regulatory regime.

Latvia does currently not have any provisions regarding this matter.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

After the Estonia incident in 2007, work has started on threat issues. However, this work is progressing very slowly.

Practically speaking, there is no national risk management process in place. Neither is specific attention given to issues pertaining to dependability and resilience of public e-communication networks.

### Question 11 : The preparedness and recovery measures

Currently, preparedness and recovery measures lie with the operators. The authority is only starting with measures to mitigate risks affecting resilience, and it will be a long way.

### Question 12 : Incident response capabilities

Latvia established a Computer Security Incident Response Team (DDIRV). It provides recommendations and consultations for IT administrators in Latvia in case of security incidents. It is a national CERT. Unfortunately, its financing is still a problem. Private companies are not willing to pay for these services yet, and therefore the DDIRV does have limited resources available. It is in fact quite small.

DDIRV basic service in case of computer security incident is available for both registered and unregistered clients, but only IT administrators of state and municipal institutions can voluntarily register for additional benefits like pre-emptive information about threats that might affect their systems. Unregistered clients can receive consultations or recommendations in case of computer security incident.

It means that DDIRV consultations and recommendations are available for every person who has submitted incident response and is responsible for security incident handling and prevention in his/her network. For individual users DDIRV first suggests to contact their technical helpdesk or internet service provider. In case of emergency, consumers can submit their computer security incident report. DDIRV starts working on a reported security incident only, after receiving a request (re-active approach).

CERT NIC.LV is providing security services and incident response for the Institute of Mathematics and Computer Science, University of Latvia (IMCS UL) constituency, both academic and commercial customers.

Furthermore, there is Latvia's Computer Emergency Response Team (LV CERT) initiative. This is a forum of incident response and security specialists from various organizations in Latvia. First meeting was held in 23rd March, 2007 and since then several workshops and meetings have been organized to discuss issues of common interest. The main goals of the forum are to exchange the contact information, to collaborate on incident response and to exchange experience on different computer security related topics. As a forum it does not handle incidents but fosters closer collaboration and better communication amongst public and private organizations in Latvia.

These organisations exchange information but they do not address reliability and dependability to improve network resilience. Hence, they address information security issues such as malware, software vulnerabilities and threats (e.g., botnet attacks, hacking attacks). However, these groups do not focus specifically one hardware, software and network architecture issues that are important for getting a handle on dependability and resilience matters pertaining to e-communications networks.

It is not known whether past incidents are analysed and whether post investigations take place.

### Question 13 : Good practice on resilience

There is not repository on good practice in place.

### Question 14 : Guidelines for procurement

Guidelines for procurement do not include clauses regarding resilience.

## References

**LV 1** Elektronisko sakaru likums 2004 adopted by the Saeima on October 28, 2004 (The Electronic Communication Law 2004).
Available: http://www.likumi.lv/doc.php?id=96611.
Last Access: September 15, 2008.
English non-binding version,
http://www.sprk.gov.lv/index.php?id=1116&sadala=193.
Particularly relevant are articles: Chapter IV

- Section 19 - Duties of Electronic Communications Merchants,
- Section 21. - Mutual Relations between Electronic Communications Merchants.

## Additional Resources

**PUC 1** Case study multi-sector regulator: Latvian Public Utilities Commission (PUC) [6.1.1].
(Available: http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2029.
Last Access: September 15, 2008.

## Additional links

**National CERT**, Computer Security Incident Response Team (DDIRV), http://www.ddirv.lv/.

**CERT NIC.LV** (academic network), http://www.nic.lv/DNS.

**LV CERT,** http://www.cert.lv/.

# National Report of Lithuania

## Introduction

### Interview

Date and Duration 30 July 2008 9:20 -11:30 h – 2 hours 10 min.

| Interviewee | Mr Valentinas KVIETKUS | Mr Zydrûnas PAOKAUSKAS | Mr Rytis RAINYS |
|---|---|---|---|
| Authority | Ministry of Transport and Communications – Division of Electronic Communications | Ministry of the Interior of the Republic of Lithuania Dep Security and Information Technology-Division Supervision Security | RRT, Communication regulatory authority of the Republic of Lithuania |
| Position title | Head of Division | Head of Security Supervision Division | Head of network and information security division |
| Task Responsibilities | eCommunications policies and legislation | Supervision of State information systems, policy of processing of classified information | Market regulation, network resilience issues |

## Authorities involved with Network Resilience

| Authority | Ministry of Transport and Communication | Ministry of Interior | RRT - National Communication Regulatory Authority |
|---|---|---|---|
| Main Tasks | Among others<br>…….in accordance with the procedure laid down by laws and other legal acts, give compulsory instructions, set tasks and place orders for economic entities that provide electronic communications networks and/or services, owners or users of the equipment to protect and maintain electronic communications networks, interconnect them and, if appropriate, restrict the public access to the networks in cases of *force majeure*, situations of extreme emergency or other emergencies, with a view to preparing for general mobilisation, national defence, ensure national security and public order;<br>……… set, within its competence, the priorities for the maintenance of public communications networks and public electronic communications services in cases of a catastrophic network breakdown or *force majeure*, as well as in situations of extreme emergency or other emergencies, to maintain the highest level of service provision; | Exercises public administration functions in the field of public safety, state border protection, state aid during emergencies and civil protection, control of migration processes, reform of the public administration and state governance system, development of local governance, regional development, creation of civil service system, **IT** and other fields attributed to the Ministry's competence. | Among others<br>….. Implementing general communications strategy in Lithuania;<br>…..ensuring an effective use of electronic communications resources, e.g., radio frequencies, telephone numbers, Internet addresses;<br>……Act as national electronic communications network and information security incidents investigator (CERT-LT);<br>….. protecting the rights and legitimate interests of users of electronic communications services, including consumers, and postal service users;<br>…… ensuring the assessment of conformity of equipment and devices used in Lithuania to the obligatory requirements, electromagnetic compatibility of the equipment and devices. |
| Reports to | Government | Government | Parliament |
| Year established | | | 2001 |
| URL | http://www.transp.lt/Default.aspx?DL=E&TopicID=2&UL= | http://www.vrm.lt/index.php?id=124&lang=2 | http://www.rrt.lt/index.php?1656941209 |

### Authorities involved but not part of the interview

| | |
|---|---|
| Authority | Service of Communication and information systems under the Ministry of Defence |
| Main Tasks | Cybersecurity, defence communications |
| Reports to | Ministry of Defence |
| URL | http://www.kam.lt/index.php/en/144439/ |
| Year agency or authority was established | |

All State institutions such as the Ministry of Defence underlie the Law on Electronic Communications (2004) (LEC 1). The Law on Electronic Communications and orders of Government mandate the different institutions to deal with their security issues. The influence of the Ministry of Transport and Communications is limited. The law is not very specific as far as resilience of public e-communication networks is concerned. Instead, the law describes the system in general terms.

## Scope and governance

### Question 1 : The authorities

According to the Law on Electronic Communications (LEC 1), all state institutions and private undertakings in Lithuania are responsible for their electronic (and other) communication networks. However, three authorities share the main responsibility for issues related to the resilience of e-communications networks:

- The Ministry of (Transport and) Communications
- The Ministry of Interior and
- RRT – the Communications Regulatory Authority of Lithuania

The Ministry of Communications is in charge of policy and legislation of publicly available e-communications. The Ministry of Interior is the coordinating institution for security goals and defines requirements for the state institutions. The National Communication Regulatory Authority (RRT) supervises the electronic communication services and networks.

In all legal documents, there is currently not much about resilience and requirements. The law lacks clarity in that respect; maybe resilience will be an issue for future legislation.

### Question 2 : The mandate of the authorities

The mandates of the authorities for public and private network communications are regulated by several articles of the Law on Electronic Communications (see LEC 1):

- Art 4.3 states that electronic communications on national matters such as national defence, national security etc are regulated by the relevant state institutions within the scope of their competence. This concerns all ministries.

- Art. 5.5 of the same law deals with the mandate of the Ministry of Communication regarding the policy and strategy for electronic communications in Lithuania.
- Art 6 and Art 7 concern the establishment and the organisation of the Communications Regulatory Authority (RRT). The mandate of the Communications Regulatory Authority is described in the same law in Art 30. According to the mandate, RRT issues drafts on security requirements and general provisions. Article 30, Paragraph 2.5. addresses conditions linked to the sharing of (buildings and) communication infrastructure; paragraph 2.16 16 deals with protection of public communication networks; and  Art 2.18 deals with issuing measures of technical requirements linked to security. These paragraphs are closely linked to the resilience of the public e-communication networks in Lithuania.

Relevant is also Art 62 of the law addressing the security of publicly available electronic communications networks and services.

As far as cooperation among authorities is concerned, Art 12 of the Law on Electronic Communications (LEC 1)  requires the cooperation between the authorities. It regulates also the procedures of cooperation in defence.

Possible Changes: In practice, there are more gaps in cooperation among the authorities than overlaps. This is particularly true for regulations addressing Internet Service Providers. It is an open question who should regulate the Information Society. At this point, different networks are regulated by different agencies. Moreover, supervision of private networks remains an issue while public authorities have their own mandates and are not regulated.

The Ministry for Communication's resources for this work including human resources available is limited. The National Communication Regulatory Authority has a mandate to establish requirements only for e-communication networks of private operators but not for information society services and systems. On the contrary, the Ministry for Interior, responsible for security issues, develops strategies and policy and has a mandate with regard to information systems of public sector. In this framework, requirements have been specified in 2007.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

As stated before, resilience issues are treated in legislative and regulatory documents on a general level only.

Common requirements for networks owned or used by public institutions, national regulation requirements regarding the management of information systems and also quality issues have been laid out in a Risk Assessment Manual (see RISK).

Regulations for security of information systems are in force. However, there is no direct regulation addressing the issue of resilience. The requirements concerning the resilience of network information systems are of secondary implication for private providers. The Department of Electronic Communication Networks within the Communication Ministry targets the private sector. However, as long as there are no attacks, little attention is given to the resilience issue.

The importance of Art 62 'security issues for services providers' must be mentioned here. There are many initiatives, nevertheless these are not specifically targeting issues pertaining to the resilience of public e-communication networks.

Regarding the future strategy, policy decision-makers are to take matters pertaining to resilience of public communication networks into consideration. They are, however, aware that more money is needed to implement some of the actions required to assure better dependability and reliability. A working group has been set up to focus on regulatory initiatives and collect information about initiatives dealing with the resilience of public communication networks. The Cabinet of Ministers has just mandated Ministry of Defence to lead a working group (WG) which focuses on issues regarding cyber-security, while the Ministry of Communication renewed the activities of WG with the mandate to address matters of network and information security at legislation level. The important role has WG on national cyber security strategy preparation that is managed by Ministry of Defence.

The Ministry of Interior has been kept informed about several initiatives. There are several WGs across ministries addressing information security matters. No documents are yet available on these discussions. Draft proposals will be made public as soon as possible. These proposals will address security matters regarding state institutions only.

The regulator expects new legislation from the government. It is likely that a future network and information security law will cover resilience issues. It will also address cooperation between the regulator and service providers. Particularly, how information exchange regarding incidents should be handled.

### Question 4 : Initiatives between providers and public authorities

There are many cases of initiatives related to resilience of public communication networks between providers and public authorities. They focus mainly on information exchange.

The regulator has carried out a special survey on the resilience of e-communication networks. With this survey, particular focus was put on investigating e-communication networks within and outside of Lithuania. Moreover, critical infrastructure was also addressed. The results from this survey including the report on these data are available[48].

Cooperation between authorities and private organisations is not mandatory (for private organisation) in Lithuania. Hence, achieving a response rate of 60% from Internet Service Provider(s) (ISPs) in Lithuania can be considered quite satisfactory. Moreover, considering market penetration, the most important ISPs in Lithuania cover 90% of the subscriber base. However, telecommunication operators were not part of this study.

[48] *The Ministry of Communication is not informed about this survey.*

Another example of cooperation as it is being practiced in Lithuania is the international Network Information Security Conference. It was held during 2005, 2006 and 2007. This international conference should again be organised for 2009. Network resilience will be an important topic to be addressed as part of the conference program.

The 23 November 2005 Memorandum on the Progress in the Area of Security of Information and Networks was signed by the Communications Regulatory Authority of the Republic of Lithuania, the Association of Lithuanian Banks and the Association Infobalt. The Parties have agreed to set up a permanent Memorandum Implementation Committee, represented by authorized representatives of the Parties. The Committee shall prepare annual Memorandum Implementation Action Plans and shall take care of implementation of these Plans.

The Ministry of Interior is not directly involved in these values that foster information-exchanges; but cooperation with private sector is one of the ways to implement the strategy the Ministry is pursuing in these matters of improving resilience of state information systems and data communication networks.

As far as initiatives between providers are concerned, a conference was held in June 2008. This conference on 'National Cyber security: Vision or Reality' was organised by a private company. During the conference initiated by the private sector, several round-table discussions involving private and public institutions took place. Half of the participants were from private organisations. The conference was dedicated to the exchanging of views and sharing of information. The conference is seen as a good example for encouraging greater cooperation, in particular, because the private sector invested resources into the organising of the conference.

Other private initiatives in the security domain take place, such as open days for data communication networks in 2007 and maybe in 2008. Projects dealing with network security share knowledge and best practices.

## Tasks

### Question 5 : Typical tasks

Among the activities in fulfilling typical tasks of the Lithuanian authorities are the following:

- According to law, all regulations need to undergo the process of public consultation.
- To foster greater exchange of information, the Communications Regulatory Authority (RRT) is organising special seminars on network security together with providers.
- Audits are not undertaken on a regular basis. Nevertheless, participants agreed that these and the necessary procedures to conduct those must be established. The Ministry of Interior did an audit on security issues in the public sector.
- For enforcement of regulations, there are general provisions in the Electronic Communication Law but no details. The Communications Regulatory Authority has

the mandate to stop activities of a service provider if it does not comply with provisions, also in the area of security requirements.

### Question 6 : Exchange of information between providers and public authorities

The ministries are not in direct contacts with operators and service providers the exception being the drafting of legal acts. From the regulator's view point it was stressed that the exchange between provider and authorities regarding the resilience of their networks is not mandatory. Nevertheless, it should be made mandatory.

On a quarterly basis, reports are published RRT web site (see RRT reports) dealing with the electronic communications sector. These reports are compiled from information provided by the electronic communication operators and the service providers. These reports give a good overview of the situation of the communication networks in Lithuania. The information also provides more insights into issues pertaining to topological and technical matters regarding network structures as well as security policy issues[49]. Since 2005, these results are made available on the RRT web site (RRT reports).

It was underlined that the collection of information is not the problem here. However, resilience issues, including but limited to incidents must be better investigated. This could foster a culture of continuous improvement. In fact, the regulator - RRT - is consulting with experts from the EU in a TAIEX project on these matters.

### Question 7 : Handling of security incidents

Since 2006 reports on incidents are made available to the public. A team of specialists from the national CERT-LT team investigates incidents. However, these reports concern only ERC computer response services. A regulation is in place (Art 62 para 2 of LEC 1) but there are no rules how to act.

Last year, a significant incident happened; no voice communication (not even 112) was available in a district of 250 000 people. The Ministry of Communication has not received any report so far. It learned about the incident through media reports. There is no clearly specified and institutionalized procedure reporting such incidents.

Confidential information that is submitted to the regulator by providers is not made publicly available. Examples for the kind of information this includes are such as:

- loss of material,
- loss of money,
- secret information

*[49] During the interview, the absence of a better use of the statistics was mentioned as a possible weakness. For instance, data collected through benchmarking or exercises testing handling of security incidents or how well information exchange works could be used as input for new legislation or for definition of requirements or best practice to follow.*

and so forth. On confidentiality issues, Lithuania follows the common CERT model and how it is used in Sweden, Finland, etc.

**Question 8 : Audits related to resilience**

In general, no audits have been made and no audit procedures are established for the resilience of public e-communications networks. In 2008 RRT started a survey to investigate Lithuanian Internet infrastructure resilience. The main task is to identify critical points of Lithuanian Internet infrastructure and possible risks. It is planned to finish till the end of 2008 and plan protection measures to be implemented.

In 2007, the Ministry for Interior carried out an audit about security and network operators although it has no direct competence in this area. Requirements have been developed and implemented for public institutional data communication networks. Here there are plans for establishing and following auditing-type procedures on a regular basis. Also, a security audit regarding data security for state institutions has been undertaken by an external auditor.

As far as auditing the measures taken to improve and attain acceptable levels of resilience of public e-communication networks is concerned, no national regulation defines who has to do this such as specifying the government agency that will do it or if it can be a contractor.

**Question 9 : Enforcement actions**

Procedures for supervision of compliance include enforcing of regulations under the mandate of Communications Regulatory Authority, as laid down in Art 72 paragraph 5 of the Electronic Communications Law (LEC 1). However, only a general provision is given. Since a real case has not happened yet, data does not exist about how well the provision might address what should be addressed. Also, the regulator enforcing resilience issues and concerns as far as providers are concerned is not planned.

## Risk Management and preparedness measures

**Question 10 : The national risk management process**

In Lithuania, there are groups working on risk management issues but there is no risk management process in place. In 2007, the Ministry of Interior has carried out an analysis of the risks in the information systems (based on the State's e-communication strategy) of the country's main public institutions. The results and statistical figures are published on the Ministry's homepage. A risk analysis – but not risk management – is planned again for 2009. An existing risk analysis guide needs an update.

**Question 11 : The preparedness and recovery measures**

<u>Possible Changes:</u> The interviewees pointed out that there is a lot of room for improvement for improving preparedness and recovery measures in cases of incidents.

## Question 12 : Incident response capabilities

The Ministry of Defence does operate incident management centres. However, these are not dealing with network security incidents but instead, with physical incidents regarding infrastructure. Lithuania has three Computer Emergency Response Team(s) (CERTs). These are:

1) the national CERT-LT - dealing with Internet incidences, improving management systems and procedures, information exchange between CERT and government institutions.
2) LITNET CERT: academic network for dealing with incidents in academia.
3) Infostruktura CERT for public data communication networks – is not working properly. Infostruktura is subordinated to the Ministry of Interior.

The CERT system will be re-structured in order to achieve effectiveness gains in the coming year.

The open academic CERT LITNET is quite cooperative with the National CERT-LT. They hold meetings and bilateral face-to-face contacts. More working cooperation between the three CERTs is planned for the future.

Cooperation with other countries happens via ENISA meetings, where the National CERT-LT is quite active. During 2006, a special workshop was conducted by TRANSIT. The National CERT-LT is also an active member of FIRST.

Past incidents are analysed according to the CERT model. The Ministry of Interior has developed software to compare current with previous incidents. These data points are updated on regular basis.

## Question 13 : Good practice on resilience

There is no repository of good practice on resilience in Lithuania. It was mentioned that good practice could emerge from the quarterly reports mentioned above.

## Question 14 : Guidelines for procurement

Guidelines affecting the procurement of public communication networks with clauses concerning resilience do not exist. However, the Ministry of Interior has established procurement guidelines for public communication networks and defined requirements. These guidelines are adopted by government agencies.

## References

**LEC 1** Law on Electronic Communications (Parliament of the Republic of Lithuania/Law/IX-2135/2004 04 15/came into force 2004 05 01/Official Gazzette Valstybės žinios'2004 Nr.69-2382).
Official translation, available:
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=242679.
Last Access: 28 August 2008.
Particularly relevant Articles: 4.3, 5.3, 6.7, 12, 30, 62
Amendments:
Elektroninių ryšių įstatymo 65 straipsnio pakeitimo ĮSTATYMAS (Parliament of the Republic of Lithuania/Law/X-1092/2007 04 12/came into force 2007 09 01/Official Gazzette Valstybės žinios'2007 Nr.46-1723) *(in Lithuanian)*.
Elektroninių ryšių įstatymo 3 ir 37 straipsnių pakeitimo ir papildymo ĮSTATYMAS (Parliament of the Republic of Lithuania/Law/X-1711/2008 07 15/will come into force on 01 01 2009/Official Gazzette Valstybės žinios'2008 Nr.87-3468) *(in Lithuanian).*
**RISK -Risk Assessment Manual**, Vilnius 2005, Bluebridge Contract N° 5831503-02-01-0002 [not online].

**LEC 2** Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą (Resolution on authorization according Law on Electronic Communications - Adopted by: Government of the Republic of Lithuania/ Resolution/ No.1593/ 2004 12 06/ Official Gazzette Valstybės žinios‘2004 No.177-6569; 02.05.2005 No.17 (*correction*).
Available:
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=246673&p_query=&p_tr2=
Last Access: 10 September 2008.

**REG 1** Dėl Lietuvos Respublikos Vyriausybės 1998 m. rugsėjo 15 d. nutarimo Nr. 1117 "Dėl Lietuvos Respublikos susisiekimo ministerijos nuostatų patvirtinimo" pakeitimo, Regulations of the Ministry of Transport and Communications of the Republic of Lithuania (Adopted by: Government of the Republic of Lithuania/ Resolution/ No.338/ 2008 04 09/ Official Gazzette Valstybės žinios‘2008 No.46-1727).
Available:
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=318304&p_query=&p_tr2= *(in Lithuanian)*.
Last Access: 10 September 2008.

**REG 2** Dėl Lietuvos Respublikos Vyriausybės 2001 m. kovo 14 d. nutarimo Nr. 291 "Dėl Lietuvos Respublikos vidaus reikalų ministerijos nuostatų patvirtinimo" pakeitimo, Regulations of the Ministry of Interior of the Republic of Lithuania (Adopted by: Government of the Republic of Lithuania/ Resolution/ No.333/ 2008 04 09/ Official Gazzette Valstybės žinios‘2008 No.46-1722).
Available:
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=318241&p_query=&p_tr2=
Last Access: 10 September 2008.

**REG 3** Resolution on the approval of the Regulations of the Communications

Regulatory Authority (Government of the Republic of Lithuania/Resolution/No.1029/2004 08 19/came into force 2004 08 25/Official Gazzette Valstybės žinios'2004 Nr.131-4734), (RESOLUTION No. 1029 ON THE APPROVAL OF THE REGULATIONS OF THE COMMUNICATIONS REGULATORY AUTHORITY 19 August 2004) *unofficial translation*.
Available:
http://www.rrt.lt/get_file.php?file=YVh4cGJwbG1aNEpybXBXcm5MTnRoV2EzbTVUSDFKZWtrYXRvbEppbVlKTndwWjZUWnAyY25YR2hsSm1aMUoxaWFOcHR5OGJMbVo1Z25HallhbWlWeW11aG1xQm1uR2RsYlcxc2FjYWFjV0Z1MDV6SnhNakdiWktEYWJlYVdaVzJhNHB4aUcxWG02S2RxbXlqbWRSd3AyM0VidG5EdzVhYlo1Wml5bXVua3BKdXFHeVltWjJZYjV0d2FnJTNEJTNE.
Last Access: 10 September 2008.

**ORDER 1** Dėl saugos dokumentų turinio gairių patvirtinimo (Adopted by: Ministry of Interior of the Republic of Lithuania/Order/ No.1V-172/ 2007 05 08/ Official Gazzette Valstybės žinios'2007 No.53-2070).
Available:
http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=297532&p_query=&p_tr2=
Last Access: 10 September 2008.

## Additional Resources

none

## Additional Links

**RRT reports,** http://www.rrt.lt/index.php?-1222743352.

**National CERT,** http://www.esaugumas.lt/index.php?-451375411.

**LITNET CERT,** http://cert.litnet.lt/.

# National Report of Luxemburg

## Introduction

### Interview

Date and Duration 25 August 2008 – 1 hour 45 minutes.

| Interviewee | Mr François Thill | Mr Pascal Steichen |
|---|---|---|
| Authority | Ministry of the Economy and Foreign Trade – Directorate for eCommerce and Information Security | Ministry of the Economy and Foreign Trade - Directorate for eCommerce and Information Security |
| Position title | Assistant director | Assistant Director |
| Education/Training | Engineer | Engineer |
| Task and Responsibilities | Awareness raising<br>CIP Energy<br>Certification 27001 | Awareness raising<br>CERT |
| If applicable, rel.ship to ENISA | Management Board Member | Management Board Member |

### Authorities involved with Network Resilience

| Authority | Main Tasks | Reports to | Year established | URL |
|---|---|---|---|---|
| ECO - Ministry of the Economy and Foreign Trade | Awareness raising;<br>CIP Energy;<br>Certification 27001;<br>CERT | Minister of the Economy | | www.eco.public.lu;<br>www.cases.lu;<br>www.circl.lu |
| CCG -Centre de Communication du gouvernement | Management of governmental networks;<br>Advise in communication, cryptography and security;<br>Governmental Security Body for Telecommunication and IT;<br>Running and emergency Hotline 24/24 | Prime Minister | | www.ccg.public.lu<br>(Mr. Jean-Marie Laures) |
| CIE - Central IT department | Supervision of the governmental network;<br>Implementation of preventive measures;<br>Protection of the governmental network | Ministère de la Fonction Publique | | www.cie.public.lu<br>(Mr. Patrick Houtsch) |
| HCPN - Haut Commissariat à la Protection Nationale | Risk and threat assessment;<br>Prepare for and plan reaction for crises scenarios; Coordinate reaction | Prime Minister | | www.hcpn.public.lu<br>(Mr. Roland Bombardella) |
| ILR – Institut Luxembourgeois de Régulation | National regulator;<br>Market competition | Minister of Telecommunications | | www.ilr.lu<br>(Mr. Camille Hierzig) |
| SMC –Service des Medias et de la Communication) | Policy in the area of communication | Minister of Telecommunication | | http://www.mediacom.public.lu/<br>(Mr. Paul Schuh) |

## Scope and governance

Luxembourg wishes to point out that the Government is running its own network connecting the vast majority of ministries and administrations. Emergency planning and resilience are guaranteed by governmental bodies, whereas emergency planning and response in the private sector is only partially regulated by government. Presently this regulation is indirect via the security level imposed on the professionals of the Financial Sector. Henceforth the new law on the National Protection Structure aims to introduce some direct regulative tools.

The national regulator, even if it is not actively regulating aspects of resilience, is in constant contact with the operators as they have to report quality indicators on a yearly basis. These indicators cover aspects of availability, incidents and coverage. Through these reports, ILR is capable of monitoring the operators in the area of quality, coverage and resilience. Good practice in the areas of preparedness, protection and response are available within the different governmental bodies.

The research networks, mainly controlled by the RESTENA foundation, are not discussed in this paper. In the case of an emergency, RESTENA can provide connectivity and has additional response capabilities with its own CERT. This is especially true as many research locations are in close vicinity of governmental entities or with Professionals of the Financial Sector.

### Question 1 : The authorities

The mandate of the national regulator, ILR (Institut Luxembourgeois de Régulation), is mainly focused on market competition (ILR 1). Its regulative power oversees several security aspects, but does not focus on resilience.

The CCG (Centre de Communications du Gouvernement) is a service attached to the state department (Ministère d’Etat). It is, apart from general considerations and general security aspects, responsible for the resilience of the governmental network. Together with the CIE (the central governmental IT department), it implements security policies and provides for good practice in many areas of security. Regarding security both entities are part of the governmental CERT which is formed by specialists of the CCG, the CIE, the Ministry of the Economy and the Ministry of State[50].

The National Protection Structure comprises the

- Ministerial Council for National Protection (CMPN),
- High Council for National Protection (CSPN),
- High Commission for National protection (HCPN),
- Crisis Cell (CC); and
- National Committees (CONAT).

[50] *On the level of local governments, the SIGI (http://www.sigi.lu/) plays the same role and has similar powers.*

The National Protection Structure acts under the direct authority of the Prime Minister.

The CSSF (Commission de Surveillance du Secteur Financier) i.e the banking supervision authority is indirectly acting as a regulator in the telecommunication sector. The CSSF has created the concept of PFS (Professional of the Financial Sector), and imposes strict security rules on these entities. As Luxembourg has a large number of PFS and as they all have to implement business continuity plans (CSSF 1-5), the CSSF is indirectly but very efficiently acting as a regulator in the area of resilience in telecommunication.

The CNPD (Commission National pour la Protection des données CNPD [1]), the national commission for data protection has a certain indirect regulatory power too. Due to the strict legislation in the area of data protection, minimum security requirements have been defined. The enforcement of these rules has a certain regulative impact on Luxembourg networks. Due to the young age of the commission, this impact is not of the same magnitude as the one from CSSF which is considerable.

In the time of national crisis or a catastrophe, the government has the ability to requisition, for a limited period and following the principle of proportionality, public networks. [Telco 1 art 5.] The conditions under which such a requisition is possible, the coordination with operators and the procedures that have to be followed are defined within the CONATEL, a National Committee of the National Protection Service (National Committee of the National Protection structure).

**Question 2 : The mandate of the authorities**

The mandate of the ILR in the area of telecommunication networks focuses on the following responsibilities:

- the creation of a competitive environment in the sector of the electronic communications and the free exercise of these activities in respect of the legal framework
- regulation of access to electronic communication networks and their associated resources, as well as their interconnection in order to promote the establishment of a durable competition and to guarantee the compatibility of the electronic networks
- establishment of rights of the consumers and end-users and the corresponding obligations of the companies providing the networks

The focus of the ILR is on market competition. The ILR has no mandate to act in the area of resilience, but addresses security and integrity of public networks. ILR also collects quality and security indicators on a regular basis. The mandate of the CCG comprises of:

- The management of OTAN - UEO - UE – OSCE networks,
- Advising the government in areas of telecommunication, cryptography and security,
- Acting as Governmental Security Body for Telecommunication and IT,
- Running an emergency Hot-line 24/24.

The mandate of the CIE in the area of governmental networks comprises of:

- The supervision of the governmental network,
- The implementation of preventive measures,
- The protection of the governmental network.

The mission of the National Protection Structure consists of crisis prevention as well as protecting the country and its population against the impact of a crisis.

The HCPN initiates, coordinates and monitors the execution of measures and activities related to critical infrastructure identification, designation and protection, whether they are public or private, European or national.

Critical infrastructures are divided into the following sectors: energy, health, transport, dangerous goods, communications and information, epidemics, natural disasters, water, supplies, finances, industry, public/rescue services, administration, public and symbolic sites. E-communications fall within the communication and information sector.

The legal basis of the HCPN is founded in a Grand Ducal Decree and subsequent regulations (HCPN 1 to HCPN 5). A new law giving HCPN a more powerful tool set has been submitted to parliament ("Projet de loi 5347").

The mandate of the CSSF is the supervision of the Professionals of the Financial Sector (CCSF 2). The CSSF does not regulate the e-communications sector but via its regulatory work it strongly promotes a high level of resilience in the public e-communications sector. The governmental telecommunication network is run by governmental services, namely the CCG and the CIE (Centre Informatique de l'État; the governmental IT department).

**Question 3 : Regulatory issues of resilience of public and other essential e-communications networks**

The national e-communications regulator ILR is mainly focused on market competition. However in the areas of mobile communication, every operator has to assure a minimum coverage. Every operator has to report quality indicators to the ILR. These indicators are used for measuring availability and coverage. Incidents have to be reported to the ILR. The CCG together with the CIE regulates resilience within governmental networks.

Due to the very strict regulation of banking in Luxembourg, partial regulation of telecommunication networks can be attributed, at least indirectly, to the CSSF, the banking supervisory authority. Especially the obligation for banks and associated entities to comply with security standards quoted in the laws regulating the Professionals of the Banking Sector (PFS) (see CSSF 1 to CSSF 3 in the reference list).

The new law on National Protection aims to develop and implement measures which will improve levels of preparation, protection and response to any crisis situation. Public authorities as well as private owners and operators of critical infrastructures will be expected to develop measures in order to improve their resilience particularly in relation to business continuity plans.

The government as such, advised by CONATEL, has the ability, in the case of a national crises or a catastrophe, to requisition, for a limited period and following the principle of proportionality, public networks. [Telco 1 article 5.].

**Question 4: Initiatives between providers and public authorities**

Initiatives between providers and public authorities in the area of resilience are for the moment infrequent and not regularly organized. However efforts to improve this situation are ongoing. Most notably the governmental CERT intends to organize meetings with major operators on a regular basis.

The governmental structure for promoting awareness, CASES showcases best practice in the area of IT security for citizens, SME and government. (Protection of the nodes protects the communication channels between these nodes). CASES meets with operators on regular basis. With the main operator, implementation of awareness between respective customers and employees is ongoing. Upon this base, many common projects can be launched.

ANIS – the Association of Normalization of the Information Society is a private organization although created by government. ANIS organizes the standardization in the area of IT security. ANIS has a sub- committee on 27000 family of standards. This group is looking for a country-wide consensus on how Luxembourg should adopt these standards. Luxembourg intends to use ISO/IEC 27001 and adapted standards for the certification of operators of critical infrastructures.

CLUSSIL is the security club of Luxembourg. CLUSSIL IT deals with different aspects of IT security and develops a Code of good practice, guidelines and codes of conduct.

The CSRRT (Computer Security Research and Response Team) is co-financed by the Ministry of the Economy and Foreign Trade. Among others things, it deals with malware analyses and archiving of incidents; it also organizes the "hack.lu conference".

ILR and operators meet on a regular basis. The main topic on the agenda is not network resilience, but market regulation. The CCG, has together with the main Luxembourg operator implemented crisis communication handling in the terrestrial telephone network. This has been done via a common resilience improvement project.

Possible Change: Regular meetings between CERT and operators as well as between regulator and operators should be put in place. This will necessitate additional human resources for the CERT/CASES, although a common basis already exists (see also Q. 12).

## Tasks

**Question 5 : Typical tasks**

The National Communications Committee (CONATEL) and the National Committee for Critical Infrastructure Protection (CONATIC) develop policy and technical advice in matters of ICT in general and e-communications in particular. CONATIC and CONATEL meet regularly.

The CCG promotes good practice in the area of communication security. The protection of the governmental network is realized by CCG working closely together with the CIE (central governmental IT department).

Several governmental bodies such as the banking authority CSSF are publishing minimum security requirements (for the Professionals of the Financial Sector). These requirements often deal with availability, integrity and confidentiality of communication services as well as with PFS which promotes the resilience of public communication networks.

CASES works in the area of increasing awareness and promotes the adoption of security reflexes. CASES works with citizens, SME and governmental entities, but banks and operators increasingly use the CASES tools or CASES skills internally. The governmental CERT works in the area of incident response for the governmental network.

Cooperation among authorities in Luxembourg regarding information security takes place on several levels. The Directorate for e-Commerce and Information Security of the Ministry of the Economy support the National Protection Structure and especially the HCPN as an adviser in the area of risk assessment, best practice and coordination. The governmental CERT is run by members of the Directorate for e-Commerce and Information Security of the Ministry of the Economy, by members of the CCG, the CIE and members of the State department. The governmental CERT (on an operative level) as well as the National Protection Structure (on a strategic and tactical level) are the main cooperation hubs of the Luxembourg government in the area of security. Both enable close cooperation and a high level of information sharing.

### Question 6 : Exchange of information between providers and public authorities

Operators have to provide quality indicators to the national regulator ILR. These statistical reports cover availability aspects, coverage and incident reports. Most reports have to be delivered on a yearly basis.

The new law for the National Protection Structure will introduce a mandatory mechanism for the exchange of information between providers and public authorities. This exchange comprises all information necessary for crisis prevention and management.

Presently operators exchange incident information on a sporadic basis with governmental services. This exchange is not yet mandatory, but is performed in the case of serious incidents, such as network overload due to SMS flooding on peak times as it happened once on Sylvester.

The governmental CERT, as well as the CCG forward information on specific vulnerabilities or threats to the national operators. This is not done on a regular, but on a spontaneous basis. The governmental CERT, the CIE and CASES publish best practice in various areas, which can be adopted by the private sector. The private sector presently cannot be forced to adopt measures. There is no regulator checking the implementation. Only the financial sector (together with sub-contractors) has to apply to security standards defined by the banking supervision authority CSSF.

Once a year, the CSRRT-LU together with the Ministry of the Economy organizes an IT security conference. This conference focuses on different aspects of IT security and brings together experts from government and from the private sector.

### Question 7 : Handling of security incidents

The new law for the National Protection Structure will introduce a mandatory mechanism for the exchange of information between providers and public authorities. This exchange encompasses all information necessary for crisis prevention and management.

Within governmental networks, incidents are handled by either the CCG, the CIE or the governmental CERT. The government CERT currently liaises with each of the government departments on the basis of one or two contact persons for reporting incidents (trusted partner within the administration). The incidents are reported via telephone, e-mail or fax according to a form which is designed for incident reporting. Incidents can however also be reported by system sensors that are constantly watching the network. Strange behavior in the network triggers alarms and necessary steps are taken to react efficiently and in a timely manner. Operators report on a voluntary basis incidents to the governmental authorities. Serious incidents have to be reported to the national regulator, such as it happened once the overload of SMS networks on Sylvester's eave.

### Question 8 : Audits related to resilience

The National Protection Structure foresees no formal audits. Compliance is monitored through mechanisms used in the development and implementation of measures and business continuity plans, coupled with physical inspections.

As regards audits of the governmental networks, both, the network of the central government and the network for the cities/villages, are closely monitored. If a governmental entity does not comply with the IT security measures or technical obligations it's sub-network can be disconnected from the governmental backbone. Each administration is connected to the governmental backbone through a firewall controlled by the operators of the governmental backbone (CIE). A strict policy of partitioning the governmental network has been implemented. Crisis can be kept local by this strict policy.

The banking authority CSSF is closely auditing the Professionals of the Financial Sector. Due to the business continuity plan obligations, operators are indirectly controlled. The Professionals of the Finance Sector are audited on a yearly basis.

### Question 9 : Enforcement actions

The coming law on National Protection enforces the implementation of protective and corrective measures in the realm of national critical infrastructure in general, and the ICT sub-sector in particular.

The government as such, advised by CONATEL, has the ability, in the case of a national crisis or catastrophe, to requisition, for a limited period and following the principle of proportionality, public networks. [Telco 1 article 5.]. It can take, always under the guise of proportionality, any kind of action to either nullify a crisis or reduce its impact.

In case networks of the central government do not comply, they will be disconnected from the governmental backbone. The IT department running the governmental backbone is the only service providing network access to the public administrations. Each public administration is separated from the backbone by a firewall driven by the central IT department. If an administration should not comply with the security guidelines or if it should present a threat to other governmental bodies, the respective firewall can be closed.

Professionals of the Finance Sector must have redundant connectivity through different operators (see CSSF 1- to CSSF 5). These entities are obliged to find providers with physically independent networks. This strict regulation promotes an increased redundancy and resilience in Luxembourg networks. Nowadays network providers in Luxembourg often have their own physical infrastructure. This infrastructure is interlinked, but is mostly independent. Enforcement of regulations is addressed by the law with the imposition of fines a possibility for non compliance.

The regulator ILR however does not have the capability to impose fines in the area of resilience. However it is able to impose a minimum coverage to all mobile operators.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

A national risk management process is under development by HCPN in cooperation with all participating agencies such as CCG, the Luxembourg CERT and CASES. A common and harmonised risk assessment approach is foreseen i.e. Risk = Threat * Vulnerability * Impact. Emphasis is placed on common understanding of the taxonomy of threats and the methods to evaluate impacts. On this basis, a common vocabulary is adopted, so that cooperation and especially coordination and rapid threat analysis is possible. Operators of critical infrastructures will be integrated in this process of risk assessment and risk mitigation.

In the future, the Luxembourg CERT (CIRCL) will invite national telecommunication operators on regular basis to facilitate exchange of good practice knowledge and share incident response strategies. CASES promotes the usage of a common risk assessment process by promoting best practice in this area.

Due to the fact, that Professionals of the Financial Sector have to comply with the strict security rules elaborated by CSSF, they have to run risk assessments and also implement appropriate improvements to the infrastructures they use. Without these assessments, they would not be able to implement the obligatory business continuity planning.

## Question 11 : The preparedness and recovery measures

In the private as well as in the governmental communication networks, high priority is given to redundancy of communication networks. The former national operator has highly redundant networks, and due to the creation of a highly competitive environment, redundancy should still be increased. Government has undertaken several measures in order to further improve the level of redundancy.

The strict supervision CSSF imposes upon the PFS (professionals of the Financial Sector) promotes this redundancy. All PFS must have business continuity plans in place. The Luxembourg government has implemented a high availability communication network and runs an alerting network that is capable of using different technologies to reach key personnel. In order to still improve the situation, Luxembourg also participates in a European R&D project to improve the current situation[51].

Many actions have been undertaken to harmonize risk assessment and improve coordination and response strategies. This approach will improve communicative and reactive competences of the Luxembourg government and operators of critical infrastructures.

## Question 12 : Incident response capabilities

The HCPN, the associated national Committees and the CCG have capabilities for crisis management. In order to increase the level of preparedness and the capabilities of response, a governmental CERT has been created: CIRCL (Computer Incident Response Centre Luxembourg). It is planned to be the operative arm of the HCPN as HCPN has the mandate to coordinate CIRCL activities together with other governmental response activities.

The government as such, advised by CONATEL, has the possibility, in the case of a national crisis or a catastrophe, to requisition, for a limited period and following the principle of proportionality, public networks. [Telco 1 article 5.].

Incidents are collected and analysed, the outcomes of crises management of CIRCL are also fed into the CASES (awareness raising node in Luxembourg). CIRCL's approach is based upon the common recommendations existing for CERTs.

## Question 13 : Good practice on resilience

Within the national CERT of Luxembourg – CIRCL – and within CCG and HCPN a repository of good practice on resilience is available. The repository is being updated regularly.

[51] *u-2010: Ubiquitous IP-centric Government & Enterprise NGN Vision 2010 (funded by the European Commission) : http://www.u-2010.net/*

The CSSF also publishes minimum requirements in the area of security. While these may not be considered as good practice, nevertheless, they are important as they impose a minimum standard.

**Question 14 : Guidelines for procurement**

The CCG and CIE impose security measures in governmental networks. Most procurement for IT material for these governmental networks are done either by CIE or by CCG. This procedure guarantees that the security level imposed by CIE and CCG is respected. However there is no special procedure for procurements.

In the private sector, there is no special procedure for procurements, however because of the CSSF-law, a certain level of security is imposed.

## References

**TelCo 1** Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques ; Mémorial A n° 73 de 2005 Paquet télécom. Publié le 07.06.2005.
Available: http://www.legilux.public.lu/leg/a/archives/2005/0073/index.html.
Last access: September 27, 2008.

**ILR 2** Règlement 08/132/ILR du 18 juillet 2008 concernant le marché pertinent de la fourniture en gros d'accès dégroupé (y compris l'accès partagé) aux boucles et sous-boucles locales (marché 11), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre.
Available:
http://www.ilr.public.lu/telecommunications/decisions/2008/08132.pdf.
Last access September 27, 2008.

**ILR 3** Règlement 08/133/ILR du 18 juillet 2008 portant sur la définition des marchés pertinents de la fourniture en gros d'accès à large bande (marché 12), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre.
Available:
http://www.ilr.public.lu/telecommunications/decisions/2008/08133.pdf.
Last access September 27, 2008.

**ILR 4** Loi du 21 mars 1997 sur les télécommunications (telecommunication law).
Available:
http://www.ilr.public.lu/telecommunications/legislation/vd_loi_du_21_mars.pdf.
Last access September 27, 2008.

**HCPN 1** Arrêté grand-ducal du 31 décembre 1959 concernant l´organisation générale de la protection nationale ; Au Mémorial A n° 1 du 09.01.1960.
Available
http://www.legilux.public.lu/leg/a/archives/1960/0001/1960A00041.html.
Last access: September 27, 2008.

**HCPN 2** Règlement grand-ducal du 25 octobre 1963 concernant l'organisation générale de la protection nationale; Au Mémorial A n° 62 du 14.11.1963.
Available:
http://www.legilux.public.lu/leg/a/archives/1963/0062/1963A09771.html.
Last access: September 27, 2008.

**HCPN 3** Règlement ministériel du 20 novembre 1964 concernant la création d'un Comité Mixte civil-militaire des Transports ; Au Mémorial A n° 90 du 21.12.1964.
Available:
http://www.legilux.public.lu/leg/a/archives/1964/0090/1964A16211.html.
Last access: September 27, 2008.

**HCPN 4** Règlement ministériel du 20 octobre 1969 concernant la création d'un comité mixte de protection sanitaire. Au Mémorial A n° 55 du 28.10.1969.
Available:
http://www.legilux.public.lu/leg/a/archives/1969/0055/1969A12621.html.
Last access: September 27, 2008.

**HCPN 5** Règlement ministériel du 2 mars 1970 concernant la création d'un comité mixte de protection du territoire. Au Mémorial A n° 13 du 12.03.1970.
Available:

http://www.legilux.public.lu/leg/a/archives/1970/0013/1970A03371.html.
Last access: September 27, 2008.

**CSSF 1** Law of 23 December 1998 as amended establishing a supervisory commission of the financial sector (a "commission de surveillance du secteur financier").
Available:
http://www.cssf.lu/uploads/media/lawcssf_231298_update110108.pdf.
Last access September 27, 2008.

**CSSF 2** Law of 13 July 2007 (only Title I) on markets in financial instruments.
Available: http://www.cssf.lu/uploads/media/MIFID_Law130707_01.pdf.
Last access September 27, 2008.

**CSSF 3** Grand-ducal regulation of 13 July 2007 (only in French) relating to organisational requirements and rules of conduct in the financial sector.
Available:
http://www.cssf.lu/uploads/media/rgd_exigences_regles_conduite_130707_01.pdf.
Last access September 27, 2008.

**CSSF 4** Circulaire 96-126 Administrative and accounting (includes aspects of security).
Available:
http://www.cssf.lu/uploads/media/iml96_126_modifiee041005_01.pdf.
Last access September 27, 2008.

### Additional resources

**CSSF 5** Guidance can be found in "specific reports ".
Available: http://www.cssf.lu/index.php?id=32&L=1.
Last access September 27, 2008.

**CNPD 1** Legislation in the area of Data protection.
Available: http://www.cnpd.lu/en/legislation/index.html.
Last access September 27, 2008.

### Additonal links

**CASES,** http://www.cases.public.lu/fr/index.html.

**CLUSSIL,** http://www.clussil.lu/tiki-page.php?pageName=Clussil.

**CSSRT Malware Database,** http://www.csrrt.org/maldb/index.pl.

**Hack.lu Conference,** http://www.hack.lu/index.php/hl/index.

**CIRCL – National CERT of Luxembourg,** http://www.circl.lu/.

# National Report of the Netherlands

## Introduction

### Interview

Date and Duration 2008-08-19 – 110 minutes.

| Interviewee | Mr Simon van Merkom | Mr Edgar R. de Lange | Mr Roman Vols |
|---|---|---|---|
| Authority | Ministry of Economic Affairs Directorate-General for Energy and Telecom -- Telecom Market Directorate | Ministry of Economic Affairs Directorate-General for Energy and Telecom Telecom market Directorate | Ministry of Economic Affairs Directorate-General for Energy and Telecom Telecom market Directorate |
| Position title | | | |
| Education/Training/Degree | Policy | Policy | Law |
| Task and Responsibilities | | | |
| If applicable, relationship to ENISA | NLO for NL | | |

**Authorities involved with Network Resilience**

| Authority | Ministry of Economic Affairs (MINEZ) Directorate-General for Energy and Telecom Telecom market Directorate | Ministry of the Interior and Kingdom Relations (BZK) | OPTA - Onafhankelijke Post en Telecommunicatie Autoriteit) | RA – Radiocommunications Agency |
|---|---|---|---|---|
| Main Tasks | | | OPTA independently regulates compliance with legislation and regulations in the areas of post and electronic communications. | The three main tasks of Radiocommunications Agency Netherlands are to obtain, allocate and protect frequency space. |
| Reports to | | | OPTA is a governmental body and non-departmental agency of the Ministry of Economic Affairs that operates as an Autonomous Administrative Authority. | RA is a specialised agency of the Ministry of Economic Affairs |

| | | | | |
|---|---|---|---|---|
| URL for agency or authority | http://www.ez.nl/ | http://www.bzk.nl/ | http://www.opta.nl/ | http://www.agentschap-telecom.nl |
| Year agency or authority was established | | | 1 August 1997 | |

## Scope and governance

### Question 1 : The authorities

Assuming network resilience is interpreted as resilience of infrastructure incl. services, incl. information security and incl. activities for user protection, there is no centralized agency responsible for issues regarding network resilience. No formal dependency or authority is responsible for the full subject. Instead, several authorities or agencies are involved in regulating and improving network and information security to achieve better resilience as interpreted above. There is no official organizational chart available illustrating how these agencies interact and the possible hierarchy.

The various ministries involved have different agencies reporting about their work. For instance, the Ministry of the Interior and Kingdom Relations (BZK) is responsible for public order and safety but resilience is not part of public order and safety in the Netherlands. The Ministry of Economic Affairs (EZ) supervises the Directorate-General for Energy and Telecommunications, the OPTA (independent regulator) and the Radiocommunications Agency (RA).

The interview partners pointed out that in the Dutch system, it is preferable to use a happy medium between a centralized and decentralized approach. To achieve this, close collaboration and participation of various stakeholders is highly encouraged.

### Question 2 : The mandate of the authorities

Different agencies operate under the ministries involved in network resilience issues. The Directorate of Crisis Management, the National Co-ordination Center (NCC), and the government computer emergency response team GOVCERT.NL, all report to the BZK. Hence, these activities support the ministry's efforts regarding public order and safety except GovCert, their activities support network and information security.

The Directorate-General for Energy and Telecommunications must undertake the necessary regulatory steps to ensure the continuation of supply of critical energy and telecommunication services to citizens and companies. This directorate reports to the EZ. The EZ is responsible for national CIP/CIIP policy for the private energy and telecommunication sectors which includes several approaches to raise awareness and cooperation with as well as the private industry, including SMEs. The telecom regulator OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) is an autonomous administrative authority and non-departmental agency of the EZ.

OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) describes its mission on its webpage as follows:

> *OPTA independently regulates compliance with legislation and regulations in the areas of post and electronic communications. The legislation and regulations are intended to promote competition on these markets, resulting in more choice and fair prices for consumers.*
>
> *OPTA is a governmental body and non-departmental agency of the Ministry of Economic Affairs that operates as an Autonomous Administrative Authority.*

OPTA operates within the EU Telecommunications Regulatory Framework (a.o. Universal Service Obligation) and has to take action when something happens regarding reliability and dependability of telecommunication as far as this falls within the scope of the Framework. Accordingly, The Netherlands have divided the full range of subjects within the scope of resilience and of network & information security between EZ, OPTA, RA and BZK.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

Addressing the question four factors need pointing out. These are outlined below. The regulatory issues are addressed thereafter.

First, the country's communication networks were started in a regulatory environment with a monopoly provider KPN[52]. As well, the national telecom provider – PTT (Post, Telegraph and Telecom) was government owned at the time. This resulted in a gold plated network. More important for today's situation is, however, that this has resulted in the market demanding a high level of dependability and reliability from communication network services. All else considered equal, this demand provides an incentive for providers to act accordingly and deliver resilient networks at competitive prices.

Second, deregulation, including the unbundling of the last mile in The Netherlands has resulted in a quite concentrated market where about a limited number of national scale operators dominate the market. In part, this is due to market pressure whereby a certain size is required to achieve the economies of scale required to be able to compete. KPN is the incumbent and largest telecommunications company in the Netherlands with a ubiquitous national network. Ziggo is the largest cable operator in the Netherlands with 3.2 million connections, serving 7.8 million people. The company is a three-way merger of the cable operators Casema, @Home en Multikabel.

[52] *KPN is obliged to offer universal service without compensation for at least 12 months after it informs the Minister that it intends to end its USO provision. If, upon KPNs withdrawal, market forces prove unable to provide universal service, the Minister organises a tender, whereby the provision of universal service will be awarded to the operator which has tendered the lowest price. KPN has an obligation to participate in this tender. The cost of providing universal services will be shared by all telecommunications companies. For details see the EU regulatory Framework , implemented in NL Telecommunications Act (Minez 1)*

Nevertheless, the major telecom providers as well as one major cable provider own or control about 90% of the infrastructure[53].

Third, The Netherlands are pursuing to two-thronged approach. It has the regulator OPTA that checks if for those regulations for which authority is mandated to OPTA are met and takes legal steps if necessary against those that have violated regulations (e.g., against spammers during 2008). A more gentle and collaborative approach is exemplified with the NC0-T, the National Continuity Forum Telecommunications (see Minez 3 in reference list – more details also under Question 4). While membership is required for main operators, participation is voluntary. Important is that if this group agrees and comes up with a solution on how to deal most effectively with something such as risk management, then it becomes binding for this group of operators. In turn, it affects over 90% of The Netherlands's telecommunication infrastructure.

Fourth, in the Telecommunications Act the issue of resilience is only referenced is relation to preparing for a possible State of Emergency (Minez 1 in reference list). Based on this part of the Act NL has taken the approach to develop policy initiatives through focussing on getting the main players to collaborate and exchange information on a voluntary basis. A working group called NCO-T exists. NCO-T formulates practical approaches that become part of guidelines. NCO-T can approve or agree to follow such jointly developed tools and recommendations. Thereafter, recommendations or guidelines become the standard that is followed by the providers of critical public telecommunications infrastructure and/or services (Minez 3).

Besides the above four factors that are important to consider when addressing regulatory and other issues pertaining to public network resilience in the Netherlands, the law stipulates that larger network failures or breakdowns require reporting. However,

- the Netherlands have no strict definition of crisis; therefore, it depends on the specific case and requires the operator to a certain extent to make a decision if an incident can be classified as a crisis;
- when there is a disturbance above a certain level, then there has to be a report to the crisis management centre of EZ that is on 24/7 call; depending on the incident, the report might move rapidly up to the chain of command initiating national agreed escalation procedures; in severe cases all the way to ministerial level.

Nevertheless, to make the above more structured and easier to execute, the Telecom Market Directorate together with the operators has developed through NCO-T and based on the operators' internal guidelines about escalation procedures a guideline to identify under which conditions each operator must inform the Telecom Market Directorate.

[53] *Regardless of ownership of infrastructure and type of technology used, whenever voice and/or data communication is involved and services are sold on the open market, the network is considered to be public. In turn, the operator or owner is subject to telecom regulation.*

As well, the Netherlands follows the principle-based approach[54] for regulation whereby guidelines agreed by NCO-T members must be followed but they are not as detailed and specific as some rule-based standards might be in other countries. However, what is critical here is that benchmarking NCO-T members is a regular exercise happening every two to three years. The foundation for this work is the guidelines and recommendations NCO-T members agreed to follow. According to data submitted by operators to the Directorate on Telecom (e.g., contingency planning and risk management), their resilience and security efforts are being assessed by a third party (see also Q5).

The findings from such a benchmarking exercise are then shared anonymously with the NCO-T group. This may trigger new guidelines or changes.

Possible Changes: Reporting obligations for incidents are such that more extensive observation is needed. For instance, how well the reporting works according to time, type of reporting, channels used, and subsequent assessment for reducing the likelihood of the same incident happening again requires some analysis of past reports.

The European Commission is trying to introduce a specific chapter that outlines measures regarding security, dependability and reliability of networks in order to improve resilience. This will require that The Netherlands change its Telecommunication Act (Minez 1 in reference list). We believe this will happen soon.

Regarding privacy regulation considering who is responsible for abuses and acting against violators including spyware requires a better way to address this issue. There might be legal, procedural and enforcement that can be better fine-tuned to improve the situation as compared to today.

Better resilience levels would also necessitate that the quality of services provided under the universal service obligations[55] are being assessed. However it was underlined by the interviewees that quality of services is a phenomenon, which is difficult to use and they do

*[54] Principle-based standards or guidelines outline the objectives but leave it to the operator to decide how to fulfil or reach these. However, the operator must be able to demonstrate that best practice was being followed or else be able to justify not doing so, while achieving the objectives set regarding network resilience.*

*[55] Services of general economic interest (SGEI) are a legal category in the EC Treaty that is designed to enable proportionate restrictions on the Treaty's market freedoms (including competition) in so far as necessary to attain legitimate public policy objectives defined (in the first instance) at national level. In principle this concerns those cases where market failures cannot be effectively remedied with market-based solutions.*

*Universal service obligations (USO) that guarantee universal access are one of the most important examples of the way SGEI are operationalised. USO is referring to a set of general interest requirements to be satisfied by telecommunications and postal service operators throughout the Community. The object of the resulting obligations is to make sure that everyone has access to certain high quality essential services at prices they can afford.*

*To attain this service level, an operator can be given special provisions and funding. In turn, it has to meet very strict quality and security levels and enforcement of regulation is clearly defined and applied. For instance, availability of connection, number of fault reports per connection establishing satisfactory performance and repair time in case of incident is specified. Failure results in funding being cut accordingly.*

*The Community framework for financing the costs of universal service envisages payments being made (i) into an independent universal service fund at a national level which would make payments to operators providing universal service or (ii) directly to operators providing universal service as an additional payment to the commercial charges for interconnecting with their network.*

not use it in their resilience policy/approach in the same way as in the EU Telecom Framework. The resilience policy dossier of the interviewees does not do anything with universal service. Other dossiers do work with universal service, like tariffs, 112, privacy, spectrum, etc; these dossiers are addressed by other sections in EZ and in OPTA.

Possible Changes: One of the issues the Netherlands will have to address is greater dispersion of providers of smaller size. An example of today's developments is that some municipalities are considering providing telecom services to people living in that city. These municipal networks could be considered public and could become part of the regulatory framework. But it should be considered if and/or how these *public* organisations' initiatives relate to a free *private* market.

**Question 4 : Initiatives between providers and public authorities**

Four initiatives were mentioned which are summarized as follows.

A) NC0-T, the National Continuity Forum Telecommunications[56].

> *Via the NCO-T, providers are given the opportunity to be involved in the specification of specific obligations. However, the Minister of Economic Affairs is and shall continue to have ultimate responsibility in this respect (Minez 3 in reference list).*

For infrastructure operators, membership is mandatory. However, participation in meetings and activities is voluntary. Nevertheless, because its decisions are binding it is in the best interest of operators to be active participants.

The NCO-T can periodically review designation criteria:

- Critical services (user groups, impact when disrupted, “market share”)
- Providers of critical services (market share, in control of own infrastructure)

NCO-T is conducting the benchmarking exercises as mentioned in the answer to Q3 already. At the time this document is written the eight national critical operators are part of a benchmarking exercise. This will help to get a better idea about how to deal with crisis as well as continuity management. NCO-T will discuss findings and decide what actions operators must take. All this being done to help improve dependability and reliability of public communication networks (see also Q3 and Q5).

B) The Directorate of Crisis Management under the Ministry of the Interior and Kingdom Relations (BZK), when carrying out activities in the scope of CIP or Crisis management preparation will request the operators which are members of the NCO-T to cooperate on issues pertaining to national crisis management.

[56] *NCO-T has replaced the public-private partnership between telecom operators and the government that operated under the Nacotel framework. Under Nacotel, agreements were made on minimum requirements for the form and manner in which preparations for the provision of the electronic transmission of data in exceptional circumstances should be undertaken*

C) The Ministry of the Interior and Kingdom Relations (BZK) has an initiative that includes the national police, National Intelligence, GOVCERT, (i.e. the Dutch National Government CERT – see reference list for links) together with OPTA (the telecom regulator). The members of this initiative are working on a procedure that will enable a more systematic and effective response to phishing attacks. By September 2008, this group is finalising these procedures.

D) Financial industry has an Information Exchange Point with a closed forum to discuss resilience, dependability and cybercrime issues. Companies such as banks must apply in order to join. Work is in progress to establish an information exchange point for the telecom sector. This Information Exchange Point for the Telecom Industry should be in operation by spring 2009 [57].

Possible changes: As pointed out under Q3, for those regulations for which authority is mandated to OPTA, OPTA has to take action when something happens that affects reliability and dependability of telecommunication, but not security in communication. The RA addresses frequency issues, and supervision of telecom interception. Eventually, The Netherlands must address who will administer and regulate the areas that are open at this stage and if a resilience article will become part of the Telecom Act (Minez 1).

Today, communication law does not have an article specifically addressing network resilience and information security. In turn, The Netherlands does not have ordinances or regulation that focuses on network dependability and reliability. Nor is there an ordinance regarding resilience and information security. Nevertheless, even though there is little regulation, voluntary cooperation has so far been enough to improve the situation in The Netherlands rapidly and to far higher levels than around 2003.

While legislation that we expect to come will be helpful, it is necessary to keep operators involved and find practical ways to improve the situation without making it a bureaucratic nightmare. All stakeholders in The Netherlands are, however, aware of this challenge and working closely together to get there.

Telecom operators are the experts on these issues and, based on our liberalized telecommunication market, competition and customer demand puts pressure on operators to deliver dependability and reliability, or else loose market share.

In turn, this market pressure encourages operators to work with regulator and ministry as well as agencies to find workable regulation. In turn, mutually-agreed approaches can be put in practice. This achieves better resilience and, therefore improves dependability and reliability of public e-communication networks in The Netherlands to the desired levels.

[57] *More about this also under Q6 - National Infrastructure Cyber Crime (NICC)*

## Tasks

### Question 5 : Typical tasks

There are regular public consultations with providers and through means as working groups (e.g., NCO-T). Enforcement is still placed with the Ministry of Economic Affairs (EZ), – as part of the Directorate-General for Energy and Telecom the Telecom Market Directorate administer NCO-T agreements made by industry.

Light enforcement: NL follows a philosophy of light enforcement. Hence, operators are legally obliged to let the ministry know once a year about continuity and crisis management (see MINEZ 1 – Chapter 14.4 and 14.6).

NCO-T developed a procedure on how operators and infrastructure owners can prepare and conduct their work regarding continuity and crisis management and how to report this. As discussed in Q3 and Q4, every two to three years these efforts are benchmarked.

An independent 3rd party will conduct the work and assessment required to benchmark. It is based on the operator's report about continuity and crisis management as submitted to Ministry of Economic Affairs - Directorate-General for Energy and Telecom -- Telecom Market Directorate. This report is then handed to the third party that takes the report and then conducts what some would call a light audit, which resembles to benchmarking, on the operator's premises. Information from the benchmarking exercise is shared anonymously with other NCO-T members.

Possible Change: Until now, the benchmarking exercise has not resulted in findings that would indicate that an operator falls below acceptable levels of performance regarding reliability and dependability.

This scenario has not occurred yet. In turn, there exists no experience how to best proceed in cases were an operator fails to meet the benchmarks as developed and mandated by the NCO-T group.

However, the Telecom Market Directorate can point out to an operator that if it fails to meet the benchmarks, this could result in additional regulation (e.g., article in the law and/or regulation). Once this happens, the regulator could then enforce the article and in case of failure penalize the operator. The NL policy in this is that collaboration, mostly done in public-private partnership like activities, helps avoid this scenario.

Experience in The Netherlands has shown that business and government interests regarding reliability and dependability of public e-communication networks overlap. The biggest positive force for change by operators is to provide clients with dependable and reliable service in order to stay competitive.

For policy and national supply reasons, the government shares this interest in achieving greater dependability and reliability of public e-communication networks.

## Question 6 : Exchange of information between providers and public authorities

The National Infrastructure Cyber Crime (NICC) brings public and private parties together for information exchange on incidents and developments in cyber crime and how to prevent or respond in different economic sectors. Data about best practices and experience in fighting cyber crime between these parties is encouraged. Since 2006 a number of information exchange points have been in operation, such as the one for the financial sector and the sector on provision of drinking water.

An information exchange point on cyber crime for the telecom sector is being established by NICC. This Information Exchange Point for the Telecom Industry will be operational by spring, 2009 (see Q4 d).

The Netherlands generally begin work regarding resilience and cyber security in the area of crisis management. Once a mechanism for information exchange is in place, practicable solutions and recommendations will result. Once agreement has been reached between stakeholders in the area of crisis management, this footprint is then used to work through to issues pertaining to normal operations.

The telecom operators do not have a crisis response team or something similar to a CERT due to financial consideration. However, The Netherlands are trying to form a crisis coordination unit in the near future. The general viewpoint presented by operators is that in case of crisis, extensive cooperation amongst them will happen anyway.

Regarding resilience, crisis management, CIP, etc. sharing of information and experience is also taking place at NCO-T level, since this forum operates a non-disclosure agreement.

## Question 7 : Handling of security incidents

Security incidents in the Netherlands are handled as described in the following.

It is possible that the NCO-T group agrees to share information which always confidential. Bilateral talks between operators happen. Nevertheless, EZ is not necessarily privy to such talks. Reporting is made about security incidents that happen as well as about the expected repairs that are necessary. EZ receives a copy of the confidential report as prepared by the operator’s reporting centre.

While such reports are voluntary, in practice it has become part of the best practice approach in NL. In turn, operators see the advantage of doing so. Sometimes, EZ hears about an incident in the media. In turn, a call to the operator could reveal that the incident is far less severe than it might have appeared considering the media coverage given to the incident.

## Question 8 : Audits related to resilience

The Netherlands does not use audits related to resilience of networks. Nevertheless, as discussed in Q5 under Light enforcement, the benchmarking exercises as conducted by a third party according to an agreement amongst NCO-T group members are kind of an audit. However, its primary objective is to help operators to improve in their work including disaster recovery, continuity and crisis management not to enforce regulation.

**Question 9 : Enforcement actions**

Enforcement actions have been outlined above regarding OPTA. OPTA checks if regulations are met and takes legal steps if necessary against those that have violated regulations. Also, the mechanisms for the light audit that NCO-T group members have agreed to follow make the need for enforcement actions quite unlikely (see also Q3 and Q7).

Possible Changes: In the future, NL will have to assess how telecom regulation may have to be re-aligned between regulators (e.g., OPTA) and the ministry (e.g., handles resilience at this point).

## Risk Management and preparedness measures

**Question 10 : The national risk management process**

A project for a national risk management process began during 2002. It addresses all critical infrastructures including such as drinking water, food supply, telecommunication networks, transport and so forth. Whenever this group addresses telecom issues, EZ asks NCO-T members to join and help with these issues.

A first report that included recommendations was submitted to the Dutch Parliament in 2005 (see Minez 5 for more details on this). At the moment, a next cycle of risk management analyses on critical services, dependencies, threats, etc is being prepared to start in Q4 of 2008. Meanwhile a the Project on National Security is analysing: possible risks at national level, existing protection measures, large multi-sectoral threats, etc.

**Question 11 : The preparedness and recovery measures**

The Netherlands do not have priority communication system installed within its network grid. There is a separate dedicated national emergency network only for use by government and critical users, police, fire department.

This is currently under review and the situation will likely change. The basis of the new situation will be the same as the current:  to assure that the dedicated network or service will function properly even when all others may go off line.

Room for Change: There are quite a few recommendations pertaining to preparedness and recovery measures. Nonetheless, nothing very specific regarding preparedness and recovery is currently available.

Operators want to have certification ISO 27000 series (i.e. follow a rule-based standard[58]). Unfortunately, how realistic these measures are and work in practice is unclear. A rule-based approach and, particularly prescriptive rules make it easier to comply according to the law. However, The Netherlands follows the approach whereby operators understand their business and know how to implement guidelines into their operations and networks when it comes to details and how it is best done.

### Question 12 : Incident response capabilities

The NCO-T is trying to establish a structure to help incident response capabilities. There is a general crisis management structure in place with Ministry of the Interior and Kingdom Relations (BZK). The National Coordination Center - 24/7 coordinates between all ministerial crisis management centres. In a national emergency, that group takes the lead. If it is a local crisis, however, the municipality is in charge.

Developing of a bi-lateral agreement between operators and municipalities in NL is under development.

The GOVCERT, the Dutch National Government CERT has incident response capability with a national alert service. However, this service does not cover the area of dependability and reliability of public e-communication networks.

Possible Changes: A more formalized structure for incident response capabilities between operators and municipalities will be developed.

### Question 13 : Good practice on resilience

Good practice is shared in the NCO-T. There is an incentive to share good practice in a forum such as the NCO-T group. However, there are no monetary incentives to do so.

There are some efforts undertaken to build up a repository on good practices. Nevertheless, operators have numerous forums available to discuss these issues over coffee with each other and they do.

### Question 14 : Guidelines for procurement

Guidelines for procurement are not available as of now. However, the Ministry of Interior has some guidelines about government networks. Nevertheless, such procurement rules do not address resilience of e-communication networks specifically.

[58] *Rule-based standard may be prefered by operators since they reduce the risk for litigation, as long as one can show that one has followed the specified rule by the letter. For instance, in the litigious US legal system prescriptive rules make it easier for one to demonstrate that one has followed the rules and, therefore, the law.*

## References

**Minez 1** Telecommunicatiewet , 19 oktober 1998, (Telecommunications Act , 19 October 1998).
Available NL version online :
http://wetten.overheid.nl/cgi-bin/deeplink/law1/title=Telecommunicatiewet.
English non-binding version not online.
Particularly relevant are articles:
- 14.4, 14.6 (to prepare for a state of emergency),
- 18.9 (last resort, to allow the Minister to act urgent in case of state security or of criminal threat against a person/citizen).

**Minez 2** Regeling voorbereiding buitengewone omstandigheden sector telecommunicatie 2007, 20 december 2007, (Ministerial Regulation on Preparation to Exceptional Circumstances Sector Telecommunications 2007 , 20 December 2007 ).
Available: http://wetten.overheid.nl/cgi-bin/deeplink/law1/title=Regeling%20voorbereiding%20buitengewone%20omstandigheden%20sector%20telecommunicatie%202007.
Last Access: August 31, 2008.
English English non-binding version not online.
Particularly relevant are articles:1.a, 1.b, 1.c, 2.1, 3, 4, 5

**Minez 3** Instellingsbesluit nationaal continuïteitsoverleg telecommunicatie 2007, 1 february 2008, (Decision establishing the tasks and responsibilities of the National Continuity Forum Telecommunications 2007 , 1 February 2008).
Available: http://wetten.overheid.nl/cgi-bin/deeplink/law1/title=Instellingsbesluit%20NCO-T%202007.
English non-binding version not online.

**Minez 4** Summarized information on the telecom/ICT policy with regard to resilience.
Available:
http://www.ez.nl/english/Subjects/Digital_security/Continuity_and_Crisismanagement.
Last Access: August 31, 2008.

**Minez 5** Letter to Parliament about CIP in The Netherlands - general part - September 2005.
Available NL version (letter and report):
http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/43821/beleidsbrief_vitale_infrastructuur.pdf
http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/43821/rapport_bescherming_vitale_infrastructuur.pdf.
Last Access: 26 September 2008.
English version not online.

### Additional Resources

Article in Newsletter on Crisis management (issued bimonthly by Ministry of the Interior) about NCO-T (April 2006). Available:
http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/65625/nieuwsbriefcbapril2006.pdf.
Last Access: August 31, 2008.

English translation not online.

Presentation held at meeting of IRG working group on Network Security (November 2006) on NCO-T. Not public, only for usage by IRG working group.

**Additional Links**

For more information about the **OPTA** (Onafhankelijke Post en Telecommunicatie Autoriteit) including technical regulations and administration visit http://www.opta.nl/asp/en/aboutopta/

Information from the **Ministry of the Interior** on the policies regarding National Security, Public safety, Crisis management , etc.
In Dutch: www.minbzk.nl/onderwerpen/veiligheid
In English: www.minbzk.nl/bzk2006uk/subjects/public-safety

**The National Infrastructure Cybercrime (NICC).**
Website of the NICC organisation (in Dutch) : www.samentegencybercrime.nl

**The Government Cert: GOVCERT**
In Dutch: www.govcert.nl
In English: www.govcert.nl/render.html?it=41

# National Report of Poland

## Introduction

Because of governmental (ministries and agencies) formal procedures, participation of Poland in a phone interview was not possible. After some planning the country supplied written answers in Polish, with a translation provided as attachment. The responses here are based on three sets of written answers (BBN, ABW and NASK) that were merged.

### Interview

Date and Duration – no interview was possible – written answers only.

**Authorities providing information about Network Resilience for this report**

| | | | |
|---|---|---|---|
| People providing written answers | Mr Krzysztof Silicki and Mr Miroslaw Maj | Mr Lucjan Bełza | Mr Tomasz Prząda |
| Authority | NASK / CERT Polska | BBN (National Security Bureau) | ABW (Internal Security Agency) / CERT.GOV.PL |
| Position title | NASK Technical Director, Chief of CERT Polska | Director of Internal Security Department | Chief of CERT.GOV.PL |
| Education/Training/ Degree | | | |
| Task and Responsibilities | | | |
| If applicable, rel.ship to ENISA | ENISA Management Board Member, Polish National Liaison Officer for ENISA | | |

**Authorities involved with Network Resilience**

| Author -ity | ABW - Internal Security Agency | Office of Electronic Communications | Ministry of Interior and Administration / National Crisis Management Center |
|---|---|---|---|
| Main Tasks | Investigation, prevention and combating threats against the State's internal security, its constitutional order, and specifically its sovereignty and international position, independence and territorial integrity, as well as national defence<br>Carrying out, within the limits of its powers, the tasks of the state security authority and performing the function of the national security authority in relation to the protection of classified information in international relations<br>Collection, analysis, processing and reporting to appropriate bodies information which may be significant to the protection of the State's internal security and its constitutional order<br>Carrying out other tasks specified in separate laws and international agreements | The performance of tasks related to the regulation and supervision of telecommunications services' markets, spectrum management, orbital and numbering resources, as well as the enforcement of compliance with electromagnetic compatibility requirements;<br>Intervening in matters related to the functioning of the market for telecommunications and postal services, the equipment market and the settlement of disputes between telecommunications undertakings;<br>Co-operation with domestic and international telecommunications and postal organisations, other competent national authorities, the European Commission and Community institutions, as well as other NRAs;<br>Co-operation with the President of the Office for Competition and Consumers Protection in matters related to the enforcement of the rights of parties using postal and telecommunications services, and with the National Broadcasting Council. | Coordinates all national resources during crisis including telecommunication, electricity grid, etc.<br>Protection of information provided within resorts' internal telecommunication networks and IT systems which security is within area of responsibility of MSWiA, as well as crisis management systems.<br>Defining guidelines for creation of security policies of IT systems used by government institutions, local government authorities and other units of public administration participating in creation of or utilising IT infrastructure.<br>Cooperation with government institutions, organisational units subordinate to or supervised by the Minister as well as organisational units of the Ministry of Interior and Administration in terms of cryptographic protection of information provided within the networks and systems for the government administration and crisis management sys**tems.** |
| Report s to | Prime Minister | Parliament | Ministry of Interior and Administration |
| URL for Agency or Authori ty | http://www.abw.gov.pl/ | http://www.uke.gov.pl/ | http://mswia.gov.pl/ |
| Year establi shed | 1989 | 1989 | 1989 / 2008 |

## Scope and governance

### Question 1 : The authorities

The responsibility applies in particular to the following:

- Ministry of Interior Affairs and Administration – responsible for the computerization of the country (public administration), the management of ICT infrastructure, including the police, and the prosecution of computer crimes;
- Ministry of National Defence;
- Military Counter-Intelligence Service - responsible for security of the infrastructure that is relevant to the defence of the country;
- The Ministry of Science and Higher Education –provides specialist education, including defining requirements for auditors of telecommunications systems (The Ministry of Internal Affairs and Administration’s exam);
- The Ministry of Infrastructure is responsible for communication networks. The basis for action are legal acts specifying activities for identified bodies as well as laws and regulations of an industry, such as the law on the protection of classified information, banking law, the regulation on documentation processing of personal data, and organizational and technical conditions to be met by equipment and information systems to be used for the processing of personal data
- Ministry of Finance;
- The Internal Security Agency (ABW), part of which is CERT GOV PL – responsible for network and systems security that form the critical infrastructure of the country, co-operation with administrative authorities and economic entities managing the infrastructure, as well as prevention, combating and detection of cybersecurity threats;
- Office of Electronic Communications (UKE) - responsible for the control and intervention in the telecommunications market, drawing up legislation on telecommunications services, and analysis of the functioning of the services market;
- Inspector General for the Protection of Personal Data (GIODO);
- Polish Commitee for Standardization (PKN);
- Office of Competition and Consumer Protection (UOKiK);
- Polish Financial Supervision Authority (KNF);
- The National Institute of Telecommunications;
- Research and Academic Computer Network (NASK);
- NASK / CERT Polska;
- PIONIER-CERT;
- Information System Audit Control Association (ISACA);
- Information Systems Security Association Polska (ISSA Polska).

### Question 2 : The mandate of the authorities

Ministry of Interior and Administration (MSWiA) is involved in tasks related to computerization and information society. For these it is the coordinating and supervising body. Experience and past work include projects in such areas as:

- IT infrastructure, telecommunication systems and networks;
- IT technologies, techniques and standards;
- computerization of government and local administration;
- support for investments in the field of IT;
- computer education, IT and multimedia services;
- applications of IT systems for information society, in particular in economy, banking and education; and
- realisation of international commitments of Republic of Poland related to computerization.

In terms of security of computer networks used by government organizations, municipalities and so forth, tasks and responsibilities of the Ministry include but are not limited to:

1. protecting of information provided within a departments' internal telecommunication networks and IT systems, whereby security is the responsibility of MSWiA, as well as crisis management systems;
2. defining guidelines for creating security policies of IT systems used by government institutions, local government authorities and other units of public administration participating in creation of or utilising IT infrastructure; and
3. cooperating with government institutions, organisational units supervised by the Ministry as well as organisational units of the Ministry of Interior and Administration in terms of cryptographic protection of information provided within the networks and systems for the government administration and crisis management systems**.**

Ministry of National Defence (MON) is responsible for maintaining, developing and securing telecommunication networks managed by the Ministry of National Defence (MON), including those belonging to the Polish Army. These tasks within MON are realised by the Department of Computing and Telecommunication.

Subordinate to this department is the IT structure consisting of IT Systems Management Centre (CZST), Communication Centre of the Ministry of National Defence (CWŁ MON) and eight regional communication centres (RWŁ), Centre of Computing and Communication of National Defence (CIiŁON), Implementation Teams in Warsaw, Bydgoszcz and Wroclaw, Military Communication and Information Security Agency (WBBŁiI) - running the military CERT, Military Office for Frequencies Management (WBZC).

Military Counter-Intelligence Service (SKW), is a service responsible for the security of the country in terms of protection of classified information processed in the army and military institutions, also processed in the telecommunication networks.

Internal Security Agency (ABW)

- In terms of protection of classified information, ABW realises, within its mandate and area of competence the necessary tasks and plays a role of the national security authority in international relations.
- Within structures of ABW the CERT GOV PL (Computer Emergency Response

Team GOV PL) was established with a superior role over all national institutions, organisations and departmental entities in terms of cyberspace security.

The team provides and enhances capabilities of organisational units of Republic of Poland to protect them against cyber threats. Particular attention is directed toward attacks against the infrastructure including systems and networks, destruction of which would constitute a threat to life or health of people, the heritage or the environment at large, cause large material losses, or disrupt the functioning of the state. CERT GOV PL also coordinates the flow of information between various entities when fighting cyber threats.

Ministry of Finance (MF)

- Supervises and controls financial telecommunication systems (Besti@, CELINA, EBTI, ECS/AES, e-Customs, e-deklaracje, e-Poltax, EMCS, ISZTAR-TARIC, NCTS, SEED, SIMIK, TREZOR, TQS, ZEFIR, ZEFIR – OSOZ, ZEFIR – INFOP) managed by the Minister of Finance.
- Administers the computer system of the Inspector General of Financial Information (GIIF) supporting Financial Analysis Unit - the main national centre of analysis of financial flows which might be used by criminals and terrorists.
- Services a platform for exchange of information from OLAF in AFIS system and manages information from the AFIS system, supporting actions of Polish Government Plenipotentiary for Combating Financial Abuse against Republic of Poland or European Union.

Office of Electronic Communications (UKE) regulates the telecommunication and postal markets. UKE has the powers to control and impose financial penalties on service providers.

Inspector General for the Protection of Personal Data (GIODO) can issue administrative decisions against organizations that have violated data protection regulation. GIODO investigates complaints regarding the implementation of provisions on data protection. It keeps a record of personal data sets, initiates and takes on projects that help improve procedures regarding the protection of personal data. GIODO participates in works of international organisations and institutions dealing with issues of personal data protection.

Office of Competition and Consumer Protection (UOKiK): Within the scope of its competence is combating the phenomenon of spam treated as unfair competition, and defined by UOKiK as unwanted and annoying advertisement delivered by electronic mail, telephone, facsimile, mobile phone (as SMS or MMS), instant messaging, chat services (IRC) or web pages.

Research and Academic Computer Network NASK is a research and development unit. The research conducted by NASK is aimed to develop mechanisms and algorithms to increase the efficiency and reliability of modern networks and security of both the telecommunication networks and services.

NASK is the registry of the .pl internet domain. Under contract between NASK and the Ministry of Interior and Administration, NASK is also a Government Validation Point, i.e. a government entity reviewing applications for registrations of .eu domains to EURid. The review is carried out in accordance to guidelines of the European Commission provided in the whitepaper „.eu Launch Guidelines for Member States". The review is done in order to check whether the applying entity exists, is a public body and if its representative is authorised for signing documents.

CERT (Computer Emergency Response Team) Polska working within a structure of NASK is a team set up to respond to incidents affecting the security of .pl Internet. Its tasks are:

- registering and handling security incidents,
- alerting users in case of an imminent threat,
- cooperation with other IRT (Incidents Response Team) teams within FIRST,
- carrying out activities aimed to increase security awareness,
- conducting research and preparing reports on the safety of Polish Internet,
- working on development of best practises in incident handling and registration, classification and generation of statistics.

Information System Audit Control Association (ISACA), administrates issuing certificates of Certified Information Systems Auditor (CISA). ISACA also gives certificates of Certified Information Security Manager (CISM). It develops international standards of auditing and inspecting of information systems in organizations of which the best known one is COBIT[59].

Information Systems Security Association Polska (ISSA Polska), ISSA Polska - The association for Information Systems Security is working on the promotion of knowledge about the security of information systems and promoting principles and guidelines ensuring confidentiality, integrity, availability and accountability of information resources, as well as promotion and development of its members by raising their professional skills related to the protection of information systems.

Poznan Supercomputing and Networking Centre (PCSS), is affiliated with the Institute of Bio-organic Chemistry of Polish Academy of Sciences (PAN). PCSS is the operator the metropolitan network POZMAN connecting all scientific units (universities, research institutes) and is the operator of the nation-wide network Pionier - Polish Optical Internet. PCSS keeps a promotion centre in the field of modern information structure - networking and computing. PCSS also provides telecommunication services (electronic mail, teleconferences, WWW, news etc.). The Centre also manages regional databases (for libraries and scientific information).

PIONIER-CERT, is the incident response team (CSIRT) for the PIONIER network. The basic tasks of the team include active involvement in incident handling and response, guaranteed with more than five years of experience of the Security Group of Poznan

[59] *This is a US-based not-for-profit assocation of auditing and governance experts in the IT and data management domains. Membership is worldwide.*

Supercomputing and Networking Centre. The PIONIER-CERT team coordinates incident handling as far as the PIONIER network members are concerned. It collects and processes information about incidents and shares data with interested parties.

The National Institute of Telecommunications (IŁ), is the coordinator and main contractor for a multi-year program (2005 – 2008) – Development of telecommunication and postal services in times of information society.

This multi-year program is not a direct investment in infrastructure, but an indirect investment, accelerating growth of the market of telecommunication, information and postal services. It will launch and implement a new, adaptive system of state services in terms of telecommunication, information and post. This will support the development of the information society and is compatible with the Lisbon strategy of the European Council. It also is part of PL's efforts regarding post-accession adaptation of the telecommunication and information infrastructure to the requirements of the European Union.

The state services system will allow for fast, adaptive verification of information and opinions about the telecommunication infrastructure and directions of its development. It will assure independence of information and opinions from the market and their base on sound science.

Polish Financial Supervision Authority (KNF): Current regulations in terms of security of data processing in bank computer networks are defined by the Recommendation D issued by the Inspector General of Bank Supervision (GINB). This set of recommendations was supported by KNF which took over competencies related to bank supervision from GINB. The Recommendation includes recommendations of the Basel Committee on Bank Supervision regarding rules of risk management in electronic banking.

Polish Committee for Standardisation (PKN): In accordance with Polish law, a public body develops, modifies according to the needs, and implements security policies for telecommunication systems used by the public body for completing public responsibilities. When developing security policies, a public body should take into account provisions of the Polish Standards in the area of information security.

In terms of network security PKN has implemented in the Polish system two ISO standards: PN ISO/IEC 27001 *Information security management systems -- Requirements* and PN ISO/IEC 17799 (27002) *Code of practise for information security management*.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

According to the principle of division of powers, each head of an organisational unit (e.g. institution) is required to evaluate the level of risk and take adequate preventive measures and safeguards.

It should be noted that the scope and nature of counteraction and precautions cannot be reduced to some general recommendations or policies. All instructions and recommendations are not and cannot be binding for a head of a unit. Any obligation to act in particular way may arise only from applicable laws (the competent authorities in this respect have been listed in the previous section).

There is a lack of legal requirement to apply "national risk management process". However, various risk assessment mechanisms are used across individual institutions. General principles of the strategy in the field of information are shown in the following projects:

*Plan of the national computerization 2007-2010* (developed by MSWiA) This document sets out:

- The priorities and objectives for the computerization of the country, on the basis of which the telecommunication systems used for completing public responsibilities should be developed,
- A summary of sectoral and cross-sectoral projects which will be used to carry out specific priorities and services, detailed descriptions of projects together with information about the estimated costs of their implementation, possible sources of financing, entities responsible for their implementation,
- The action program of the development of the information society, taking into account the levels of implementation priorities for the development of information systems, consistent with the initiative i2010 "A European Information Society for growth and employment", adopted by the European Commission on June 1st, 2006.
- The public responsibilities which should be implemented electronically (priority services for citizens and businesses). Entities responsible for implementing specific services and dates for commencement of their implementation were identified.

The Plan sets out 5 cross-sectoral and 22 sectoral projects. It also defines the schedule of tasks for individual resorts in terms of development of the information society and computerization of public administration.

*Multi-year program 2005 – 2008 - Development of telecommunication and postal services in the era of information society* (developed by The National Institute of Telecommunications)

The main contractor and coordinator for this project is The National Institute of Telecommunication, supervising is the Ministry of Infrastructure.

The objective of the multi-year program comes directly from the strategic objective defined in the National Development Plan (NPR) 2004-2006. The strategic objective of the National Development Plan is the development of a competitive economy based on knowledge and entrepreneurship. This means being capable of long-term, harmonious development, ensuring the growth of employment and improving social cohesion. It must also coordinate with the European Union at regional and national levels. The objective of the program is consistent with the assumptions of the NPR for years 2007-2013. The current work also entails the Government Protection Program of Cyberspace for the Republic of Poland. The strategic objective is to increase the level of the cyber-security of the state.

Achieving the strategic objective requires the creation of organizational and legal framework as well as the system of effective coordination and information exchange between the entities of public administration and other entities whose resources form a critical ICT infrastructure of the country, in the event of a terrorist attacks involving public ICT networks. The list of the specific objectives of the Program is as follows:

- Increasing the level of security of ICT critical infrastructure resulting in an increase of the safety of the state against cyber-terrorism,
- creation and implementation of the policy on the safety of cyberspace, coherent for all entities involved in public administrations and other entities that form critical ICT infrastructure of the Polish state,
- decreasing the effectiveness of cyber-terrorist attacks, and thus reducing the costs of their after-effects,
- the creation of a permanent system of coordination and exchange of information between public and private entities responsible for ensuring the safety of cyberspace of the state and those in charge of resources which form the critical ICT infrastructure of the country,
- increasing competence (regarding the cyberspace security) of entities involved in critical ICT infrastructure protection and other systems and networks of public administration,
- increasing the awareness of electronic system and teleinformatics network users (including citizens) about methods and security measures.

According to the Program, it is necessary to define responsibilities of those entities in the private sector whose protection against cyber threats is important for the proper functioning of the state. This group of entities should include amongst others the owners of telecommunication infrastructure. However, it should be emphasised that the matter of protection of cyberspace is not limited to telecommunication area, but also other areas of services, such as the banking sector.

Achieving real cooperation between state administration and the private sector is a challenge. Such cooperation is possible only when in the established solution the benefits of cooperation outweigh the risks resulting from even a partial loss of control over information. The effect of the Program will be organizational and legal solutions fostering the effective cooperation of private entities with public administration in the context of critical infrastructure and ICT protection of the state.

In the light of the above, actions will be taken to develop cooperation between private parties in charge of those parts of the critical ICT infrastructure of a similar nature, and thus vulnerable to similar types of cyber threats and attacks methods. One of the forms of cooperation could be the creation of bodies appointed to the internal exchange of information and experiences as well as to cooperation with public administration in the protection of critical ICT infrastructure.

In accordance with the objectives of the Program, the concept of critical ICT infrastructure protection will be developed and legal foundations for tasks in this regard will be prepared to be performed by the state bodies. Protection of cyberspace in terms of critical ICT infrastructure should also apply to private entities.

In order to protect critical ICT infrastructure it is necessary to ensure the correctness and reliability of the functioning of the systems and teleinformatics network. Facilities and installations important for the internal security of the state must be part of such work. As well, to ensure the smooth functioning of transport, communications and electricity, water and gas supply networks must be included. In fact, if the latter are damaged or destroyed this can constitute a threat to human life or health, cultural heritage and the environment (in significant quantities), or cause serious material damage, and also disrupt the functioning of the state.

Currently, in the Act of 26 April 2007 on crisis management there is defined the concept of critical infrastructure without detailing either the concept of critical infrastructure or tasks and roles of the various actors involved in its protection. As a result, the Ministry of Internal Affairs and Administration will prepare and launch in 2009 proposals for legislation changes defining the objectives, principles and forms of critical ICT infrastructure protection, and define the powers of the competent bodies for the protection of such infrastructure. Scope of the legislation should apply to all bodies, involved with a cyber-security policy, including the private sector. The law should regulate the activities in this area such as:

- the authorities and government administration
- state and municipal legal persons,
- state and municipal bodies,
- organs of local self-government,
- organizational units which do not have legal personality,
- social organizations and businesses that offer services of public utility if they use a system, object or installation which is a part of the critical infrastructure.

Moreover, there have been created appropriate legislation acts and programs, designed to bring the service of the country to the requirements of the information society - for example:

- computerization program for the state, coordinated by the The Ministry of Internal Affairs and Administration – the program assumes government offices to be equipped with systems and networks, to improve the work of officials and to make services of public administration as on-line services; creating of regulations for hardware requirements are primarily aimed to standardize the quality of equipment and tools,
- state and industry regulations - on protection of classified information include: guidelines for networks and systems designed to processing of classified information, similar solutions, taking into account the conditions in the area of their application, can be found in acts on the protection of personal data, banking law, etc.

Based on the pertinent legislation, an agency may then issue guidelines such as in the area of information security and network resilience. The Internal Security Agency defines the guidelines for networks and information systems at the stage of their design.

The regulations also provide legal obligation to specify in detail the requirements of the hardware, applications, procedures of use, risk analysis, and to take control operations - these rules are reflected in security policies, documents regarding safe operating procedures, etc.

In addition, the rules impose duties on public administration (both government and local council) to create procedures for emergency situations that may be caused by severe incidents.

**Question 4 : Initiatives between providers and public authorities**

The scope and form of initiatives do not result from a legal obligation but from individual will of the concerned entities. Examples of initiatives with nationwide coverage:

*ARAKIS GOV (Aggregation, Analysis and Classification of Network Incidents)*

Thanks to cooperation between CERT Polska and the Internal Security Agency ARAKIS GOV was created as a government-dedicated version of ARAKIS NASK project. The ARAKIS system (Aggregation, Analysis and Classification of Network Incidents) is a project of the CERT Polska team which is part of NASK. The objective of the project is to create an early warning system directed at network security threats. The system is aimed at detecting and describing new automated threats, and particularly new exploits used across the network. The system is located in a network of institutions and is provided to them free of charge. So far, about 50 sensors of ARAKIS GOV were located in the government institutions.

*Cooperation between ABW - CERT GOV PL and Microsoft*

As part of the implementation of the agreements, ABW - CERT GOV PL is part of the Government Security Program (GSP) and Security Cooperation Program (SCP). Thanks to participation in these programs, CERT GOV PL receives early information about vulnerabilities discovered in Microsoft software.

In 2005, The Internal Security Agency and CERT Poland operating under the Scientific and Academic Computer Network began the process of implementing an early warning system against threats from the Internet - ARAKIS GOV, in 50 units of public administration. The system architecture of ARAKIS is based on a distributed set of sensors installed in protected institutions at the interface between production networks and the Internet. The central parts of the system are servers, making, among other things, correlation of events received from various sources and then presenting the results of the web-site. The primary task of the system is detecting and specification of new threats emerging on the Internet. It is worth to mention that, in contrast to the commonly used solutions ARAKIS GOV does not primarily rely on the existing attack signatures, but thanks to the advanced analysis of network packets and correlation of events (including those from external sources) creates signatures for previously unseen threats, which can then be used in commercial products. ARAKIS GOV is thus not a typical protective system and in any case does not replace the functionality of the standard network security systems such as firewalls, antivirus tools or IDS / IPS systems.

However, due to its specificity, it can be successfully used as a complementary solution to the above-mentioned systems, providing information on:

a) new emerging threats on the Internet - common to all participatory systems, including:

- new detected self-propagating threats such as worms,
- new types of attacks, observed from a large number of locations,
- trends of the activity of network traffic at various ports,
- trends of the activity of viruses broadcasted via e-mail,

b) local threats associated with a particular, protected location:

- the lack of up-to-date anti-virus signatures,
- infected computers in the internal network,
- vulnerable configuration of the edge firewalls,
- scanning attempts of public addresses from both the Internet and the internal network.

The project is financed from the budget of the Internal Security Agency. There is informal initiative between providers related to security issues, especially incident handling capabilities. In 2005 on NASK's (Research and Academic Computer Network in Poland) initiative the ABUSE-FORUM was established. The members of this forum are Computer Security Incident Response Teams and security teams within the biggest Polish Internet Service Providers. All of these teams are responsible for network incidents handling in their networks.

The forum is organizationally managed by Research and Academic Computer Network in Poland (NASK) (CERT Polska team). NASK covers all meetings costs as well as found yearly a free entrance for member representatives for SECURE conference – http://www.secure.edu.pl/ (this conference is co-organized for last 4 years with ENISA). The forum meets quarterly and regularly more then 10 members are present. The main topics of discussion and activities are:

- Cooperation between forum teams and LEAs in Poland
- Exchanging of experiences between the teams, especially related to the operation of a team within their company organizational structure and methods of contacting and cooperating with the teams' constituencies.
- The undertaking of technical actions in the teams' networks, with the goal of improving the security of the teams' parental organizations, as well as their customers.

Recently the forum was joined by two CERT teams representing public sector – Polish governmental CERT and Polish military CERT.

## Tasks

### Question 5 : Typical task

All of these tasks are carried out, depending on the needs:

- The most significant consultation with the network operators, experts outside the administration are carried out in the preparation of individual projects - the strategy, projects of normative acts,
- The official exchange of information with The Internal Security Agency occurs primarily in the course of their inspection of systems and networks, or in the event of an incident,
- Audit or control of networks and information systems carried out by the competent authorities according to their destination - such as The Internal Security Agency - certification of networks for the processing of classified information, the Inspector General for the Protection of Personal Data - control of the fulfilment of the requirements for the protection of personal data, The Office of Electronic Communications - control of telecommunications services,
- Implementation of the law in case of security regulation is primarily administrative proceedings to control the application of the security policy, and may take the repressive form (penal and administrative enforcement).

### Question 6 : Exchange of information between providers and public authorities

Providers are to deliver information to LEA case by case according to investigation procedures.

### Question 7 : Handling of security incidents

In principle, there is no legal obligation to exchange information and inform the authorities responsible for the network security.

However, in situations when the computer incidents have elements of criminal offences (crimes) or represent a serious threat to the operation of the networks that are relevant to the state's security, the incident must be reported. Such obligation is due to the general provisions of criminal law.

Regardless, the state authorities responsible for public safety are equipped with the powers that allow them to request certain information or to demand an infrastructure owner or network operator to supply them with documentation, testimonies, expertises and so forth.

### Question 8 : Audits related to resilience

There is no legal mandate to conduct audits and neither are assessments at this time undertaken regarding the resilience of e-communication networks and their dependability.

### Question 9 : Enforcement actions

When regulations and requirements are not being followed by operators, system and network administrators, managers of organizational units or other entities, enforcement actions can be taken. Enforcement provisions allow the imposing of fines for not complying with the requirements for information security, such as:

- Article 51 on the Protection of Personal Data Law- which imposes sanctions for unauthorized access to data and,
- Article 209 paragraph 26 on the Telecommunications Law (see PL 1 in reference list) – which imposes penalties for processing the data that are subjected to the rules of the telecommunication privacy law.

The rules also empower individual authorities to command the appropriate behaviour or receive a certificate entitling him to use ICT system - for example, after inspection, the Internal Security Agency may impose on a controlled entity the obligation to bring the construction of telecommunication system under the penalty of taking away powers.

## Risk Management and preparedness measures

All issues related to the questions 10 and 11 are addressed in The Crisis Management Act, 2007 (see below: The legal acts related to the survey – see PL 2 in reference list) and they will be also organized according to Governmental Program of Protecting Polish Cyberspace (see answer to the question 3 in the ABW's answers).

### Question 10 : The national risk management process

The tasks referred to in the questions below will be fulfilled by the National Security Center (Rządowe Centrum Bezpieczeństwa). This Center was established in August 2008 according to the Prime Miniser decree issued on 10th of July 2008.

### Question 11 : The preparedness and recovery measures

Efforts will be also organized according to Governmental Program of Protecting Polish Cyberspace (see answer to the question 3 in the ABW's answers). The tasks pointed in the questions will be fulfilled by the National Security Center (Rządowe Centrum Bezpieczeństwa).

This Center was established in August 2008 according to the Prime Minister decree issued on 10th of July 2008. Hence, Poland is beginning to work on its national risk management process.

### Question 12 : Incident response capabilities

Since 1996 the role of national CSIRT is served by the CERT Polska team. Earlier (from 1996 till 2001) it was known as CERT NASK. Apart from the CERT teams, some specific tasks and powers are assigned to the Internal Security Agency (ABW).

ABW, and within its structures the Information Security Department (DBTI) deals with telecommunication security issues in a comprehensive way. The unit focuses its strength and resources not only on the management of IT security, but primarily on identifying mechanisms of actions which may be a threat to the national IT infrastructure and on IT security incidents such as cyberterrorism or electronic wiretapping and effective combating and prevention of them. The specialists of the Department have been working on the effectiveness of IT security solutions and their appropriate selection for years, especially in the context of developing cyberthreats.

Fast development of IT technologies implies using these technologies also against the law, which undoubtedly influences security of electronically processed information. It is the role of DBTI to minimise this unwanted phenomenon. For this reason the Department is equipped with professional background, such as Certification Unit, specialised laboratories researching cryptographic and electromagnetic security, highly qualified and experienced staff and system solutions.

The effect of comprehensive actions of DBTI allows us to shape the IT security policy at high level and propagate it amongst the users of the systems and networks in the form of recommendations as well as during specialised trainings, and above all execute its implementation with processes of accreditation and implementation related to IT security.

The objective of CERT GOV PL is to ensure and develop capabilities of organisational units of the Republic of Poland to protect against cyberthreats, especially attacks directed at the infrastructure including telecommunication systems and networks, which if destroyed or disrupted would cause a threat to lives, health of people, the heritage or the environment at large, cause large material losses, or disrupt the functioning of the state.

- Creation of policies for protection against cyberthreats;
- Coordination of flow of information between entities in relation to cyberthreats;
- Detection, identification and prevention of cyberthreats;
- International cooperation in terms of cyberspace protection;
- Playing an overriding role in relation to all national institutions, organisations and resorts in terms of cyberspace protection;

Tasks of CERT GOV PL:

- Accumulation of knowledge about the state of security and threats to the critical IT infrastructure;
- Response to security incidents, particularly related to the critical infrastructure;
- Digital forensics;
- Creation of policies for protection of Polish cyberspace;
- Trainings and awareness building;
- Consulting and advice in the area of cybersecurity.

In January 2008, the Minister of Internal Affairs and Administration and the Head of the Internal Security Agency adopted a common position on the protection of cyberspace of the Republic of Poland. An important result of cooperation of both ministers is the creation of the Government Response Computer Incidents Team: CERT GOV PL. The aim of the team is to providing and developing the ability of government administration units of the Republic of Poland to protect against cyberthreats, with a particular focus on attacks aimed at infrastructure of ICT systems and networks, whose destruction or disruption may constitute a threat to a human life and health, cultural heritage and the environment in significant quantities, or cause serious material damage, and also disrupt the functioning of the state. According to the plan for the protection of cyberspace of the Republic of Poland, the tasks of the Government CERT GOV PL team will include:

- creating of a policy on protection against cyberthreats,
- coordinating the flow of the information between bodies in this field,
- detection, identification and counteract cyberthreats,
- cooperation with national institutions, organizations and departmental entities for the protection of cyberspace,
- representation of the Republic of Poland in international relations.

Additionally, tasks of GOV CERT PL team will include the following:

- collecting of knowledge on the state of security and threats to critical ICT infrastructure,
- responding to security incidents with a particular focus on critical ICT infrastructure of the country,
- carrying out forensic analysis tests,
- creating of a policy for teleinformatics systems and networks protection,
- training and raising awareness about cyberthreats,
- preparing periodic reports in the field of teleinformatics security of the state,
- consultancy and advice on cyber-security.

In addition, for the systems belonging to the critical ICT infrastructure of the state, tasks performed by the CERT GOV PL will include such activities as:

1. keeping the registry of the critical ICT infrastructure of the state.
2. collecting and processing information in the registry as well as its sharing,
3. developing of analysis of the critical ICT infrastructure of the country
4. controlling of the protection system or network entered in the register,
5. international cooperation in the protection of telecommunication infrastructure state. The Head of the Internal Security Agency in international relations should serve as a national system for protection of critical infrastructure, telecommunication country.

As a result of arrangements between the Internal Security Agency and the Ministry of National Defence, the Head of The Internal Security Agency with a technical resources will be a National Focal Point in the protection of NATO cyberspace and will occur as a direct partner of the authority set up in 2008 and responsible for the management and coordination of NATO and its member states in the field of cyberspace - NATO Cyber Defence Management Authority (CDMA).

The actual implementation of these arrangements will be a co-operation between the CERT GOV PL team and the NATO Computer Incident Response Capability in responding to computer incidents.

In addition, when the full operational capability is reached, CERT GOV PL plans to become a member of international organizations associating teams which respond to computer incidents (e.g. FIRST - Forum of Incident Response and Security Teams).

### Question 13 : Good practice on resilience

Not until now.

### Question 14 : Guidelines for procurement

Not until now.

## References

**PL 1** Prawo Telekomunikacyjne z 2004 r. (The Polish Telecommunication Act, 2004). Available: http://isip.sejm.gov.pl/servlet/Search?todo=file&id=WDU20041711800&type=1&name=D20041800L.pdf.
Last Access: October 1, 2008.

**PL 2** Ustawa o zarządzaniu kryzysowym z 2007 r.(The Crisis Management Act, 2007). Available: http://isip.sejm.gov.pl/servlet/Search?todo=file&id=WDU20041711800&type=1&name=D20041800L.pdf.
Last Access: October 1, 2008.

**PL3** Plan Informatyzacji Państwa na lata 2007-2010 (State Informatisation Plan for the years 2007-2010). Not online.

### Additional Resources

None

### Additional Links

Internal Security Agency (ABW – Agencja Bezpieczeństwa Wewnętrznego), http://www.abw.gov.pl/eng/index@option=com_content&task=view&id=128&Itemid=338.html.

National Security Authority, http://www.abw.gov.pl/eng/index@option=com_content&task=view&id=129&Itemid=339.html.

# National Report of Portugal

## Introduction

### Interview

Date and Duration - 2008-07-31 – 75 minutes.

| | | |
|---|---|---|
| Interviewee | Manuel de Barros | Paulo Pereira |
| Authority | ICP – ANACOM | ICP – ANACOM |
| Position title | Head of Communications Security Office (CSO)-- | Member of Communications Security Office |
| Task Responsibilities | Responsible for the Communications Security Office | Supports office activities |

The ICP-ANACOM's Communications Security Office has as its mission *"To ensure the execution of ICP_ANACOM's powers and responsibilities with regard to the security of communications networks and services, namely the access to emergency services, as well as to plan and to implement an internal security policy and the coordination of communications standardisation"*.

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | ICP – ANACOM |
| Main Tasks | The aim of ICP - ANACOM is to regulate, supervise and represent the communications sector under the terms of its statutes and the law. |
| Reports to | ICP - ANACOM is independent in the exercise of its functions, in the context of law, without prejudice to the guiding principles of communications policy set by the Government, according to constitutional and legal terms and the acts subject to ministerial tutelage (Minister for Public Works, Transport and Communications) under terms anticipated by law and in these statutes. |
| Year established | 1989 – establishment and beginning of ICP activities with publication of its statutes.<br>2001 – change into ICP – Autoridade Nacional de Comunicações or ICP – ANACOM (see ANACOM 3 in reference list).<br>Communications Security Office was established in March 2007 |
| URL | http://www.anacom.pt/ |

### Authorities involved but not part of the interview

| | |
|---|---|
| Authority | CERT.PT |
| Main Tasks | Portuguese National Educational and Research Network's user community |
| Reports to | |
| Year established | |
| URL | http://www.CERT.pt |

## Scope and governance

### Question 1 : The authorities

As outlined above, ANACOM regulates matters of resilience of public eCommunication networks. ICP-ANACOM addresses all the issues raised in Q1, including regulation, policy development, co-operation with providers, advice and best practices (see also ICP – ANACOM 1). ANACOM was established in 1989, year that it was given its statutes. These were enhanced with a decree law 2001 when ICP changed its designation to ICP-ANACOM and its responsibilities were updated. In 2007 adopted its current internal organisation when it's Board decided to create the CSO – Communications Security Office. (see ICP - ANACOM 2, 3, & 4).

### Question 2 : The mandate of the authorities

The legal basis for ICP-ANACOM's mandate is given by its statutes (see ICP – ANACOM 3), the Electronic Communications Law (see ICP – ANACOM 1) and further legislation. Its powers and responsibilities are elaborated in Chapter 2 Article of the statutes and embrace a wide range of tasks.

In addition, the Electronic Communication Law has certain articles pertaining to resilience. This law is the transposition of part of the EU telecom regulatory package. The privacy and data protection directive is transposed into national law by dl41/2007 e artigo 13 do dl7/2004. Nevertheless, there is no specific legislation, law or regulation addressing network resilience in particular.

### Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks

ICP-ANACOM's CSO was established in March 2007 (see also ICP – ANACOM 6). Presently CSO staff is composed of two engineers, one economist and the head of the office. Currently, it conducts various studies and interviews with stakeholders to allow it to take an inventory regarding e-communication networks' resilience. Regulation of resilience and security was recognized by ICP-ANACOM's Board as an issue last year resulting in the establishment of ANACOM CSO.

In its review of the regulatory framework, the EU published a set of proposals for the regulatory framework for eCommunications in November 2007. ICP-ANACOM organised three workshops during January 2008. The objective was to raise awareness and promote a public debate regarding the proposals presented by the European Commission with respect to this review and to cooperate in defining the position of ANACOM in this respect.[60]

[60] *Three workshops on reviewing the regulatory framework for electronic communications (January 2008). Available: http://www.anacom.pt/template13.jsp?categoryId=261847 Last Access : August 23, 2008.*

Beyond these activities there is no additional legislation in the works.

ICP-ANACOM has launched several studies that are the beginning of its activities to provide additional guidance and regulation if needed. The studies will allow ICP-ANACOM to conduct a systematic inventory on what are the issues, what are the problems and potential risks and where do operators, users and other stakeholders see a need for improvement. Examples of the studies having been launched or being in the process of being conducted are:

- Evaluation and identification of the main network nodes for international and for interregional traffic exchange.
- Evaluation and identification of the interdependences between Civil Protection Policies and Communications Public Policies.
- Evaluation and identification of the interdependences between State Private Networks and Public Electronic Communications Networks.

Studies will be the starting point for determining if there are further guidelines to be developed based on these data and analyses thereof.

ICP-ANACOM expects first results around the end of 2008 – 2009. These studies are based on formalized procedures that usually involve the following steps:

1) collection of legislation/ regulation in place,
2) based on point 1, preparing of a draft survey to be administered,
3) fine-tuning of the survey collecting feedback from various parties including outside experts, and
4) sharing revised draft questionnaire with main stakeholders to collect feedback.

Once the questionnaire has been finalized, data collection will be launched. Thereafter, the following approach is used:

1) analysing data collected and reporting first findings,
2) fine-tuning findings,
3) organizing workshop to report findings to stakeholders, and
4) presenting findings and workshop input to government

As regards to future strategies, the above research projects and findings thereof will provide the basis for developing a strategy for security of public communication networks (resilience).

Responding to the above survey during data collection period is a mixture between voluntary, required and so on. Some people do it voluntarily. Voluntary participation is most effective because it generally occurs when stakeholders have come to the conclusion that participation will be beneficial.

Step 8 will contain suggestions for possible regulatory changes or the development of new guidelines. Such changes, if approved by the Government, will then have to be implemented.

### Question 4 : Initiatives between providers and public authorities

The studies mentioned above do require participation by various stakeholder groups including infrastructure owners, telecommunication providers and so on. Last year's ARECI study gave the country the opportunity to discuss with various stakeholders the issues pertaining to resilience of public e-communication networks. Information included from Portugal in the final report of the study included input from operators and infrastructure owners (see also Additional Links).

The public concession (see ANACOM 4) was a Public-Private Partnership (PPP) in its beginning. The concession does encompass security-related matters that the operator must take care off.

Working groups exist on security planning. They meet regularly; an example is the working group for civil defence. One goal of the working groups is to come up with requirements for network security issues.

As regards efforts by operators for self-regulation in the area, not much activities are going on which would be known to ICP-ANACOM. We do acknowledge the ARECI recommendations concerning initiatives between providers as well as between providers and the government. Nevertheless, operator responses we have received so far indicate that whilst they are willing to do more in the area of self-regulation, budgetary constraints are seen as a major obstacle to such initiatives.

In turn, operators have looked toward ICP-ANACOM to take the first steps and getting important stakeholders to the table. We have to wait and see how this will work out. Bilateral cooperation with operators on 112 issues takes place.

## Tasks

### Question 5 : Typical tasks

Within its legal mandate, ICP-ANACOM holds public consultations, exchanges information with providers, audits and enforce regulation. The regulator can make an investigation after an incident or an audit as it sees fit. However, until now the regulator has not done any audits or incident investigations pertaining to network resilience (dependability and reliability).

### Question 6 : Exchange of information between providers and public authorities

There is limited exchange of information between providers and it appears that the initiative for standing committees that will institutionalize exchange and collaboration will have to come from the regulator.

We are trying to learn more about general issues. Also, once an incident happens in the network, we ask the operator to provide us with information about:

a. how they plan to fight the problem  or better to resolve issue,
b. what measures they took before and during the incident. AND
c. what the operator will do afterwards to minimize the future risks for this to happen again.

ICP-ANACOM is trying to work/verify, and measure how the operator has worked to resolve this issue. Nevertheless, we are working on specific regulation that will enable us to ask operators to provide this information automatically after an incident. Here, it is especially important to have a basis to develop an agreed upon timetable for such a report, the latter's structure and content. Particularly, what information ICP-ANACOM needs to conduct its work according to its mandate in this area must be clarified.

**Question 7 : Handling of security incidents**

Severe incidents are reported. But, there is:

a. no formal way to report (e.g., as outlined under Question 6, defining in practical terms what is a severe incident, timetable for reporting, structure and content for reporting a severe incident), and
b. a need for a regulation that specifies the requirement for formal reporting of severe incidents.

The severe incident reporting could be implemented in a general regulation on reporting and information exchange.

**Question 8 : Audits related to resilience**

ICP-ANACOM does not yet conduct audits pertaining specifically to network dependability and reliability / resilience issues regarding public e-communication networks.

Because there is no specific regulation pertaining to resilience, there is no legal foundation for conducting a formalized audit. Neither do we have a regulatory basis to demand an operator response when finding shortcomings through an audit. In turn, we could not demand remedial work to rectify the problem be taken within a certain timeframe and following a specific procedure.

**Question 9 : Enforcement actions**

Here we must make a distinction between resilience in general and license to operate in a particular spectrum. If the matter is covered under the operator's license or the concession for the concessionary, we have greater leverage and steps. In fact, the license is very clear about how the problem must be resolved in case of deficiencies we find. As well, financial sanctions are possible.

If the matter is covered under our Communication Law (see ICP – ANACOM 1) things are more difficult. For instance, if the matter involves resilience or certain network resources not being online (dependability), thereby causing an accident, a legal investigation is undertaken.

Possible Changes: There needs to be a procedure put in place whereby based on an incident and subsequent analysis, operators can take the necessary steps to improve reliability and dependability. This collaborative approach through a working group including telcos and regulator(s) would help in developing pro-active best practice approaches that are being followed. In turn, assessments checking how well such practices have been implemented and sharing the information with the working group can again result in learning how to improve resilience of e-communication networks.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

There is none at this point.

### Question 11 : The preparedness and recovery measures

Until now, neither preparedness nor recovery measures to mitigate risks affecting the resilience of public networks exist. This work is in progress and it is expected to come up with the definition of requirements in the near future.

### Question 12 : Incident response capabilities

As regards incidents response capabilities, Portugal does not have a national CERT

Fundação para a Computação Científica Nacional (FCCN) manages an academic CERT. The academic CERT is responsible for the network that serves universities and schools, the Internet domain .pt, the international exchange and Portugal's connection to the Internet backbone. Another CERT is currently being developed in the Porto region.

However, so far there is no formalized way to collaborate between different agencies (e.g., public and private groups, academic CERT and others). Instead, limited cooperation happens on an informal and ad-hoc basis. The academic CERT is a member of FIRST and exchanges information with other CERTS. The academic CERT through FCCN collaborates with various government agencies.

### Question 13 : Good practice on resilience

Not until now.

### Question 14 : Guidelines for procurement

Not until now.

## References

ICP – ANACOM pertains to regulation relevant to that agency.

**ICP – ANACOM 1** Law of Electronic Communications (see Essential Public Services Law).
Available:
http://www.anacom.pt/render.jsp?categoryId=97279#horizontalMenuArea.
Last Access: August 15, 2008.
Particularly relevant are articles: 5(4-f), 15, 27(1), 29, 40, 49, 73 and 92.

**ICP – ANACOM 2** Telecommunication law (several laws).
Available:
http://www.anacom.pt/render.jsp?categoryId=60172.
Last Access: August 15, 2008.

**ICP – ANACOM 3** Decree-Law no. 309/2001, of 7 of December (ICP-ANACOM mandate – statutes).
Available: http://www.anacom.pt/render.jsp?contentId=17645.
Last Access: August 15, 2008.
Particularly relevant are articles: Annex: 6, 9 and 17.

**ICP – ANACOM 4** Decree-Law no. 31/2003, of 17 of February  the public telecommunications service concession.
Available: http://www.anacom.pt/render.jsp?contentId=89968.
Last Access: August 15, 2008.
Particularly relevant are articles: Annex: 2, 5, 6, 7, 8 and 25.

**ICP – ANACOM 5** Personal Data and Privacy Protection Law,
http://www.anacom.pt/render.jsp?contentId=221691&languageId=1.
Relevant articles: 3 and 4.

Unsolicited Communications (Decree Law 7/2004 of 7th January)
http://www.anacom.pt/render.jsp?contentId=221668&languageId=1
Article 22.

**ICP – ANACOM 6** Organization chart - Instituto das Comunicações de Portugal (ICP-ANACOM).
Available:
http://www.anacom.pt/streaming/organogramauk.gif?contentId=600601&field=ATTACHED_FILE.
Last Access: August 25, 2008.

**ICP – ANACOM 7** Security and Emergency Networks Integrated System (Resolution of the Council of Ministers),
http://www.anacom.pt/render.jsp?contentId=97807&languageId=1.

### Additional Resources

The ARECI Study (Final Report) PSC-Europe/RD/024 (March 2007). **Availability and robustness of electronic communications infrastructures** (Final report). Brussels: Prepared for the European Commission by Alcatel-Lucent.

Available:
http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334
Last Access: August 25, 2008)

### Additional Links

Academic CERT, http://www.cert.pt/index.php?newlang=English

# National Report of Slovenia

## Introduction

### Interview

Date and Duration – 2008-09-15 - 45 minutes.

| | | |
|---|---|---|
| Interviewee | Prof. Dr. Denis TRČEK (information given to the best of interviewee's knowledge, without any official approval from Slovenian state authorities) | Mr Gorazd BOŽIČ (information given to the best of interviewee's knowledge, without any official approval from Slovenian state authorities) |
| Authority | Laboratory of e-media, Faculty of computer and information science, University of Ljubljana | SI-CERT, Academic and Research Network of Slovenia (ARNES) |
| Education/Training or Degree | PhD | Dipl. ing. comp. sci. |
| Position title | Head of laboratory | SI-CERT Team Manager |
| Task Responsibilities | Teaching, research | |
| If applicable, rel.ship to ENISA | Slovenian representative (alternate) to ENISA Management Board | Slovenian representative to ENISA Management Board |

### Persons who provided input but did not participate in interview

| | | |
|---|---|---|
| Interviewee | Mr Albin Poljanec | Mr Jože Unk |
| Authority | APEK - Post and Elecronic Communications Agency of the Republic of Slovenia | |
| Position title | Specialist for Supervisoin of Telecommunications | |
| Education/Training/ Degree | | |
| Task and Responsibilities | | |
| If applicable, rel.ship to ENISA | | |

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | ARNES SI-CERT |
| Main Tasks | Coordination of security incidents involving networks or systems in Slovenia<br>Distribution of security-related information<br>Providing technical expertise on network security |
| Reports to | Government of the Republic of Slovenia |
| Year established | 1995 |
| URL | http://www.arnes.si/english/si-cert/ |

### Authorities involved but not part of the interview

| Authority | APEK – Post and Electronic Communications Agency of the Republic of Slovenia | Ministry of Economy, Inspectorate for Electronic Communications, Electronic Signature and Post | Administration for Civil Protection and Disaster Relief |
|---|---|---|---|
| Main Tasks | Supervise the quality of emergency call service (operators are obliged to adopt a plan of measures to ensure demanded QoS).<br>Assures compliance with Ministry of Economy prescribed measures that must be adhered to by operators. | Supervises measures in the event of a state of emergency:<br>- how operators adjust their networks so as to give priority to communications from certain network termination points over communications from other network termination points (hereinafter: priority function). | - Administrative and professional tasks related to the organisation, preparation and operation of the system of protection against natural and other disasters;<br>- The communications and information system; |
| Reports to | Ministry of Economy and Administration for Civil Protection and Disaster Relief | Government | Ministry of Defence |
| Year established | 2001 | | |
| URL | http://www.apek.si/en | http://www.mg.gov.si/en/ | http://www.mors.si/index.php?id=13&L=1#42 |

## Scope and governance

Resilience of communications is part of a broader issue, i.e. resilience of critical infrastructures.

A distinction is made between

1) infrastructure owners, whereby Telekom Slovenia d.d., the incumbent operator, owns between 80-90% of all the fixed lines network. The remainder is owned mainly by the two new operators: T-2 d.o.o. and AMIS d.o.o.
2) service providers, whereby Telekom Slovenia (Telekom Slovenije d.o.o) has 98 percent of market share for fixed-line telephony. About 5 percent of subscribers use alternative providers for voice telephony services.

There are eight IP providers of voice services. The penetration of residential fixed telephone lines is 75% of all households in the case of PSTN and ISDN, while VoIP takes nearly 9%. The largest cable operator, in cooperation with a smaller fixed alternative operator, has also started providing voice services using IP.

Broadband penetration stands at 17.3%. There were 347 492 fixed broadband lines in January 2008, many of these based on high-capacity ADSL2+ and VDSL2 technology. Slovenia has three mobile operators. The incumbent's mobile operator is Mobitel d.d. and holds 67% of the customer base, while the main competitor Si.mobil d.o.o. controls 25% of the market.

In the business segment, however, the market leader holds about 85 percent of the market. The new entrant T-2 d.o.o., that is also active in providing fixed telephony services. It started providing GSM services in autumn 2007, based on a national roaming agreement with the market leader. Its infrastructure is limited and it acts primarily as a mobile virtual network operator (MVNO).

### Question 1 : The authorities

The following authorities deal with issues of resilience of public e-communications networks in Slovenia:

- APEK – The Post and Electronic Communications Agency which is an independent regulatory authority;
- The Directorate for Electronic Communications in the Ministry of Economy;
- The Directorate for e-Government and Administrative Processes in the Ministry of Public Administration;
- SI-CERT which is the national CERT run by ARNES (Academic and Research Network of Slovenia); and
- The Administration for Civil Protection and Disaster Relief.

Of course, police and the army also deal with issues of resilience of public e-communications networks.

### Question 2 : The mandate of the authorities

On an operational level, only ARNES SI-CERT and the Administration for Civil Protection and Disaster Relief are responsible for resilience of e-communication networks. Police and army have their own independent systems (e.g.TETRA).

Possible Changes: Currently there is not much being done regarding resilience and dependability of public e-communication networks on a national level.

### Question 3 : Regulatory issues of resilience of public and other essential e-communications networks

A majority of the main bodies (in public sector) are following international standards and best practices in this area (e.g. ISO 27000 family of standards).

The e-Communications Act (see SI 1 in reference list) addresses security of networks but it does not focus on dependability and resilience of public e-communications networks in particular.

### Question 4 : Initiatives between providers and public authorities

Currently, initiatives between providers and public authorities are not known.

## Tasks

### Question 5 : Typical task

Among the typical tasks of the authorities in Slovenia are exchanging information between providers and authorities, audits and enforcement of legislation.

Possible Changes: There is no clear procedure or way that would assess performance regarding resilience in a systematic fashion. APEK should be informed about a disaster but how this works in practice is not so clear.

### Question 6 : Exchange of information between providers and public authorities

Providers in Slovenia are not obliged to exchange information with public authorities.

Possible Changes: In the future there might be some structure or forum in place, where stakeholders from industry and government (e.g., regulator) could discuss resilience and information security issues regularly. In turn, best practices and so forth could be developed.

### Question 7 : Handling of security incidents

Providers do disclose incident information, but on a voluntary basis to security research organizations (or companies). The information is given on an anonymous basis. Legally, providers are not obliged to report security incidents.

Possible Changes: In the future there could be changes regarding when and how infrastructure owners and operators have to report what type of incident (e.g., level of severity).

### Question 8 : Audits related to resilience

Audits typically include procedures according to ISO 27000 and COBIT/ISACA. But there are no audits regarding dependability of public e-communications networks and their resilience.

### Question 9 : Enforcement actions

Local enforcement actions in the area of resilience are not known.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

There is no national risk management process in Slovenia

### Question 11 : The preparedness and recovery measures

Unknown

### Question 12 : Incident response capabilities

SI-CERT (Slovenian Computer Emergency Response Team) was established in 1995 and operates within the national research and education network ARNES. As the name suggests, SI-CERT handles security incidents for all Slovenian networks. Reporting of incidents to SI-CERT is voluntary.

As part of the national research and education network,  SI-CERT has strong ties with the academic community. It is also directly involved in the national Safer Internet project and cooperates with researchers, awareness-raising projects and law-enforcement on various activities. Internationally SI-CERT is well connected with European CSIRT group (TERENA TF-CSIRT) and FIRST (Forum of Incident Response and Security Teams).

Past incidents are analysed for large-scale problems and when identifying new trends.

Possible Changes: Currently it is not clear when, how and what kind of incidents must be reported by an infrastructure owner. Neither is it clear how the quality of service assessment can be used to inform consumers about providers' performance, in turn, empowering consumers to make choices influenced by operator performance statistics including dependability of networks.

### Question 13 : Good practice on resilience

A repository on good practice does not exist.

### Question 14 : Guidelines for procurement

There are no special clauses in procurement guidelines relating to resilience. Only the above mentioned international standards (ISO 27000 and COBIT/ISACA) are implemented.

## References

**SI 1** Zakon o elektronskih komunikacijah [The electronic communications act], Uradni list RS, št. 13/2007 z dne 15.02.2007 [Official Gazzette No. 13/2007, 15.02.2007].
Available: http://www.uradni-list.si/1/objava.jsp?urlid=200713&stevilka=594.
Last access: October 2, 2008.
Non-binding English text
http://www.mg.gov.si/fileadmin/mg.gov.si/pageuploads/DEK/Novi_dokumenti_2008/B.P._Groselj_-_ELECTRONIC_COMMUNICATIONS_ACT_Official_consolidated_version__ZEKom-UPB1_.pdf.

### Additional Resources

none

### Additional Links

SAFE-SI, Slovenian safer internet awareness node, http://www.safe.si.

SI-CERT, Slovenian Computer Emergency Response Team, http://www.cert.si.

# National Report of Spain

## Introduction

### Interview

Date and Duration 2008-09-16 – 120 minutes.

| | | |
|---|---|---|
| Interviewee | Mr Agustín Díaz-Pinés | Mr José Luis Aráez |
| Authority | State Secretary for Telecommunications and Information Society (SETSI) – Ministry of Industry, Tourism and Trade (MITYC) | National Centre for Critical Infrastructure Protection (CNPIC) |
| Position title | Engineer/Technical Advisor | Physical security manager |
| Education/Training/ Degree | MSc. Engineering | MSc. Physics |
| Task and Responsibilities | Technical advice on telecommunications regulation (QoS, broadband, universal service) | Physical security management within CNPIC |
| If applicable, rel.ship to ENISA | n/a | n/a |

People involved in filling out the questionnaire and reviewing contents (not part of interview itself)

| | |
|---|---|
| Participant | Mr Abad Arranz |
| Authority | National Centre for Critical Infrastructure Protection (CNPIC) |
| Position title | |
| Education/Training/ Degree | |
| Task and Responsibilities | |
| If applicable, rel.ship to ENISA | n/a |

### Authorities involved with Network Resilience

| | | |
|---|---|---|
| Authority | State Secretary for Telecommunications and Information Society – Ministry of Industry, Tourism and Trade (**MITYC**) | National Centre for Critical Infrastructure Protection (**CNPIC**) |
| Main Tasks | Provides telecom regulation, develops regulation and policy, submits regulation proposals to ministry | Supports efforts for securing critical infrastructure and economic supply against terrorist attacks. |
| Reports to | Minister of Industry, Tourism and Trade | Secretary of State for Security (Home Office) |
| URL for Agency or Authority | http://www.mityc.es | http://www.mir.es/SES |

| | | |
|---|---|---|
| Year established | | December 2007 |

### Preliminary elements

A general overview of the Spanish electronic communication market[61] shows that the incumbent operator, Telefonica, (in terms of revenue) has about 80% market in fixed telephone service, 48 % of the mobile telephone service and around 63 % of Internet access service. Besides, there are some cable technology fixed communications operators that reach around 54 % of the population (i.e. population having the possibility of cable connection).

One can group mobile network operators into two categories:

1. those having spectrum resources – Telefonica, the incumbent operator, and three others as well as cable operators; and
2. those not having spectrum allocation **-** Mobile Virtual Network Operator (MVNO) that sometimes do not own network infrastructure.

Spain has given four licenses to operate mobile networks: Telefonica has got around 48 % market share, Vodafone 33 %, Orange 17 % and Yoigo (Telia/Sonera) with no more than 1% market share. Mobile virtual network operators (MVNO) have a low market share, less than 1 mio subscribers.

Public electronic communication networks are those used to provide services available to the public. If an electronic communication network does not fulfil this condition it may be exempt from some of the obligations stated in the provisions.

## Scope and governance

### Question 1 : The authorities

The authorities in charge of network resilience issues in Spain are the following:

- *Centro Nacional de Protección de Infraestructuras Críticas* – (CNPIC, the National Center for Protection of Critical Infrastructures), reporting to the Secretary of State for Security (SES, within the Home Office - Ministerio del Interior). This unit was founded in December 2007 and has eleven people staff. Three experts deal with physical security, one to two experts address IT security, resilience and dependability of public e-communication networks (also called logical security) and the rest is for administration and overhead. The creation of the CNPIC is in response to efforts from the European Union (see ES 5 in reference list). CNPIC is supposed to help prepare against and if needed to address terrorist attacks in progress
- *The Secretary of State for Telecommunications and Information Society*

[61] *CMT´s January-March 2008 quarterly report (http://www.cmt.es/es/publicaciones/anexos/IT_08.pdf)*

(Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información – SETSI) and the Ministry of Industry, Tourism and Trade (Ministerio de Industria, Turismo y Comercio – MITYC). The SETSI reports to the MITYC. SETSI is one of the contact points for infrastructure operators and service providers in the telecom industry.

- *The Regional Delegations of the Central Government* (Delegaciones del Gobierno)

As specified in the Telecoms Act (see art 46, ES 1 in reference list), it is part of MITYC's and SETS'sI mandate to ensure that the public service obligation is being met, consumer interests are addressed and spectrum regulation is done according to the law. When it comes to user rights, MITYC promotes Quality of Service, particularly by making QoS transparent, publishing performance data on the internet for consumers to see ES 6).

Possible Changes: On request from the CNPIC, SETSI provides advice regarding telecommunications networks. Beyond this formalized type of collaboration, a modus operandi is needed for better and faster collaborative efforts including informal consultations and joint projects.

**Question 2 : The mandate of the authorities**

The CNPIC is responsible for leading and coordinating activities concerning protection of critical infrastructures. Public electronic communication networks are considered, at least partly, as critical infrastructures. Furthermore, an Agreement of the Council of Ministers entitles the CNPIC as national contact point, concerning critical infrastructure protection, to the European Commission, to other States, and to critical infrastructure owning and managing enterprises or bodies.

The SETSI is concerned with ensuring transparency, including QoS publication:

A) In carrying out a periodic surveillance of Quality of Service parameters, including network parameters (see ES 6 for information and results).

B) When an event causes a disruption of publicly available telephone service (PATS) or Internet access service, that affects more than 100,000 subscribers, the SETSI is the recipient of the compulsory notifications concerning such disruption and may demand correcting actions.

As specified in the Telecommunications Act (see ES 1 in reference list), the MITYC (as well as the Home Office and the Ministry of Defence), within its competences, may submit proposals to the Government (Council of Ministers) to establish security, surveillance, information diffusion, risk prevention and protection measures and systems for facilities associated to the provision of electronic communication services.

Additionally, the MITYC will advise the CNPIC, upon request, on technical matters concerning protection of public electronic communications networks, as well as by requesting and exchanging information with sectoral stakeholders.

By certain large service disruption events, the Regional Delegations of the Central Government are in charge of leading and coordinating stakeholders providing critical services (health care, security, defence, etc.) using telecommunication networks, electronic communications network providers, other authorities and stakeholders, to enable service recovery.

The Regional Delegations of the Central Government (Delegaciones del Gobierno) play an important role in such large network failures. They are involved on a case-by-case basis. For instance, two years ago a submarine cable was cut. As a result, Melilla (on the African coast) was without communication to the Spanish mainland. In turn, an ad-hoc working group chaired by the Regional Delegation of Melilla was formed involving telecom operators (Telefonica), hospital managers, defence and security authorities and so forth. It was in charge of coordinating different stakeholders, setting priorities, exchanging information and allowing for recovery.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

Spain follows the principle-based approach when it comes to standards. This is preferable to rule-based ones[62] In turn, practical approaches are developed. There is no specific regulation pertaining to resilience and dependability of networks in the Telecommunication Act itself. It would be the legislation to place such requirements. Neither has the CNPIC so far come up with a recommendation regarding regulation and resilience of e-communications networks. Once CNPIC will come forward with guidelines they will focus on how infrastructure protection can be improved including the electricity grid.

Major electronic communications providers are obliged (see ES 3) to carry out a quarterly publication of QoS parameters (services concerned: fixed publicly available telephone service (fixed PATS), mobile PATS, Internet access and directory service).

Additionally, electronic communications providers are obliged to report to the SETSI any disruptions of PATS or Internet access service, that affect more than 100,000 subscribers. Additionally, the SETSI may demand correcting actions.

The Regulation on the provision of electronic communications services, universal service, and user protection (see ES 4) forces electronic communications network providers and public telephone service providers to guarantee their networks´ integrity.

The above mentioned proposal (Q2) made by MITYC, Home Office and Ministry of Defence to establish security, surveillance, information diffusion, risk prevention and protection measures and systems is still to be made.

[62] *Principle-based standards or guidelines outline the objectives but leave it to the operator to decide how to fulfil or reach these. However, the operator must be able to demonstrate that best practice was being followed or else be able to justify not doing so, while achieving the objectives set regarding network resilience.*

Possible Changes: It is hoped that the CNPIC will develop some new guidelines regarding infrastructure protection and resilience and dependability of public e-communication networks in particular.

### Question 4 : Initiatives between providers and public authorities

Telecommunications operators provide information (as stated in Art. 9 of Telecom Act) regarding their infrastructures to the MITYC (compulsory upon request, when it is needed for enforcing the Telecommunications Act or other provisions).

Incident Management Committees are formed by the Regional Delegations of the Central Government (Delegaciones del Gobierno), in events of large service disruption affecting critical services (health care, security, defence, etc.). The SETSI, critical services managers and involved electronic communication providers take part in these committees and exchange information with each other, set priorities and collaborate within their competence scope.

Topics addressed deal with these regarding disruption events, such as:

- elements involved,
- expected recovery time and actions,
- contingency measures,
- priority setting,
- possible causes, and
- damages
- measures to be taken to avoid similar future incidents.

There are similar initiatives among providers. For instance, telecommunications operators have their own risk preparedness and management plans. However, there is no information exchange group in operation where telecom providers and infrastructure owners meet on a regular basis to address resilience and/ or security issues including dependability of networks.

Nevertheless, telecom network owners and service operators have got their own coordination bilateral mechanisms, such as a committee addressing technical issues, including network resilience. For instance, a service operator using a network infrastructure that it does not own must be in close contact with the infrastructure owner.

The advisory Committee CATSI[63] advices the MITYC on issuing provisions (such a regulation, a Law, etc) regarding MITYC´s role as policy maker. It is compulsory that MITYC requests CATSI´s advice (see ES 7). It meets 2-3 times a year (2008-07-18 last meeting). Often 20-25 people attend representing such stakeholders as the MITYC, consumer groups, telecom operators, disabled users, representatives of unions and infrastructure owners.

[63] *Consejo Asesor de Telecomunicaciones y de la Sociedad de la Información – Advisory Committee on Telecommunications and Information Society – see ES 7 in reference list*

This committee is not focusing on resilience of public e-communication networks in particular but all issues pertaining to telecommunication services and markets. Nevertheless, the regulator may push for changes in the resilience and dependability domain without first having to get CATSI advice.

Possible Changes: The Central Government (at the proposal of MITYC, Home Office and Ministry of Defence proposals), must establish security, surveillance, information diffusion, risk prevention and protection measures and systems. These have yet to be established.

## Tasks

### Question 5 : Typical task

The SETSI exchanges information with providers on large disruption events (as mentioned above and may demand correcting actions.

While operators must inform in case of such events, these are relatively rare incidents. In severe cases such as the submarine cables in Melilla or Canary Islands , information is, of course, collected and data are being analyzed to learn from the incident.

Telecom providers must report quality of service parameters. These data are annually checked by an external auditor to see if the procedures used were compliant with the agreed criteria and procedures. However, these measures focus on quality and not necessarily resilience (ES 5 and ES 6 – see also answer given for Q 9)

Neither operators nor infrastructure owners have been fined recently due to problems regarding network resilience and dependability (see also Q 9 for number of investigations and fines issued in Spain).

Possible Changes: Developing a working group between operators, regulators and critical infrastructure owners to exchange ideas and develop best practices for improving network resilience and dependability. Such best practice may then be applied by infrastructure owners and assessed on a regular basis. The findings could be shared to accelerate learning and improve resilience further while keeping things practical.

### Question 6 : Exchange of information between providers and public authorities

The CNPIC requests information about electronic communication networks from SETSI, which collects the information from providers. As a result, SETSI asks infrastructure owners and service providers to share a summary of recovery plans, of which infrastructure is considered critical, of business continuity plans and so forth.

Possible Changes: SETSI may check the quality of the information, for instance, when having some serious doubts about the quality of the information it got from the infrastructure owner. SETSI may decide to conduct a spot check (e.g., operator claims to have an exchange in a remote area, we could visit the site to confirm that it really does exist).

Important is to understand that while the possibility of undertaking inspections exists, it depends on the nature of the information. When it comes to network resilience, currently there are no inspections undertaken. Two reasons can be given

1) this is not one of the specific area in which SETSI has been given the human capital required, and
2) this is not an area for which there is ad-hoc regulation providing the legal foundation needed to conduct spot and other checks regarding network resilience.

**Question 7 : Handling of security incidents**

In cases such as the above mentioned large disruption events (e.g., Melilla), the involved telecommunications operators will provide SETSI, on a mandatory basis, with the following information:

a. During the first 2 hours of disruption: preliminary report identifying the event (including physical location, starting time, end-users involved, possible causes, on-going correcting measures and scheduled recovery time).
b. If the event lasts more than 6 hours: any necessary reports to update the initial information, a report including the adopted measures and any additional information requested by the SETSI.
c. By the end of the event, during the following 2 hours: closing event report, including exact time of recovery of each element involved.
d. During the following 10 days after the recovery: a thorough report including, among other aspects, the disruption scope, affected users and damages, compensating actions, cause assessment, correcting measures and recurrence likelihood assessment.

Data submitted are treated as being confidential. Information about such large disruption events (such as disasters caused by nature such as avalanches or flooding, expected recovery time, contingency measures, possible causes, damages, etc …) is exchanged within the Incident Management Committees established by The Regional Delegations of the Central Government (Delegaciones del Gobierno .- see Q 5)

**Question 8 : Audits related to resilience**

Audits do not take place.

**Question 9 : Enforcement actions**

The Telecommunications Act includes an infringement procedure for non-collaborating providers. Fines and penalties can be imposed for not meeting obligations. Each regulatory authority may impose fines within its competence scope, as stated in the Telecoms Act.

Some figures about penalty procedures issued by the Secretary of State for Telecommunications are provided in the table below. It lists the procedures issued each year and the total yearly amount of imposed fines. Inspection and penalties regime is addressed in Title VIII of Telecommunications Act (art. 50 and on – see ES 1 in reference list).

| | 2004 (since 1/4/2004) | 2005 | 2006 | 2007 | 2004-2007 |
|---|---|---|---|---|---|
| Number of procedures started | 1,456 | 1,706 | 2,335 | 1,727 | 7,224 |
| Number of procedures finished | 1,350 | 1,501 | 2,675 | 2,396 | 7,922 |
| Total amount of fines imposed | 1,485,919 € | 9,336,150 € | 9,340,605 € | 3,815,681 € | 23,978,355 € |

**Infringement procedures and penalties issued by the Ministry of Industry, Tourism and Trade**

Title VIII of Telecommunications Act (art. 50 and on) also provides some examples of possible reasons to issue an infringement procedure and eventually impose a fine, such as:

a. the hindering of inspection processes and lack of cooperation during a required inspection. (art. 53 k);
b. the repeated failure to meet the requests for information submitted by an authorized Government Agency, while performing its functions. (art. 53 p);
c. "serious or repeated failure by the operators to meet the conditions for rendering services or operating electronic communications networks. (art. 53 s).

## Risk Management and preparedness measures

### Question 10 : The national risk management process

There is none at this point. It is also unclear how the CNPIC uses the information it collects for a risk assessment procedure as far as the critical infrastructure is concerned.

Possible Changes: Critical infrastructure (e.g., water, electricity, communications) need to be included in a national risk assessment process. In turn, a national telecommunications emergency plan can thenbe developed with the operators outlining what must be done in case of an emergency or terrorist attack.

As well, exercises are needed to test if measures put in place to manage these risks are satisfactory and to allow the various agencies participating (e.g., power outage simulation) to share information and improve their response capabilities accordingly.

### Question 11 : The preparedness and recovery measures

Until now, neither preparedness nor recovery measures to mitigate risks affecting the resilience of public networks exist. This work is in progress and it is expected that a definition of requirements will be agreed upon in the near future. However, the measures must be issued by CNPIC once they have been agreed upon.

## Question 12 : Incident response capabilities

INTECO is a public body and acts as a CERT for citizens and SMEs., including issuing alerts and so fort (see additional links in reference list). The Spanish GovCert is CNI-CCN (see reference list) elorates guidelines to guarantee security of governmental ICT systems.

It is unclear what kind of formalized procedure Spain uses if any to analyze data and issue recommendations.

## Question 13 : Good practice on resilience

Not developed at this point.

## Question 14 : Guidelines for procurement

Not until now. There is no standard clause on e-communications security or pertaining to resilience. Nevertheless, this does not stop government departments and agencies from carrying out procurement procedure concerning electronic communications that include security requirements to be fulfilled by the providers.

Due to the specific nature of such procurement, it makes sense that setting up such requirements is decided by the public body in charge of the procurement procedure

## References

**ES1** Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (Telecommunications Act) – published 4/11/2008.
Available: http://www.boe.es/boe/dias/2003/11/04/pdfs/A38890-38924.pdf, for update see, http://noticias.juridicas.com/base_datos/Admin/l32-2003.html.
Last Access: September 19, 2008.
Particularly relevant is article, 4.4.

**ES 2** Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril. (Regulation regarding conditions for electronic communications services provision, the universal service and users´rights protection) – published 29/4/2005.
Available: http://www.boe.es/boe/dias/2005/04/29/pdfs/A14545-14588.pdf, updated version http://noticias.juridicas.com/base_datos/Admin/rd424-2005.html.
Last Access: September 19, 2008.
Particularly relevant are articles: 18, 19 and 34.

**ES 3** Orden Ministerial ITC/912/2006, de 29 de marzo, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas (Ministerial Order on conditions of quality of service for electronic communications services provision) (2006-03-31). **BOE** Nr. 77, pp. 12464 – 12438.
Available: http://www.mityc.es/NR/rdonlyres/199573A0-803F-4293-AFE7-DAEB5A679310/0/10OrdenCalidad_ITC912_2006.pdf, updated version http://noticias.juridicas.com/base_datos/Admin/o912-2006-itc.html.
Last Access: September 19, 2008.
Ministry provision concerning quality of service conditions for the provision of electronic communications services.
Particularly relevant is Chapter VI.

**ES 4** REAL DECRETO 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. (Ministerial decree - universal service – requirements and protection of users) (2005-29-04). **BOE** Nr. 102, pp. 14545 – 14588.
Available: http://www.usuariosteleco.es/NR/rdonlyres/34C7AE5C-0402-4BE1-95F4-2ADC0E55DB44/0/RDServicioUniversal2005.pdf, updated version http://noticias.juridicas.com/base_datos/Admin/rd424-2005.html.
Last Access: September 19, 2008.

**ES 5** COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Critical Infrastructure Protection in the fight against terrorism - COM(2004) 702 final. 2004-10-20.
Available: http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf Last Access: September 19, 2008). Spanish version: http://eur-lex.europa.eu/LexUriServ/site/es/com/2004/com2004_0702es01.pdf.
Last Access: September 19, 2008

**ES 6** Consejo de Ministros (Council of Ministers) (Nov. 2007) Centro Nacional de Protección de Infraestructuras Críticas – (CNPIC) (the National Center for

Protection of Critical Infrastructures) [decision made to establish CNPIC - reporting to the Secretary of State for Security (SES, within the Home Office - Ministerio del Interior)]. Confidential document in Spanish.

**ES 7** CATSI (Consejo Asesor de Telecomunicaciones y de la Sociedad de la Información – Advisory Committee on Telecommunications and Information Society), it is regulated by Regulation 1029/2002, on members and procedures of CATSI. Available: http://www.mityc.es/NR/rdonlyres/3901EE59-8EEA-494F-99EE-21C90CEBAE18/0/RD1029_2002.pdf – short summery is provided here http://www.mityc.es/Telecomunicaciones/Organizacion/Consejos/ConsejoTeleco.htm.
Last Access: September 23, 2008.

## Additional Resources

**ES 6** Regularly published results from findings concerning quality of service conditions for the provision of electronic communications services.
Available:
http://www.mityc.es/Telecomunicaciones/Secciones/CalidadServicio/2informe/.
Last Access: September 19, 2008.

## Additional Links

INTECO (Instituto Nacional de Tecnologías de la Comunicación – National Institute for Communication Technologies) – Spanish Gov. Cert, http://www.inteco.es/.

INTECO CERT, http://www.inteco.es/rssRead/Security/INTECOCERT_1.

INTECO Information Security Observatory, http://www.inteco.es/Seguridad/Observatorio.

CCN-CERT (Centro Criptológico Nacional – National Chryptology Center) – Spanish GovCERT / reports to the Minsitry of Defence, http://www.ccn.cni.es/quienes_somos.html.

# National Report of Sweden

## Introduction

### Interview

Date and Duration 2008-08-27 – 105 minutes.

| Interviewee | Mr Björn Scharin | Mr Per Bergstrand | Mr Eric Wedin | Mr Staffan Lindmark |
|---|---|---|---|---|
| Authority | PTS - Security and Addressing Unit | PTS - Security and Addressing Unit | PTS - Robust Electronic Communications Unit | PTS - Security and Addressing Unit |
| Position title | Senior adviser | Expert advisor | Senior adviser | Legal adviser |
| Education/Training or Degree | Informatics | Lawyer, LLM | | Lawyer, LLM |
| Task and Responsibilities | Internet security, electronic signatures, secure electronic communications | Internet security, privacy | PPP, resilience projects | secure electronic communications |
| If applicable, rel.ship to ENISA | Swedish NLO | | | |

### Authorities involved with Network Resilience

| | |
|---|---|
| Authority | Swedish Post and Telecom Agency (PTS) |
| Main Tasks | The Swedish Post and Telecom Agency (PTS) monitor the electronic communications and postal sectors.<br>'Electronic communications' includes telephony, the Internet and radio. The Agency works with consumer and competition issues, efficient utilisation of resources and secure communications. |
| Reports to | Ministry of Enterprise, Energy and Communications |
| Year establish-ed | 1992 |
| URL | http://www.pts.se |

### Authorities involved with network resilience but not part of the interview

| Authority | Ministry of Enterprise, Enrgy and Communications | Swedish Emergency Management Agency (SEMA)[64] |
|---|---|---|
| Main Tasks | Electronic communications<br>http://www.sweden.gov.se/sb/d/2156/a/19950<br>The objective of electronic communications policy is to ensure that individuals and government agencies have access to efficient and secure electronic communications. These electronic communications should be the most worthwhile possible in terms of choice of transmission services, price and quality. In these respects Sweden should be at the forefront of international developments. Electronic communications should be sustainable and useable and should accommodate the needs of the future.<br>The primary means to this end should be to establish conditions for effective competition, free of distortion and limitations, and to promote international harmonisation. The state should bear responsibility in areas in which public interests cannot be satisfied by the market alone. For more information, see information leaflet on Electronic Communications Act to the right<br>The overall policy objective for electronic communications, IT and postal services is to ensure that everyone has access to an infrastructure and associated public services that are efficient in terms of the economy as a whole and sustainable in the long term | SEMA co-ordinates the work to develop the preparedness of Swedish society to manage serious crises.<br><br>SEMA works together with municipalities, county councils and government authorities, as well as the business community and several organisations, to reduce the vulnerability of society and improve the capacity to handle emergencies. It has overall responsibility for information assurance in Sweden, conducts IT security analyses and gives advice and issues recommendations |
| Reports to | - | Ministry of Defence |
| Year established | - | 2001 |
| URL | ☐http://www.regeringen.se | http://www.krisberedskapsmyndigheten.se |

[64] *SEMA defines crises as:*
... events that disrupt the functioning of society or jeopardize the conditions to govern the life of the population. They include serious crises in times of peace as well as war. Such situations demand good emergency management if they are not to undermine confidence in the Government and authorities and potentially threaten the national security and democracy of Sweden
(http://www.krisberedskapsmyndigheten.se/templates/Page 19.aspx)

Sweden does have about 460 service providers. About 10-20 of these, own their infrastructure. There are over 160 smaller networks, for instance owned by the energy company within a municipality. However, these are usually in smaller communities only.

The largest 10 operators have above 90% market share. Market competition plays an important role when it comes to resilience. Accordingly, if customers demand better dependability and reliability, operators try to offer acceptable levels of resilience to survive in the market. Sweden follows the philosophy that market demand (e.g., public procurement) and regulation can create a business environment that rewards operators delivering the goods.

Under Sweden's regulatory regime a network that is open for anybody to connect to is considered a public e-communication network. Private networks are not public. Very small networks, for instance within a building complex, are not deemed public.

To illustrate, envision an e-communication network used by banks to serve their Automated Teller Machines (ATMs or cash dispensers). If this network uses telecom services or infrastructure from the operators it is labelled a public network and does, therefore, fall under PTS regulation.

## Scope and governance

### Question 1 : The authorities

The Swedish Emergency Management Agency (SEMA) is responsible for the coordination of information security and preparedness for crisis management. The Swedish society is divided in to different sectors, electronic communications, water, energy, food etc. There is a responsible authority for each sector. The National Post and Telecom Agency (PTS) is responsible for the electronic communications sector, and also for issues regarding network resilience for public electronic communications network and services.

The various agencies involved report to different ministries. For instance, PTS - the communication regulator - reports to the Ministry of Enterprise, Energy and Communications, while the Swedish Emergency Management Agency (SEMA) reports to the Ministry of Defence.

Accordingly, the interview partners stressed that because Sweden considers itself an open society, it is expected that issues pertaining to resilience of public e-communication networks are communicated to the public using various channels such as traditional media and the internet.

Moreover, while the Swedish system is not as centralized as others are. When it comes to telecom issues, including regulation, PTS is involved. For instance, PTS provides an annual risk assessment report regarding telecommunication that it submits to SEMA as do other sectors for instance the energy sector. SEMA then use this to make a risk assessment and submit it to the Ministry of Defence.

The police and blue light agencies (e.g., fire) have their own network that functions under their own rules and legislation. Nevertheless, PTS assesses the public electronic communications issues. The same is true for the energy sector and the electricity grid in Sweden.

**Question 2 : The mandate of the authorities**

The Electronic Communications Act forms the basis of all regulation regarding telecommunication (see PTS1 in reference list). The ordinance on instructions for The Swedish Postal and Telecom Agency (see PTS2) explains the purpose of the agency.

PTS's organizational chart[65] on the web shows that it has 10 departments. One of these is the Network Security Department. It describes its mission as follows:

> *Responsible for PTS's work with robust communications and issues concerning security, integrity and addressing; for example, supervision and the numbering plan* (http://www.pts.se/en-gb/About-PTS/Organisation/ scroll down).

The Network Security Department has the following units:

A) Security and Addressing Unit – deals with regulatory issues regarding e-communication networks (16 staff whereas two on temporary leave)
B) Robust Electronic Communications Unit – addresses resilience and works with operators to improve dependability and reliability of e-communication networks (five staff)
C) Swedish IT Incident Centre, SITIC (currently 11 staff and hiring another two) (see SE3 in reference list)

In the context of this survey, we focus on units A and B and less on C.

*Robust Electronic Communications*: This unit has an annual budget of about 200 mio Kroner (about € 22 millions) to support collaborative efforts to help improve resilience. For instance, during 2007 the unit was participating in 91 projects. If labor and other resources would have permitted, possibly the unit would have been active in 200 projects.

One of the important projects is MIMER-P (Multipurpose Information Management and Exchange for Robustness Prototype) that is co-financed by the European Commission within the framework of European Programme for Critical Infrastructure Protection and other agencies and telecom operators in Sweden (see MI 1 in reference list – also addressed in Q4 and Q6 in more detail).

The *Security and Addressing Unit* also enforces regulatory issues regarding privacy and data protection in electronic communications.

[65] http://www.pts.se/en-gb/About-PTS/Organisation/ *scroll down to see the organization chart.*

Important is that sometimes Unit B may have information that is not passed on to Unit A. The latter is required to enforce regulation (the stick). In contrast, Unit B focuses on collaboration and improvements (the carrot). Therefore, it tries to create an environment of trust and confidence that encourages operators and providers to work with them to improve network resilience.

Nevertheless, both units report to the same manager within PTS. The Security and Addressing Unit has more staff. Nevertheless, the Robust Communications Unit has a larger budget. This is primarily due to PTS also being able to co-share financing and research efforts regarding resilience that are considered to be of critical interest to Swedish society.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

The Electronic Communications Act (2003:389) (see PTS 1 in reference list) does address resilience in chapter 5 article 6a. This part of the law has been translated (PTS 1) except for this critical article. An unofficial translation looks like this:

> *"A party that provides a public electronic communication service or a public electronic communication network shall ensure that the service and the public network satisfy reasonable demands for good function and technical security and also for sustainability and accessibility in the case of extraordinary events during peacetime [Chapter 5, Section 6a of the Electronic Communications Act (EkomL)]."*

During 2005, Sweden experienced a very bad storm. During that time, the above act applied to fixed line networks only. The storm and experiences from it forced the country to revisit this issue. Hence, Article 6a does now apply to all public e-communication networks while the prior article was limited to fixed line telephony. PTS consulted with operators and others to issue a regulation that would apply Chapter 5, Article 6a (see PTS 1) to all networks (e.g., wireless and cable). This was agreed upon and the result was PTSFS 2007:2 (see PTS 6).

Sweden follows the principled-based standard approach[66]. Accordingly, in contrast to rule-based standard[67] descriptions regarding continuity planning as well as incident planning are quite general. In turn, much interpretation is left to the operator who experiences pressure by the market to provide adequate resilience at a competitive price. As well, regulations require that operators demonstrate adequate measures were taken to assure satisfactory reliability and dependability of public e-communication networks (see also PTS 4, 5 and RP1, 2, 3 in reference list).

[66] *Principle-based standards or guidelines outline the objectives but leave it to the operator to decide how to fulfil or reach these. However, the operator must be able to demonstrate that good practice was being followed or else be able to justify not doing so, while achieving the objectives set regarding network resilience.*

[67] *Rule-based standard may be prefered by operators since they reduce the risk for litigation, as long as one can show that one has followed the specified rule by the letter. For instance, in the litigious US legal system prescriptive rules make it easier for one to demonstrate that one has followed the rules and, therefore, the law.*

A major supervision activity was with 55 service providers and infrastructure owners. It started during fall of 2007 and finished during spring 2008.

**Summary of findings**
The Swedish Post and Telecom Agency's (PTS) "General Advice on good function and technical security" has been available since May 2007. The General Advice explains the provisions and serves as PTS's recommendations as to how security work can be carried out in order to fulfil the requirements laid down by the Electronic Communications Act (LEK). In this case, security work means preventing interruptions, interference and disruptions by carrying out risk analyses and risk management, planning for the management of inter-ruptions, interference and disruptions and following them up when they occur.

In the autumn of 2007 and spring of 2008, PTS carried out scheduled supervision of compliance with the provisions concerning good function and technical security. These are the overall conclusions of this supervision:

- Security work is being carried out and the provisions contained in LEK and PTS's General Advice are largely complied with

- Increased focus on security work among service providers

- Security work should be documented to a greater extent

- Service providers without own technical infrastructure should also carry out security work

- Management should assume responsibility and more often follow up security measures that are taken

The results and conclusions presented in this report are based on a questionnaire and subsequent follow-up interviews. The supervisory work encompassed 53 service providers, which together represent a very large proportion of all end users in the Swedish market. Five service providers were selected for follow-up interviews based on the questionnaire responses.

The aim of such supervisory work includes spreading awareness of how security work can be carried out to comply with the provisions concerning good function and technical security in order to promote preventive work and preparedness for the management of interruptions, interference and disruptions on the part of service providers. The anticipated impact of supervision is an increased proportion of service providers carrying out regular and systematic security work[68].

Planning for 2009 supervision activities has begun. Based on the data gathered during the 2007/2008 exercise, it must be decided which operator and or which area will be assessed again. Most important will be to determine what we will address with the operator and

[68] *A summary of the report on the supervision and its findings can be viewed here:* *http://www.pts.se/upload/Rapporter/Internet/2008/Tillsyn-god-funktion-och-teknisk-sakerhet-PTS-ER-2008-13.pdf*.

where the company has to improve based on the results achieved during the 2007/2008 supervision exercise.

Possible Changes: Regulation regarding Universal Service Obligations (USO)[69] exists in Sweden. However no operator has been issued any obligations under USO. Traditionally the incumbent TeliaSonera has been the provider of fixed telephony access. However, in recent years this has become a challenge because the operator does not longer repair or deploy fixed lines in the more rural areas.

PTS is at the moment evaluating different approaches to the USO-problem. One way is to have a type of USO-obligation with some operators for particular geographical regions. There is also a financial issue since the costs could be exorbitant.

Finally, the Robust Communications Unit uses a three year strategy to decide prioritized areas. In turn, this may result in a shift of funding priorities for resilience work regarding public e-communication networks.

**Question 4 : Initiatives between providers and public authorities**

There are specific topics to be addressed but usually with our supervision, the focus is on a 12 month timeframe.

In 2008, the Robust Communications Unit is involved in 91 projects. A description of some of the projects follows here.

One important activity has been the co-financed MIMER-P activity (see also Q2 and Q6 for more details). Here, participants come from Spain, NL, FI and NO. The idea is to get a common feel on how to report errors (see MI 1). A pre-cursor of this is already running for customers on TeliaSonera’s website (see MI 2 in reference list).It is a web-based software that allows operators to get an idea where problems may be happening right now in their networks. The tool helps in visualizing these effects.

One other important project deals with geographical data for construction and repair work. Before doing constructions anywhere, a contractor can access the system to see if there are other infrastructures, such as water pipes or power lines or fibre optics cable, in the geographical area nearby the construction site. Hence, eventually the system will offer a national system for parties to check first before starting to dig. In turn, this helps reducing the risk for power outage or network failure due to cutting lines.

[69] *Universal service obligations (USO) guarantee universal access. USO is referring to a set of general interest requirements to be satisfied by telecommunications and postal service operators throughout the country. The object of the resulting obligations is to make sure that everyone has access to certain high quality essential services at prices they can afford.*
*To attain this service level, an operator can be given special provisions and funding. In turn, it has to meet very strict quality and security levels and enforcement of regulation is clearly defined and applied. For instance, availability of connection, number of fault reports per connection establishing satisfactory performance and repair time in case of incident is specified. Failure results in funding being cut accordingly.*

The Robust Communications Unit has, in cooperation with four mobile operators purchased 30 mobile base stations to be used in areas where problems with coverage occur. Operators have 5-10 mobile base stations each. They are free to use the units when extra capacity is needed. For instance, during winter events or musical festivals additional capacity might be needed, even though there is no crisis at hand[70].

The unit is responsible for National Telecommunications Crisis Management Co-ordination group. This group's membership is based on experience gained from past national cross-sector exercises. For instance, the storm "Gudrun" provided information that is now used to further improve resilience of e-communications networks. The group is a voluntary co-operative forum with members from:

- major telecommunications providers as well as
- the Swedish Urban Network Association,
- the Armed Forces,
- the National Post-and Telecom Agency, and
- PTS.

PTS chairs this group. The group has the aim to support the restoration of the national infrastructure for electronic communications during critical disturbances in our society, such as terrorism, extreme weather. The individuals within the group representing each member are of great importance for their own network operation. The group meets 'virtually' and uses secure communications.

As well, PTS together with the Swedish Urban Network Association (SSNF) developed recommendations regarding robust nodes, robust networks and documentation of networks (see RP2).

## Tasks

### Question 5 : Typical task

As mentioned earlier, Sweden follows the idea that less regulation and using a principle-based approach is more practical and better for the economy. As outlined under Q3, during 2007 through 2008 PTS (i.e. the Security and Addressing Unit) conducted a major supervision activity with 55 service providers and infrastructure owners (see also exercise results discussed in Q 3).

The above work can then be used to develop new regulation and advice with the operators. In turn, follow-up supervision can help in assuring that laggards are catching up next year. Moreover, risk exposure can than be reduced.

[70] *Find out more information regarding this effort about mobile base stations here: http://www.pts.se/upload/Faktablad/SE/Faktablad_mobila_W.pdf (Information in Swedish)*

While penalties can be applied to a violator, none have been issued within the last 12 months regarding resilience. However, incidents are investigated and the information collected may result in the regulator leaning on the operator to change or else face tougher regulation (see also Q9).

**Question 6 : Exchange of information between providers and public authorities**

There is no fixed format on how to report an incident. However, the forerunner of MIMER-P is the beginning for raising awareness. It will help systematize and arrive at a common approach for reporting incidents that affect network reliability and dependability (see MR 1 and MR" – also Q2 and Q4 for more details). MIMER-P is one approach for finding a better way to share and exchange information about the networks. It also helps reduce the number of calls made by the public to the service centres and offers answers and solutions online for customers. Information from MIMER-P is applied to address the following issues:

a. Where is what kind of disturbance?
b. Who is affected by the communication network disruption or failure?
c. When will the disturbance be over?

In turn, it enables users and consumers to switch their operator with the help of this information. The main collaborators are the utilities because without power a public e-communication network cannot function. Nevertheless, when the utility tries to repair power lines or a transformer station, communication with people involved is a necessity.

In Sweden, whenever dependability and reliability become an issue, the root is very likely the power supply (see also RP 2).

Possible Changes: Information exchange with providers is being done on a regular basis. The same cannot be said for suppliers of network hardware and software. There might come a time when such information exchange becomes more important. Ever more often network problems relate to power supply and software glitches. Considering such issues when designing hardware and software as well as building more reliable and dependable architecture into networks helps reduce risk exposure (e.g., see RP 2 or RP 5 for why this could matter). There is more information about this also under Q 13.

**Question 7 : Handling of security incidents**

Consumers can call in their concerns to their operators usually between 7:00 to 22:00 hours. Accordingly, consumers call operators about network failures or issues affecting reliability and dependability of public e-communication networks. Often, before they call the operator, consumers try to investigate themselves by using an online facility. An example would be TeliaSonera's 'forerunner' of MIMER-P (see MR 2) (See also Q5 – learning and improving risk management).

PTS is reachable 24/7 for operators and other authorities within the crisis management system. Based on an incident, the Robust Communications Unit may ask for improvements from the operator (see also PTS 4, 5, 6). Usually, the latter follows these suggestions. This approach seems to work fine in Sweden (see also RP 2, 3, 4 in reference list).

### Question 8 : Audits related to resilience

See also Q3 and Q5. Sweden prefers to conduct supervision activities instead of full-blown audits. All regulatory work is conducted by the Security and Addressing Unit (the regulatory folks – see Q2). Whilst it may hire outside experts to do part of the job, it will keep responsibility and will be the lead on the project.

The Robust Communications Unit stays away from such work because its focus is to work closely together with operators to improve resilience. Enforcing regulation, however, might jeopardize trust and reduce operators' willingness to share information

### Question 9 : Enforcement actions

While penalties can be applied to a violator, none have been issued within the last 12 months regarding resilience. However, incidents are investigated and the information collected may result in that the regulator demands that the operator improves security and takes action to avoid that the same incident would occur again leaning on the operator to change or else face tougher regulation (see also Q 5). Issuing fines or penalties is somewhat against our philosophy that follows the mantra – fix it before it results in network problems (see also PTS 6, RP 2).

## Risk Management and preparedness measures

### Question 10 : The national risk management process

An agency that manages ordinances and regulations needs also to consider risk management. The regulator will use information provided to decide which activities should be prioritized for next year (e.g., RP 1).

SEMA does require an annual assessment of risks regarding each sector. Telecommunication is part of this. In turn, the regulator submits a risk assessment report regarding telecommunication and public e-communication networks.

Insights gained from this work may help the regulator to decide which areas require more attention to improve risk management (RP 2).

### Question 11 : The preparedness and recovery measures

A good example here are the Telö exercises. The last one happened in 2007 (see SE 4 in reference list). The exercise uses an overall scenario. During 2007, weather had caused serious disruptions to telecommunication and internet services. The scenario required that members of the National Telecommunications Coordination Group had to work closely together to address the challenges[71].

Until now, neither preparedness nor recovery measures exist that could mitigate risks affecting the resilience of public networks. This work is in progress. Expectations are that it will arrive at a definition of requirements soon.

Another interesting matter here is that such issues are very much an operator challenge. To generate revenue, the operators need to get their mobile network up as fast as possible if it was ever down or avoid having it down in the first place.

The operator has no obligation to inform the regulator on planned or unplanned outages. The operators do, however, have to inform the PSAP (responsible for the 112 emergency service) on planned and unplanned disturbance and outages. The regulation (PTS 7 in reference list)[72] does not address any fixed availability obligation.

**Question 12 : Incident response capabilities**

There are several CERTs operating in Sweden. These exchange information with each other informally but not using a standardized procedure. They are all, however, connected to the international community (e.g., Government Cert meets with other ones from around Europe). All are members of FIRST and TF-CSIRT. The Government CERT (see SE 3 reference for more information) addresses issues pertaining to government networks. Sitic is involved in the European governmental CERT network, EGC. Sitic is also involved in a Nordic network of CERT’s including governmental and academia, NCF (Nordic Cert Forum). Sitic have 24/7 incident response capability.

CERTs have little to do with resilience or the issue of dependability and reliability of public e-communication networks. They do spread vulnerability information in advance, mange incidents during occurrence.

Possible Changes: Currently Sweden does not have a regulation that addresses reporting of incidents. Hence, how reporting is done is open to interpretation.

There are pros and cons regarding voluntary reporting of incidents. Voluntary reporting is all about establishing trust and competence and the added value to report. The ones reporting is getting an added value and valuable help in managing the incidents rather than an obligation to report.

Because of this regulation being missing, it is not easy to discuss reporting of incidents and exchanging information freely. One could conclude from this that some kind of regulation would make it easier to share such information between operators and the

*[71] A factsheet has been published in Swedish about the exercises that can be downloaded here: http://www.pts.se/upload/Documents/SE/Faktablad_NTSG_W.pdf. Member States interested can obtain an English summary directly from the regulator.*

*[72] The current regulation will be replaced this October but there will be no changes regarding the described obligation.*

regulator on a confidential basis. But our interviewees felt that such an approach would not necessarily be the most suitable for Sweden.

**Question 13 : Good practice on resilience**

There is no repository for good practices on resilience.

However, a strategy for improving robustness exists as well as does regulation that should help to build more robust networks and network nodes. These efforts focus on organisations that build infrastructure (e.g., PTS 5, 6, RP 1, 3, 4 in the reference list).

Information exchange between the regulator and vendors is limited. Consultations are indirect, whereby operators may bring vendors to meetings. As well, informal discussions may be held with a vendor (see also Q 4). However, if the regulator talks with vendors, such as Alcatel-Lucent or Ericsson, it is usually about technology. Even if a vendor runs a network, the firm does it as sub-contractor to a telecom provider. Hence, Sweden’s regulator talks to the infrastructure owners who are responsible.

**Question 14 : Guidelines for procurement**

Until now Sweden has not had guidelines for procurement. However, work began in 2007 to arrive at guidelines regarding procurement for companies and the public sector. The idea is that having such guidelines will help corporations and public organizations to demand better resilience when purchasing networks, infrastructure and services.

## References

**PTS 1** Lagen (2003:389) om elektronisk kommunikation [The electronic communications Act (2003:389).
Available:
http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=2003:389.
Last Access: September 3, 2008.
English non-binding version[73],
http://www.pts.se/upload/Documents/EN/The_Electronic_Communications_Act_2003_389.pdf.
Particulary relevant are: Chapter 5 article 6a and 7, All of Chapter 6.

**PTS 2** Förordning (2007:951) med instruktion för Post- och Telestyrelsen, (Ordinance on instructions for The Swedish Postal and Telecom Agency).
Available:
http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=2007:951.
Last Access: September 3, 2008.

**PTS 3** Förordning (2006:942) om krisberedskap och höjd beredskap (Ordinance on crisis management.
Available: http://www.notisum.se/rnp/sls/lag/20060942.htm.
Last Access: September 3, 2008.

**PTS 4** Förordning (2003:396) om elektronisk kommunikation (Ordinance on electronic communications).
Available:
http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=2003:396.
Last Access: September 3, 2008.

**PTS 5** Säkerhetsskyddslag (1996:627), The security protection act.
Available:
http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=1996:627.
Last Access: September 3, 2008.

**PTS 6** PTSFS 2007:2 - PTS allmänna råd om god funktion och teknisk säkerhet (General advice on good function and technical security).
Available:
http://www.pts.se/upload/Documents/SE/PTSFS_20072_allmanna_rad_god_funktion_teknisk_sakerhet.pdf.
Last Access: September 3, 2008.
English non-binding summary: http://www.pts.se/en-gb/Documents/Consultations/2006/General-Advice-on-good-function-and-technical-security ---18-december-2006/

**PTS 7** PTSFS 2002:4 PTS föreskrift om förmedling av nödsamt till samhällts alarmerings- och räddninngstjänst.
Available:
http://www.pts.se/upload/Documents/SE/PTS%20foreskrifter%20om%20formed

[73] *The English translation misses chapter 5 article 6a that says (unofficial translation):*
*"A party that provides a public electronic communication service or a public electronic communication network shall ensure that the service and the public network satisfy reasonable demands for good function and technical security and also for sustainability and accessibility in the case of extraordinary events during peacetime [Chapter 5, Section 6a of the Electronic Communications Act (EkomL)]. "*

ling%20av%20nodsamtal%20till%20samhallets%20alarmerings-%20och%20raddningtjanst_PTSFS_2002_4.pdf.
Last Access: September 24, 2008.
The above regulation will be replaced with a new one in October 2008.

Post- och Telestyrelsen, Swedish Post and Telecom Agency – more information is provided in English at: *Introducing PTS* [Online] (Available: http://www.pts.se/upload/Ovrigt/Om-PTS/infomaterial/introducing-pts.pdf Last Access: September 3, 2008)

**Additional Information**

| | |
|---|---|
| **SE 1** | The Swedish country page on ENISA's website (descirbes some of the different projects that are being undertaken regarding resilience by the Swedish Government, associations and agencies – includes many hyperlinks to relevant websites and documents).<br>Available:<br>http://enisa.europa.eu/doc/pdf/Country_Pages/country_pag_sweden_20080314.pdf.<br>Last Access: September 3, 2008. |
| **SE 2** | Emergency planning - General information about the robustness unit work.<br>Available: http://www.pts.se/en-gb/Industry/Telephony/Emergency-planning/.<br>Last Access: September 3, 2008. |
| **SE 3** | Swedish IT Incident Centre (Sitic) Fact sheet.<br>Available: http://www.pts.se/EN-GB/DOCUMENTS/FACT-SHEET/2002/FACT-SHEET-THE-SWEDISH-IT-INCIDENT-CENTRE---SITIC---PTS-F-20027/.<br>Last Access: September 3, 2008. |
| **SE 4** | FAKTA om övningen Telö 07 (fact sheet from Telö 07 – crisis exercise).<br>Available: http://www.pts.se/upload/Documents/SE/Faktablad_Telo_07_W.pdf.<br>Last Access: September 3, 2008.<br>English summary page:<br>http://www.pts.se/upload/Documents/SE/Faktablad_Telo_07_W.pdf. |
| **MI 1** | Multipurpose Information Management and Exchange for<br>Robustness Prototype (MIMER-P) fact sheet.<br>Available: http://www.telia.se/privat/link.do?tabId=3&channelId=-103360&sl=teliase_kservice_driftinfo_mob.<br>Last Access: September 3, 2008. |
| **MI 2** | Example of Mimer from TeliaSoneras customer service, information on disturbance in the mobile network or service. (It is a GIS system click anywhere to zoom).<br>Available: http://www.telia.se/privat/link.do?tabId=3&channelId=-103360&sl=teliase_kservice_driftinfo_mob.<br>Last Access: September 3, 2008. |
| **RP 1** | God funktion och teknisk säkerhet i elektroniska kommunikationer - PTS-ER-2008:13 (Report on the supervision following the general advice).<br>Available: http://www.pts.se/upload/Rapporter/Internet/2008/Tillsyn-god-funktion-och-teknisk-sakerhet-PTS-ER-2008-13.pdf.<br>Last Access: September 3, 2008. |

| | |
|---|---|
| | English summary – titled Abstract - on p. 8 of Swedish document (see above link). |
| **RP 2** | Robusta elektroniska kommunikationer - Strategi för åren 2006-2008 - PTS-ER-2006:19 (Robuts electronic communication – Strategy for years 2006-2008) (not available in English).<br>Available: http://www.pts.se/upload/Documents/SE/Robusta_elektroniska_kommunikationer_Strategi_2006_2008.pdf.<br>Last Access: September 3, 2008. |
| **RP 3** | Utformning av fysisk säkerhet i noder i öppna neutrala bredbandsnät (Robust nodes - A report from the Swedish Urban Network Association) (February 2004).<br>Available: http://www.ssnf.org/upload/Projektdokument/robusta_noder.pdf.<br>Last Access: September 3, 2008.<br>English version http://www.pts.se/en-gb/Documents/Reports/Internet/2004/Robust%20nodes%20-%20A%20report%20from%20the%20Swedish%20Urban%20Network%20Association%20-%20February%202004/.<br>The recommendation was a result of a common project between PTS and the Swedish Urban Network Association (SSNF). The recommendations are being maintained by SSNF |
| **RP 4** | Robusta nät rekommendationer - förläggning av robusta nät. Kanalisation, kablar och kopplingsställen (Recommendation for robust electronic communications networks (September 2005).<br>Available: http://www.ssnf.org/upload/Projektdokument/Robusta nät förläggning oktober 2005.pdf.<br>Last Access: September 3, 2008. |
| **RP 5** | SKA (Säker KundAnslutning) projeket Secure client access (mainly about routing) (February 2006).<br>Available: http://www.ssnf.org/upload/Projektdokument/SKA.pdf.<br>Last Access: September 3, 2008. |

## Additional Links

Swedish Post and Telecom Agency, http://www.pts.se/EN-GB

Swedish IT Incident Centre (Sitic) - State and Government CERT, http://www.Sitic.SE.

*National Report of Sweden*

# National Report of United Kingdom

## Introduction

### Interview

Date and Duration 2008-08-14 – 150 minutes.

| Interviewee | Mr Mike Purdom | Mr Andrew Powell | Mr Ben Willis |
|---|---|---|---|
| Authority | BERR - Department for Business Enterprise & Regulatory Reform | CPNI -Centre for the Protection of National Infrastructure | Ofcom - Office of Communications |
| Position title | Senior Policy Advisor – Communications and Content Industries Team. (Telecommunications Resilience issues) | Manager of Advice Delivery for the Communications, Emergency Services and the Health Sector | Head of Technology Intelligence |
| Education/Training/ Degree | BA (Nottingham) | BSc, MSc, PhD (London) | MEng |
| Task and Responsibilities | Responsibility for liaising with Industry and OGD's on resilience issues. | Assessing risk to Critical National Infrastructure (CNI) and providing protective security advice to organisations in the sectors covered | Resilience issues within the regulation of the Telecoms industry |
| If applicable, rel.ship to ENISA | n/a | n/a | n/a |

### Authorities involved with Network Resilience

| Authority | BERR - Department for Business, Enterprise and Regulatory Reform | CPNI[74] - Centre for the Protection of National Infrastructure | Ofcom - Office of Communications |
|---|---|---|---|
| Main Tasks | Overall | Responsibility for | Regulation of the |

[74] CPNI is an interdepartmental organisation, with resources from a number of government departments and agencies. These include MI5, CESG (Communications Electronics Security Group) - the UK's National Technical Authority for Information Assurance (see www.cesg.gov.uk/) and other Government departments responsible for national infrastructure sectors.

| | | | |
|---|---|---|---|
| | Responsibility for Telecoms Resilience issues | the protection of the UK's CNI | UK Telecoms industry |
| Reports to | Secretary of State for Industry | Director CPNI. CPNI is an interdepartmental centre accountable to the Director General of the Security Service (MI5) | UK Parliament |
| URL | www.berr.gov.uk | www.cpni.gov.uk | www.Ofcom.org.uk |
| Year established | 2007 | 2007 | 2003 |

## Scope and governance

The UK wishes to point out that telecoms emergency planning and response is lightly regulated and no general powers of direction are available to the Secretary of State.

There are nine sectors which deliver essential services, meaning that these are considered part of the UK's critical infrastructure: energy, food, water, transport, telecommunications, government & public services, emergency services, health and finance. Hence, telecommunication (broadcasting, postal services, ISPs, fixed line and mobile telephone services) is one of these nine critical infrastructures.

The incumbent provider for retail customers is BT. The primary alternative is Virgin Media cable network. These two infrastructure providers hold about 98% of the market. Nevertheless, while BT provides infrastructure supporting services and is dominant here, its market share in the retail market is low. For the business market, London has plenty of operators that have their own infrastructure besides BT, such as Cable & Wireless and COLT (City of London Telecommunications).

### Question 1 : The authorities

The regulator for communications networks is the Office of Communication (Ofcom), but the focus is on market competition rather than on security or resilience.

A new initiative is being developed by the British government - led by Ofcom and BERR (the Department for Business, Enterprise and Regulatory Reform) and supported by the Cabinet Office, the CPNI (Centre for the Protection of National Infrastructure) and CESG (national information assurance authority) with the communications service providers (through the Network Interoperability Consultative Committee and NGNUK) to deliver a minimum security standard for interconnection in UK telecommunications industry.

This minimum security standard will be used as the basis of arbitration by Ofcom in the event of a dispute between operators where one refuses or terminates interconnect with another on security grounds, and is scheduled for delivery by the end of 2008.

- BERR is the lead for the communications sector on resilience.
- CPNI supports BERR by providing protective security advice on critical national infrastructure and
- CESG sets IA standards within the government sector.

The Electronic Communications Resilience and Response Group (EC-RRG), formerly the Telecommunications Industry Emergency Planning Forum (TI-EPF), is a quarterly, tripartite meeting between industry, government and Ofcom.

The EC-RRG fosters the development and sharing of best practice and owns the:

- National Emergency Plan for Telecoms along with its associated alert process –
- NEAT (National Emergency Alert for Telecoms) (see UK 8).

**Question 2 : The mandate of the authorities**

BERR describes its mission on its webpage as follows[75]:

> *BERR helps ensure business success in an increasingly competitive world. We are the voice for business across Government.*

BERR is the department of state and oversees the running of the communications sector. A secretary of state can direct communications service providers and Ofcom. BERR also focuses on resilience issues in the sector and works closely with industry via the Electronic Communications - Resilience and Response Group (EC-RRG).

CPNI describes its mission on its webpage as follows:

> *We are the Government authority which provides protective security advice to businesses and organisations across the national infrastructure.*
> *Our advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer.*

CPNI is focussed on advising industry on protection against national security threats but looks at resilience in order to focus advice on single points of failure (physically) and common failure modes (electronic).

CPNI provides protective security advice and has teams for each sector. In turn, resilience of networks is approached from the point of view where such advice can be given best. Often such advice results in a set of recommendations. If such advice or recommendations are ignored, the CPNI may approach the department responsible (see also UK 12 in reference list).

[75] *For more details and links to the web pages of the organisations mentioned here, see Additional links in Reference section)*

The Cabinet Office co-ordinate activity across government and is the national lead on civil resilience.

CESG – The National Technical Authority for Information Assurance describes its mission on its webpage as follows:

> *CESG is the Information Assurance (IA) arm of GCHQ and we are based in Cheltenham, Gloucestershire, UK. We are the UK Government's National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing to help our customers achieve their business aims.*

In short, CESG represents the information assurance needs of the government sector itself.

Ofcom describes its mandate on its webpage as follows

> *We are an independent organisation which regulates the UK's broadcasting, telecommunications and wireless communications sectors. We also set and enforce rules on fair competition between companies in these industries.*

As the above indicates, besides the Communications Act 2003 (UK 1) and its general reference to promoting interests of European citizens there is little about resilience of e-communication networks. Nevertheless, within this general notion security and integrity of public e-communication networks must be addressed.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

Resilience is not a regulated area. BERR and Cabinet Office run the Electronic Communications - Resilience and Response Group (EC-RRG)[76] to develop initiatives in resilient telecommunications, and there is an industry run alerting bridge, the National Emergency Alert for Telecommunications process, which provides a method of quick and effective communication for EC-RRG members. CPNI (then NISCC, the National Infrastructure Security Co-ordination Centre) published a guide to telecommunications resilience which is currently being updated (see UK 12 in reference list)

The strategy is one of partnership with industry, as exemplified by the new minimum security standard. EC-RRG and NEAT will continue.

Ofcom also uses the General Conditions of Entitlement. These distinguish between three main types of network or service provider, and the type of network or service provided by the operator determines which of these conditions apply to the operator.  The three main types of network or service provider are as follows:

- providers of Electronic Communications Services or Networks

[76] *Sometimes instead of EC-RRG the abbreviation ECRRG is used by government and private organizations alike. The official abbreviation is, however, EC-RRG*

- providers of Public Electronic Communications Services or Networks
- providers of Publicly Available Telephone Services (PATS) or Public Telephone Networks

Each of the 21 General Conditions of Entitlement impose obligations on Communications Providers. As well, each condition includes its own definition of that broad term for the purposes of that condition (see UK 14). In practice, those operators offering PATS, for instance, are expected to take all the necessary steps to offer reliable and dependable networks.

Possible Changes: Traditional telecommunications (telecoms) networks were developed to carry a single type of service, such as voice calls. In contrast, Next Generation Networks (NGNs) carry all types of services, including voice, video and e-mail, on a common platform[77].

NGNs offer significant cost savings to operators and new services to consumers, but there are also challenges in maintaining the quality, reliability and security of communications.

**Question 4 : Initiatives between providers and public authorities**

BERR and Cabinet Office run the Electronic Communications - Resilience and Response Group (EC-RRG) to develop initiatives in resilient telecommunications. The operators also contribute to the Electronic Communications - Resilience and Response Group (EC-RRG), which supports cooperation across the industry in response to emergencies affecting telecommunications in the UK. All major telecom players are part of it as well as BERR, CPNI and Ofcom to mention a few.

EC-RRG is planning to conduct a one day table top exercise that will involve a complete telecommunications failure, in November 2008. In 2009, a tier 1 exercise will be conducted focusing on a small number of larger regions.

The flooding during 2007 showed that communication network resilience was robust.

The EC-RRG owns the Industry National Emergency Alert for Telecoms (NEAT) process (see UK 8).

When an operator experiences a problem it informs either "Cable and Wireless" or BT. Nevertheless, the telecommunication network has not failed in recent history, and operated well even during terrorist attacks and bombings.

The EC-RRG meetings are currently hosted by government, the meetings are held at no cost to industry participants. Topics and proposals are agreed on a consensus basis by all

[77] *According to the UK's Parliamentary Office of Science and Technology (Postnote December 2007) BT's planned rollout of its £10bn '21st Century Network' (21CN) by 2012 will make the UK the first country to replace its incumbent telephone network with an NGN (see UK 12 in reference list)*

participants. All issues of resilience and business continuity are discussed. Each year there is participation in an emergency planning exercise.

There is no similar initiative, involving operators or infrastructure owners only. It is important to point out that based on the work conducted by a risk management board co-ordinated by the Cabinet Office (with membership from BERR, CESG and CPNI) a government-industry working group (WG) was established. This WG is developing the Next Generation Network (NGN) standard that builds on earlier work (e.g., see procurement and UK 13) and a draft standard has been developed (UK 11). Such work is needed now to assure satisfactory reliability and dependability levels (e.g., software and hardware architecture) for the NGN's. The necessary infrastructure investment and installation work will be launched soon to have the networks fully deployed by 2012.

## Tasks

### Question 5 : Typical tasks

BERR is the lead for liaison with the European Commission and sets policy on the communications sector, including resilience and infrastructure protection. BERR is also the government lead for input to EC-RRG. CPNI produces a range of publications (on www.cpni.gov.uk) on all aspects of security, runs closed information sharing groups with industry (the Network Security Information Exchange in the case of telecommunications), and provides one to one advice to telecommunications companies on protective security (producing written risk assessment reports).

Ofcom does conduct public consultation with BERR support. The Cabinet Office, BERR (EC-RRG), CPNI, CESG (Communications Electronics Security Group) – the UK's National Technical Authority for Information Assurance (NTAIA) can all conduct audits. However, there are two things to be considered:

- There is no legal mandate to conduct audits - CESG provides information security advice on public sector networks and CPNI on private sector national infrastructure. And
- to our best knowledge, no audits have been conducted addressing reliability and dependability of networks.

The United Kingdom does not really want to conduct audits. Similar to some other Member States, the UK prefers to follow the collaboration model whereby principle-based standards are preferable to rule-based ones[78.] In turn, through collaborative means solutions and guidelines are being developed together with industry and stakeholders to assure reliability and dependability levels protecting the UK's national interests. Ofcom will arbitrate in the event of a dispute.

[78] *Principle-based standards or guidelines outline the objectives but leave it to the operator to decide how to fulfil or reach these. However, the operator must be able to demonstrate that best practice was being followed or else be able to justify not doing so, while achieving the objectives set regarding network resilience.*

Possible Changes: Monday (2008-09-08) the London Stock Exchange (LSE) experienced a seven-hour breakdown[79]. Here the UK feels that it is inappropriate for public bodies to design a public network like the one offered by the LSE to traders.

It was mentioned that any regulatory intrusion is most likely unable to make it better. Nevertheless, the dependence of financial markets on the LSE board for prices and the industry's importance for the City's economy cannot be ignored. To improve the reliability and dependability of its trading network some collaborative work may be necessary, though there are no current plans for this. This will help in better managing risks and making the necessary infrastructure (software and hardware architecture) changes that will reduce the likelihood of another shut down to an acceptable level.

## Question 6 : Exchange of information between providers and public authorities

Information on vulnerabilities and incidents which may undermine security and resilience are discussed at NSIE[80]. Good practice on resilience is shared at EC-RRG. For networks used by government, information security policies, design documents, test plans etc are shared with government as part of the accreditation ("risk management") process.

Generally, the information is used to improve good practice in industry by industry. In the latter case where government networks are involved, the information is used for risk management.

The UK does not have a specified number regarding how many connections may go offline before operators need to inform the appropriate bodies including but not limited to Ofcom. The only recent case was a fire in the East End of London. In this case, several operators' infrastructure might have been affected by the fire and the National Emergency Alert for Telecoms (NEAT) was used. However, no measures had to be taken. Similarly, the flooding during 2007 did not reveal major problems regarding the e-communication infrastructure.

If a particular incident happens, information is gathered and meetings will be held where minutes will be taken. The latter are held by the government. Ofcom may receive the minutes and have to investigate with the operator if the government decides that it needs to know exactly how the operator dealt with this particular incident or crisis.

*[79] Monday (2008-09-08) the London Stock Exchange (LSE) experienced a seven-hour breakdown. TradElect a proprietary system crashed due to overload and a software bug. Hence, traders around the city could no longer execute trades on the LSE's board – communication simply broke down.*
*LSE has touted that the system will enable it to expand and speed up its capacity for trades. September 2008 was the deadline given for the system to show that it can reach and handle without problems 10,000 continuous messages per second (see http://blog.cytrap.eu/?p=375).*

*[80] UK Network Security Information Exchange (UK-NSIE) was formed in April 2003 to share sensitive information in the information and communications technologies sector. It currently includes IP providers; core mobile operators; and traditional telecommunications providers, as well as CPNI. Participating companies now cover over 80% of the telecommunications market in the UK. It is linked to NSIE in USA. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include: a guide to the procurement of resilient telecoms; best practice guidance on the secure implementation of BGP (http://www.cpni.gov.uk/Products/information.aspx).*

### Question 7 : Handling of security incidents

There is no obligation to report but communications sector organisations can report to the CSIRTUK (CPNI Combined Security Incident Response Team)[81]. CSIRTUK will contact communications service providers who are involved in an incident that has been reported.

UK Network Security Information Exchange (UK-NSIE) members discuss security incidents that have affected them and how they dealt with that information. This helps other members. All reporting is voluntary. The above illustrates the two mechanisms being used in case of a security incident:

- The UK-NSIE is meeting to discuss what happened and share information; and
- the CSIRTUK may investigate and get confirmation on a bilateral basis.

If the incident shows a pattern or trend, then an advisory will be issued. The National Emergency Alert for Telecoms (NEAT) may also be used to inform operators.

Ofcom does not have data about when a case related to resilience issues was investigated last time. In general, there are a few examples only, where the regulator stepped in to investigate. Moreover, there are no formalized procedures for this and, instead, investigation depends entirely upon the case.

### Question 8 : Audits related to resilience

No such audits are performed in the UK.

### Question 9 : Enforcement actions

Enforcement actions are not applicable as the area of resilience is not regulated. In the case of the minimum standard, Ofcom will arbitrate in the event of disputes.

However, if the operator of a Publicly Available Telephone Services (PATS) violates any of the general conditions of entitlement (UK 8), a fine can be imposed. According to the law, the fine imposed may be up to and including 10 percent of turnover from relevant UK telecom operations (UK 1).

BT is the provider for the Universal Service Provision (UPS) except for one area in the country, Hull (North of England). Here, due to historical reasons, 100,000 people are being served by KCom that operates PATS in this region.

The scope of the Universal Service Obligations ('USO') is defined by the EC Universal Services Directive ('USD') (see also UK 16 and UK 17).

[81] *CSIRTUK (CPNI Combined Security Incident Response Team) http://www.cpni.gov.uk/products/alerts/3268.aspx*

## Risk Management and preparedness measures

### Question 10 : The national risk management process

A national risk management is in place (see UK 10 in reference list – download report). Besides the national risk register (UK 10) there is also the Civil Contingencies Act 2004 (UK 2) and background material further clarifying the issues (see UK 3). The national risk assessment process is run by the Cabinet Office and includes threats and hazards relevant to all sectors, including communications. The national risk assessment has input from all departments of state but does not involve industry directly. BERR leads the policy setting in communications, and risk management of the sector lies also with BERR.

The UK national telecommunications emergency plan (see UK5) outlines some of the steps that operators must take.

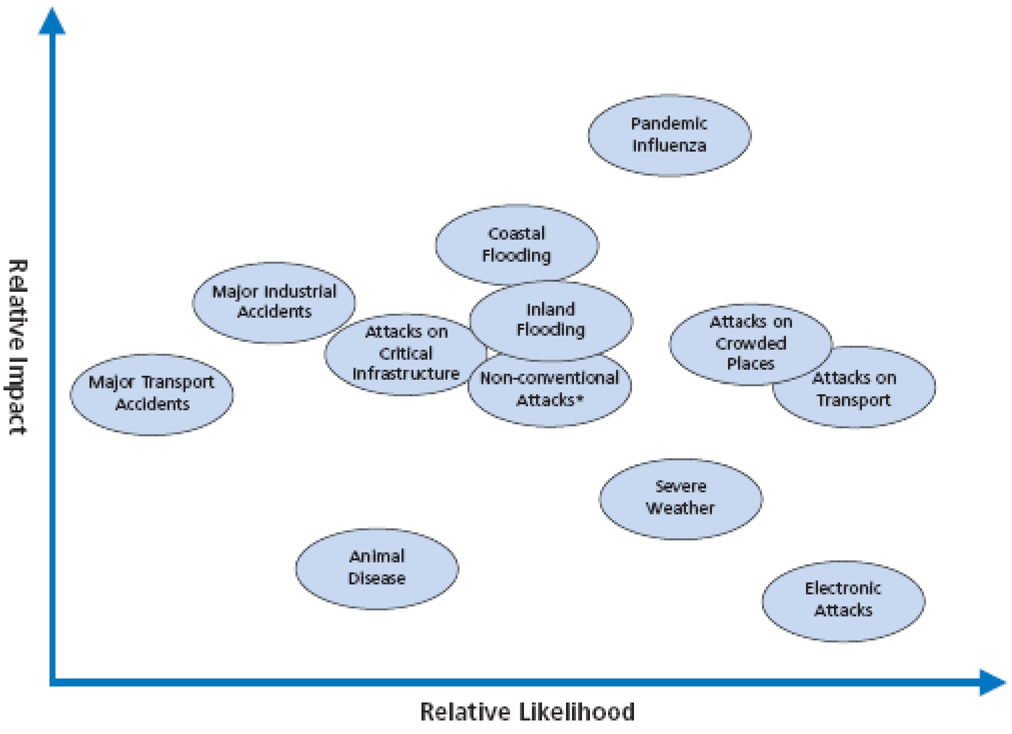


Figure 1: *An illustration of the high consequence risks facing the United Kingdom*

* The use of some chemical, biological, radiological and nuclear (CBRN) materials has the potential to have very serious and widespread consequences. An example would be the use of a nuclear device. There is no historical precedent for this type of terrorist attack which is excluded from the non-conventional grouping on the diagram.

Source: National Risk Register, p. 5 (see UK 10 in reference list)

### Question 11 : The preparedness and recovery measures

The NEAT (National Emergency Alert for Telecoms) (see UK 8) process is an industry mutual-assistance programme that helps recovery. The EC-RRG promotes good practice and has an exercise programme, which helps to establish preparedness (UK6, UK7). The EC-RRG ensures that the guidelines are up to date through regular exercises.

If restoration of parts of the network is needed, telecom providers deal with it amongst themselves. This has always worked well, and it would only be challenged in the case of the Prime Minister's office requiring something very specific.

In case of a national crisis or other crisis situations, the Cabinet Briefing Office Room (COBR – where the cabinet meets) may have to convene to address the problem. This crisis management meeting also decides about the telecom sector, and BERR passes on the decisions taken to industry and the telecom sector.

### Question 12 : Incident response capabilities

CSIRTUK (part of CPNI) provides co-ordination of incidents affecting communications networks.

GovCERTUK (part of CESG) deals with incidents affecting government networks. While the UK GovCERT has an archive regarding its advisories, most vulnerability and threat information is stored on spreadsheet. The UK does not have a web-based database to provide access to such information.

Some companies have their own CSIRT capability, such as BT. Other provide commercial CSIRT services, such as Symantec. Meetings of UK CSIRTs take place on a periodic basis. UK CSIRTs co-operate with CSIRTs in Europe (e.g. European Government CSIRTs, EGC, and TERENA's TF-CSIRT) and worldwide (through FIRST). Post incident investigations are performed by CSIRTUK and by other UK CSIRTs.

The UK Network Security Information Exchange (UK-NSIE) has 14 members and about 30 people that participate in its six weekly meetings. Organisations wanting to join UK-NSIE must apply for membership, and members have to agree before another organisation can join the network. This group discusses incidents and vulnerabilities that have or might affect company networks and infrastructure. It has been running for five years.

UK universities are represented by JANET CERT.

### Question 13 : Good practice on resilience

Most information on good practice on resilience can be found on the CPNI web site and it provides further links (e.g., regulation, laws, standards, best practice).

Both, the CPNI public web site (see additional links) and CPNI extranet (for trusted industry contacts), contain good practice security guidance, based on working groups of the UK Network Security Information Exchange (UK-NSIE).

There are no financial or other incentives available for achieving better hardware and software architecture to secure better resilience of e-communication networks. Nevertheless, CPNI provides guidance for free with its reports, studies, guidelines, white papers that is accessible via the web.

### Question 14 : Guidelines for procurement

Procurement guidelines for public e-communication networks exit for Next Generation Networks (see UK 10). The so-called 'best practice' procurement standards and guidance will assist buyers of NGN-based telecommunication services and set standards that service providers will need to meet in order to supply to government (UK 13).

## References

Some of the referenced documents below are not in the public domain. However, the UK would be happy to share any relevant information with any other member countries who request it:

**UK 1** Communications Act 2003 – Chapter 21 (67 pages).
Available: http://www.opsi.gov.uk/ACTS/acts2003/ukpga_20030021_en_1.
Last Access: September 18, 2008.

**UK 2** Civil Contingencies Act 2004 – Chapter 36.
Available:
http://www.opsi.gov.uk/Acts/acts2004/ukpga_20040036_en_1.
Last Access: September 18, 2008.
Civil Contingencies Act (CGA) 2004 is in two parts:
-Part 1 covers emergency planning and designates telecoms as Category 2 responders and requires them to share information and co-operate with Category 1 responders (LAs, blue light services), principally through Local Resilience Forums.
-Part 2 comprises emergency powers that enable HMG essentially to implement any measure - in relation to our and other designated sectors - to mitigate and direct the response to an emergency.

**UK 3** Civil Contingencies Act - Background to the civil contingencies act.
Available: http://www.ukresilience.gov.uk/preparedness/ccact.aspx#background
Last Access: September 18, 2008.

**UK 4** Civil Contingencies Act - civil contingencies act documents.
Available: http://www.ukresilience.gov.uk/preparedness/ccact.aspx#documents.
Last Access: September 18, 2008.

**UK 5** UK National telecommunications emergency plan.
Available:
http://www.ofcom.org.uk/static/archive/Oftel/ind_groups/emer_plan/index.htm
Last Access: September 19, 2008.
The Plan is maintained through The Electronic Communications Resilience & Response Group (EC-RRG). The EC-RRG is a tripartite Group comprising Industry (Communications Service Providers covering fixed line, mobile and Internet services), Government and the regulator OFCOM.

**UK 6** Emergency preparedness - civil contingencies act - Category 2 Responders - Generic emergency planning arrangements Telecommunications (Telephone service providers - fixed and mobile).
Available:
http://www.ukresilience.gov.uk/preparedness/ccact/cat2_info/telecoms.aspx.
Last Access: September 19, 2008.

**UK 7** EC-RRG resilience guidelines for providers of critical national telecommunications infrastructure. Short title: 'EC-RRG resilience guidelines (Working Title) V0.7 (March 2008).
Available online:
http://www.ukresilience.gov.uk/~/media/assets/www.ukresilience.info/telecoms_ecrrg_resilience_guidelines1%20pdf.ashx.
Last Access: September 19, 2008.

**UK 8** National Emergency Alert for Telecoms (NEAT) – (not publicly available).
National Emergency Alert for Telecommunications (NEAT) is a conference bridge that enables Telco's to talk to each other and government during an emergency. An MoU amongst the companies supports the response process.

**UK 9** National risk register.
Available: http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx.
Last Access: September 19, 2008.
A register of the likelihood, and likely severity, of risks to the UK.
Divides risks into natural events, major accidents and malicious attacks (see Q 10 in this report).
The National Risk Register is intended to capture the range of emergencies that might have a major impact on all, or significant parts of, the UK. It provides a national picture of the risks we face, and is designed to complement Community Risk Registers, already produced and published locally by emergency planners. The driver for this work is the Civil Contingencies Act 2004, which also defines what we mean by emergencies, and what responsibilities are placed on emergency responders in order to prepare for them. Further information about the Act can be found on the UK Resilience website.

**UK 10** Electronic Communication – Resilience & Response Group (EC-RRG) (not dated) 3 pages.
Available:
http://www.ukresilience.gov.uk/~/media/assets/www.ukresilience.info/flu_telecoms_support_emergency%20pdf.ashx.
Last Access: September 19, 2008.
More supporting documentation is available.

**UK 11** Next generation telecoms networks (December 2007) UK's Parliamentary Office of Science and Technology Postnote, Nr. 296 (4 pages).
Available: http://www.parliament.uk/documents/upload/postpn296.pdf.
Last Access: September 19, 2008.

**UK 12** Good practice guide – telecommunications resilience V2.0 (currently being revised) (March 2006). National Infrastructure Security Co-ordination Centre (NISCC), 35 pages.
Available: http://www.cpni.gov.uk/docs/re-20040501-00393.pdf.
Last Access: September 19, 2008.

**UK 13** Next generation networks - procurement standards, guidance and model clauses (not dated). The Next Generation Networks (NGN) Procurement Standards Project, Office of Government Commerce OGC, 51 pages.
Available: http://www.cpni.gov.uk/docs/re-20040501-00393.pdf.
Last Access: September 19, 2008.
*'best practice' procurement standards and guidance that will assist buyers of NGN-based telecommunication services and set standards that service providers will need to meet in order to supply to government*'.

**UK 14** General conditions of entitlement (guidelines) Ofcom (not dated).
Available: http://www.ofcom.org.uk/telecoms/ioi/g_a_regime/gce/gcoe/.
Last Access: September 19, 2008.

**Additional Resources**

**UK 16** Statutory Instrument 2003 No. 1904 - The Electronic Communications (Universal Service) Order 2003 (2003-07-25).
Available: http://www.opsi.gov.uk/si/si2003/20031904.htm.
Last Access: September 19, 2008.

**UK 17** Review of the Universal Service Obligation – Statement – Ofcom (2006-03-14).
Available: http://www.ofcom.org.uk/consult/condocs/uso/uso_statement/.
Last Access: September 19, 2008.

**Additional Links**

BERR -Department for Business, Enterprise and Regulatory Reform, http://www.berr.gov.uk

CPNI – Centre for National Infrastructure Protection, http://www.cpni.gov.uk/aboutcpni188.aspx, CPNI was formed from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC).

GovCertUK | CESG, http://www.govcertuk.gov.uk/, GovCertUK provides CESG's CERT function to UK government. The CESG GovCertUK Incident Response team provides a 24/7 (24 hours 7 days a week)

Ofcom – Office of Communications, http://www.ofcom.org.uk/consumeradvice/guide/.

CESG (Communications Electronics Security Group) – the UK's National Technical Authority for Information Assurance (NTAIA), http://www.cesg.gov.uk/).

# National Report of Norway

## Interview

Date and Duration: 13 August 2008 1,5 hours.

| | | |
|---|---|---|
| Interviewee | Mr Håkon STYRI | Mr Tor Inge SKAAR |
| Authority | Norwegian Post and Telecommunications Authority | Norwegian National Security Authority |
| Position title | Senior Adviser<br>Department for Internet and Security | Chief Engineer VDI |
| Education / Training or Degree | B. Sc. Eur. Ing. | M.Sc. Telematics, NTNU |
| Task responsibilities | Security and preparedness in electronic communication networks | VDI /NorCERT<br>VDI , Varslingssystem for Digital Infrastruktur, is the Norwegian Alert and Early Warning System for Digital Infrastructure identifying, classifying and issuing warnings about IT attacks against Norway. |

### Authorities involved with network resilience

| | | |
|---|---|---|
| Authority | NPT<br>Norwegian Post and Telecommunications Authority | NSM<br>Norwegian National Security Authority |
| Reports to | Norwegian Ministry of Transport and Communications | Norwegian Ministry of Defence and the Norwegian Ministry of Justice and the Police. |
| Year established | 1987 | 2003 |
| URL | http://www.npt.no | http://www.nsm.stat.no/ |

## Scope and governance

According to the Norwegian experts, the term network resilience or dependability of public e-communication networks as proposed in this survey is not used in this way in Norway. Instead, the term preferable used is ICT security[82].

[82] *The framework of the Norwegian policy and actors with regard to resilience of communication systems and networks is well explained in Chapter 9 of the Report No. 17 (2006–2007) to the Storting An Information Society for All (see NO 5 in reference list). The term 'resilience' in this context is covered by what is called 'ICT Security'.*

### Question 1 : The authorities

Basically there are two authorities in Norway (NPT and NSM) dealing with regulatory issues of resilience of public and other essential e-communication networks.

- NPT - Norwegian Post and Telecommunications Authority- is an autonomous administrative agency under the Norwegian Ministry of Transport and Communications.
- NSM - Norwegian National Security Authority, a professional and supervisory authority within the protective security services in Norway[83].

Both authorities are actively involved in regulation and cooperation with the providers. Both authorities give input for policies, policy development and legislation to the Ministry of Government Administration and Reform (development and coordination of the use of information technology), the Ministry of Transport and Communication (telecommunication), and the Ministry of Defence (security and communication).

### Question 2 : The mandate of the authorities

The legal basis and the mandate of NPT are defined in the Regulations on Electronic Communications Networks and Services (Ecom Regulations) (see NO 2) and The Electronic Communications Act (see NO 1).

The main tasks of NPT are securing user access to high quality telecommunication services. Their mandate is quite broad. Part of the 'Security and Internet Department' is dedicated to the legislation of security of telecommunication and, among others, to issues of resilience[84].

The primary mandate of NSM is the enforcement of the national Security Act (NO 3) dealing with mostly classified information regarding government, companies, municipalities and other organisations on issues such as defence. NSM is the certification authority for IT systems and companies. It holds also the Norwegian CERT called NorCERT (see reference list) which is the national CERT for Norway. NorCERT handles major ICT incidents.

As regards cooperation between both – NPT and NSM - there is some overlap in responsibilities considering the Norwegian part of the Internet, the NPT dealing with the electronic communications physical infrastructure and general electronic communications services, and NSM dealing with Internet services. On an operational level, NorCERT provides NPT with insights about threats and similar matters.

[83] *NSM as an organisation is relevant to security of classified information + the national CERT; NorCERT*
[84] *Both interviewees used quite often 'robustness' and 'availability' as equivalents for resilience.*

A formalised cooperation agreement between the two authorities is in place and documented. It was underlined that the agreement is quite simple but that it is nevertheless a formal agreement.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

*NPT* **-** *Norwegian Post and Telecommunications Authority*

A number of regulations are in place concerning the resilience of public e-communication networks laid out in the Electronic Communications Act (NO 1). Several sections are relevant to resilience

- Section 2-10 is the most important one dealing with security and preparedness. *"Providers shall offer electronic communications networks and services with the necessary security for the users in peacetime, crises and war. Providers shall maintain the necessary preparedness and entities important to the community shall be prioritised when necessary. Providers shall communicate important messages from the State authority. To ensure the fulfilment of national requirements for electronic communications security the Authority may issue regulations, issue individual decisions or conclude agreements that providers shall implement measures pursuant to the first paragraph. Such measures may include inter alia:*
  *1. introduction of special functions and services in electronic communications networks, operating systems and operating organisations;*
  *2. contingency planning and preparedness plans, including contributing to national preparedness plans and participation in drills;*
  *3. physically securing of important installations in electronic communications networks. The Authority may order providers to enter into cooperation with other national or international activity when this is laid down in an international agreement. In principle, providers shall meet costs of security and preparedness measures pursuant to this section. Providers' actual additional costs connected with provision of security and preparedness measures will be reimbursed by the State on the basis of satisfactory documentation furnished by providers. "Additional cost" means the cost that would not materialise in the absence of this provision, beyond the cost of a purely commercial solution. Providers may be refused access to the market if this is necessary in the interest of public safety, health or other special circumstances "*

Also relevant are the following sections dealing with issues covered by the questionnaire.

- Section 2-3 impose requirements for networks, services, associated equipment and installations*: "… and the use of standards to ensure interoperability between networks and services, quality, efficient utilisation of capacity in networks that are used by more than one provider and to protect life and health or avoid harmful interference" " issue regulations or individual decisions on the matters governed by the first paragraph, including ordering providers to take action to prevent and limit the quantity of bulk electronic messages ("spam"), malicious software ("malware") and similar."*
- Section 2-5 deals with permitted restrictions of use on electronic communications networks and services: *"… in the interest of national security or other important societal consideration …"*
- Section 2-7 deals with communication protection, for instance: *"The provider shall implement the necessary security measures for the protection of communications in the*

*provider's electronic communications networks and services. In the event of a particular risk of breach of security the provider shall inform the subscriber of the risk."*

- Section 10-3 addresses the duty to provide information
- Section 10-4 and 10-5 imposes providers to cooperate for supervision and internal control.
- Section 10-5 addresses instructions given by the authority to the operator to take corrective action and make changes.
- Section 10-7 focuses on regulatory measures in case of failures, such as issuing fines or imposing penalties on the operator.

The Act regulates also cooperation with other national and international authorities and addresses the issue of possible other or joint-activities.

In cases where the operator or telecom service provider is required by NPT to implement security measures, additional costs of implementation may qualify for reimbursement by the state (see Section 2-10 of Electronic Communications Act above). The provision is such that providers are expected to take over the share of the costs that can be recovered from market participants. Reimbursement applies for any additional costs incurred due to measures implemented that are outside traditional commercial activities. Norway believes this is a viable strategy for enhancing and improving resilience. An example is that providers have been reimbursed for acquiring additional diesel generators dedicated to preparedness tasks. A certain percentage of Norway's budget is dedicated to finance these types of measures.

The Ecom Regulations (see NO 2) has a few relevant sections in chapter 8 (Security and preparedness) that address dependability and reliability issues regarding infrastructure:

- Section 8-1 refers to the obligation to have and to provide information;
- Section 8-2 obliges the providers to prepare and maintain emergency preparedness plans and exercises;
- Section 8-4 deals with the prioritising of services; and
- Section 8-5 addresses the issue of Notification of significant operational and technical problems.

NPT demands regularly information from the providers on contingency plans, incidents, and security measures. However, these are not annually assessed. The information is then used to make a decision about financial contributions to the costs of taking the necessary steps to fulfil these measures.

*NSM - Norwegian National Security Authority*

The national guidelines for improving the information security - current version 2007 – 2010 – are updated on a yearly basis (see NO 4). These specify many tasks that NorCERT must perform. They are formally provided by the ministries, mainly the Ministry of Government Administration and Reform, but are by large guided by the Information Security Coordination Council.

The Electronic Communications Act (NO 1) deals with security, but mostly with non-public acts[85].

A list of all current documents (mostly in Norwegian) containing guidelines and recommendations is kept up-to-date continuously.

The *Information Security Coordination Council* (see KIS), composed of high-level representatives from various public authorities and government, discusses issues pertaining to network resilience. The Council does not take decisions. Instead, it is a platform for advice. Its functioning corresponds to a working group that exchanges information on a regular basis and coordinates work. The Ministry of Government Administration and Reform chairs this working group. Representatives from 5 other ministries, the Prime Minister's Office and from 10 Government Directorates are members of the Council.

The National Guidelines for Information Security 2007- 2010 (see NO 4) outline's the country's future strategy. The document focuses on the following areas, whereby the actions marked in bold relate to the issues raised in the ENISA questionnaire, in particular:

- Critical ICT infrastructures must be considerably more protected (p.11)
- Regulations on information security must be made more consistent and intelligible
- Information and information systems should be categorized to facilitate assignment of action items
- Risk and vulnerability analysis should be carried out by everyone, especially by all owners of critical infrastructrures (p.13)
- Efforts to raise awareness and disseminate knowledge must be increased (p.14)
- Warning and event handling shall occur in an expedient and coordinated manner (p.15)
- All Ministries should promote the use of standards, certification and self-regulation
- Ministries should promote research and development (R&D), education and competency development on information security.
- A coordinated arrangement should be established for identity management and electronic signature across sectors.
- The Ministries international collaboration on information security shall be further developed.
- Information security efforts shall be coordinated through the National Information Security Council (KIS)

## Question 4 : Initiatives between providers and public authorities

Many initiatives between providers and public authorities focus on exchanging information during regularly held meetings and workshops.

[85] *The Electronic Communications Act (NO 1) has provisions regarding security. However, these are limited to information not in the public realm, not classified according to the security act. Hence, official information may be exempt from compulsory publication pursuant of several acts including security act, ecom act, electric supply act health information act.*

The NPT authority is organising forums and workshops every year with different stakeholder groups on different topics. These may cover any subject ranging from security and robustness of public e-communication networks to awareness raising for safe use of the Internet.  The public authority is meeting organizer and invites. Participating stakeholders contribute the agenda items.

In the framework of NorCERT, the NSM authority is organising:

- Two annual forums and workshops for representatives coming from public and private sector involved with critical infrastructure.
- Regular meetings - workshops take place with the 10 biggest ISPs in Norway. The ambience during these workshops is informal. This increases participation by operators and helps build trust between them and NSM. That way, NSM receives a lot of valuable information from the providers. The topics discussed during such events are security related such as discussing details about incidents, response matters, detection and so forth. As well, security threats that might be caused by new technologies are also addressed and how to regulate Spam and other matters.
- There is also a NorCERT Expert Council – a small group of critical infrastructure experts – that meets twice a year and provides guidelines and input for future development of NorCERT.

A public-private partnership or PPP is used for developing the national strategy of information security. Here NorCERT and NorSIS (Norwegian Centre for Information Security – NGO) work together on information security issues. NorCERT represents the critical infrastructure community and NORSIS the rest of society.

As regards to initiatives between providers, both authorities are aware of one initiative called ITAKT (see reference list). Members of ITAKT are operators. The initiative helps improve efforts including awareness to fight cyber-crime. Government authorities are not member of ITAKT but invited occasionally for purposes of information exchange.

## Tasks

### Question 5 : Typical tasks

Both NPT and NSM report that they are holding public consultations with providers. During these consultations fostering of information exchange is the main purpose while this can help the enforcing of regulation. NPT may audit ISPs while NSM audits only companies that are concerned by the Security Act.

An NSM audit is performed either routinely at fixed intervals, or as a result of risk assessment. It may happen as a result of a reported security incident. NSM audits have traditionally been detailed inspections of security routines or classified systems.

In addition, NSM has also the task to collect reports from companies and other organisations under attack. In that case, NSM is provides both operational (technical and practical) and higher-level assistance. NorCERT performs this important task for NSM (see reference list)

Possible Changes: NSM audits have traditionally been detailed inspections of security routines or classified systems.

There is a paradigm change now in progress. We expect that future audits will concentrate on security management and will be based in part on compliance with ISO 19 011

**Question 6 : Exchange of information between providers and public authorities**

Exchange of information between providers and public authorities takes place at different levels and at different frequencies.

NPT is collecting information about important security measures. Examples are:

- information security policies,
- business continuity plans,
- preparedness measures,
- information on geographical,
- topological and technical network structures,
- locations with high infrastructure density.

All the above information is collected yearly from a selected group of operators. This selected group consists of about ten of the biggest and most important electronic communications network providers in Norway. The actual list of selected providers may change from year to year.

On a continuous basis NPT may collect information on incidents from any provider where the seriousness level of an incident is high. The information and reports are not analysed further if the incident is not important.

NPT uses the reports:

- to assess the vulnerability and the high risks of the telecom infrastructure,
- to discuss and suggest new measures to be implemented,
- to decide on what money should be spent (the reports are is considered very useful for making this decision),
- a secondary use comes for planning exercises and planning scenarios.

However, it should be kept in mind that the database with information and reports cannot be used for real time management of incidents as it is a snapshot of the infrastructure and out of date as the infrastructure is changing with time.

Therefore, only guidelines are developed from NPT’s incident database. NPT does not share this information with other authorities in Norway.

Security incidents are reported to NSM only if they concern security breaches of a certain gravity (falling under the security act, i.e. concerning classified matters). For all other cases of incident information, NSM has an active sensor network in place which is run by the NSM department NorCERT.

Companies falling under the National Security Act are required by law to report incidents to NSM. Incoming cases are assessed in the NSM as to their potential damage relative to the Security Act. Cases judged to be of sufficient gravity are referred to the Police for investigation, including criminal investigation.

NSM uses the reports and information for risk and threat assessment. A yearly formal report is made to the Ministry of Defence, but status and situation reports are more regularly sent to other ministries as well, depending on the situation at hand.

### Question 7 : Handling of security incidents

In general, it depends very much on the level of a security incident whether it is notified or not. Providers are supposed to send notification regarding serious security incidents at least as a general description with the level of detail provided to mass media. There is no template for notifications.

A serious incident is defined by NPT as an incident affecting ether 10.000 subscribers or the geographical area larger than a municipality, and lasting more than five hours.

In cases of serious incident, a post-incident report may be requested by NTP. For the reporting, a template (skeleton structure) is made available to the provider covering the nature of the incident, organisations affected by the incident and a description of provisions made to avoid such an incident in the future.

NSM is aware of an anonymous survey on security incidents with 5,000 firms in Norway. This survey is carried out in regular intervals (3-4 years) in the public and the private sector. It is called ‘Hidden Statistics’ and is organised by the Business Security Council (NO 5, in particular pp. 71-73, and NO 6)

### Question 8 : Audits related to resilience

The NPT authority may perform audits as part of the information collection (see Question 6). Annual interviews take place with each of the about 10 selected operators about measures and compliance with the telecom law. The main focus of these interviews is to check documentation and infrastructure against the existing legislation.

An audit may also be carried out if a significant incident has been reported. A request may be made to implement additional security measures, and in such cases there may be a follow up audit to check whether the measures have been put in place.

NSM audits on systems and companies that fall under the Security Act. Regular audits take place, and the companies are notified beforehand.

In these audits, the collaborators of NSM are the auditors. There is a protocol of how an audit should be carried out in place; it should not be considered as a certification scheme, though. The NSM auditors mostly inspect documentation, but also have the mandate to do system penetration

### Question 9 : Enforcement actions

To enforce existing regulations, NPT may inflict penalties such as daily fines on providers. These daily fines are cumulative and progressive. Another way for NPT of enforcing a regulation is not to pay the compensation, i.e. providers will not be reimbursed by the state for additional costs of implementation of security measures[86] .

NSM puts in place enforcement actions depending on the outcome of the audit. If there are only minor discrepancies, a warning is given or a re-audit is carried out after some time. In case of serious violations, NSM can shut down the entire system.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

There is no formal risk management process in place in Norway. However, several activities are undertaken to deal with risk management:

a. Ad-hoc risk management work is performed but not in a formalised project.
b. The National Information Security Coordination Council collects reports from authorities but not specifically on resilience.
c. NPT is doing a yearly ad-hoc review on threats and vulnerabilities based on the information collected from the providers (see Question 6).

### Question 11 : The preparedness and recovery measures

Preparedness and recovery measures to mitigate the risk affecting the resilience of public e-communication networks are established on several levels.

For preparedness/readiness on high level, NSM has established a system called SBS (in Norwegian; Forward-based system in English). The activities of SBS (Sivilt beredskapssystem - civil emergency management) are classified.

On an operational level, NSM has a structure in place called VDI. VDI, Varslingssystem for Digital Infrastruktur, is the Norwegian Alert and Early Warning System for Digital Infrastructure identifying, classifying and issuing warnings about IT attacks against Norway. The system is developed and maintained by NorCERT (see reference list). VDI is a cooperation between the private sector and the government and focuses on critical infrastructure protection. Sensors monitor the Internet connectivity.

[86] *see Section 2-10 of the Electronic Communications Act mentioned in Question 3 above*

For keeping such activities accurate and up-to-date, NSM is organising with other organisations the IKT'08 (National Cyber Exercise), to be held in December 2008. These exercises will provide much relevant information that helps improve resilience of public e-communication networks further. As well, regular exercises with ISPs and critical infrastructure organisations are also organised.

NPT participates in defining which services are critical to society. Specifically, priority services such as telephone and mobile phone as well as service availability in emergency situations. Provisions for enhancing the robustness of critical services may be identified and implemented.

NPT cooperates with electricity providers on the mutual dependency between power grid and Internet: many providers report critical/ important installations to the electricity power providers in order to enhance preparedness.

To assess the preparedness and recovery measures, NPT is frequently in contact with the key people among the providers. NPT wants to organise exercises every second year, whereby participants come from other sectors as well as the electronic communications sector. Furthermore, exercises covering smaller geographic regions will be organized. Main emphasis is on getting the power grid sector and local government involved.

**Question 12 : Incident response capabilities**

Different structures in Norway deal with incident response:

- NorCERT is the Norwegian national CERT. It coordinates responses to serious IT security attacks against critical infrastructure and information, as well as warns about serious vulnerabilities in vital computer systems in our society. It is the national contact point for security incidents.
- UNINETT runs the academic CERT for Norway.
- NorSIS (see reference list) – is the Norsk senter for informasjonssikring (Norwegian Centre for Information Security) - provides information and advisories to the general public, but is not involved in incident management.

NorCERT is in close cooperation as regards incident handing with the European Government CERTs Group (EGC), as well as with other national CERTs in the world. They exchange regularly with other national CERTS, and participate in meetings, exercises and workshops.

As regards analysis of past incidents and post-investigations, the NSM authority analyses only current incidents. In very severe situations, NSM might do a post-investigation.

NPT may do post-investigations in case of serious incidents and when an incident is caused by any new kind of problems. Usually, providers handle incidents. Analysis of past incidents is carried out on an ad-hoc basis. Such work helps in finding out whether new measures are needed or else current ones require change. These analyses might lead to new requirements imposed on providers involved in an incident or to a change in legislation.

### Question 13 : Good practice on resilience

The best online repository of good practice can be found on NORSIS web site (see reference list). Of course, it is in Norwegian.

NSM gives guidelines for specific cases on its web site.

NPT has a web site for safe use advice and similar good practices called Nettvett.no (see reference list). It targets private users, SMEs and others.

The challenge is to assure that none of these organizations provide conflicting advice. As well, coordination between these actors and defining best practice is important.

Sorting out and managing problems on their own is seen as the best incentive to help improve resilience. During workshops (see above) providers discuss among themselves how to handle important issues and to avoid regulation.  It is preferable to set industry standards instead of regulation. The providers make a choice about the technologies and they will choose the most competitive.

### Question 14 : Guidelines for procurement

There are no guidelines for procurement except for all procurement which is covered by the national security law; these do not address resilience in particular.

NPT has one guideline dealing with the creation of service level agreements (SLAs). Here robustness and availability (resilience) are mentioned. There are 3 different SLA templates for different types of services. All kind of relevant issues are mentioned such as repair time etc.

## References

Legislation and other official documents are generally available in Norwegian only (NB: there are two official standards for written Norwegian).

**NO 1** LOV-2003-07-04-83Lov om elektronisk kommunikasjon (ekomloven). (The Electronic Communications Act) Act No. 83 of 4 July 2003 Most recently amended: Act No. 2 of 11 January 2008 from 15 January 2008.
Available: http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20030704-083.html&emne=lov*+om*+elektronisk*+kommunikasjon*&.
Last Access: September 4, 2008.

**NO 2** FOR 2004-02-16 nr 401: Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) (Regulations on electronic communications networks and services) Ecom Regulations. Laid down by the Norwegian Ministry of Transport and Communications on 16 February 2004, Amended by Regulations No. 1136 of 22 July 2004 (entry into force), No. 40 of 14 January 2008.
Available: http://www.lovdata.no/for/sf/sd/xd-20040216-0401.html.
Last Access: September 19, 2008.

**NO 3A** LOV-1998-03-20-10 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). (The Security Act).
Available: http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-19980320-010.html&emne=lov*+om*+forebygge*+sikkerhet*&.
Last Access: September 19, 2008.
http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-19980320-010.html&emne=lov*+om*+forebygge*+sikkerhet*&

**NO 3A** LOV-2008-04-11-9 Lov om endringer i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) (Changes to the security act).
Available: http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20080411-009.html&emne=lov*+om*+forebygge*+sikkerhet*&.
Last Access: September 19, 2008.

**NO 4** Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010 (National guidelines on information security 2007-2010 Norway).
Available: http://www.regjeringen.no/Upload/FAD/Vedlegg/IKT-politikk/fad%20lav.pdf.
Last Access: September 19, 2008.

**NO 5** St.meld. nr. 17 (2006-2007) (Report No. 17 - 2006-2007) Et informasjonssamfunn for alle (Report No. 17 -- 2006-2007 -- to the Storting - An information society for all).
Available:
http://www.regjeringen.no/Rpub/STM/20062007/017/PDFS/STM200620070017000DDDPDFS.pdf.
Last Access: September 20, 2008.
Non-binding English version - summary
http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/stm17_2006-2007_eng.pdf (see pp. 71-73 – 'Hidden Statistics').

**NO 6** Informasjonssikkerhet - årets NSR mørketallsundersøkelse! (Hidden

Statistics/Mørketallsu ndersøkelsen ) Business Security Council.
Available:
http://www.nso.no/?module=Articles;action=Article.publicShow;ID=623.
Last Access: September 2, 2008.

## Additional Resources

**KIS,** Koordineringsutvalget for forebyggende informasjonsikkerhet - Information Security Coordination Council – publications, http://www.nsm.stat.no/Om-NSM/Samarbeidspartnere/KIS/Publikasjoner/Rapporter-fra-KIS/.

**NSM NorCERT,** Norwegian Computer Emergency Response Team is a department of the Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet - NSM), http://www.nsm.stat.no/ and http://www.cert.no.

**NorSIS,** Norsk senter for informasjonssikring (NorSIS) (Norwegian Centre for Information Security), http://norsis.no/.

## Additional Links

**KIS**, Koordineringsutvalget for forebyggende informasjonsikkerhet (Information Security Coordination Council), http://www.nsm.stat.no/Om-NSM/Samarbeidspartnere/KIS/Global-meny/Et-annet-valg/.

**ITAKT**, **I**nternett- og **T**elebransjens **A**nti-**K**riminalitets **T**iltak (Internet and telecom operators' anti-cybercrime group), http://www.itakt.no/1_bakgrunn/1_bakgrunn.htm.

**Nettvett.no**, Provides information for better IT security and data protection for consumers, SMEs and others, http://www.nettvett.no/.

**UNNINETT CERT**, The CERT for Norway's academic network http://cert.uninett.no/, Non-classified regulations and laws , http://www.nsm.stat.no/Regelverk/.

# National Report of Switzerland

## Introduction

### Interview

Date and Duration 2008-08-14 – 150 minutes, held in Bienne at the offices of OFCOM.

| | | |
|---|---|---|
| Interviewee | Mr Mark Fitzpatrick | Mr Peter Lehmann |
| Authority | Federal Office of Communications, OFCOM | Federal Office of National Economic Supply (FONES) |
| Position title | Engineer | Manager |
| Education/Training | Engineering | Business |
| Task and Responsibilities | Responsible for Information Security issues, working on technical & administrative regulations, projects (e.g., universal service and local loop unbundling), standardization | ICT infrastructure related matters such as risk analysis |
| If applicable, rel.ship to ENISA | N/A | N/A |

**People who provided input but did not participate in interview**

| | |
|---|---|
| Interviewee | Dr Ruedi Rytz |
| Authority | Federal Office of National Economic Supply (FONES) |
| Position title | Director |
| Education/Training/ Degree | MSc. |
| Task and Responsibilities | ICT infrastructure related matters such as risk analysis |
| If applicable, rel.ship to ENISA | N/A |

**Authorities involved with Network Resilience**

| | | |
|---|---|---|
| Authority | Federal Office of Communications, OFCOM, part of the Department of the Environment, Trans-port, Energy and Communications, DETEC | Federal Office of National Economic Supply (FONES) part of the Federal Department of Economic Affairs (FDEA) |
| Main Tasks | Regulator for telecoms (services & equipment), Radio and Television, radiocommunications , develops regulation and policy, submits regulation proposals to ministry, prepares and enforces the relevant legislation. | Responsible for the national economic supply of essential goods and services in the case of serious shortages that the private sector itself is unable to counteract. |
| Reports to | Federal Counsellor heading DETEC | Federal Counsellor heading FDEA |

| | | |
|---|---|---|
| URL for Agency or Authority | http://www.bakom.admin.ch | http://www.bwl.admin.ch |
| Year established | 1992 | 1982 |

**Authorities involved but not part of the interview**

| Authority | Federal Strategy Unit for IT (FSUIT) | MELANI | SONIA | GovCERT |
|---|---|---|---|---|
| Main Tasks | The FSUIT is the administrative unit of the Federal IT Council (FITC). It prepares the basis for decisions on the strategic orientation of IT in the Federal Administration.<br>In the field of information assurance FSUIT has responsibility for three bodies: MELANI, SONIA and GovCERT. | Within MELANI, the Reporting and Analysis Centre for Information Assurance, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures. MELANI is a joint venture between FSUIT and the Federal Office of Police (FEDPOL). It works closely together with over 40 operators of critical infrastructure. | The Special Task Force for Information Assurance (SONIA) intervenes in crisis situations caused by problems in the information and communication infrastructure. It comprises decision-makers from the public and private sectors (critical infrastructures) and is headed by the Delegate for the Federal Strategy Unit for IT. | The GovCERT within FSUIT undertakes various activities for the federal administration (e.g., alerting, incident handling, malware analysis, forensic investigation). As a part of MELANI it offers typical CERT services to the 40+ operators of critical infrastructures. |
| Reports to | Federal Councillor heading the Federal Department of Finance (FDF) | FSUIT | FSUIT | FSUIT |
| URL | http://www.isb.admin.ch | | | |
| Year agency or authority was established | | 2004 | 2000 | 2008 |

## Scope and governance

### Question 1 : The authorities

There is no single central agency responsible for issues regarding network resilience. Instead, several authorities or agencies are involved with regulating and improving network and information security to achieve better resilience. Contact and cooperation between these bodies is regular and effective. There is no organizational chart available illustrating how these agencies interact and the possible hierarchy. However, there is a five-page description illustrating who is involved and how in network resilience. This document has also been submitted during Spring 2008 to ENISA to the awareness raising division (details see under references – FONES 4).

The various agencies involved report to different ministries. For instance, OFCOM the communication regulator (see organizational chart – OFCOM 6) reports to the Department of the Environment, Transport, Energy and Communications, with Federal Councillor[87] Moritz Leuenberger, while the Federal Office of National Economic Supply (FONES) (see organisational chart – FONES 6) reports to the Councillor of Economic Affairs – Doris Leuthard.

Accordingly, the interview partners stressed that the Swiss system is the opposite of a centralized approach. The federal system makes a decentralized approach the norm. You can see advantages and disadvantages to both centralised and decentralised approaches.

To illustrate, the decentralised approach allows various bodies to concentrate on those aspects related to resilience most important to them and for which they are most competent. Nonetheless, a central agency could have an advantage focussing efforts and resources on specific problem areas.

### Question 2 : The mandate of the authorities

OFCOM describes its responsibilities and tasks on the Web (http://www.bakom.ch/index.html?lang=en) as follows:

> *The Federal Office of Communication (OFCOM) (Bundesamt fuer Kommunikation – BAKOM) handles questions related to telecommunications and broadcasting (radio and television). In this sphere, OFCOM fulfils all sovereign and regulatory tasks. The Office prepares the decisions of the Swiss government (the Federal Council), the Swiss Federal Department for the Environment, Transport, Energy and Communication (DETEC) and the Swiss Federal Communications Commission (ComCom). OFCOM is also developing important international activities.*

The telecommunications side of its work is based on the Telecommunications Act- SR 784.10 1st Article (see references – OFCOM 1) which is also the foundation for its responsibility in the area of resilience of public communications networks.

[87] *The Swiss Federal Council is the seven member executive authority in Switzerland. Each member, called Federal Councillor – is elected by the United Federal Assembly for a four-year term of office. Each Councillor (comparable to a federal minister) heads one of the seven departments (comparable to ministries in other countries) - http://www.admin.ch/br/index.html?lang=en*

The regulations pertaining to the universal service provision (SR 784.101.113/1.2 (see reference OFCOM 4) are also very relevant to this area.

FONES describes its responsibilities and tasks on the Web (http://www.bwl.admin.ch/index.html?lang=en) as follows:

> *Political or economical crises, technical breakdowns, natural disasters or terror attacks can disrupt our country's supply with essential goods and services. To prepare for such crises is the main task of the National Economic Supply (NES).*

FONES regulates based on the Landesversorgungsgesetz SR 531 --- (see references – FONES 1)

The above has 2-3 specific articles that concern IT and risk / resilience – IT infrastructure is an essential part for civil society. More details under the reference section (particularly FONES 1 and 2).

FONES interacts with these agencies and private industry to assure the secure supply of information and communication services. FONES operates an information and communication information infrastructure unit (ICT-I). It draws on IT security professionals of Switzerland's relevant operators of the critical infrastructure.

The Federal Strategy Unit for IT (FSUIT) is the administrative unit of the Federal IT Council (FITC). It prepares the basis for decisions on the strategic orientation of IT in the Federal Administration. It has various security activities among which is responsibility for the Reporting and Analysis Centre for Information Assurance abbreviated MELANI. FSUIT also leads the Special Task Force for Information Assurance (SONIA) that intervenes in crisis situations involving problems in the information and communication infrastructures.

MELANI is a joint effort between FSUIT and the Federal Office of Police (fedpol) and is in constant operation for the benefit of its partners as well as industry and the public in general. In the event of a crisis it has an important role supporting crisis management. Particularly important for Melani is the Geschlossener Kundenkreis (loosely translated – closed customer group – see: http://www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=en). The parties included in this group are typically critical infrastructure operators such as financial institutions, electric utilities, large firms and telecom operators. These firms inform Melani in cases of severe incidents. An example might be a new wave of spam mail trying to lure banking customers to malicious websites.

For confidentiality reasons the reporting company can define who can and should be informed by Melani (e.g., a bank reporting a specific problem might require that the information be distributed only to the other banks). Again, participation by private sector firms is voluntary (e.g., financial sector, utilities and large corporations).

SONIA is a virtual task force (http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html?lang=en) that comes in contact during a crisis that can no longer be managed by the private companies involved alone. The Task Force includes the information and communication infrastructure (ICT-I) section of FONES (i.e., experts from public and private companies and agencies - see Melani/Sonia 1 in reference list as well as under section of additional links for more information). It is supported by MELANI.

Sonia provides information, advising private firms involved and acting as liaison to the political leadership such as the Federal Council (see also Footnote 1 above). To test how well this task force Sonia can work in a 'real' crisis, exercises were organised to test its procedures and viability during:

- Strategic Leadership Exercises 1 or 2 (Schwarzenburg) several years ago organised by the Federal Chancellery.

**Question 3 : Regulatory issues of resilience of public and other essential eCommunications networks**

There are four important factors one should consider when addressing this question. These are outlined below and subsequently, the regulatory issues are addressed.

First, the country's communication networks were started in a regulatory environment with a monopoly provider. As well, the national telecom provider – PTT (Post, Telegraph and Telephone) was government owned at the time. This resulted in a very high quality 'gold plated' network. Importantly for today's situation this has resulted in the market expecting and demanding a high level of dependability and reliability of communication network services, not only from the incumbent but also from the new service providers competing with it. This demand provides an incentive for providers to act accordingly and deliver reliable services at competitive prices.

Second, deregulation, including the unbundling of the last mile in Switzerland has resulted in a market where several hundred telecommunication companies, including CATV operators, offer services. These entities are private companies or public entities (e.g., utilities, communes). Nevertheless, of these 500+ providers, there are four major telecom operators: Cablecom, Orange, Sunrise and Swisscom that own or control the large part of the infrastructure[88].

Third, risk analyses carried out in recent years identified problem areas. One response was that the major players signed a memorandum of understanding. It outlines how they will collaborate and support each other's efforts in case of a crisis. This voluntary agreement resulted in establishing of a Crisis Reaction Team Telecom (CRTT). The CRTT can be called upon in cases where any of these four companies feel they cannot cope on their own with an incident or else feel their troubles might affect reliability and dependability of other providers' networks.

[88] *Regardless of ownership of infrastructure and type of technology used, whenever voice and/or data communication is involved and services are sold on the open market, the network is considered to be public. In turn, the operator or owner is subject to OFCOM regulation.*

Fourth, most regulatory initiatives focus on getting telecom service providers to collaborate and exchange information on a voluntary basis. Also, a permanent working group exists in the framework of the ICT-Infrastructures section of the National Economic Supply. In this group the main players including the public sector (FONES, OFCOM) meet several times during the year. These meetings serve to formulate approaches that are then included in guidelines and result in best practices that are used across the industry.

The above four factors are important to consider when addressing regulatory and other issues pertaining to public network resilience in Switzerland. In addition, the law stipulates that larger network failures or breakdowns require the informing of OFCOM (the regulator) (see OFCOM 2, Article 96). In practice, OFCOM and operators have agreed that where 50,000 or more people are affected, the incident is considered severe and must be reported to the regulator.

As well, Switzerland follows the principle-based approach[89] for regulation and as a first step has issued Guidelines for the Security and Availability of Telecom Infrastructures and Services (see OFCOM 5). These guidelines are not binding but could form the basis for regulations should firmer measures be judged necessary. Switzerland tries to find the right balance between achieving better resilience while avoiding too many rules and administrative procedures. The guidelines are intended to be a help to smaller operators who may have limited resources available for security measures by pointing them in the right direction. For example, the guidelines could form a basis for discussion between a small operator looking to improve his operation and an external security consultant.

The universal service is one of the very few areas where there are any formal quality of service requirements from the regulator (OFCOM 4). Combined with the price limits which apply to the universal services these quality requirements set a baseline for the price / quality of the basic telecom services in Switzerland. Other service providers can then choose to compete with the universal service on quality and / or price.

<u>Possible Changes</u>: This is seen in the area of the reporting obligation whereby more consistent application is needed. OFCOM is looking at how to improve the process. For instance, how well the reporting works both according to time, type of reporting, channel used and subsequent assessment for reducing the likelihood of the same incident happening again requires some analysis of past reports. In turn, procedures have to be defined by the regulator in collaboration with the providers. After implementation of any new reporting procedures, regular assessment will be required. To assure effectiveness while keeping the administrative burden to a minimum will certainly require good thought.

Publication of some quality parameters would help to reinforce the universal service baseline principle mentioned above. A possible obligation for telecom service providers is the requirement to publish performance data. This requirement could use the parameters

[89] *Principle-based standards or guidelines outline the objectives but leave it to the operator to decide how to fulfil or reach these. However, the operator must be able to demonstrate that best practice was being followed or else be able to justify not doing so, while achieving the objectives set regarding network resilience.*

that are part of the universal service quality requirements. In turn, using such parameters would improve transparency for consumers and commercial clients. In turn, competition would play an even greater role than it does today due to a lack of these performance parameters being assessed and released to the public.

### Question 4 : Initiatives between providers and public authorities

Cooperation is such that the operators are being consulted before regulations are drawn up. Any consultation will include as a minimum the four biggest operators, these are the operators that run over 90% of the infrastructure. To some extent they set the standards and the rest of the market follows (e.g., type of services offered, costs, redundancy services, etc.).

OFCOM has various working groups with industry. Depending on the subject, ad-hoc groups may also be used as has been the case in the area of network and information security.

The ICT-Infrastructure Unit from FONES has a standing working group (WG). OFCOM and the four operators have each a member on that WG. Besides these organizations, T-Systems (telephone, ISP, leased lines, etc.), Telekurs AG (national e-payment system) as well as three banks (UBS, CS, Swiss National Bank) are permanent members of this WG. The WG's major focus is on risk assessment and they are meeting at least four times a year.

The Crisis Reaction Team Telecom (CRTT) (see question 3 above) was one initiative that culminated from close consultation between regulator and operators.

Regarding initiatives among providers, there is a Swiss Association of Telecommunication (Schweizerischer Verband der Telekommunikation) called ASUT. Information security and resilience is, however, not a core activity.

Infosurance was a foundation primarily supported by funds from the federal government and industry that conducted a thorough risk analysis about telecommunication, Internet, etc. during 2002. It published a report at the conclusion of the work. However, these days Infosurance has changed its legal form to an association and has focussed its work on the IT security of small and medium sized enterprises. It is no longer very active in the area of critical information infrastructure protection.

Possible Changes: One issue that needs to be addressed soon is if regulatory efforts and working groups addressing resilience-related matters do not have to include hardware/software providers. For instance, while Sunrise owns infrastructure, it has outsourced the operation of its network to Alcatel-Lucent. How this affects regulatory administration, enforcement, reporting and achieving best practice must be clarified. Who is responsible for what and must report to regulator is just one of the tasks that must be discussed amongst stakeholders.

There needs to be progress on considering network infrastructure, design, R&D issues and how this will affect network dependability and reliability in a few years. Without closer collaboration with hardware/software providers regarding network architecture, however, this will be impractical.

At this point, Switzerland has not addressed such new developments and how they affect the regulatory framework and its administration. Another example are mobile virtual network operators (MCNO) that are currently not part of an advisory or working group. However, their market share is growing (e.g., M-Budget, Coop, Tele 2, Cablecom). In some cases, the MCNO (e.g., M-Budget from Migros, largest food and non-food retailer) outsources management of the virtual network, in other cases part of the network is managed by the MCNO or the hardware provider. Risks and resilience issues warrant consultation between varies stakeholders and the regulator.

## Tasks

### Question 5 : Typical tasks

Typical work performed is developing guidelines and best practice approaches in close collaboration with industry and other experts. Public consultations are necessary in case of a new law or ordinance.

One important ordinance that came out of working together with operators was Guidelines pertaining to security and availability of telecommunication infrastructure and services (see OFCOM 5 in reference list).

### Question 6 : Exchange of information between providers and public authorities

There are various channels for information exchange between public authorities, operators and large users. Melani's Geschlossener Kundenkreis (loosely translated – closed costumer group) (see Question 3) shares information on a daily (and confidential) basis amongst its members.

As outlined under Question 3, OFCOM and operators have agreed that in case where 50,000 or more people are affected, the incident is considered severe and must be reported to the regulator.

Possible Changes: As mentioned in question 3 above, OFCOM is looking at how to improve incident reporting by telecom operators.

### Question 7 : Handling of security incidents

As addressed in Questions 3 and 6, OFCOM and operators have agreed that in case where 50,000 or more people are affected, the incident is considered severe and must be reported to the regulator.

As examples show, things do not work as one might hope. In practice OFCOM often hears about problems in the media before any direct report from the operator involved is received.

Possible Changes: For 2008 OFCOM has set itself the objective to review the reporting procedure to find a more effective solution. Any new solution would be discussed with the operators to ensure their support.

### Question 8 : Audits related to resilience

The universal service provisions (see reference OFCOM 2, Article 21) give OFCOM the means to audit the provider Swisscom that supplies these services. The ordinance stipulates that an audit by an independent 3rd party is possible. Normally, the universal service provider gives OFCOM/Comcom an annual report on the quality of the universal service. To date there has never been an independent check of the results. However, a third party audit can be ordered. To illustrate, the Communications Commission as the authority responsible for the universal service licence might order such an audit. This could be due to concerns regarding the quality of the universal service, or with the performance parameters reported by the universal service provider.

### Question 9 : Enforcement actions

OFCOM can impose fines if operators fail to follow provisions (e.g., OFCOM 5). Theoretically the fine can be up to 10% of the turnover the operator has made in the past year in Switzerland. However, in practice penalties have to be in proportion to the violation and would not be so draconian.

*Resilience or security*: So far we have not handed out any fines and indeed have not seen any problems that would have merited such a penalty. Switzerland follows the philosophy that the first priority is to resolve the problem. Penalties or fines would not necessarily foster good cooperation. They could make achieving the aim of risk reduction more difficult. This would be a result to be avoided. Instead, finding a mutually acceptable solution in any cases of network or service breakdown for example that helps mitigate and manage the risk more effectively in the future is the approach to be followed.

## Risk Management and preparedness measures

### Question 10 : The national risk management process

There is no overall risk management process in place per se. However, quite a few things have been done regarding sectoral efforts to manage risks better.

For instance, there are reports available from FONES and others outlining which risks must be addressed and dealt with to achieve proper risk management. There exists no formal means to force operators to follow these reports and take the necessary steps. Nevertheless, operators are motivated to take account of the results out of self-interest.

Switzerland is undertaking a large project to develop a national strategy for critical infrastructure protection. It includes communication networks. The project is being coordinated by the Federal Office of Civil Protection (see DDPS 1 reference). 18 departments/federal offices agencies are involved in the work.

The first report was produced in 2007 setting out general definitions and goals. At this stage, government administration people are involved only. Nevertheless, at some point when there will be a need to look at each individual sector of industry, the latter will have to be involved and participate (see DDPS 1).

Also in the framework of the CIP project Switzerland has performed a model analysis of an earthquake in Basle. Of interest was how this would affect the electricity grid, transport, logistics and so on. Beyond the analysis itself this work is intended to test and improve the methodology for application to further scenarios later in the project.

**Question 11 : The preparedness and recovery measures**

Until now, neither preparedness nor recovery measures to mitigate risks affecting the resilience of public networks exist in the public sector. The communications infrastructures are generally in the hands of private companies and they are responsible for them.

Political crisis management teams for severe situations are organised at the cantonal level[90.] This is a core activity of the civil protection staff (see DDPS). An example of such a situation have been the extensive flooding experienced during summer in recent years, where such crisis management teams were formed at the local/cantonal level.

Here it is important to point out that Switzerland does not have a specific set of rules or a handbook outlining exactly who gets what kind of service back first in case of a crisis. This approach is based on our experience that big disasters will not occur according to a known pattern. Therefore, the causes and effects will differ and the appropriate response(s) must be launched accordingly.

**Question 12 : Incident response capabilities**

A National CERT was established on April 1 2008. It has 3-4 people. It will be cooperating with other CERTS in Switzerland and other countries.

Reporting and information exchange between private CERTs, the National CERT as well as the Switch CERT (academic network) is not institutionalized. It works based on personal relationships and this is how the CERT community works. If people can and want to work together, they will.

In case of a national emergency, the National Emergency Operations Centre plays a large part in incident response (see NEOC 1). It provides support for the political leadership during national crisis. The NEOC has use of an electronic communication system that can be used to accumulate and disseminate data regarding the emergency. The universal service provider (i.e. Swisscom see OFCOM 4) was recruited into this scheme at an early stage. The system provides secure access and has priority communication status.

*[90] Political subdivision of Switzerland. Each of Switzerland's 26 cantons and half-cantons has its own constitution, legislature, executive, and judiciary. In France, the canton is a territorial and administrative subdivision of an arrondissement but not an actual unit of local government.*

## Question 13 : Good practice on resilience

There is no centralized archive storing such information for all of Switzerland across all agencies.

OFCOM provides encouragement in the form of guidelines.  The best incentive for providers is the marketplace, whereby customers demand reliable and dependable service at a competitive price. The universal service provider – Swisscom has to follow stricter guidelines than other operators do and, therefore sets the level that others must reach if not beat to be competitive.

## Question 14 : Guidelines for procurement

The Telecommunications Act together with the Ordinance on Telecommunications Installations sets the rules for telecommunications equipment in Switzerland and thus has some general relevance for network resilience.

The government itself may address resilience/security issues in its requirements when procuring.

## References

**BAKOM** (OFCOM in English = Federal Office of Communications) pertains to regulation relevant to that agency, while FONES (Federal Office of National Economic Supply) goes for relevant regulation and documents applying to the work of the latter.

**OFCOM 1** SR 784.10 Fernmeldegesetz vom 30. April 1997 (FMG) Federal (Federal Telecommunications act – not available in English).
Available: http://www.admin.ch/ch/d/sr/c784_10.html.
Last Access: August 15, 2008.
Particularly relevant are articles: 1, 17, 20, 26 (monitoring of radio spectrum),
31, 32, 32a, 34 (equipment and installations), 47 (telecom services for police etc.), 48 (priority services), 48a, 60.

**OFCOM 2** SR 784.101.1 Verordnung ueber Fernmeldedienste (FDV) (Ordinance on telecom services – not available in English).
Available: http://www.admin.ch/ch/d/sr/c784_101_1.html.
Last Access: August 15, 2008.
See articles: 6 (measures relating to terminal equipment affecting the network), 21, 27-30 (emergency call), 90 to 96.

**OFCOM 3** SR 784.101.2 Verordnung ueber Fernmeldeanlagen (FAV) (Ordinance on telecom installations – not available in English.
Available: http://www.admin.ch/ch/d/sr/c784_101_2.html.
Last Access: August 15, 2008.
Sets the basic requirements on telecom equipment used in Switzerland.

**OFCOM 4** SR 784.101.113/1.2 Technische und administrative Vorschriften betreffend die Dienstqualität der Grundversorgung Ausgabe 5 (Quality of the Universal Service). 11.6.2007 Inkrafttreten : 1.1.2008. Federal Office of Communications OFCOM.
Available:
http://www.bakom.admin.ch/org/grundlagen/00563/00564/00663/index.html?lang=de&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN0fX19bKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w==.pdf.
English here:
http://www.bakom.admin.ch/org/grundlagen/00563/00564/00663/index.html?lang=en (quality of the universal service).
Last Access: August 15, 2008.

**OFCOM 5** Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und –diensten (Guidelines pertaining to security and availability of telecommunication infrastructure and services). (2007-04 2nd edition). Federal Office of Communications OFCOM.
Available:
http://www.bakom.ch/themen/telekom/00462/01477/index.html?lang=de.
Last Access: August 15, 2008.

**OFCOM 6** BAKOM/OFCOM organizational chart,
http://www.bakom.ch/org/organisation/00537/index.html?lang=en.

**FONES 1** SR 531 Bundesgesetz ueber die wirtschaftliche Landesversorgung

(Landesversorgungsgesetz [LVG]) vom 8. Oktober 1982 (Stand am 13. Juni 2006) (Federal law on the national economic supply) (2006-10-08).
Available: http://www.admin.ch/ch/d/sr/5/531.de.pdf.
Last Access: August 15, 2008.
English non-binding version
http://www.bwl.admin.ch/org/00451/index.html?lang=en.
Particularly relevant are articles: Art. 2 /2b and Art. 22 /2.

**FONES 2** SR 531.11 Verordnung ueber die Organisation der wirtschaftlichen Landesversorgung (Organisationsverordnung Landesversorgung) vom 6. Juli 1983 (Stand am 22. Juli 2003) (Ordinance about the organization of the national economic supply). (1983-07-06).
Available: http://www.admin.ch/ch/d/sr/5/531.11.de.pdf.
Last Access: August 15, 2008.
Particularly relevant are articles: Art. 4 /c und Art. 14, http://www.admin.ch/ch/d/sr/531_11/a4.html.

**FONES 3** SR 531.12 Verordnung ueber die Vorbereitungsmassnahmen der wirtschaftlichen Landesversorgung vom 2. Juli 2003 (Stand am 22. Juli 2003) (Ordinance regarding pareparedness measures for national economic supply) (2003-07-02).
Available: http://www.admin.ch/ch/d/sr/5/531.12.de.pdf.
Last Access: August 15, 2008.
Particularly relevant are articles: Art. 8.

**FONES 4** National organisations active in Network and Information Security – Switzerland (2008) Originally prepared for the Who is Who Directory on Network & Information Security 2008 published by ENISA (never made it into the publication – not available on the web – provides all the necessary URLs to the various agencies, institutes and so on involved in information security)

**FONES 6** FONES organizational chart, http://www.bwl.admin.ch/org/00450/index.html?lang=en.

**Federal Strategy Unit for IT: Melani/Sonia 1** SR 172.010.58 Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Ordinance about informatics and telecommunication within the federal administration) 26. September 2003 (Stand am 1. August 2007).
Available: http://www.admin.ch/ch/d/sr/c172_010_58.html.
Last Access: August 15, 2008.
Particularly relevant are articles: Art. 10 (for Sonia).

**Additional Resources**

**DDPS 1** Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen (First Report to the Federal Council of Switzerland about the protection of critical infrastructure) (2007-06-20). Bern: Eidgenoessisches Departement für Verteidigung, Bevoelkerungsschutz und Sport VBS Bundesamt für Bevoelkerungsschutz BABS (Federal Department of Defence, Civil Protection and Sports DDPS and Federal Office for Civil Protection).

Available:
http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.51233.downloadList.66685.DownloadFile.tmp/9039.pdf.
Last Access: August 15, 2008.

Improving the protection of critical infrastructure – press release (2007-07-04). Federal Department of Defence, Civil Protection and Sports DDPS and Federal Office for Civil Protection. [Online] (Available:
http://www.news.admin.ch/message/index.html?lang=en&msg-id=13516
Last Access: August 15, 2008)

**DDPS 1** Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen (First Report to the Federal Council of Switzerland about the protection of critical infrastructure) (2007-06-20). Bern: Eidgenoessisches Departement für Verteidigung, Bevoelkerungsschutz und Sport VBS Bundesamt für Bevoelkerungsschutz BABS (Federal Department of Defence, Civil Protection and Sports DDPS and Federal Office for Civil Protection).
Available:
http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.51233.downloadList.66685.DownloadFile.tmp/9039.pdf.
Last Access: August 15, 2008.

**NEOC 1** The National Emergency Operations Centre (NEOC).
Available: https://www.naz.ch/index_en.html.
Last Access: August 18, 2008.

**ETH Zurich, Centre for Security Studies,** International Critical Information Infrastructure Protection Handbook 2008/2009,
http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663.

**Additional Links**

For more information about the Federal Office of Communications OFCOM including technical regulations and administration visit
http://www.bakom.admin.ch/org/grundlagen/00563/00564/index.html?lang=en

Melani, http://www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=de.

http://www.melani.admin.ch/

Sonia, http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html?lang=en.

# Appendix 1

## *MTP 1: Improving resilience in European e-Communication networks*

In 2008, this MTP will focus on stocktaking, best practices identification and analysis of gaps of measures deployed by both National Regulatory Authorities (NRAs) and network operators and service providers. MTP 1 will also analyse the suitability of currently deployed backbone internet technologies regarding integrity and stability of network. In 2009, the MTP 1 will compare the findings against similar international experiences and results, issue guidelines, and finally formulate consensus-based recommendations after broad consultation with concerned stakeholders. The recommendations will be widely promoted to the concerned policy and decision makers. This MTP will follow and support, as appropriate, the reviewing and updating of the EU Electronic Communication Directives.

## *2.1.1 WPK 1.1: Stock taking and analysis of national regimes to ensure security and resilience of public communication networks*

MTP Name
Improving resilience in European e-Communication networks

WORK PACKAGE NAME :

### *WPK1.1: Stock taking and analysis of national security regimes to ensure security resilience of public communication networks*

### *DESIRED IMPACT (KPIs linked to S.M.A.R.T. goals):*

SMART goal: the analysis covers at least 50% of Member states
KPI: # Member States
SMART goal: at least 3 references in official EU publications or peer reviewed papers
KPI: # references
SMART goal: at least 5 references to official ENISA recommendations
KPI: # references

***DESCRIPTION OF TASKS:***
Across Europe, the obligations and requirements to ensure and enhance the security and resilience of public communications networks, including fixed, mobile, Internet and new IP-based networks appear to be fragmented. The activity would focus on collecting and analysing information and data on the existing national regimes that provide guidance to network operators and/or service providers regarding security and resilience requirements. Analysing the current situation is important to understand how to meet the need of

European and global players for common requirements, rules and practices across the EU that would support the smooth functioning of the Internal Market.

The scope of this work package would primarily include existing security regimes at national level that define requirements and/or practices concerning areas like emergency call management, contingency plan, business continuity and pre-arranged priority restoration, crisis management, mutual assistance, consumers rights against privacy breaches, etc.

ENISA will engage a discussion and work with stakeholders to gather information and conduct the analysis of the way the provisions on security and resilience in the relevant legislation are instantiated in national regimes throughout Europe, with an identification of common approaches and gaps.

The activity will build on the relevant work carried out by European groups (e.g. ERG and IRG), sector associations (such as EICTA, ETNO, EURISPA etc.) and/or by trans-border companies (e.g. Telcos and large ISP) as well as on the findings and results of the earlier national and European studies (like ARECI study).

At the end of 2008, the findings would provide a clear picture on the situation in a number of areas where gaps exists and an effort could be made to improve e-resilience of the public communication networks throughout Europe.

An initial discussion with the relevant stakeholders will help ENISA defining the priority and scope of the work, in particular for what concerns focussing on specific areas.6 ENISA

## *WORK PROGRAMME 2008 2. Multi-Annual Thematic Programmes*

## *OUTCOMES AND DEADLINES:*

- Report on the analysis of security regimes at national level (end of Q4 2008)
- 2 Workshops with relevant stakeholders (Q1 and early Q4 of 2008)
- Plan on the future steps (Q1 2009)

**STAKEHOLDERS**
NRAs, national and EU policy makers, sector associations, large Telcos and ISP

RESOURCES FOR 2008 (person months and budget)
- 7 person months for 2008
- € 200.000 (consultancy)

**WORK PACKAGE PROPOSED BY:**
Commission, 2 Member States

**LEGAL BASE**
ENISA Regulation, articles 3a), c), d), and k)

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Above comes out of pages 15 and 16 from

ENISA Work Programme 2008 Build on Synergies – Achieve Impact. Heraklion, Greece: European network and Information Secuirty Agency (ENISA)

# Appendix 2

## Questionnaire used for the interview

In the context of its Multi-annual Thematic Program One (MTP 1[91]) ENISA intends to take stock of Member States (MS) regulatory and policy environment related to the resilience of public eCommunications Networks.

The stock taking aims at identifying at national level all relevant authorities (stakeholders) and will focus on their tasks, existing policy initiatives and regulatory provisions, exchange of information between authorities and providers, national risk management processes, and preparedness and recovery measures.

Stakeholders could use the findings of the stock taking to identify common approaches, confirm the appropriateness of their measures and activities, and be inspired by the initiatives of other stakeholders from other Member States.

The stock taking will be performed through targeted interviews of small groups of identified stakeholders in each Member State. Interviews are based on the below given questionnaire and will be conducted electronically (i.e. telephone conferences) from July to September 2008 by an external contractor appointed by the Agency. Participating stakeholders will be given enough time to prepare their answers and optionally reply in writing. Written statements will be used by the contractor to better guide the interviews.

The topics of the stock taking were identified by key stakeholders during ENISA's first workshop on the resilience of public eCommunications networks[92]. The questionnaire is a result of extensive consultation with Member States' relevant stakeholders including a dedicated workshop in Brussels on 16th of June.

The proposed questionnaire is organised in three main sections, namely:

- *Scope and Governance*: questions related to mandate, roles of authorities, existing policy and regulatory provisions including voluntary ones,
- *Tasks*: questions related to tasks of authorities, exchange of information between authorities and providers, reporting of incidents,
- *Risk management and Preparedness measures*: questions related to national risk management process, incident response capabilities, response and preparedness measures and best practices.

The results of the stock taking will be validated by the relevant stakeholders through a workshop that ENISA will organise in November. Stakeholders will comment on the

[91] *More information about MTP 1 can be found under:* http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf.

[92] *2. More information about ENISA's first workshop*: http://www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf.

findings of the stock taking and express their opinion on the topics and areas that require additional analysis by ENISA next year. In 2009 ENISA aims at analysing in depth the suggested topics and proposing, in co-operation with the Stakeholders, guidelines for improving the current status.

## Questionnaire

### Scope and Governance

1. Which authority(ies) in your country is(are) responsible for issues related to resilience of public and/or other essential eCommunications networks (e.g. regulation, policy development, co-operation with providers, advice and best practices, etc.)?

2. What is the mandate of each authority in respect to resilience of public and/or other essential eCommunications networks (e.g. roles, responsibilities, co-operation among authorities, etc.)?

3. Are there any regulations, recommendations, guidelines and/or administrative provisions in force in your country related to resilience of public and/or other essential eCommunications networks? Which areas do they cover (e.g. prevention and sustainability measures, preparedness and reaction measures, reporting, implementation measures)? Please provide as detailed answers as possible.

> a. What is the future strategy of your country in this field (e.g. new policy and/or regulatory initiatives, new co-operation initiatives with providers, improvement of preparedness and recovery measures, etc.)?

4. Are there any initiatives between providers and public authorities in your country on issues related to resilience of public and/or other essential eCommunications networks (e.g. public private partnerships, working groups, exchange of information, development of best practices, etc.)?

> a. Which topics are addressed, what is their outcome, how are they financed?
> b. Are there any similar initiatives among providers (e.g. self-regulation, mutual co-operation agreements, exchange of information, etc.)? What is the role of public authorities in these initiatives?

### Tasks

5. What are the typical tasks of the above listed authorities(y) in accordance with their legal mandate?

> a. Public consultation with providers to review existing or develop new regulations, guidelines or recommendations?
> b. Exchange of information between providers and authorities?
> c. Audit?
> d. Enforcement of regulation?
> e. Other? Please elaborate.
> N.B. Make more than one selections as appropriate

6. Do providers in your country exchange information with authorities regarding the resilience of their networks?

a. What kind of information is exchanged, to which authority(ies), under which conditions and how often (e.g. information security policies, business continuity plans, preparedness measures, information on geographical, topological and technical network structures, locations with high infrastructure density, etc.)?
b. How do you use the collected information?

7. Do providers report security incidents (e.g. security breaches, network failures, service interruptions, etc.) affecting the resilience of their networks?

a. What kind of information is disclosed, to whom (e.g. authorities, users, media/public, etc.) and under which conditions (e.g. confidentiality)? Is it done on a voluntary or a mandatory basis?

8. Are providers in your country audited on issues related to the resilience of their networks? What is usually the purpose of such audits (e.g. assess regulatory compliance with existing regulations, etc.)?

a. Who performs these audits (e.g. public authority, third party provider, etc.), how often and under which conditions? (e.g. regularly, randomly, after a notification of an incident, after analysing information received from providers)?

9. What kind of enforcement actions are envisaged under the existing regulations in cases of providers that do not fully comply with them (e.g. penalties)?

## Risk Management and Preparedness Measures

10. Is there a national risk management process in your country related to the resilience of public and/or other essential eCommunications networks?

a. How knowledge, experience and information from providers, incident response capabilities, and other relevant authorities are used to identify risks and develop a solid national risk management process?

11. Which preparedness and recovery measures are established in your country to mitigate risks affecting resilience of public and/or other essential networks (e.g. measures to restore priority communications, definition of priority services, co-operation with relevant public authorities, etc.)? How do these measures remain realistic, accurate, and updated (e.g. exercises, trainings, etc.)?

12. Which incident response capabilities are established in your country for public and/or other essential eCommunications networks (e.g. incident management centres, crisis management centres, CSIRT, etc.)?

a. How do those centres co-operate on a regular basis with commercial and academic centres (e.g. incident identification and analysis, etc.)? Do they also co-operate with centres of other countries (e.g. exchange of information and knowledge)?

b. Are past incidents properly analysed and is that outcome used to update accordingly the preparedness and recovery measures (e.g. ex-post investigations, etc.)?

13. Is there, in your country, a repository of good practices on the resilience of public and/or other essential eCommunications networks (e.g. standards and/or international practices)? Are there any incentives given to providers to deploy good practices?

14. Are there guidelines or policies affecting the procurement of public and/or other essential eComunications networks in your country? Which clauses promote the resilience of these networks and to what extend?

## Glossary

*Audit*: The method by which procedures and/or documentation are measured against pre-agreed standards. [ENISA_08]

*Availability*: The property of being accessible and usable upon demand by an authorized entity. [13335]

*Data integrity*: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [RFC2828]

*Electronic Communications (e-Communication) Network*: Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed [2002/21] (see below definition on public communication networks)

*Emergency Preparedness*: The capability that enables an organisation or community to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage. [ENISA_08]

*Incidence response*: The response of an organisation to an incident that may significantly impact the organisation, its people, or its ability to function productively. [ENISA_08]

*Interconnection*: The physical and logical linking of public communications networks used by the same or a different undertaking in order to allow the users of one undertaking to communicate with users of the same or another undertaking, or to access services provided by another undertaking. Services may be provided by the parties involved or other parties who have access to the network. Interconnection is a specific type of access implemented between public network operators. [2002/19]

*Priority communications*: Are the communication of a government authorised caller placing a call that is marked as priority by the network and given preferential treatment to increase its probability of completion (also known as authority-to-authority calls). [ARECI]

*Public communications network*: An electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. [2002/21]

*Resilience*: The ability of a network to provide and maintain an acceptable level of service in the face of various challenges to normal operation.

*Risk management*: The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. [ENISA]

*Certification*: In the information security domain, certification programmes lend a level of credibility to a practitioner's experience and training, allowing managers to confidently determine the suitability of potential employees or service providers to an information security task. [APEC07]

## References

[RFC2828] Internet Engineering Task Force, RFC2828, available at http://www.ietf.org/rfc/rfc2828.txt .
[APEC07] APEC Guide to Information Security Skills Certification, available at http://www.siftsecurity.net/Static/Download.aspx .
[ENISA], European Network and Information Security Agency, available at http://www.enisa.europa.eu/rmra/glossary.html .
[2002/21] Directive 2002/21/EC of the European Parliament and of the Council, of 7 March 2002, on a common regulatory framework for electronic communications networks and services, Framework Directive.
[2002/19] Directive 2002/21/EC of the European Parliament and of the Council, of 7 March 2002, on access to, and interconnection of, electronic communications networks and associated facilities, Access Directive.
[13335] ISO/IEC 13335-1:2004, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management.
[ARECI] The ARECI Study, www.bell-labs.com/ARECI
[ENISA_08] European Network and Information Security Agency, Business and IT Continuity: Overview and Implementation Principles, available at, http://www.enisa.europa.eu/doc/pdf/deliverables/busin_cont_report_200802.pdf .

# Appendix 3

## Template for Member States

Below you find the information provided to countries

### *People who participated in interview*

| Interviewee | Name | Name | Name |
|---|---|---|---|
| Authority | Department of the Environment, Trans-port, Energy and Communications, DETEC - - Federal Office of Communications, OFCOM | Infrastructure Units (Transport, Industry, ICT-I, Manpower) - - Federal Office of National Economic Supply (FONES) | National Crisis Management Center |
| Position title | Engineer/Architecture Senior Specialist | Manager | Director |
| Education/Training/ Degree | MSc. Engineering | MBA | Master in Public Policy |
| Task and Responsibilities | Responsible for Information Security issues, working on admin regulations, unbundling of services, standardization | ICT infrastructure related matters such as risk analysis, risk management, threat prevention | Managing the center including ICT related matters and critical infrastructure protection – preparing for and leading in cases of national crises |
| If applicable, rel.ship to ENISA | National Liaison Officer ENISA | | |

### *People who provided input but did not participate in interview*

| Interviewee | George Roussopoulos | S. Maniatis,<br>P. Trakadas |
|---|---|---|
| Authority | Hellenic Data Protection Authority | Hellenic Authority for the Information and Communication Security and Privacy |
| Position title | Auditor | |
| Education/Training/ Degree | | Engineer |
| Task and Responsibilities | | |
| If applicable, rel.ship to ENISA | | |

### Authorities involved with Network Resilience

| Authority | Department of the Environment, Transport, Energy and Communications, DETEC - - Federal Office of Communications, OFCOM | Infrastructure Units (Transport, Industry, ICT-I, Manpower) - - Federal Office of National Economic Supply (FONES) | National Crisis Management Center |
|---|---|---|---|
| Main Tasks | Provides relecom regulation, develops regulation and policy, submits regulation proposals to ministry | Secures critical infrastructure and economic supply | Coordinates all national resources during crisis including telecommunication, electricity grid, etc. |
| Reports to | Counsellor (Minister) of Communications | Counsellor (Minister) of Economic Affairs | Federal Council = the highest body in the country – 7 Counsellors = all ministers |
| URL for Agency or Authority | http://www. | http://www. | http:// |
| Year established | 1960 | 1975 | 2003 |

### Authorities involved but not part of the interview

Table 3

| Authority | Xyz | Xyz |
|---|---|---|
| Main Tasks | Establish and run virtual information exchange and consulting group | Protect National Infrastructure |
| Reports to | Ministry of Finance- | Melani |
| URL | http://www.melani.admin.ch | See melani |
| Year agency or authority was established | 2005 approved by parliament | 2008 |

# Appendix 4

## Template for Member States

### References

This reference list provides those acts, governmental and ministerial decrees' which are related to the resilience of public eCommunications networks and points out their particularly relevant articles.

**HR 1** Act XX. of 1949., "1949. évi XX. Törvény A Magyar Köztársaság Alkotmánya" (Hungarian Constitution – available in English).
Available, http://net.jogtar.hu/jr/gen/getdoc2.cgi?dbnum=1&docid=94900020.TV.
Last Access: September 25, 2008.
English non-binding version http://www.servat.unibe.ch/icl/hu00000_.html and http://www.mkab.hu/en/enpage5.htm.

Particularly relevant are articles: 35.§ (1) i), 59.§ (1).

**HR 2** Act LXXIV. of 1999. "1999. évi LXXIV. Törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről" (Direction, organization of defence against catastrophes, and defence against grave accidents concerning dangerous materials – Act on Crisis Management).
Available: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99900074.TV.
Last Access: September 25, 2008.
English non-binding version - only Section 4 of the Act (paragraphs 3, 4, and 30 to 43) http://www.mkeh.gov.hu/Konyvtar?Search=1&topic_id=29&page=3 (near to bottom of the page).

The full law deals with crisis management and its organization, concentration, (mainly on dangerous materials).

Particularly relevant are articles: 5.§ a) and e), 14.§ d) and e), 46.§. to 48.§.

### Additional Resources

**DDPS 1** Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen (First Report to the Federal Council of Switzerland about the protection of critical infrastructure) (2007-06-20). Bern: Eidgenoessisches Departement für Verteidigung, Bevoelkerungsschutz und Sport VBS Bundesamt für Bevoelkerungsschutz BABS (Federal Department of Defence, Civil Protection and Sports DDPS and Federal Office for Civil Protection).
Available,
http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.51233.downloadList.66685.DownloadFile.tmp/9039.pdf.
Last Access: August 15, 2008.

Improving the protection of critical infrastructure – press release (2007-07-04). Federal Department of Defence, Civil Protection and Sports DDPS and Federal Office for Civil Protection.
Available, http://www.news.admin.ch/message/index.html?lang=en&msg-id=13516.
Last Access: August 15, 2008.

**DDPS 1** Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen (First Report to the Federal Council of Switzerland about the protection of critical infrastructure) (2007-06-20). Bern: Eidgenoessisches Departement für Verteidigung, Bevoelkerungsschutz und Sport VBS Bundesamt für Bevoelkerungsschutz BABS (Federal Department of Defence, Civil Protection and Sports DDPS and Federal Office for Civil Protection).
Available,
http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.51233.downloadList.66685.DownloadFile.tmp/9039.pdf.
Last Access: August 15, 2008.

**NEOC 1** The National Emergency Operations Centre (NEOC).
Available: https://www.naz.ch/index_en.html.
Last Access: August 18, 2008.

**Additional Links**

**FI 11** Finnish Communications Authority -- CERT-FI incident report form.
Available English: http://www.ficora.fi/englanti/lomake/TIe.pdf.
Last Access: September 22, 2008.

**FI 12** Finnish Communications Authority -- Form for reporting fauls and disturbances in communications networks and services.
Available English: http://www.ficora.fi/englanti/lomake/TIe.pdf.
Last Access: September 22, 2008.

National Emergency Supply Agency (NESA), http://www.nesa.com, http://www.nesa.fi/organisation/national-board-of-economic-defence/, which is nowadays NESC.