The Potential of AI and Data Science in Reducing the Vulnerability of Ports to Undermining Crime

Nienke de Groes

Dutch Police Academy & Leiden University[1]

Willem-Jan van den Heuvel

Jheronimus Academy of Data Science

Pieter Tops

Jheronimus Academy of Data Science, Dutch Police Academy & Leiden University

Abstract

The port of Rotterdam is an important gateway to Europe and an important logistic hub for global trade. However, factors that ensure the competitive position of the port of Rotterdam are also attractive for drug criminals. In this paper the findings of an empirical study on the potential of AI and data science in securing ports against undermining crimes are presented. The study consisted of a qualitative research, which was conducted through semi-structured interviews, in-depth interviews, and an expert meeting. The findings of this research show that developments in Data Science and AI at ports could have a strong effect on reducing the vulnerability of ports against illegal activity. With the advent of smart technologies, the vulnerable human factor (in the context of undermining crime) in port processes could, gradually, become less important and be replaced by technology. However, new vulnerabilities may arise in the field of data ownership and cybersecurity. To realise the potential of AI and Data Science to protect ports from undermining crime, attention must be paid to these vulnerabilities, as well as ensuring the acceptance of the new (automated) technologies and adopting a systems approach.

Keywords: data science, artificial intelligence, undermining crime, seaports

1 Corresponding author's email: nienkedegroes@gmail.com

Introduction

In this contribution[2], we describe the possibilities that technological developments (in data science and Artificial Intelligence) at ports could offer for reducing the vulnerability of ports to undermining crime. In addition, we consider what would be required to realise this potential of data science and AI in the short and long term and what new vulnerabilities may arise. This contribution is based on international academic literature and the results of our own exploratory research[3], which focused on the relationship between technological developments in seaports (the movement towards Twin Harbours) on the one hand, and the vulnerability of ports to undermining criminal activities (particularly the import of drugs) on the other (see Tops, P., van den Heuvel, W., de Groes, N., & Gravenberch, V., 2021).

Seaports play an important role in world trade and are also a major hub in the international drugs trade. Incidentally, it is not only about drug trafficking (although that is a very important category), but also about arms trafficking, human trafficking, and trade in counterfeit products. The intrinsic interconnection between the legal and illegal world plays a major role in the daily reality of ports. This also applies to the Dutch seaports, with the port of Rotterdam in the lead (see also Staring et al., 2018). Rotterdam is the gateway to Northwest Europe and an important logistics hub for world trade (Port of Rotterdam 2019; Jacobs 2000, in Roks, Bisschop & Staring, 2021). The quality of the port facilities and the logistical efficiency of the Port of Rotterdam are not only beneficial for the legal economy, such as excellent accessibility by water, rail and road; high-quality port infrastructure and the efficient handling of containers and cargo (Port of Rotterdam, 2019; Van der Horst et al., 2019; in Roks, Bisschop & Staring, 2021), but also for undermining crime. This has led, among other things, to the port of Rotterdam becoming the main gateway for cocaine for Europe (UNODC, 2018, in Staring et al., 2019). With a certain regularity, reports on new 'record drugs seizures' appear in the Dutch media. In September 2021, an enormous quantity of cocaine of 4,022 kilos was intercepted in the port of Rotterdam, with a probable street value of more than 301 million euros (Public Prosecutor, 2021). In the same month, the police removed nine suspects from a container in the port of Rotterdam. These persons had broken into the container to take drugs out of the container and called the police after they had trouble breathing in the container (NOS, 2021). In 2020, over 40.000 kilos of cocaine were detected in containers in the port of Rotterdam. This was approximately 7.000 kilos more than in 2019 when 33.732 kilos of cocaine were intercepted. The total street value of cocaine seized was over EUR 3.5 billion. There is a trend in the interceptions towards increasingly large shipments: in 2020, 12 consignments above 1.000 kilos were intercepted (HARC team, 2021). It is assumed that the above figures of drug seizures in the port of Rotterdam are just the tip of the iceberg, as only a small proportion of the 7.5 million containers that pass through Rotterdam annually are checked (NOS, 2021).

The most vulnerable factor at ports from an organised crime perspective is the human factor (Hiemstra & de Vries, 2021). After all, there are tens of thousands of people working in the ports who – given their relatively low incomes – can 'easily' be bribed or threatened (Tops et al., 2021). The consequences of undermining crime at seaports are great:

- The corruption of organisations, such as security companies, customs, transhipment companies (see Nelen & Kolthoff, 2017; Bisschop et al., 2019);
- The attraction to young people in particular, who for example take the drugs out of the containers (see Verseput & de Haan, 2021; Ghosen, 2021)
- The use of violence, in the form of liquidations, mistaken murders, shooting incidents (see, among others, Meeus, 2019).

Interestingly, the vulnerable human factor (in the context of undermining crime) is likely to disappear from the ports as the role of technology increases and gradually takes over human activities. Digitalisation means that the human factor could be removed from the process. For example, crane operators could be replaced by automated cranes, border police could be replaced by smart containers, truck drivers could be replaced by self-driving cars and harbour masters could be replaced using smart ships that contact docks directly to check availability and make reservations without the need for human intervention (Van den Heuvel & Tops, 2021). These technological developments can potentially play an important role in securing ports against undermining crime. For example, the development of

2 The authors wish to thank dr. Vlad Niculescu-Dincă (Institute of Security and Global Affairs, Leiden University) for his stimulating comments on an earlier version of this contribution.

3 Throughout the text this research is referred to as Tops et al. (2021) or short *the study*.

'smart containers' will probably make it considerably more complicated to use containers for criminal purposes. Smart containers can only be opened at specific geographical endpoints, so-called 'geofencing', and accurately record (permanently and in real time) the contents, weight (and changes in weight) and transport movements of the container. These technological developments could make the criminal exploitation of containers for criminal purposes less attractive, as criminals choose the path of least resistance (Tops et al., 2021).

This contribution explains, from a long-term perspective, how vulnerabilities in seaports could be reduced through the application of Data Science and AI. This contribution addresses an important gap in the scientific literature; the lack of literature about the use of digitisation and Data Science to reduce the vulnerability of ports to criminal (drugs) activities. A literature review by Van den Heuvel and Tops (2021) on (improved) security of (smart) ports, revealed that the vast majority of the analysed scientific literature relates to potential (new) technologies, tools and methodologies, while the number of actual experience reports, longitudinal studies, empirical experiments and case studies is limited. Only a few papers explicitly address the relationship between ports and security (e.g. Lokulaluge et al., 2012; Poikonen, 2021). However, the role that digitisation and Data Science can play in reducing the vulnerability of ports to criminal (drug) flows has not been studied yet. As one of the main pioneers in the application of Data Science and AI technology in ports, and also a location where a lot of drug-related crime takes place, the Port of Rotterdam serves as a good case study to explore the potential of Data Science and AI in securing ports against undermining crime. Furthermore, this contribution emphasises that strong attention should be paid to the human factor – even in an automated and very digitalised future of seaports. This strong suggestion is highlighted by proposing that the leading model in studying acceptance and usage of new technologies – the Technology Acceptance Model, which assumes an active user and close proximity to the technology – should be reviewed for automated environments in which the user could have a more supervisory and distant role in the interaction with the technology.

Content

This contribution begins with an explanation of the methods used in the research and with a further explanation of the Technology Acceptance Model. We outline the trend of smart ports that could increasingly operate autonomously using the example of a smart container (Container 42). We then discuss the potential of Data Science and AI in reducing the vulnerability of ports to undermining crime using the findings of our own research, after which we consider important conditions to realise the potential and new vulnerabilities that might arise. We conclude this contribution by presenting a conclusion and recommendations.

Methods

This article draws mainly on the exploratory research of Tops et al. (2021). This practical exploration of the potential of Data Science and AI in reducing the vulnerability of ports to undermining crime consisted of two phases. The first phase consisted of an exploratory phase where relevant stakeholders were interviewed using semi-structured interviews with a topic list, which also included relevant questions related to the acceptance of automated technologies in order to discover new factors that might be of relevance to adjust the Technology Acceptance Model for automated technologies. The interviewees were selected based on their involvement in and knowledge of the issue of undermining crime at seaports. Amongst them were security professionals from the port of Rotterdam and the port of Moerdijk, the seaport police of Rotterdam and a senior researcher on port economics. In the second phase, the conclusions and observations from the interviews of the previous phases were presented to a broader forum of experts during an expert meeting and were tested against their experience and expertise, using the Delphi method.

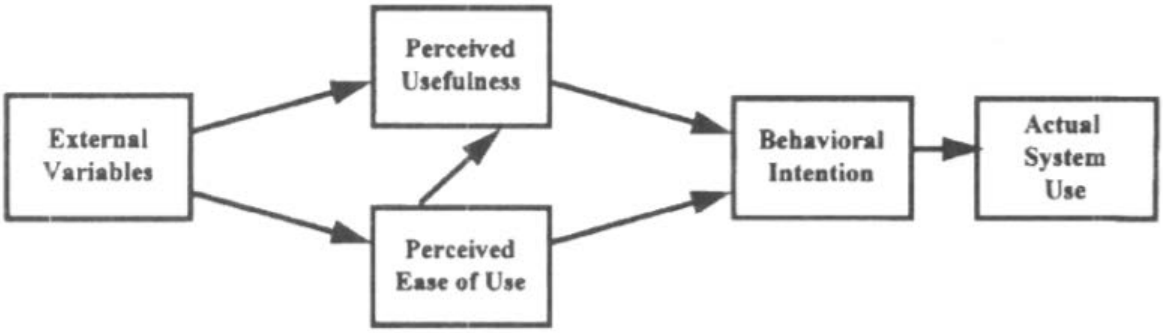
Technology Acceptance Model

While a wide range of models exist that focus on the acceptance of new technologies by the active user, few if any models focus on the acceptance of automated technologies – where the role of the human (the user) is tending to decline. Technology-acceptance models, like the *Technology Acceptance Model* (TAM) (Davis, 1986), focus on the acceptance of technologies where a user has an active role. However, in the case of smart ports, the role of the user could gradually be-

come smaller, more passive or could even disappear completely in the long run. Therefor it is important to reconsider the factors that stimulate acceptance and usage of the new automated technologies in the TAM and consider a new acceptance model for automated technologies. In the research of Tops et al. (2021), the TAM was used as guideline to discover and analyse if and what new factors could be of relevance for the acceptation and usage of automated technologies in future smart seaports.

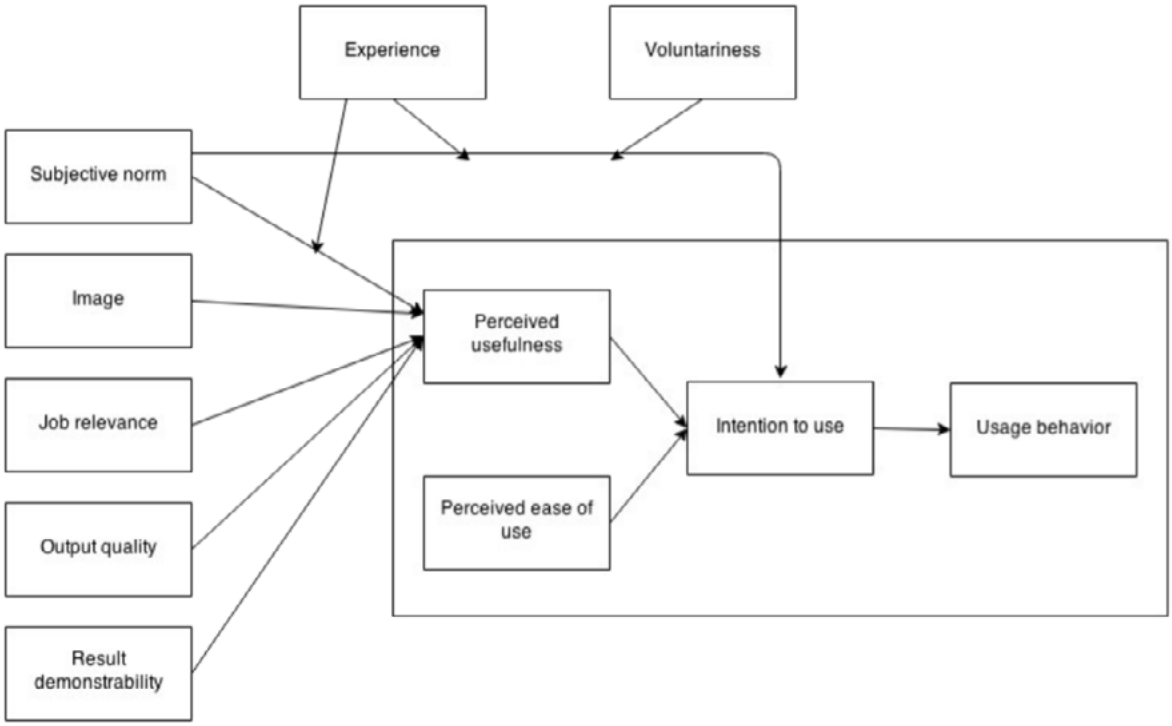
The TAM (Davis, 1986) is a leading model for explaining or predicting individual technology acceptance. This model illustrates how users come to accept and use technology. The TAM states that users' behavioural intention to use technology is influenced by the perceived usefulness and perceived ease of use of the technology (Venkatesh & Davis, 2000). According to Davis (1989), perceived usefulness – the belief that using the new system will increase performance – and perceived ease of use – the extent to which a person believes that using a particular system will be effortless – are the two main indicators that influence the use of technological systems. Davis, Bagozzi and Warshaw (1989) stated that the ability of TAM to explain individuals' attitudes and behaviour towards technological systems also depends on external variables. These external variables simultaneously influence perceived ease of use and perceived usefulness. What these external variables are, depends on the environment in which the research is conducted. Colvin and Goh (2005) validated the TAM for police officers and showed that the findings of the TAM were empirically supported in law enforcement environments.

Figure 1. Technology Acceptance Model (TAM) (Venkatesh & Davis, 1996, p. 453).



Venkatesh and Davis (2000) extended the original TAM by including subjective norms and cognitive processes, resulting in TAM2 (Lin et al., 2004). Social influence processes, subjective norms, voluntariness, image, cognitive processes, job relevance, output quality, demonstrability of results and perceived ease of use are included as factors in TAM2.

Figure 2. Technological Acceptation Model 2 (TAM2) (Venkatesh & Davis, 2000).



The trend towards 'digital twins' and 'smart ports'

Digital Twins are a digital reflection of a physical or cyber-physical object and were developed in the Smart Industry (Industrie-4.0), also known as the fourth industrial revolution. The fourth (and current) revolution is characterised by new technologies that increasingly influence social, industrial, economic, and governmental disciplines, such as big data applications, artificial intelligence, robotics, 3D printers, autonomous vehicles, mobile internet, Internet of Things (IoT) and Cloud technology (Ernst et al., 2019). According to Schwab (2016), with the advent of big data and technological innovations, a fourth revolution has begun that, more than previous industrial revolutions, is unique in scope, complexity and speed. Digital twin technology is applied in the domain of smart cities, but this technology has also made its appearance in the domain of seaports (Van den Heuvel & Tops, 2021).

The ambition of the Port of Rotterdam is to become the 'smartest port' in the world (Port of Rotterdam, 2019) and to this end, it has joined forces with several global IT players (IBM; CISCO) to develop a digital twin of the port; Twin Harbour. The development of digital twins aims to go beyond what is possible in the physical world using traditional processes. This approach is made possible by recent advances in IoT technologies, including sensors, wireless connectivity, and artificial intelligence. In theory, digital twins enable a holistic digitisation of harbour objects within their spatial-temporal context, going beyond simple automation and digitisation of traditional human processes. The Twin Harbour forms a system-of-systems in which every object in a harbour, ranging from building, dock to bollard, can be imitated, observed, and controlled by means of a digital twin. In a Twin Harbour, physical objects will – in theory – be digitally available and interact with each other in an automated way without human intervention. This means *de facto* that the need to exchange (electronic) documents through human actors could gradually disappear and make way for direct communication between the digital 'smart' objects in a Twin Harbour through automated messages. This could lead to 'smart harbours' that are increasingly populated by autonomous smart objects, ranging from 'static' smart containers to dynamic vehicles including trucks and ships.

A crucial part of (smart) seaports, are containers. Approximately 90% of all trade is conducted via maritime containers, of which more than 500 million are shipped annually in the supply chain. This incredible quantity of containers travelling by sea from country to country and continent to continent makes them a prime target for individuals or organised groups involved in illicit drug trafficking, arms

trafficking, or human trafficking and for those involved in the production and supply of counterfeit products (Tops et al., 2021). Both customs and other authorities were surprised during the 1980s with the use of containers by international drug cartels and smugglers. The latter made clever use of the anonymity, relative concealment, reliability, and efficiency of containers to transport drugs (Levinson, 2016). For example, essential raw materials for synthetic drugs, the so-called precursors, are mainly produced in China. From China they are transported to the Netherlands, often via containers, to be converted here into the desired end product, i.e., ecstasy, amphetamine and methamphetamine. A large proportion of these end products are then distributed around the world. Without a sophisticated international logistics system, none of this would be possible; containers play a crucial role here (Tops, van Valkenhoef, van der Torre, & van Spijk, 2018). This has allowed local drug producers to grow into international players where the location of customers is of minor importance, given the low costs of transport. After all, containers proved to be just as efficient for transporting legal as illegal products, including drugs, immigrants, counterfeit products, and weapons/munitions. The global dependence on maritime trade, combined with sophisticated methods of concealment by drug traffickers or product counterfeiters and diverse smuggling routes, make successful interception and intervention a difficult task. Previously, the focus was mainly on the physical security of containers; the demarcation of container storage areas and access controls. However, this focus is broader nowadays, due to the many possibilities offered by AI and Data Science. For example, container security is increasingly equipped with 'smart' automated systems, for example biometric access controls that use computer vision technology, resulting in 'smart containers'.

A concrete example of a smart container can be found in the port of Rotterdam under the heading of 'Container 42'. The 'Container 42' project is a good example of the digital transformation that the Port of Rotterdam is pursuing, as the port has the ambition to become the smartest port in the world (Port of Rotterdam, 2019). The 'Container 42' project, which started in 2019, is committed to developing a smart container equipped with dozens of sensors to detect vibration, temperature, GPS position, noise, and air pollution, among other things. The data generated by these sensors will enable the container to make decisions autonomously to a certain extent. An essential part of the smart container is a 'smart lock' that can determine exactly where and when a container was opened and can indicate in advance where a container may be opened by applying 'geofencing' technology (Van den Heuvel & Tops, 2021). Thanks to the smart lock, containers can be used less easily for criminal purposes (such as the illegal transport of drugs). Containers are an essential part of seaports, and thus also of the concept of 'smart ports', and could potentially make the port system less vulnerable to criminal exploitation.

Figure 3. Container 42 (Onze Haven, 2020).

The potential of AI and Data Science in reducing the vulnerability of ports to undermining crime

In this section, we explain the potential of AI and Data Science in reducing the vulnerability of ports to undermining crime. We do this by using relevant literature and findings from our own research (Tops et al., 2021). This section focuses on the following argumentation, which will then be discussed step by step.

1. Recent years have shown increasingly better physical security at ports (e.g. through better surveillance, access passes, smart fencing);

2. As a result, criminal attention has shifted to the human factor (bribing people to gain access to the port area); Therefore,

3a. On the short term, we need to pay more attention to the human factor because this risk is not likely to disappear soon.

3b. On the long term, we could reduce these vulnerabilities by investing in promising technological developments (Twin Ports, Container 42, AI, Data Science) which announce amongst others to diminish the importance of the human factor.

Step 1. Recent years have seen an increase in the physical security of ports (e.g. through better surveillance, access passes, smart fencing)

Seaports constitute logistical infrastructures that are vulnerable to international drug trafficking; it is a phenomenon that has been extensively documented (Staring et al., 2019; Sergei et al., 2021; Noordanus et al., 2020; Tops & Tromp, 2021) and also acknowledged in government documents (BOTOC, 2018). In recent years, there has been significant investments in the physical security of ports, including the deployment of entrance gates, guards, surveillance vehicles and extensive camera surveillance (Roks, Bisschop, & Staring, 2020). Based on interviews, Nelen and Kolthoff (2017) found that stakeholders in the port have succeeded in using combined efforts to significantly raise the threshold for criminal activities in the port area through risk analysis and stricter supervision.

In this and other ways, ports have worked on improving their physical security in recent years. They all have in common that they try to make it more difficult for 'unauthorised persons' to gain access to port areas.

Step 2. As a result, criminal attention has shifted to the human factor (bribing people to gain access to the port area)

However, the downside of success in improved security is that criminals increasingly rely on contacts within the port area to secure and relocate drugs or other illegal goods (Nelen & Kolthoff, 2017). With the improvement of physical border gates to the port, the focus from the criminal organisations has shifted to trying to influence the human factor (Roks, Bisschop & Staring, 2020). Hiemstra and de Vries (2021) therefore conclude in their report that the greatest vulnerability, exploitation, and risk associated with any port processes is the human factor. After all, a wide range of port employees have physical access to port sites, insight into the refinement of port logistics and detailed knowledge of container numbers and -locations, security measures and supervision (Roks, Bisschop & Staring, 2020). They represent the human vulnerabilities at ports, as they can be corrupted or coerced by criminals into involvement in drug trafficking. These workers range from port workers (including crane operators, security staff) to police officers and customs officials (Nelen & Kolthoff, 2017; Meeus, 2019).

Both the literature consulted, and the experts interviewed in the research of Tops et al. (2021) underline the development that better physical security has led to a shift in criminal attention to the human factor at the port.

Step 3a. However, on the short term, we need to pay more attention to the human factor because this risk is not likely to disappear soon

The ambition of ports such as Rotterdam and Moerdijk to operate as 'smart ports' within ten years may have major consequences for the required human workforce, which is expected to diminish. The vulnerability of ports in terms of undermining crime could therefore decrease. However, the exploratory study by Tops et al. (2021) shows that the human factor at ports will not disappear completely in the short term, the redundancy of the human factor as a result of technological developments at ports might only be realistic in the long term. In the current phase (and in the near future) of smart ports, human resources still have an important role to play. First of all, for data analysis. In the long run, it may be possible for technology itself to inter-

pret data from dashboards by training AI technologies, without the need for human analysts. However, the experts interviewed in our own research do not see this happening in the near future. Moreover, some physical functions will remain reserved for humans – at least in the near future – such as lashers, rowers, pilots and steersmen. Lashers are people who secure all kinds of cargo in ships, also known as cargo-lashing. A rower is someone who helps seagoing vessels to dock and undock in ports. Pilots advise the captain or helmsman when entering or leaving the port. Helmsmen have the task of ensuring that all tasks on board are carried out properly and safely. They are an essential link between the skipper (or captain) and the rest of the crew and must be able to replace the skipper if necessary. The experts interviewed in the study strongly agree that these functions will still be performed manually in the near future and will not be replaced by technology soon. Even if the consultation for entering and leaving the port takes place remotely instead of physically on board, this must – because of the possible dangerous consequences of an error – still be done by people, according to a port expert.

Step 3b. On the long term, we could reduce these vulnerabilities by investing in promising technological developments ((Twin Ports, Container 42, AI, Data Science) which announce amongst others to diminish the importance of the human factor

Digital Twins at ports seems a (distant) prospect, but developments are already underway. Digital twins can be defined as "the right data available at the right time and place, anytime and anywhere", according to an interviewed employee of the Port of Rotterdam (Tops et al., p. 81). For example, a container ship in 'the smart port of the future' can be considered as "a large amount of data on the move, bundled in many thousands of intelligent containers on the ship" (Kuipers, Koppenol, Paardenkooper, & van Driel, 2018, p. 167). Interestingly, the vulnerable human factor (in the context of undermining crime) could disappear from ports as the role of technology increases and gradually takes over human activities in the smart ports of the future. These technological developments can potentially play an important role in securing ports against undermining crime. A concrete example of the development of Digital Twins at ports is Container 42. The development of 'smart containers' is likely to make it significantly more difficult to use containers for criminal purposes, due to technological security mechanisms (such as geofencing) and accurate recording of the container's movements, weight and temperature (and deviations within these factors). Container 42 illustrates that a solution to securing logistic hubs, such as ports, against undermining crime does not lie in Data Science alone, but in a combination of Data Science with physical modifications of (objects of) the port. Container 42 is a physical development coupled with data and is therefore an example of the vision of a digital twin (a data development) reduced to one object (a physical development).

How to realise the potential of AI and Data Science to make ports less vulnerable to undermining crime

The findings of Tops et al.'s (2021) research show that it might be worthwhile to continue to monitor technological developments at ports, with an eye to what it can deliver in the fight against undermining. Indeed, the discussed technological developments at ports, and thus the trend towards smart ports in the future, may have several positive effects in the long term:

- Making it physically more difficult to enter ports and containers.
- Detecting contraband.
- Provide detection information using smart sensors on the container.
- Reducing human actions in the process of container transport.

However, the technological developments should not be taken for granted or considered a silver bullet solution in themselves. To realise the potential of AI and Data Science to protect ports from undermining crime, attention must be paid to the following aspects:

a) ensuring the acceptance of the new (automated) technologies.

b) adopting a systems approach.

Ensuring the acceptance of the new (automated) technologies

As described in step 3a (section 5), the human factor is still here to stay; in the short term for physical processes in the port, but also in the long term for the design of algorithms. The study enabled the exploration of factors that port experts consider relevant for the acceptance and usage of these new technologies. The Technology Acceptance Model (TAM) was used as a guiding model to explore these factors.

First of all, the results of the interviews with port experts show that a socio-technical approach is desirable when discussing the potential of these new technologies. The majority of the experts talked about the technological innovations in a rather deterministic way, for example "The technology *will lead* to better security" or "The obligation of smart containers *will lead* to more stakeholders making use of it" (personal communication, 29 November 2021). However, as the field of Science and Technology Studies (STS) points out, it is important to consider *the interaction* between the technology and practitioner (e.g. Tromp, Hekkert & Verbeek, 2011; Mali et al., 2017; Meijer et al., 2021). For example, in studies about the use of algorithms in policing it is shown that human employees still have the task to enrich the data from algorithms to come to meaningful insights to act on the output when performing their working tasks (Mali et al., 2017) and that the outcome of the process of organizational rearrangement around the use of an algorithm is not determined by the technological features itself but by social norms and interpretations of the facilities of algorithmic systems (Meijer et al., 2021).

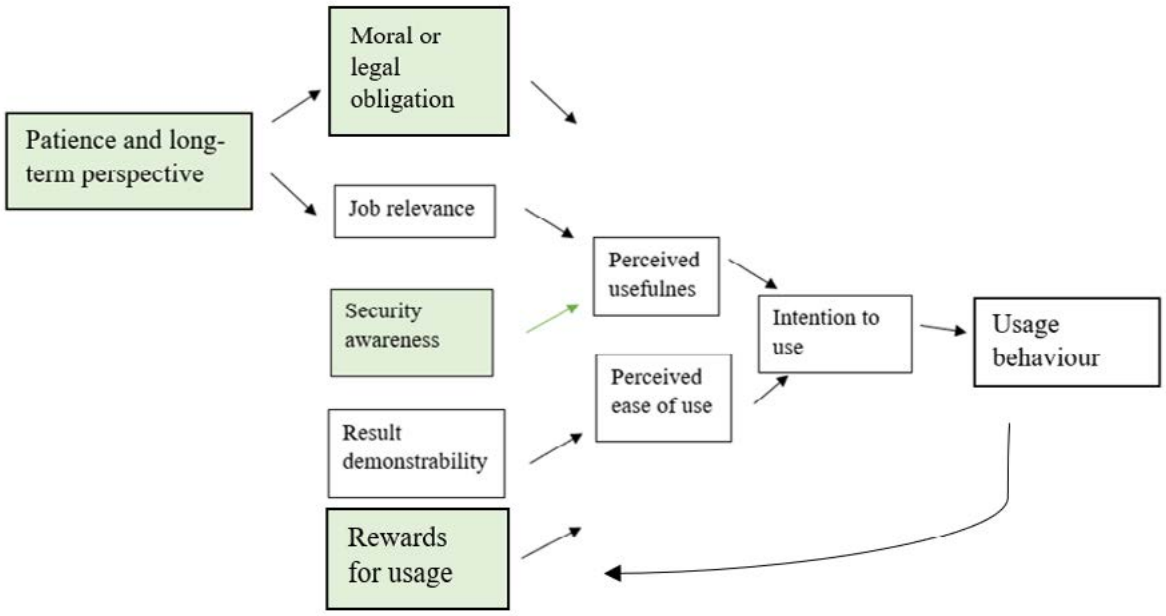
Keeping that in mind, the interviews from the study by Tops et al. (2021) gave a first impression of new factors that might be relevant for the acceptance and usage of new automated technologies. Two factors were considered by the experts to have a positive influence on the external factor 'job relevance' of the TAM. The experts stated that ports (and their stakeholders) must be prepared to accept that some technological innovations will not have an impact within ten years but may have an extremely positive impact in the longer term. This underlines the importance of patience in the acceptance and use of new technologies in smart ports. Innovation is often accompanied by frustration, as organisations need to see technological innovations in a long-term perspective and consider the long-term relevance of innovations. Patience and long-term perspective relate to job relevance.

The factor 'result demonstrability' from the TAM was considered to remain relevant in smart ports. In the study, this is illustrated by the programme manager of the Port of Rotterdam: "People see objections in things that may not matter, such as solar panels of containers being blocked when stacking containers. But that is not the point: for example, you can spray the container with special paint that extracts energy from sunlight. People are surprised by the world suddenly changing." (personal communication, 27 September 2021). Resistance is an unintended effect that can occur when using new technology (Manning, 1992). Knowledge of the underlying reasons why a new system may or may not be beneficial has a positive effect on the intention to use new technology.

According to expert statements in the study, there must be a sense of urgency among port employees to secure the port against undermining crime. The perceived usefulness of technology is expected to be influenced by security awareness. Security awareness among port employees and stakeholders could be an important factor to have a positive effect on the perceived usefulness of new technologies at smart ports.

In the study, interviewed experts suggested that the voluntary factor in the TAM could be replaced by moral or legal obligation in the case of smart technologies; transport services and users of container transport should be mobilised to use smart containers to ensure the safe transport of goods with little or no opportunity for undermining crime. For example, by introducing a so-called fast lane in which organisations receive a discount for the use of safe containers. Another possibility is to legally require the use of safe (smart) containers. Another solution suggested in the study is to reward the use of smart containers (or other smart technologies); a form of moral obligation. However, replacing voluntariness with obligations does not necessarily mean a greater acceptance and usage of the technologies. Here again it should be stressed that a socio-technical approach is needed that takes into account the interaction between the practitioner and technology.

Figure 4. An adjusted TAM for automated technologies in smart ports, with in green the factors found to be relevant by port experts (based on TAM2 (Venkatesh & Davis, 2000), adjusted by the authors).



Adopting a systems approach

The expert meeting that took place in the study confirms that technological developments in the field of Data Science and AI have the potential to reduce the vulnerability of ports to undermining crime. However, this potential could only be realised when stakeholders feel responsible to invest in the developments. The stakeholders involved, however, face the dilemma of who can be held responsible for undermining crime within the container transport chain. Because of the many different stakeholders involved – shipping companies, ports, cargo owners, etc. – each with their own interests, the question of responsibility is one that is often wrestled with. The stakeholders involved are dependent on each other in the logistics chain; "We are all part- and moral owners... No one feels ownership to solve it either." (Tops et al., 2021, p. 84). The dilemma of responsibility is of great importance in the context of tackling undermining crime, because a shared sense of responsibility can drive new (technological) innovations. There is an awareness among those involved that several stakeholders must be mobilised to achieve technological developments in container transport and that technological developments must therefore be viewed from a systematic approach and with a long-term perspective.

The expert meeting revealed the need for an exchange of knowledge and expertise between the parties. On the one hand, to learn from each other's issues – and the projects currently being carried out in this area – and, on the other, to prevent a waterbed effect in which criminals move to ports that are technologically less developed. Since criminals also continue to develop (technologically), it is important to join forces and work together. "Alone you go faster, together you get further" (ibid., p. 86). The experts in the study make two recommendations in the context of this desired cooperation. First of all, they recommend to create a joint agenda with projects in the field of undermining crime and technology at ports. This can help to prioritise and distinguish between the fragmentations of projects in this area. The second recommendation relates to benchmarking: establishing a lower limit and making effects measurable. Establishing a lower limit for minimum performance can help in addressing other ports, also at the European level. In addition, benchmarking can possibly contribute to measuring the effects of technological implementations.

Possible new vulnerabilities at smart ports

To realise the potential of Data Science and AI in protecting ports from undermining crime, it is necessary to consider possible new vulnerabilities that may arise as a result of digitalisation. One potential new vulnerability consists of digital attacks that can lead to the interruption of port processes. The interviews in the study by Tops et al. (2021) outline the expectation that in the future the context of ports – or the digital infra-

structure – will be attacked, so that from that context the port becomes vulnerable; "In the future, you will not be attacked yourself, but digitally, without damaging the physical object" (ibid., p. 82). For example, you only need to attack one terminal to bring down the whole system. The 2017 Russian cyber-attack victimising the Maersk container company demonstrates the dependence on digital infrastructure. Russian military hackers spread the ransomware NotPetya via vulnerabilities in Ukrainian accounting software, which they had previously hacked into. The spread of the ransomware was not limited to Ukraine and affected various companies and organisations worldwide, causing damage estimated at many billions of euros. The Rotterdam branch of the container company Maersk was also a victim. Container transport via the port, motorway and railway came to a stop, resulting in traffic jams (Scientific Council for Government Policy, 2019). Another example comes from the port of Antwerp. In the port of Antwerp, hackers manipulated the terminals of two large container handling companies on behalf of a Dutch drug gang. The IT specialists used malicious software that was sent by e-mail. They also broke into offices to get information. This enabled the gang to get to the containers before the carrier did (Van Maanen, 2019). These examples underline the importance of cyber security in ports, a necessity that is also increasing with the increasing digitalisation of ports.

Not only the technology itself, but also the people behind the technology can become targets for criminal purposes, what – again – stresses the need for a socio-technical approach when monitoring the technological developments of smart ports (e.g. Niculescu-Dinca, 2021). Although technological progress can be seen as reducing the opportunities for illicit trafficking by fragmenting chains of authorities and creating shared information storages, it also brings new challenges and shifts certain risks (Sergi, 2020b). By making technologies more secure, people who have access to them may themselves become targets. Since it can be difficult for most criminals to remotely access computer systems, this can lead to attempted corruption of back office personnel rather than port workers at terminal sites (Easton, 2020, in Tops et al., 2021).

Conclusion and recommendations

This contribution shows that Dutch ports have both the ambition and the potential to operate as 'smart ports' within ten years and to minimise the vulnerable human factor in ports in terms of undermining crime. The developments of smart ports are promising, for example smart containers. How relevant these technologies are going to be 'tomorrow' is constructed today. We can do that by carefully studying and building knowledge about their potential and in this way working towards fulfilling their potential. Tops et al. (2021) recommend that the undermining domain, much more than now, take this development into account in the process of developing different types of approaches to undermining.

However, the technologies should not be taken for granted or considered a silver bullet solution in themselves. Therefore, based on this study and arguments, we call attention to the following aspects:

1) To realise the potential of AI and Data Science to protect ports from undermining crime, two things are important:

a) ensuring the acceptance of the new (automated) technologies. The fact that the human factor is for now and in the near future still here to stay, calls for a socio-technological approach when monitoring the practitioner-technology interaction with the automated technological innovations in smart ports.

b) adopting a systems approach. The long-term goal is system change; container 42 is a metaphor for this and a concrete starting point. In this case, Container 42 should not be seen as a separate project, but as a fundamental realisation of a change strategy.

2) Even if fully implemented, criminals may find a different modus operandi (therefore the importance of cybersecurity in ports). Not only the technology itself, but also the people behind the technology can become targets for criminal purposes. What calls for the continued need to pay attention to the human factor (security partitioners and their interaction with technologies) also in the future?

So, in light of all these insights, we make a couple of concrete recommendations:

- Keep a good eye on AI and Data Science developments at ports. This applies to professionals active in the undermining domain, ranging from academics as well as law enforcement practitioners. Herein also lies a task for the government to provide insight and overview in how these developments will evolve. This does not only apply to developments in large ports such as Rotterdam, but also in smaller ports. The government could for example be of assistance in the alignment of various projects and the development of policy for smaller ports.
- Discussing of data governance between the stakeholders – who owns the data, who is allowed to use the data, what is the quality of the data and what possibilities do investigative bodies have for accessing this data? These discussions are gaining new inputs as a result of developments – including trustworthy AI. The insight into data is shifting towards insight into the AI models that underpin the new generation of digital technology with which ports will be managed, using the Twin Harbour metaphor. This calls for new policies and regulations regarding the sharing of data and models.
- Developing a common and orchestrated strategy on Data Science and AI at ports and its connection to undermining crime at ports, on a national and international level. The consequences and significance for not only the Port of Rotterdam but also other (smaller) ports in the Netherlands will have to be closely monitored and the knowledge (including the technology) will have to be transferred, also in an EU context, to prevent a waterbed effect.
- The entire chain (logistics, justice and production) will have to be included in a holistic system approach. Try to develop technology or standards together with the other partners in the chain (e.g. for improved sharing of (big) data and/or AI models); so-called smart logistics. The chain should also be approached in a European or even an international context. After all, the Netherlands could take the responsibility and lead the way, but we need to get everyone on board on an international scale to bring about real change, and to continue to lead as the Netherlands' trade and distribution country.

References

- BOTOC (2018) Uitwerking breed offensief tegen georganiseerde ondermijnende criminaliteit. Available at: https://open.overheid.nl/repository/ronl-b27340ea-ce38-4e07-aa61-765a1f530cfa/1/pdf/tk-uitwerking-breed-offensief-tegen-georganiseerde-ondermijnende-criminaliteit.pdf
- Colvin, C. A., & Goh, A. (2005) Validation of the technology acceptance model for police. *Journal of Criminal Justice*. 33, 89-95.
- Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*. 12 (3), 319-40.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989) User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*. 35 (8), 982-1003.
- Ernst, S., Ter Veen, H., Lam, J., & Kop, N. (2019) Leren van technologisch innoveren: "De techniek is niet zo spannend". Apeldoorn, Police Academy.
- Ghosen, D. (2021) Danny's Wereld; Onveilige haven. Available at: https://www.npostart.nl/dannys-wereld/04-11-2021/VPWON_1332342
- HARC-team. (2021) HARC-team onderschept ruim 40.000 kilo cocaïne in 2020. Available at: https://www.om.nl/actueel/nieuws/2021/01/13/harc-team-onderschept-ruim-40.000-kilo-cocaine-in-2020
- Hiemstra & de Vries. (2021) Quick scan aanpak criminele stromen zeehavens. Commissioned by the Ministry of Justice and Security.
- Jussi, P. (2021) AI for smart ports, part 2: Optimizing vessel schedule predictions using machine learning. Available at: https://www.awake.ai/post/ai-for-smart-ports-port-call-prediction-part2
- Kuipers, B., Koppenol, D., Paardenkooper, K., & van Driel, H. (2018) Rotterdamse container kopstukken. Rotterdam, Promedia group.
- Levinson, M. (2016) The Box. How the Shipping Container Made the World Smaller and the World Economy bigger. New Jersey, Princeton University Press.
- Lin, C., Hu, P. J., & Chen, H. (2004) Technology implementation management in law enforcement: COPLINK system usability and user acceptance evaluations. *Social Science Computer Review*. 22 (1), 24-36.
- Mali, B., Bronkhorst-Giesen, C., & den Hengst, M. (2017) Predictive policing: lessen voor de toekomst. Apeldoorn, Police Academy.

- Manning, P. K. (1992) Information technologies and the police. In: Tonry, M. & Morris, N. (Eds.), Modern Policing: Crime and Justice, A Review of Research. 15, 349–398. University of Chicago Press.
- Meeus, J. (2019) De Schiedamse cocaïnemaffia. Amsterdam, Nieuw Amsterdam.
- Meijer, A., Lorenz, L., & Wessels, M. (2021) Algorithmization of Bureaucratic organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems. *Public Administration Review*. 81, 837-846. https://doi.org/10.1111/puar.13391
- Nelen, H., & Kolthoff, E. (2017) Schaduwen over de rechtshandhaving. Georganiseerde criminaliteit en integriteitsschendingen van functionarissen in de rechtshandhaving. The Hague, Boom Criminologie.
- Niculescu-Dinca, V. (2021) Theorizing technologically mediated policing in smart cities. An ethnographic approach to sensing infrastructures in policing practices. In M. Nagenborg, T. Stone, G. Woge, & P. Vermaas (Eds.), Technology and The City: Towards a Philosophy of Urban Technologies. New York: Springer, pp.75-100.
- Noordanus, P., van der Torre, E., Tops,P., & Kester, J. (2020) Een pact voor de rechtsstaat; een sterke terugdringing van drugscriminaliteit in tien jaar. The Hague, Aanjaagteam ondermijning.
- NOS (2021, oktober 29) Tussen frituurvet en ananassen: meer dan 1500 kilo coke onderschept in haven Rotterdam. Available at: https://nos.nl/artikel/2403484-tussen-frituurvet-en-ananassen-meer-dan-1500-kilo-coke-onderschept-in-haven-rotterdam
- NOS (2021, september 13) Negen mensen in ademnood uit container op maasvlakte gehaald. Available at: https://nos.nl/artikel/2397655-negen-mensen-in-ademnood-uit-container-op-maasvlakte-gehaald
- Onze Haven (2020) Reisverslag van de slimste container. Available at: https://onzehaven.nl/2020/01/03/reisverslag-van-de-slimste-container/
- Perera, L., Oliveira, P., & Soares, C. (2012) Maritime Traffic Monitoring Based on Vessel Detection, Tracking, State Estimation, and Trajectory Prediction. *Institute of Electrical and Electronics Engineers*. 13 (3), 1188-1200.
- Public Prosecutor's Office. (2021, september 17) Douane onderschept 4022 kilo cocaïne tussen hout. Available at: https://www.om.nl/actueel/nieuws/2021/09/17/douane-onderschept-4022-kilo-cocaine-tussen-hout
- Roks, R.A., Bisschop, L.C.J., & Staring, R.H.J.M. (2021). Getting a foot in the door. Spaces of cocaine trafficking in the Port of Rotterdam. *Trends in Organized Crime*. 24, 171–188.
- Schwab, K. (2016) The fourth industrial revolution. New York, Penquin Random House.
- Sergei, A., Reid, A., Storti, L., & Easton, M. (2021) Ports, Crime and Security. Governing and Policing Seaports in a Changing World. Bristol, Bristol University Press.
- Staring, R., Bisschop, L., Roks, R., Brein, E., & van de Bunt, H. (2019) Drugscriminaliteit in de Rotterdamse haven. Aard en aanpak van het fenomeen. The Hague, Boom Criminologie.
- Tops, P., van Valkenhoef, J., van der Torre, E., & van Spijk, L. (2018) Waar een klein land groot in kan zijn; Nederland en synthetische drugs in de afgelopen 50 jaar. The Hague, Boom Criminologie.
- Tops, P., van den Heuvel, W., de Groes, N., & Gravenberch, V. (2021). Hoe zeehavens veranderen door Artificial Intelligence en Data Science en wat dat kan betekenen voor de aanpak van ondermijning. Een praktijkverkenning. Centrum voor de studie van ondermijning, Jheronimus Academy of Data Science.
- Tops, P., & Tromp, J. (2021) Nederland drugsland. Amsterdam, Balans.
- Tromp, N., Hekkert, P., & Verbeek, P. (2011) Design for socially responsible behavior: A classification of influence based on intended user experience. *Design Issues*. 27 (3), 3–19.
- Van den Heuvel, W. & Tops, P. (2021) AI en data science in de haven. Hoe Artificial Intelligence en Data Science een hefboom kunnen zijn voor Slimme(re) Havenbeveiliging. Jheronimus Academy of Data Science, Tilburg University.
- Van Maanen, M. (2019) De aansprakelijkheid van de zeevervoerder voor pincode fraude bij aflevering. Available at: https://www.vantraa.nl/media/2128/mma-de-aansprakelijkheid-van-de-zeevervoerder-voor-pincode-fraude-bij-aflevering.pdf
- Vankatesh, V. & Davis, F. D. (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*. 46 (2), 186-204.
- Verseput, S., & de Haan, M. (2021) De drugsuithalers hebben nu bijna vrij spel in de Rotterdamse haven. NRC. Available at: https://www.nrc.nl/nieuws/2021/09/22/de-drugsuithalers-hebben-nu-bijna-vrij-spel-in-de-haven-a4059311
- Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwrichting. Available at: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting