4. CASE STUDY – THE PORT INFORMATION NETWORK

The Port Information Network is incorporated as case study in this master's thesis to check whether the set criteria for the effectiveness of public private security partnerships on the waterfront as constituted in the theoretical framework is also valid in practice. In this paragraph, the Port Information Network is introduced and explained which is necessary to fully understand the analysis of the effectiveness of the Port Information Network (PIN).

The consultants port safety and security, Kathy Dua and Ronny Pauwels, first presented and mentioned the PIN in the preliminary interview: *"… and in addition to that, the whole PIN story is also part of the awareness campaign, so the collaboration is again strengthened there. This is a very wonderful example of public private cooperation with almost 600 companies joining the PIN."* (K. Dua, personal communication, 16th September 2014) The PIN is installed for one and a half year now and currently considered as the most intensive cooperative security intervention between public and private sector at the Port of Antwerp, according to the consultants safety and security. For those reasons, the PIN is the subject of the case study in this master's thesis.

4.1. INTRODUCTION OF THE PORT INFORMATION NETWORK

The term Port Information Network is a translation of the Dutch word ***B****uurt****I****nformatie****N****etwerk* (BIN), literally translated as neighbourhood information network. The first of those networks emerged on an initiative of citizens themselves. BINs are organised by citizens and for citizens in cooperation with local authorities to protect their neighbourhood by raising the awareness and increasing social control. The structure and operation of BINs are determined by the Minister Circular BINs of 10th December 2010. Where BIN's were originally established in neighbourhood areas for citizens, there are now even BINs set up for merchants in shopping areas such as the shopping street Meir in the city of Antwerp (BeSafe, 2015; Respondent D, personal communication, 29th June 2015).

The Port of Antwerp is already a few years cooperating with the police, the court and other judicial institutions, the customs and the private sector. To combat the criminality in the port with an integral approach, the Federal Judicial Police had set up some working groups. One of those working groups had to think about deterrent measures and came up with the idea of 'Very Irritating Authorities'. The intention was that the authorities had to be very present and visible in in the port area that criminals won't be able to commit their crimes. The irritating aspect is the fact that the authorities like the police, firemen, port authority, customs, etc. would be everywhere at any moment, which is not possible of course. Therefore, the working group was

thinking about the involvement of the private security companies. Many companies located in the port area are appealing on those private security companies to do identity checks and controls at the gates of those companies. If all those 'private' eyes were watching too, committing a crime in the port area of Antwerp would not be that simple anymore. By a real time information sharing on suspicious or criminal activities between the local authorities and the private companies, the success rate of committing crimes would decrease while the rate of catching criminals would increase. Because there was no network established that would make it able to share the information in real time, the Port Information Network was established with the same structures and operation methods as determined in that Ministerial Circular. Since January 2014, the Port of Antwerp is the first Belgian seaport with a Port Information Network, a structured cooperation between the companies that are located in the port area and the local authorities (Port of Antwerp, 2014; Respondent B, personal communication, 13th July 2015).

4.2. THE AMBITION OF THE PORT INFORMATION NETWORK

As already discussed above, one of the main objectives of the PIN is to share information in real time about suspicious or criminal situations in order to prevent and discourage those criminals of committing crimes. As a result, a better cooperation between the public and private actors will be generated. Because all the public authorities and the all private actors are alert, the perception of feeling secure increases and social control is encouraged. Another objective is the spread of an 'awareness thought'. All public authorities and private actors have to be aware, but as security is a common responsibility of each person that is doing business in or passing through the port area, every employee, every trucker and in general all the port users have to be aware too. Next to those security objectives, the PIN can also be useful for safety incidents. The communication in the PIN can go in two ways, from the public to the private sector and vice versa. That two-way communication can be useful to inform the private actors in case of emergency or to announce that there are events organised in that part of the port area which won't be accessible from that time to that time. Information about prevention and safety instructions can also be communicated through the PIN (Port of Antwerp, 2013; Port of Antwerp, 2015). The logo of the Port Information Network is figured below.

FIGURE 5: Logo of the Port Information Network (Port of Antwerp, 2013)

4.3. STRUCTURE OF THE PORT INFORMATION NETWORK

The structure and operation methods of the BINs are determined by that Ministerial Circular. For a PIN, this structure is adapted to the port context in a legal way. As a result, a PIN consists of the following actors which are discussed in this paragraph: public actors, private actors, a coordinator and a mandated police officer. In June 2015, the PIN counted 638 members in total but the amount of members is still increasing every month. Another two elements related to the structure of the PIN, are its geographical division in clusters and the technical/financial aspects which are also explained hereafter (Port of Antwerp, 2013; Harbour Master's Office, 2015).

4.3.1. PUBLIC MEMBERS

The list of public members is quite limited and exhausting because there are no more actors involved in the security of the port area (Harbour Master's Office, 2015):

- the Waterway Police
- the Railway Police
- the local police of Antwerp, Zwijndrecht and Beveren
- the customs
- city of Antwerp in the capacity of the emergency planning coordinator
- port authority

4.3.2. PRIVATE MEMBERS

All companies that are located in the Port of Antwerp get the chance to become a member of the PIN. The private companies do not have to pay for their membership and just have to fill in some contact information to become member of the PIN. As a result of those low entrance barriers, there is a coverage of more than 85% of those private companies. Up to now (June 2015), there are each month 'new' members on the private side joining the network (Port of Antwerp 2013; Harbour Master's Office, 2015).

4.3.3. COORDINATION

The coordination of the PIN is the responsibility of both the department port safety and security of the Harbour Master's Office, and the Waterway Police which is co-coordinator. It is the task of the coordinator to be intermediary and the point of contact of the PIN for all the administrative matters about complaints, new memberships, etc., but not for security interventions (Port of Antwerp, 2013).

4.3.4. MANDATED POLICE OFFICER

Guido Bennaerts is the mandated police officer of the PIN. He is police inspector at the local police of Antwerp where he is responsible for advising and facilitating the BINs/PIN, consulting with the coordinator and watch over the functionality of those BINs/PIN. The mandated police officer is also the intermediary between the BINs/PIN and the government. Because the PIN is (mainly) situated in the local police zone of Antwerp, the mandated police officer has to be someone of that zone. That person is also responsible for other BINs in that police zone (Port of Antwerp, 2013; Respondent D, personal communication, 29th June 2015).

4.3.5. GEOGRAPHICAL DIVISION IN CLUSTERS

The PIN is the largest network for this type of BINs. With its enormous surface of 130km², it is necessary to divide the port area in several clusters (see *FIGURE 6)*. Those geographical clusters are the same clusters that are determined by the Port Security Plan for contingency planning. Depending on the suspicious or criminal situation, all the members that are situated in that or in other relevant clusters will be informed by the PIN (Port of Antwerp, 2015; K. Dua, personal communication, 16th September 2014). Further details about the functioning of the PIN are described in paragraph 4.4.

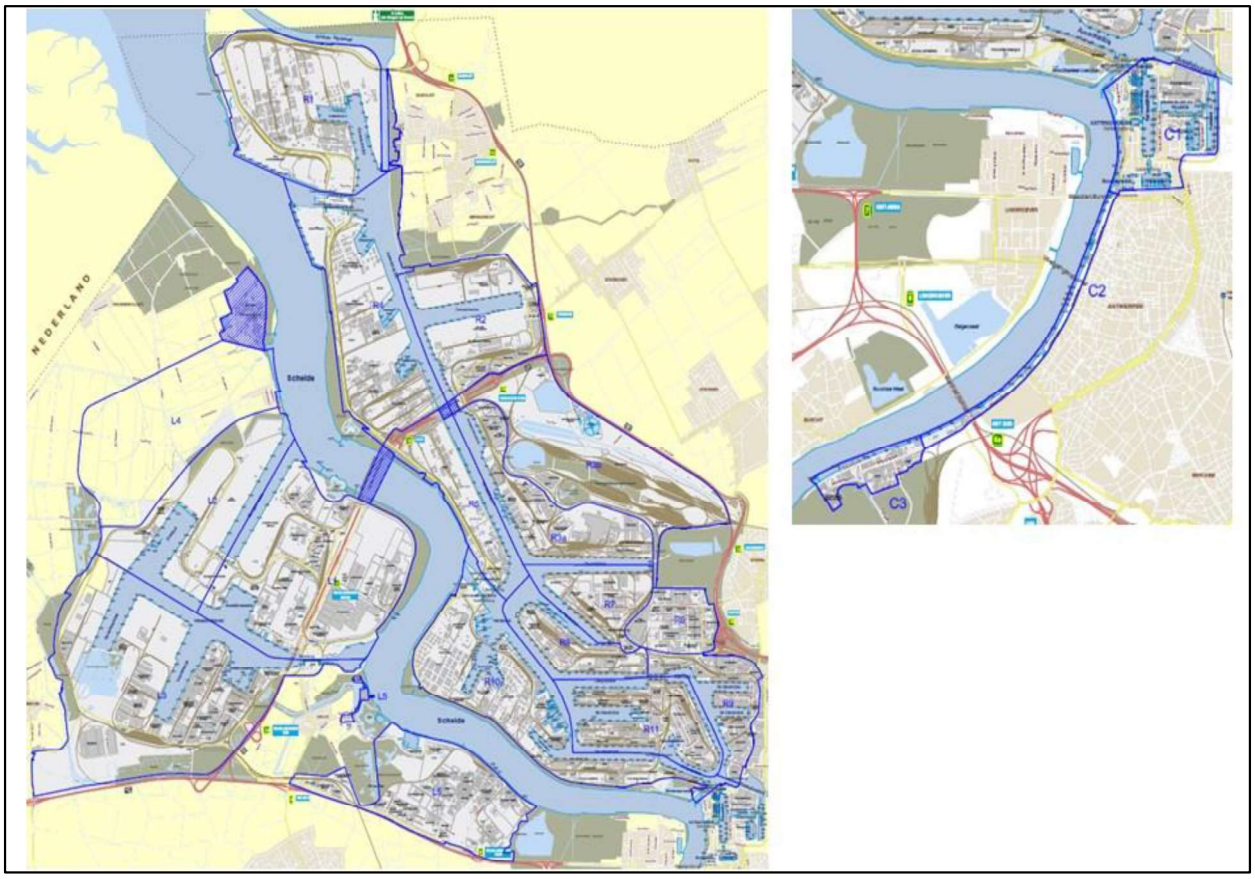

FIGURE 6: Geographical division of the Port Information Network in clusters.

(Port of Antwerp, 2013)

4.3.6. TECHNICAL AND FINANCIAL ASPECTS

If real time information is coming in through the PIN and as a consequence, real time action is needed, a message can be sent to the phones of the contact persons of each organisation or company that is part of the PIN. Sending those telephone calls, maintaining the communication platform and using a system where all information about the members and statistics can be saved, requires money. The province of Antwerp offers a uniform communication system, Enoxus, for free for police zones that are willing to set up a BIN. The maintenance of that system is also included. The remaining costs are the telephone costs which are paid by the port authority. This means that the other public and private actors have to pay nothing for enhancing their security with the PIN. Other port provinces are not offering such a system to their local police zones (Port of Antwerp, 2013; Respondent D, personal communication, 29th June 2015; Respondent G, personal communication, 1st July 2015).

4.4. ACTIVATING THE PORT INFORMATION NETWORK

In the aforementioned paragraphs, references has been made to the functioning of the PIN with telephone calls and emails. The different ways of work and the possible communication flows of the PIN are described here. To conclude this illustrating part of the PIN, some statistics are given to provide enough insight in the PIN to well understand the analysis of the effectiveness of the PNI that is generated in the following part of this master's thesis.

4.4.1. DIFFERENT WAYS OF ACTIVATING THE PIN

There are two possible communication flows in the PIN. A first communication flow follows the input of the PIN-members. The members can report all the suspicious and criminal affairs they noticed in their area. All reports have to be made by telephone to the emergency and dispatching room 101. Those people have to consult the Waterway Police in order to decide whether they will activate the PIN or not. If the decision is to activate the PIN because the situation is serious enough, the Waterway Police will select the necessary information, also taking into consideration the legislation about privacy, and the dispatching room can record a spoken message. That message is sent to all relevant PIN-members which means the members in that cluster and the surrounding clusters if the situation requires this. All member organizations and companies had to appoint one contact person and give his or her telephone number on which he or she is available 24 hours a day and 7 days a week. That person will receive the message on his or her phone and has to confirm that he or she has received the message by typing in a certain key on the phone. If there was no confirmation, the message will be automatically sent a second time after a period of 10 minutes because the information matters for that company too. This is one of the advantages of the PIN that it calls to a person

and not to a central company administration where nobody is available in the weekends and at night. PIN-members that can give extra relevant information about the situation have to report it too. This allows the Waterway Police to give their patrols the most accurate and actual information. Those patrols that are circulating in the port area can anticipate on that and hopefully, they can intercept the suspicious or criminal persons (Port of Antwerp, 2013; Respondent G, personal communication, 1st July 2015).

The message that is sent from the dispatching room to the PIN-members represents the second communication flow. There are two kind of messages that can be sent: 'hot information' by phone as described above, or 'cold information' by mail through the coordinator. The latter can contain preventive tips and tricks or feedback on an incident or on the results of the PIN. The 'cold' information is mostly safety related, but when there is a safety incident, a 'hot' message can also be sent to give the companies the right instructions. The advantage of communicating the information with the PIN is the fact that all addresses are saved in the system and you just have to click a few times to reach a very large population (Port of Antwerp, 2013; Respondent G, personal communication, 1st July 2015).

All the members of the PIN are responsible for a mutual information exchange to enhance the port safety and security. It is also important to give the right information when reporting an incident because the Waterway Police has to be able to direct their patrols on terrain. The PIN coordinators, the department port safety and security of the Harbour Master's Office, have made it very easy for the port users to report the right information by publishing and distributing a 'Suspicious Identification Card'. That card contains several critical elements and characteristics to take into account when you notice a suspicious or criminal situation (Port of Antwerp, 2013). An example of that card can be found in *APPENDIX 5*.

4.4.2. RESULTS AFTER MORE THAN ONE YEAR OF OPERATION

Based on the statistics in *TABLE 4*, the PIN is used but there is no exaggerated use. This can be a good sign because it means that there are not that much suspicious or criminal incidents to notice in the Port of Antwerp. The analysis of the effectiveness of the PIN will show whether this assumption is right or not. Other remarkable figures are those of the months November and December 2014. The explanation for the high amount of 'cold' mails are the national and regional strikes. There were also some strikers points situated in the Port of Antwerp. The coordinator than decided to use the PIN to send actual info about the impact of those strikes on the traffic etc. The other subjects of cold messages are suspicious cars, thefts, emergency exercises, tests, preventive tips, national campaign against theft, etc. (Harbour Master's Office, 2015; Respondent G, personal communication, 1st July 2015).

The coordinator also gets many mails from the PIN-members. The subject of those mails can be a report of an incident that doesn't an urgent response or an incident that has occurred in the past and where it is too late to take some actions. Other mails are sent to change the contact information, reactions on the preventive mails, questions, positive feedback, etc. (Harbour Master's Office, 2015).

Normally we would conclude this paragraph by expressing an impression of the effectiveness of the PIN, based on the statistics. However, the analysis of the effectiveness of the PIN is reserved for the following paragraph. The only thing that can be added to this paragraph is the fact that the section U.S. Customs and Border Protection of the U.S. Department of Homeland Security perceived the PIN as effective by sharing it as best practice in their Customs-Trade Partnerships Against Terrorism Bulletin (see *APPENDIX 6* for the article).

	HOT MESSAGES SENT	MAILS TO THE PIN-MEMBERS	MAILS FROM THE PIN-MEMBERS
12/2013	0	1	0
01/2014	1	3	2
02/2014	0	3	0
03/2014	0	0	0
04/2014	1	1	4
05/2014	0	2	2
06/2014	0	1	7
07/2014	0	0	0
08/2014	1	1	2
09/2014	0	3	2
10/2014	1	1	2
11/2014	0	10	15
12/2014	0	9	10
01/2015	1	2	1
02/2015	0	3	2
03/2015	0	0	0
04/2015	1	3	4
05/2015	0	4	1
06/2015	1	2	5
TOTAL	**7**	**49**	**59**

TABLE 4: Statistics about the Port Information Network.

(Harbour Master's Office, 2015)