# CYBER SECURITY IN PORTS
## BUSINESS AS USUAL?

*PROF. LOKKE MOEREL & FREDDY DEZEURE*

Vlaams Nederlandse Delta

### ABOUT VNDELTA

The Vlaams Nederlandse Delta (VNDELTA) is a governing network of the provinces of Antwerpen, Noord-Brabant, Oost-Vlaanderen, West-Vlaanderen, Zeeland and Zuid-Holland. It focuses on cooperation and networking between companies, public authorities and knowledge institutions. This allows for a pro-active response to social challenges. The country border between Flanders and the Netherlands is not a barrier – on the contrary, it is a catalyst for many opportunities and cross-border cooperation. With its multimodal network of sea ports and airports, train connections, inland shipping, roads and pipes, it is one of the top logistics regions and the gateway into Europe.

### EXECUTIVE SUMMARY

The ports are important drivers for the economies of Belgium and the Netherlands. The port of Rotterdam is the largest port of Europe, counts 3.000 companies, offers jobs to 175.000 people and contributes 3% to the GDP of the Netherlands. The port of Antwerp employs 150.000 people in some 900 companies. Even a smaller port like Gent employs 30.000 people directly and a similar number indirectly.

A lot more needs to be done to protect this logistic backbone against growing cyber threats of criminals and state actors. Adversaries are becoming more sophisticated and brazen towards our more and more IT dependent and interconnected port infrastructures.

Our paper summarizes the risks and provides concrete and pragmatic proposals to increase substantially the cyber maturity and resilience in the ports by organizing training and awareness raising, fostering cooperation and information exchange both between the stakeholders in the ports and across the ports and integrating the cyber risk into the physical security risk management processes and structures already in place within the ports. This also involves a higher degree of oversight by the Port Authorities as is already the case for other security risks than cyber.

### GENERAL OBSERVATIONS REGARDING THE BUSINESS ENVIRONMENT

The ports in VNDELTA function on the basis of a limited number of major companies and a large number of small companies. In addition, the proper functioning depends on the close cooperation between a number of public authorities (port authority, custom authority, municipality, and the seaport and municipality police).

Few of these organisations are fully autonomous. The functioning of the logistic chain for each and every movement of goods or transaction depends on individual entities each contributing to the proper functioning of the logistic chain. There is therefore a very large business interdependency in the ports. This dependency is in particular the case for the port authorities themselves and a number of critical components for the port as a whole, disruption whereof would have a major impact on the whole activity of the port. All of the entities, private or public, are more and more dependent on the proper functioning of IT systems and IT networks to operate and to interact with their customers, suppliers and partners. The paperless integration of the business processes is by now a key asset in the port's logistic service offering, even an absolute prerequisite to remain competitive. For example, the port of Rotterdam exchanges monthly 200.000 messages with nautical partners to process the shipping traffic and the 'Portbase-tool' facilitates weekly 1,5 mio digital messages to facilitate the logistical processes in the port. The Portbase-tool is considered as critical for the functioning of the port of Rotterdam. The 'Antwerp Port Community System' facilitates an equivalent number of messages.

## LEGAL ASPECTS

The **International Ship and Port Security Code (ISPS Code)** provides for a comprehensive set of measures to enhance the security of ships and port facilities and has been developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. In essence, the ISPS Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case.

The risk management activities included in the ISPS Code focus exclusively on physical risks and include a register of critical companies and facilities, the setting up of a security committee, implementation of a security plan in critical facilities and verification of those plans, implementation of incident response plans and exercises to test them are focussing exclusively on physical risks.

Each port is further required to have a Port Security Officer, who is responsible for issuing the so-called International Ship and Port Security certificates required by each company that has access to the sea. For the Rotterdam port the Port Security Officer has recently also been appointed Cyber Resilience Officer. This is not the case in the other ports in VNDELTA and it is not required by the ISPS Code.

**European Network and Information Security Directive:** The mainports of Antwerp and Rotterdam will qualify as 'operators of essential services' (OESs) under the EU Directive on Security of Network and Information Systems (NIS Directive).[1] The EU member States have until 9 May 2018, to implement the NIS Directive into their national laws. The mainports of Rotterdam and Antwerp will qualify as OESs under the NIS Directive.

The NIS Directive requires OESs to take appropriate and proportional technical and organizational measures to manage security risks, as well as prevent and minimize the impact of security incidents. OESs will have to report to the national competent authorities for cyber security (NCSC and CCB, respectively) any incident having a significant impact on the continuity of services that are deemed essential, and they will have to comply with information requests and instructions from competent national regulators.

The NIS Directive further requires that the OESs to set up so-called cyber 'information sharing and assessment communities' (ISAC's), with the aim of exchanging information on threats and successful prevention measures, supported by the respective Dutch and Belgium national cybersecurity centres. The mainports of Antwerp and Rotterdam have already set-up such ISAC.

However, given the large inter-dependency of the organizations within the mainports, the security risk management obligations under the NIS Directive are expected to require also the setting-up of prevention and mitigation measures as well as oversight over the proper implementation of these mechanisms, as well as the reporting of incidents and the response.

[1] See art. 4 and Annex II of the NIS Directive.

There is currently no formal role foreseen for the Port Authorities within the NIS Directive and its draft implementation modalities.

**Data protection:** Similar security obligations apply when organizations in the VNDELTA process personal data. When the General Data Protection Regulation enters into force in May 2018, data breach notification requirements to the Data Protection Authorities and the individuals concerned will come into force for Belgium and will replace the current (very similar) data breach notification requirements for the Netherlands.

## OBSERVATIONS REGARDING THE PORTS' IT VULNERABILITY

As more and more of the ports' *administrative business processes* (IT environment) are automated and interconnected between organisations, they depend on the internet to operate as a result of which the 'attack surface' for cyber threats is increased as these organisations become also exposed to threats coming via connected organisations and directly from the internet.

Illustrative example here is the 'Navigate' tool, which has been recently launched by the port of Rotterdam and is by now adopted in 70 countries. This tool facilitates global route planning connecting 550 ports globally, as well as provides rail and inland shipping routes to 150 European inland terminals, a company guide for the Rotterdam port as well as an 'empty depot' tool, reporting on the location of empty containers, and where they can be picked up and returned.

Another example is the Belgian e-Desk tool used in the ports of Antwerp and Zeebrugge, which facilitates paperless export of container and roro shipments. This application is used by thousands of exporting companies throughout the EU. There is an increasing part of the *operational/industrial control systems* (Operational Technology environments) that becomes connected to the network, increasing the attack surface. Examples here are handling control systems, traffic control, lock control systems, building control systems, access control systems to warehouses, utility control systems etc.). The port systems are also interconnected with customs IT systems, which get ever more sophisticated due to EU customs policies such as Single Window.

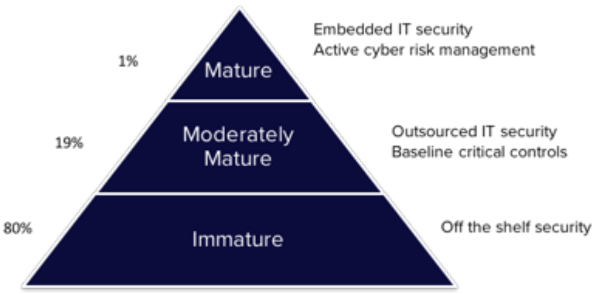
Other development is the increasing use of *Internet of Things devices* (sensors and camera's), again increasing the attack surface.

Finally, the internal networks of the larger organisations in the ports are physically exposed (outdoor) and exposed to the insertion of rogue devices by people that want to cause harm to the organisation.

In light of above developments, our general observation is that the IT security culture and cyber hygiene (awareness, inventory of assets, baseline security controls, including segmentation between the IT and OT environments, security policies and compliance, back-ups) is lagging behind developments. Most port companies rely heavily on blue-collar workers with little or no IT security awareness. Even within the office environment the awareness would deserve being increased.

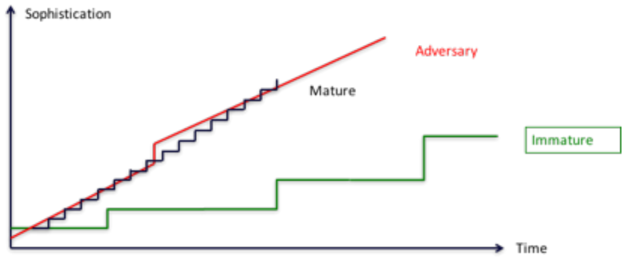
Few organisations in the ports have dedicated IT security staff and none have a mature security incident detection and response team. Few, if any, companies have an intrusion detection sensor network in place in their IT or OT networks. There is currently no specific threat intelligence available for ports, but in case it would exist the port organisations would currently not be mature enough to take benefit of it.

As indicated before, there are currently cyber information sharing communities (ISACs) set up in the ports of Antwerp and Rotterdam. They meet on a quarterly basis under the patronage of the Port Authorities with a particular focus on *awareness* raising.



In the graphical representation above we estimate that most of the organisations in the ports and the ports as a community qualify in the 80% at the lower end of the pyramid of maturity with respect to cyber security.

A consequence of this is that the gap between the level of sophistication of the adversaries, even the non-state actors, and the protection of the critical assets, is increasing over time. Whereas mature organisations are able to adapt to the increasing level of sophistication of their adversaries, the immature ones rely exclusively on off the shelf products, will increasingly lag behind.



## PERCEIVED THREATS

Cyber threats to the port activities, as with any other activity, can be subdivided in *non-targeted threats and targeted threats*. The port of Rotterdam has reported various targeted cyberattacks on companies in the port, some of which were criminal in nature but some were also attempts to sabotage and espionage by state actors. 10% of the companies in the port of Rotterdam have further reported they have experienced ransomware attacks.

**Non-targeted threats** are generic and therefore threat all sectors and organisations. These threats almost always aim for financial gain in an indiscriminate manner by using cyber-crime malware, ransomware and credential theft. Organisations active in the ports are more exposed to these generic threats than most other sectors because of their high degree of interdependency/interconnection and lack of adequate cyber hygiene and IT security culture. The impact of commodity malware with a low level of sophistication can therefore be substantial, as we recently have seen in the recent NotPetya case (see in more detail below).

**Targeted threats** are specific to an organization or activity. We currently assess the likelihood of the threats as follows:

*Highly likely:*

- Targeted cybercrime (ransomware, financial transactions, CEO fraud, invoice fraud);
- Information stealing or modification with the purpose of facilitating trafficking of goods (e.g., drugs, cigarettes, arms, illegal parallel imports) or subverting security controls;
- Information stealing with the purpose of obtaining inside information on financials, processes, customers or markets. To be noted in particular in this context are the Chinese One Belt One Road initiative[2] as a potential future competitor for the Mainports.

*Moderately likely*

- Sabotage or disruption by insiders, hacktivists or terrorists.

*Low likelihood, but potentially high impact*

- Disruptive attacks by state actors.

The most likely threat vectors ('vectors' are means to achieve unauthorized access) are currently perceived as being:

- *Spear phishing,* directly from an external sender or via a trusted partner as a spring board;
- *Insiders* gaining directly unauthorised access to information systems;
- *Rogue physical devices* (USB, Internet of Things) inserted by outsiders or insiders;
- *Cross-contamination* or lateral movements from connected networks (partners, suppliers, customers).

[2] https://qz.com/983460/obor-an-extremely-simple-guide-to-understanding-chinas-one-belt-one-road-forum-for-its-new-silk-road/

## POTENTIAL IMPACT

For illustrative purposes, we made a high-level overview of the impact of the recent NotPetya incident. The incident substantiates that the impact of disruption caused by a cyberattack on the ports can indeed be very substantial. Multi-million figures of losses have been reported by some of the impacted companies:

- More than 250 million euro financial impact for Maersk/ APM Terminals. Seventeen terminals operated by APM, including two in Rotterdam, were disrupted for multiple days and operations had to be carried out manually. APM's customer portal was disrupted and caused the company to interrupt taking customer orders. The interface between APM and the customs authority was interrupted, requiring manual customs checks. Other affected systems caused disruption of loading and unloading of containers because of the impossibility to correctly identify the shipments. As a result, trucks could not be directed to the correct location and had to be allocated additional parking space for the period of disruption. Also, the camera surveillance of the APM terminals was disrupted, requiring replacement by physical surveillance.
- TNT reported that the cyberattack may materially impact the results without being able to calculate the financial impact at this stage, a figure of 300 million euro is being quoted. One month after the incident operations were still not fully recovered. TNT indicated that it is possible that it would be unable to fully restore all of the affected systems and to recover all of the critical business data encrypted by the virus. Some customers have been waiting for a month for parcels which should have been delivered next day. Customers have been asked to re-submit documents that had been scanned into systems which were impacted by the malware.
- Customers of both Maersk/APM and TNT have experienced delays in delivery of their goods with consequential economic impact. Some transports with perishable goods may have been lost.

The NotPetya cyber incident turned out also to be very much a physical security incident, resulting in business continuity issues very much resembling 'regular' threats as fire, flooding and terrorist attacks. Noteworthy is also that in the NotPetya incident, all stakeholders very much looked at the Rotterdam Port Authority for guidance and leadership, and the Rotterdam Port Security Officer / Cyber Resilience Officer indeed managed the incident through the existing ISPS security emergency procedures and infrastructure.

## PROPOSALS

In order to increase the cyber readiness and resilience of the port communities and in anticipation of the NIS Directive being implemented in Member State laws, the VNDELTA may consider implementing the following pragmatic actions, some of which can build on the experience in other sectors (FI-ISAC in finance, ENCS in energy).

There is obviously a large variation in size and means of the different ports in VNDELTA. As in other business sectors, we note that in respect of cyber security we see as a best practice develop that 'mature helps less mature', as all communities depend on each other and competition on cyber security is to the detriment of all. The measures below will therefore in any event apply to the mainports of Antwerp and Rotterdam and may have to be scaled down for other ports (and may not be achievable in some of the smaller ports at all).

- Identify clear responsibilities for oversight, accountability, reporting and compliance for the mainports identified as 'operators of essential services' under the NIS Directive.
- Consider leveraging as much of the infrastructure set up by the ports to implement their risk management activities required under the ISPS Code;
- Develop under the authority of the Port Security Officer a common cyber hygiene baseline with minimum requirements and controls considered as necessary to thwart moderately sophisticated attacks as well as a certification mechanism based on self-assessment. Develop a set of cyber maturity indicators and a reporting dashboard;
- Validate under the authority of the Port Security Officer the compliance with the cyber hygiene baseline and cyber response plans for the critical facilities and for those organisations wishing to have external validation and receive improvement recommendations, potentially combined with a "cyber secure" label;
- Assess the opportunity of setting up a joint Cyber Emergency Response Team (CERT) for each mainport, using pooled resources (as is currently already done for physical security and emergencies, such as fire brigade) or clarify if the Dutch

and Belgium national cybersecurity centres can fulfil this role;

- Intensify the existing cyber information sharing and assessment community (ISACs) within the mainports with the aim of exchanging information on threats and successful prevention measure and increase the support by the respective Dutch and Belgium national cybersecurity centres with expertise and threat information;
- Set up a cyber community of practice for (clusters in) the ports in the VNDELTA (potentially extended to include Hamburg and Bremen) with the aim of disseminating any threat information and successful prevention measures;
- Discuss mutual support and fall-back options between ports in case of severe disruption using existing cooperation channels as much as possible. Include cyber incidents in the existing Business Continuity Plans;
- Organise on-site training (including C-Suite and Board level) and awareness raising by pooling resources/interest;
- Organise an initial and subsequent annual cyber exercise, initially within the community of a single port, at a later stage potentially across different ports.

The proposals aim to shift the level of maturity of the organisations in the ports and to allow them to follow more closely the development of the threat.

***Prof. Lokke Moerel*** *is senior of counsel with the technology focused U.S. law firm Morrison & Foerster, professor of Global ICT Law at Tilburg University and a member of the Dutch Cyber Security Council (the advisory body of the Dutch cabinet on cybersecurity).*

***Freddy Dezeure*** *was Head of the Computer Emergency Response Team of the European institutions (CERT-EU) until June 2017. At present, he is an independent consultant providing strategic advice in cyber security and cyber risk management and acting as Board Member and Advisory Board Member in several high-tech companies.*