Workshop on Protection of Electronic Communications Infrastructure and Information Sharing

Bucharest, Romania – 16th of June 2015

Venue: Intercontinental Hotel, Bulevardul Nicolae Bălcescu 4, Bucharest, 010051

Minutes of the Workshop

1 Introduction – Dr. Cédric Lévy-Bencheton, ENISA

ENISA introduces the participants and the objectives of the workshop.

The participants are:

- **Mrs. Caroline Groot**, Kadaster.nl (Netherlands)
- **Mr. Erik Wiman**, PTS (Sweden)
- **Mr. Ingemar Björk**, Skanova (Sweden)
- **Mr. Henrik Ravn Lager**, MBBL (Denmark)
- **Mr. Doekele Rienks**, Geodan (Netherlands)
- **Mr. Jörgen Nordman**, PTS (Sweden) – by videoconference

The objectives of the workshop are to understand how different Member States use and manage tools for the protection of underground infrastructure and to understand how information sharing can improve the protection of electronic communications.

For that purpose, the workshop proposed demonstration, presentations and two panels.

2 Protection of underground infrastructure

2.1 Session 1: Presentation of existing tools
Online demonstration of Ledningskollen – Mr. Jörgen Nordman, PTS (Sweden)

Ledningskollen is the system developed by PTS in Sweden to protect underground infrastructure.

After a short presentation, **Mr. Nordman** has shown a live demonstration of the tool. Audience could understand how assets owner can declare their underground infrastructure and how excavators could declare their planned civil work. The usage of Ledningskollen is voluntary and free of charge.

The system acts as a repository, linking assets owners and excavators in the areas of planned civil work. Assets owners can assess if an excavation has an impact on their underground infrastructure, and may exchange maps if needed with the requester.

Several questions were asked by the audience regarding the usage of Ledningskollen. **Mr. Nordman** answered that:

- Every industry is able to access Ledningskollen, and not only the electronic communications sector. This is needed to achieve a success, i.e. all type of infrastructure owners are represented in Ledningskollen.
- In compliance with the Directive 2014/61/CE on broadband cost reduction, Ledningskollen will become the system used for information sharing in Sweden before the end of 2015.
- Cable on poles are also integrated in the system as "aerial interests"
- CAPEX is difficult to assess but the OPEX is 1 Million euro per year.

2.2 Session 2: Evolution of the tools

Future developments of the tool "KLIC" – Mrs. Caroline Groot, Kadaster.nl (Netherlands)

KLIC is the system developed by the Cadastre, Land Registry and Mapping Agency in the Netherlands to protect underground infrastructure.

Mrs. Groot-Pennekamp presents the general functionalities of KLIC, which automates information exchange between underground infrastructure owners and excavators. In the Netherlands, the usage of KLIC is mandatory by law (WION Act) and requesters pay 21 euro per request.

Mrs. Groot-Pennekamp explains that simplification and automation are necessary to improve the adoption of the tool. For instance, future developments include the availability of KLIC on tablets with an augmented reality software that shows underground infrastructure at a given location (e-excavator) and the compliance with the INSPIRE Directive (KLIC-WIN).

Several questions were asked by the audience regarding the usage of KLIC.

Mrs. Groot-Pennekamp explained that:

- Assets owners have noticed a 60 to 80% reduction in damages
- Yet, it is difficult for assets owners to evaluate the exact savings on their business using KLIC

3 Information Sharing

3.1 Session 3: Information sharing

DIO: Online platform for information sharing between providers on unplanned and planned disruptions – Mr. Erik Wiman, PTS and Mr. Ingemar Björk, Skanova (Sweden)

DIO is the system developed by PTS in Sweden to report incidents between operators from the electronic communications sector.

Mr. Erik Wiman from PTS, developer of DIO, and **Mr. Ingemar Björk** from Skanova, user of DIO, presented the functionalities of DIO. DIO acts as an online repository that sends information to all assets owners impacted by an incident on electronic communications. It allows stakeholders to take the necessary actions.

DIO reports are accessible on the web interface with notifications available by e-mail and SMS. An application for smart phones is also available. DIO helps in resolving a crisis by simplifying and speeding up the process of incident report.

Mr. Wiman and **Mr. Björk** replied to several questions from the audience:

- The usage of DIO is voluntary and free to use.
- DIO is managed by an organisation of stakeholders (NTSG).
- There is possibility for PTS (the National Regulatory Agency for electronic communications) to access the incidents shared through the system.

4 Panels

4.1 Panel 1 – Tools for infrastructure protection

Panellists:

- **Mrs. Caroline Groot**, Kadaster.nl (Netherlands)
- **Mr. Henrik Ravn Lager**, MBBL (Denmark)
- **Mr. Doekele Rienks**, Geodan (Netherlands)
- **Mr. Ingemar Björk**, Skanova (Sweden)

The panel answered questions on five topics:

Question 1 – Adoption of the tool in your country

ENISA summarize that the tools presented in this workshop have a very specific goal: protecting the underground infrastructure.

The panel is asked to provide inputs on the following questions:

- **Difficulties regarding the adoption of the tool**
- **Incentives used to promote the usage of the tool**

Mrs. Groot-Pennekamp (KLIC) pointed out the difficulties to start in the Netherlands. She explains the importance of having a good customer care team. KLIC started with 20 operator (5 today), developed had tutorials on the usage of the system. Regarding the incentives, KLIC usage is mandatory in the Netherlands. Indeed, in the 1980's a voluntary system was deployed with no success (no participants). It was pointed out the necessity to involve every stakeholder to draft a code of conduct on the usages.

ENISA proposes that the support for operators and maybe some activities should be regulated when the context needs it.

Mr. Rienks (Geodan) explains that the model for information exchange was standardized. The small operators had difficulties in using the system (lack of resources). **Mr. Rienks** acts as a third-party operator that takes care of data exchange between final users of KLIC and Kadaster. This solution is preferred by several operators (cheaper and easier).

Mr. Björk (PTS) details the system in Sweden, which is voluntary. Before Ledningskollen, a manual system existing (reporting by phone). Ledningskollen improves the reporting. The system integrates 700 infrastructure owners and 3000 excavators. PTS proposes video tutorials on Youtube. Moreover, historical reasons have facilitated the adoption of Ledningskollen (previous campaigns, advertising, education slogan "Call first, dig after")

Mr. Ravn Lager (MBBL) explains that the system in Denmark is not free and that there is a legislation in place since 2004. Before LER, the Danish solution, there had been private solutions for 20 years but legislation was deemed necessary for a full national implementation.

ENISA concludes that tools to protect underground infrastructures need to be supported by public entities. All stakeholders should be involved at the early stages of the conception to facilitate the acceptance of the system. Moreover, legislation depends on the culture and the willingness of the stakeholders to contribute to the system.

Question 2 – Priorities for the development of new tools

ENISA emphasizes that several challenges appear during the development of these tools.

The panel is asked to provide inputs on the following questions:

- **Challenges faced during the development.**
- **Priorities and good practices to follow.**

Mrs. Groot-Pennekamp explains that the development must be considered as an on-going project, with continuous improvement and user support. To this mean, should there be fees to use the tool, she recommends to reinvest a part of the benefits for maintenance, improvements and future planning.

Mr. Ravn Lager points out the fact that IT development is relatively easy. He explains that the main challenge in Denmark is related to the high number of small network owners in the country, some of them being non-profit. These operators lack a professional organization and need an easy-to-use system. **Mr. Ravn Lager** highlights the need of keeping things simple.

Mr. Rienks adds that in the Netherlands, 70% excavator companies use tablets in order to update and get information from the system. It is indeed important to simplify the usage of the tools. He points out the importance of defining a proper data model, and the difficulty for companies to digitize the network maps (which is a required action).

Mrs. Groot-Pennekamp also recommends developers of new tools to directly integrate "advanced functions" in their tools and plan for future requirements and updates.

Mr. Björk agrees with previous statements.

ENISA concludes that new tools should be simple to use, with an emphasize on users and that they should propose advanced functionalities to be useful now and in the future.

Question 3 – Funding of the tool

ENISA explains that the funding of a tool can be a sensitive issue.

The panel is asked to provide inputs on the following questions:

- **Description of the funding scheme at bootstrap and after launch.**
- **Reinvestments of the benefits, if any.**

Mrs. Groot-Pennekamp said that the voluntary phase for assets owners to declare their assets at first allowed KLIC to collect enough data to be an efficient system. In the second phase, excavators requesting information pay a fixed fee of 21 euros.

Mr. Björk points out that PTS, the swedish national grid (Svenska kraftnät) and the swedish Transport Administration (Trafikverket) are paying for the system but operators are contributing indirectly.

Mr. Ravn Lager explains that LER has a self-sustained system, based on fees for the excavators (calculated per square meter). For example a request for 1,000 square meters costs around 2 euro. It makes it cheaper for excavators to use the system than pay a fine after for the cable cuts. Moreover, at the bootstrap LER was funded by a governmental loan that had to be reimbursed.

Mr. Rienks emphasize that even though there is a certain cost for digitize the data, it is always possible to use the maps later for something else.

ENISA concludes that funding of the tool needs public backup at bootstrap and that a business model is needed to fund future developments and maintenance.

Question 4 – Cross-border collaboration

ENISA reminds that the Internet is a cross-border network and that cross-border collaboration can be of interest in case of an outage in a neighbouring country.

The panel is asked to provide inputs on the following questions:

- **Need for cross-border collaborations**
- **Possible contributions by ENISA**

Mrs. Groot-Pennekamp describes that a lot of cables are within national borders, and remain a national.

Mr. Björk is not sure about the status of sea cables in Sweden.

Mr. Ravn Lager explains that no incident involving cross-border cable has ever happened in Denmark.

Mr. Rienks thinks that the INSPIRE Director format could be used across Europe to share information.

A participant from the audience working for the Ministry of Finance in the Netherlands explains that integrating cross-border depends upon objectives. It is difficult to deploy a formal system for cross-border assets. He proposes that ENISA explores this way but he thinks that it can be too early for this.

ENISA concludes that cross-border may not be an issue, since operators may already know their cross-border assets.

Question 5 – Future challenges

ENISA proposes to the participants to explain the future challenges linked to the developments and usages of their tools.

Mrs. Groot-Pennekamp explains that future technologies can facilitate the usage of these tools. For example, augmented reality with e-excavator.

Mr. Björk responds that the system needs to be fast in emergency situations, which is a challenge for their current system.

Mr. Ravn Lager details that today it is difficult to differentiate which information is provided by infrastructure owners. It is important to know the information exchanged, to validate the quality of information and know if it is provided in a timely manner. He proposes that some standards regarding provided cable plans may be useful.

Mr. Rienks explains that today, companies protect their pipes through landmarks.

A question from the audience asks if these systems can be used to evaluate security incidents. Panelists explain that the systems are not used in that purpose today.

Another question from the audience asks if the managers of the tools have relations with other authorities and/or operators of Critical Infrastructures. **Mrs. Groot-Pennekamp** explains that they know which areas are CIP and that the contact persons are known for different sectors.

4.2 Panel 2 – DIO for Information Sharing

Panellists:

- Mr. Erik Wiman, PTS (Sweden)
- Mr. Ingemar Björk, Skanova (Sweden)

Question 1 – Information Sharing as a Service

ENISA asks about the security of information transferred through DIO, which can be viewed as Information Sharing as a Service.

Mr. Wiman explains that this is not an issue as PTS has no view on the information exchanged and nothing is stored regarding incidents.

Mr. Björk details that DIO has contact lists, which is not a real problem as it is the purpose of the tool.

This answers to a question from the audience on requests from inspection agencies: since DIO does not store data and just act as a broker.

Question 2 – Getting momentum for the tool…

ENISA asks the panellists to detail the actions to involve actors in the system.

Mr. Wiman explains that the first action is to find main actors that have an interest in the tool. Once the system is bootstrapped, it become easy to find incentives.

Mr. Björk adds that it is important to make the operators aware so that the usage of DIO can be satisfactory for its users.

Question 3 – How to join DIO in your country

ENISA reminds that DIO can be deployed in other countries and asks about the best organisation to deploy the tool.

Mr. Wiman explains that in Sweden, the National Regulatory Agency for Electronic Communication (PTS) has started transfering the management of DIO to another body. However, the system remains hosted by PTS, which receives trust from users as a public entity.

Question 4 – Cloning of the tool

ENISA details that DIO can be deployed in any country and asks more details on the technical aspects, the updates of the source code and the license fees.

Mr. Wiman details that there is no license fees. DIO relies on a simple web server with “classic” services, with a yearly cost around 10,000.00 euros for all supporting licenses.

5 Conclusion

ENISA concludes that collaboration and information sharing is the key to enhance security. It should be done at different level, but also between the private and the public sector. The tools presented today facilitate such collaboration.

At 13:00 the workshop was closed and all participants were invited to exchange during lunch.