Cyber Assessment Rotterdam

2022

(**CA**010 2022)

Cyber Assessment Rotterdam

2022

(**CA**010 2022)

September 2022 (English) January 2022 (Dutch)

The Cyber Assessment Rotterdam 2022 is drawn up by Verdonck, Klooster en Associates (VKA) commissioned by and in collaboration with the Municipality of Rotterdam and her collaboration partners

V 1.0

Gemeente Rotterdam

VERDONCK KLOOSTER & ASSOCIATES

Table of Contents

Participants Cyber Assessment Rotterdam 2022

- Blocklab
- Centrum voor jeugd en gezin Rijnmond
- DCMR Milieudienst Rijnmond
- Deltalinqs
- Erasmus Universiteit Rotterdam
- Evides
- FERM
- Gemeente Den Haag
- Gemeente Rotterdam
- Intermax
- IT Campus
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- MKB Rotterdam Rijnmond
- Netherlands Maritime Technology
- NFIR
- Politie
- Port of Rotterdam
- Resilient Rotterdam
- RET
- Robeco
- Rotterdam Maritime Capital of Europe
- Rotterdam The Hague Airport
- Stedin
- TNO
- VeiligheidsAlliantie regio Rotterdam
- Veiligheidsregio Rotterdam-Rijnmond
- Verdonck, Klooster & Associates
- Vereniging van Nederlandse Gemeenten

Collaboration on the Cyber Resilience of Rotterdam!

Digital developments offer big social and economic opportunities for the city of Rotterdam. But these digital developments also cause new threats and vulnerabilities. New technologies open up new forms of criminality and digital crises or crises with a digital component.

Recently we have seen many examples of hacks and ransomware attacks. Such attacks have impact on entrepreneurs, citizens and the city as a whole. That worries me. I therefore believe that persistent investment in the cyber resilience of the city and her citizens, entrepreneurs, companies and other organizations is necessary.

It is important to pay attention to both the opportunities and the security aspects associated with digital developments. By collaboration we can prevent the city from being damaged by a cyberattack and ensure we utilize the added value of digitization. That is why a large number of organizations from our city have put their minds together on how cyber resilience of Rotterdam can be strengthened with the aim to take joint action. You can read the result in this cyber assessment containing concrete actions. Let us all utilize the added value of digitization and strengthen the cyber resilience of our city.

Ahmed Aboutaleb
Mayor of Rotterdam

Executive Summary

Before you lies the Cyber Assessment Rotterdam 2022 (CA010 2022). This Cyber Assessment has been prepared because of the enormous opportunities that digital developments offer Rotterdam, which entail cybersecurity aspects at the same time. Cyberattacks can be disruptive to society and cause great economic damage. Attacks can be so disruptive that they have a long-term impact on citizens, organizations and supply-chains. Rotterdam therefore pays a lot of attention to making the region more resilient against future cyberattacks.

The CA010 2022 arose from three sessions with specialists and stakeholders from the Rotterdam area. The working group has taken ten primary urban functions of Rotterdam as a starting point. These urban functions are parts of our society that are essential to the city of Rotterdam to function properly as a whole.
The working group has opted for the urban functions Mobility, Economy, Governance, Public Services, Education, Crisis Management (Public Order and Safety), Healthcare, Housing, Utilities and the Port.

Together with our partners in the city, the working group has performed a multidisciplinary SWOT analysis for every urban function, in which the strengths, weaknesses, threats and opportunities from the cyber domain have been analyzed. A multidisciplinary SWOT in this context means that organizations involved in an urban function, have also given input on other urban functions. This approach ensured that the participating organizations participated with an open mind and brought in new insights from a different perspective.

From the SWOT analysis of the urban functions, five overarching findings emerged.

1

Finding 1. Direction on a cyber resilient Rotterdam

The participants indicate that for the successful implementation of this Cyber assessment it is essential that coordination is set up in which facilitation and support of the implementation of the actions in this Cyber assessment predominate. A central management function helps to jointly realize results for the whole of Rotterdam.

2

Finding 2. Digitally skilled and a cyber resilient Rotterdam society

The participants indicate that the digital skills of residents and employees of organizations still fall short, especially when it comes to digital resilience. Many incidents are still caused by unsafe behavior by people. Inadequate digital skills can ultimately limit economic growth or cause economic damage.

3

Finding 3. Knowledge sharing between organizations

The cyber knowledge of organizations is fragmented and not every organization has the capacity or appropriate knowledge to become cyber-resilient. Knowledge sharing between organizations can strengthen Rotterdam's cyber resilience. Sharing knowledge between organizations can strengthen the cybersecurity foundation. This also ensures that organizations with insufficient capacity or expertise are able to increase their resilience.

4

Finding 4. Cyber supply chain collaboration in Rotterdam

Processes within urban functions are often interdependent. In addition, the ICT systems of organizations are often interconnected. Participants indicate that it is important to gain insight into the cyber dependencies within supply-chains. Otherwise taking measures to prevent failure gets increasingly difficult. The participants warn in this regard: More insight can certainly help, but it is impossible to fully map out all supply-chains.

5

Finding 5. Cyber impact control and crisis management

When a threat leads to an incident, it is important that a response is adequately given. By properly organizing crisis management in advance, the consequences of an incident can be mitigated. The participants need an unambiguous crisis structure in the event of cyber crises, which is in line with the existing

crisis structures. A counter function is needed for individual citizens, so that they know what to do if they suspect that their cybersecurity is at risk.

Based on these five findings, the working group has defined actions to increase Rotterdam's cyber resilience in line with the findings. These actions are further elaborated in this publication.

The organization of CA010 2022 is very grateful to all organizations that have helped with the realization of this Cyber Assessment. We hope we can also count on these organizations and individuals to take joint action according to the actions described in this publication. Only together can we make better use of the opportunities of digitization and increase the cyber resilience of the city of Rotterdam.

The Cyber Assessment Rotterdam 2022 was drawn up by Verdonck, Klooster and Associates (VKA) on behalf of and in collaboration with the Municipality of Rotterdam and its cooperating partners.

Theoratical Scenario of a Cyberattack on the Rotterdam Area

Rotterdam, September 17, 2025 - A coordinated and advanced cyberattack on the Rotterdam area causes major problems. The safety triangle led by the mayor of Rotterdam has called for calm via the activated National Emergency Net (Noodnet).

On the night of September 16, a cyberattack started, from a still unknown location, on the energy supplies in and around the city. The region's electricity grid lost its power for 4 hours as a result of the attack. Not only has the power grid been attacked, but also other basic facilities in the city. Train traffic in and around the Rotterdam area has now come to a complete standstill. All camera systems in the city have ceased to function. Police are deployed for extra surveillance.

The traffic lights in the entire downtown area no longer function, matrix signs above the A13, A15 and A16 motorways are controlled by an as yet unknown assailant and since the cyberattack, the 'Erasmus Bridge', 'Koninginnebrug' and the 'Van Brienenoordbrug' are open.

Shortly after the start of the cyberattack, the Port of Rotterdam Authority decided in consultation with the safety triangle to indefinitely stop the shipping traffic towards Rotterdam and let the shipping divert to the port of Antwerp.

Efforts are currently being made to regain control of the basic facilities of the city. As a precaution, hospitals within the region are temporarily cut off from all external networks to prevent this vital sector from also getting affected.

Purpose of the Cyber Assessment Rotterdam 2022 (CA010 2022)

The previous fictitious case shows what the consequences could be of a major cyberattack on the Rotterdam area. Cyberattacks can disrupt society and cause major economic damage. The National Coordinator for Security and Counterterrorism (NCTV) and the National Cyber Security Center (NCSC) see that both state actors and cybercriminals have used the situation created by the coronavirus to commit digital attacks. They find, that now an even greater part of our lives takes place online, it is more attractive for malicious people to attack us online.

Attacks can be so disruptive that they have a long-lasting impact on organizations and supply-chains. Cyber criminals can also cause disruption of society by, for example, disrupting vital processes. They are often as skilled as state actors and have diffuse relations with them. That's why it is difficult to distinguish what the role of the state actor is. The municipality of Rotterdam therefore pays a lot of attention to making the region more resilient against future cyberattacks.

Resilience to cyber threats requires constant collaboration between government, companies and citizens. It doesn't matter whether it concerns the telecommunications facilities, the piloting of the largest container ships in the world or keeping the basic facilities for citizens and businesses available. Every part within the region is important and some parts are even critical for the functioning of our society.

The Cyber assessment Rotterdam 2022 is based on the knowledge and experiences that companies, governments and organizations of Rotterdam have gained over the years. The aim is to gain a better understanding of today's digital resilience, making the sectors aware of potential and possibly sector

[1] Cybersecurity assessment Netherlands 2022 (CSBN 2022)

transcending cyber threats and opportunities and identify actions that ensure more cyber resilience.

The Cyber Assessment Rotterdam 2022 identifies five actions. We hope we can count on the organizations that have contributed to the creation of this publication to take joint action according to the concluded actions. We also hope that everyone who reads this publication will take action. Only together can we make better use of the opportunities of digitization and further strengthen the cyber resilience of the city of Rotterdam. We are looking forward towards a valuable collaboration to make the city of Rotterdam even more digital and more cyber-resilient.

Reading Guide

This publication describes the Cyber Assessment Rotterdam 2022 (CA010 2022). The next chapter describes the method and approach that we have followed during the creation of this Cyber Assessment. Then we describe the findings and conclusions of the Cyber Assessment 2022 and the actions with which stakeholders in the Rotterdam area can take action together to make better use of the opportunities of digitization and strengthen the cyber resilience of the city of Rotterdam.

The city of Rotterdam is looking at ten urban functions that are important for the city as a whole. We will then go into more detail on the cyber opportunities and threats for each of these ten urban functions, with recommendations for every urban function. Finally, we would like to thank all organizations, directors, managers and specialists who, with their experience and knowledge have made a valuable contribution to the development of this publication.

We wish you pleasant reading.

Method and Approach

The CA010 2022 resulted from three sessions at the end of 2021 with specialists and with stakeholders from the Rotterdam area. We have taken ten primary urban functions of Rotterdam as a starting point. Urban functions are the tasks that a city fulfills in society for its inhabitants and organizations in the city.

Urban functions are parts of society that are essential to ensure the proper functioning of a region as a whole. When an urban function does not function properly, it has an influence on society, causes economic damage and other urban functions may malfunction as a result.

Rotterdam distinguishes the following urban functions for this Cyber Assessment:

Mobility: facilities and processes for traffic and transport;

Economy: facilities and processes for economic traffic, trade and industrial processes;

Governance: facilities and processes for decision-making in both government and private organizations;

Public service: facilities and processes for the services to citizens and businesses;

Education: facilities and processes for the delivery of schooling and education;

Crisis management (public order and safety): facilities and processes for crisis prevention, management and aftercare;

HealthCare: facilities and processes for care and health;

Housing: facilities and processes for living and working;

Utilities: facilities and processes provided by utilities for the primary functioning of the city and all its inhabitants, businesses and organizations;

Port: facilities and processes for the primary functioning of the port.

Organizations that work within or influence the operation of these urban functions were involved during the creation of this cyber assessment.

In addition to the sessions mentioned above, Rotterdam has previously developed Cyber Assessments. In 2016, this was done in a small working group to make a first assessment. In 2018, this result was further developed into a resilience model that was shared with those involved, but which was not published. In 2022, these actions will result in a CA010 2022 that is widely shared. The main results from 2016 and 2018 have been integrated in this publication.

During the sessions, those involved per urban function performed a multidisciplinary SWOT analysis, in which the strengths, weaknesses, threats and opportunities from the cyber domain were analyzed. A multidisciplinary SWOT means that organizations from one urban function have provided input to other urban functions. In this way, for example, the education sector contributed ideas to the crisis management sector and the mobility sector provided input to the public services sector.

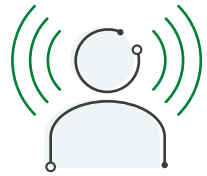
This approach ensured that the participating organizations participated with an open mind and brought in new insights from a different perspective.

The publication of the Cyber Assessment Rotterdam 2022 reports the results of the sessions.

Results CA010 2022

General developments

At the start of the sessions we have asked the participants what general developments may affect the Cyber assessment of Rotterdam, now and in the near future. We have summarized the answers of the participants in the next picture:

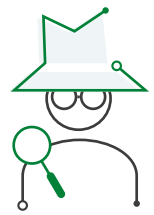


Awareness on cyber among citizens of Rotterdam

Be aware of the paradox that cyber and digitization become an increasingly important part of our lives, but that digital illiteracy in the city is still big.

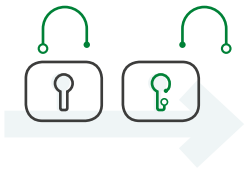
Limitations by Privacy

Privacy legislation let organizations feel restricted in innovating and digitizing. Although this does not have to be true, lack of knowledge and insight into the GDPR privacy legislation causes restraint.



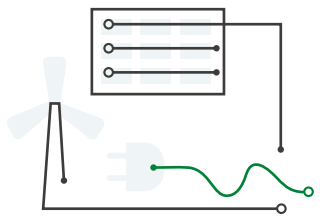
Increase in digital espionage on both large and small scale

Don't underestimate the amount of digital espionage that foreign powers carry out. This is a real threat.



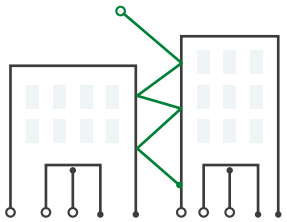
Transition from closed to open system

The time of closed systems, which we can protect by placing them behind a wall is over. Organizations and their ICT are increasingly moving towards open systems that in all kinds of ways, both organizationally and technically are connected to each other.



An energy transition is happening with many cyber aspects

The world is currently in an energy transition with a lot of momentum. Part of this transition is data and digitally driven. We can for both opportunities and threats try to piggyback on this transition.



Cross pollination between sectors

When organizations work together, it is often within their own industry. However, sectors can also learn a lot from each other. It would be nice if the CA010 2022 can be a catalyst for this.

Cyber Assessment Rotterdam 2022

From the analysis of the conversations about the individual urban functions come five overarching findings.

1. Direction on a cyber resilient Rotterdam

We notice that all participating organizations are still struggling with their cyberresilience. Everyone is looking at frameworks or technical solutions to get a certain degree of certainty, but there never is a 100% guarantee. The many cybersecurity incidents that are reported daily in the media prove this point. Trying to collaborate on this topic increases the effort that organizations need to put into cybersecurity.

This also means that in practice it proves difficult to implement initiatives such as CA010 2022. This is certainly not unwillingness, but has everything to do with the fact that currently the primary focus is internal and not external. The participants indicate that for successfully realizing this cyberassessment it is essential that coordination is set up, whereby facilitation and support of the implementation of the action lines in this Cyber assessment should be priority.

Direction is also essential in times of crisis. We see that different functions, such as public order and safety, basic facilities and the port have their own crisis management in order. What is missing is direction between functions when a cyber crisis occurs. See further recommendation five.

2. Digitally skilled and a cyber resilient Rotterdam

Deficient digital skills can lead to someone not able to make use of digital resources that are available to them, as a result of which this person may miss personal and business opportunities. In addition, the chance that someone will become a victim of digital crime becomes larger, because he is unable to recognize suspicious patterns in digital communication. Combined for example with the increasingly sophisticated phishing attacks this is a major challenge.

Since the last Cyber assessment in 2018, an important change has taken place. Education is starting to become more and more aware of the importance of basic digital skills for all students and are slowly integrating these skills into curricula. In addition, more and more initiatives are starting in Rotterdam to improve the digital skills of certain target groups. Think about the elderly, the unemployed and young people who have dropped out of school.

But this is not enough. The participants indicate that digital skills of employees still fall short, especially when it comes to digital resilience. Think of the ability to recognize malicious email messages such as phishing and CEO Fraud. This does not only apply to “older” employees, but also to young starters that come straight from school. Too many incidents are still caused by unsafe behavior of people. Deficient digital skills can ultimately even be a limitation to economic growth or cause economic damage.

3. Knowledge sharing between organizations

The available cyber knowledge is fragmented across organizations and not every organization has the capacity or the right knowledge to become cyber-resilient. Knowledge sharing between organizations can increase the cyber resilience of Rotterdam. For example, knowledge sharing can be stimulated by setting up a cyber platform Rotterdam, in which organizations from different sectors share their knowledge with each other.

Basic cybersecurity is vulnerable in many organizations. There is also a lack of people with the right expertise. By sharing knowledge between organizations, basic cybersecurity is strengthened. This ensures that also organizations with insufficient capacity or expertise are enabled to increase resilience.

In addition, sharing knowledge about threats and incidents is important. When an organization identifies a threat and shares it with other organizations in a timely manner, this can ensure that an incident is prevented at the other organizations. Not yet all organizations are reached via existing structures, for example via the NCSC, the DTC or the IBD. Also, timely sharing of information about an incident gives organizations or residents the opportunity to anticipate on a disturbance. For example when notice is given that there is a sudden disturbance on the railroad it will give people the opportunity to take the car and Rijkswaterstaat the opportunity to open an extra rush hour lane to accommodate the unexpected traffic increase.

4. Cyber supply chain collaboration in Rotterdam society

Processes of urban functions are often interdependent. The COVID pandemic teaches us that without good healthcare we will have insufficient employees to sustain our economic activities. Without mobility these same care workers cannot reach their clients. Public order and safety provides a safe social context for other functions to fulfill their role and ultimately everyone is dependent on utilities.

In addition, the IT systems of organizations more often than not are connected to each other through their own networks or the public internet.

The moment one of the connections in the supply chain is broken, it can lead to problems in several sectors. Failure of an IT system at one organization can cause a domino effect. An example is that failure of telecommunication networks cause problems for other sectors. We have had several of such failures in the Netherlands in recent years.

In many cases, the cyber dependencies within chains are not yet transparent, which

makes it unclear which systems and organizations depend on each other. Participants indicate that it is important to gain this insight, otherwise it's increasingly difficult to take measures to prevent outages.

This insight will reveal that certain sectors are insufficiently able to completely solve the problems, unless they get help from their supply chain partners. For example, think of critical suppliers of intermediate products or several care agencies that work on the same case, such as in youth care.

Please note that more insight will certainly help, but it is impossible to fully map out all chains.

5. Cyber impact control and crisis management

When a threat becomes an incident, it is important that adequate action is taken. A serious disruption at an organization or in the Rotterdam infrastructure can cause a direct disturbance in the public space and can subsequently lead to social disruption and economic damage. By properly organizing crisis management up front, the consequences of an incident can be mitigated.

The participants need an unambiguous crisis structure for cyber crises, which is in line with the existing structure for physical crises. For organizations, there is also a need for central coordination in the crisis response. However, the demand for a crisis structure is not limited to organizations. Individual citizens are also increasingly confronted with digitization, for example home automation (the automation of processes in and around the home using smart electronics and networks). Individual citizens need a counter, so that they know where to turn to for help if they suspect that their cybersecurity is at risk.

When setting up cyber crisis management it is important to take into account physical security and personnel in addition to ICT. A cyber crisis exercise can help to respond appropriately in the event of a real crisis. An exercise involving multiple urban functions mimics a realistic scenario with chain dependencies.

Conducting a cyber crisis exercise can also help raise awareness amongst executives to increase cyber resilience. This could potentially lead to more investments in cyber resilience. By practicing certain scenarios with executives, organizations become better prepared for the greatest threats.

CA010 actions

1. Direction on a cyber resilient Rotterdam

A Find a catalyst for a cyber resilient Rotterdam, who will support and direct the process but does not assume the accountability.

B Ensure cyber governance at board level and ensure a 'boosting budget', for the short and long term.

C During a launching event stakeholders from the region sign an accessible participation covenant and make a visible start with a cyber resilient Rotterdam.

2. Digitally skilled and a cyber resilient Rotterdam society

A Drive priority for cyber security and cyber awareness in education.

B Profile Rotterdam as a cyber resilient city, where the 'best mayor in the world' takes the lead.

C Focus on digital awareness and resilience of citizens and entrepreneurs by organizing projects and campaigns for both (potential) victims and perpetrators.

D Create or facilitate a virtual cyber counter for citizens and entrepreneurs.

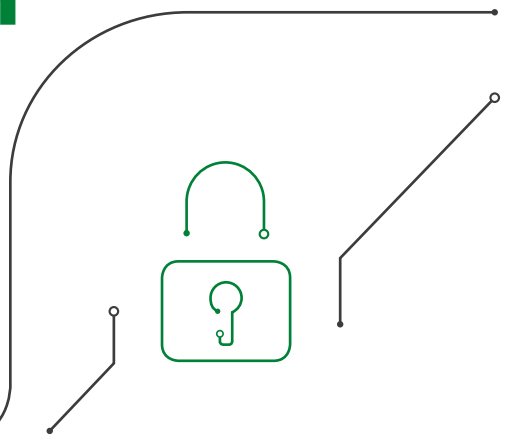
4. Cyber supply chain collaboration in Rotterdam

A Map out vital processes and chain dependencies for Rotterdam with stakeholders in the region. Work from the urban functions and give priority to what is vital for Rotterdam.

B As a municipality, take a stimulating and facilitating role in collabrations.

C Support the cooperation and the participation covenant - from action 1C - Rotterdam wide.

Cyber Assessment Rotterdam



3. Knowledge sharing between organizations

A Provide this cyber assessment and the development methodology to VNG to encourage reuse by other municipalities.

B Share knowledge in a safe context via, for example, a periodic knowledge platform.

C Learn from incidents together as relevant stakeholders in the region (disruptive learning cycle).

D Make knowledge sharing multi- and interdisciplinary. Learn both proactively as reactive from each other and involve directors, management and specialists.

5. Cyber impact control and crisis management

A Find connection with existing crisis structures and work together partners such as the veiligheidsregio and FERM.

B Also practice crisis situations at the executive level in scenarios.

C Make crisis management practical with action perspectives for concrete threats, for example ransomware, spear phishing and insider threats.

1. Direction on a Cyber resilient Rotterdam

The first line of action concerns direction to maintain the focus on collaboration for the cyber resilience of Rotterdam. The past has taught us that a group of organizations does not spontaneously become an effective and goal-oriented cooperation. Especially when organizations work together on subjects that are not their core business, maintaining focus is a challenge. A number of measures are aimed at achieving ongoing cyber resilience in Rotterdam.

The first thing is to look for a cyber-resilience catalyst that will support and coordinate the most important activities to increase cyber resilience. The catalyst does not take over the accountability of individual organizations, but he makes cyber resilience activities easier and better accessible to the participants.

This catalyst will also need a budget to implement the action plan. This budget and the emphasis on cyber resilience will only come available when there is sufficient urgency at the executive level and the need for better cyber resilience is really felt.

To further emphasize the importance of collaboration and the dependence between all parties in the city in the field of cyber, all stakeholders in the Rotterdam region want to agree on a participation covenant, in which they commit to the objectives and actions from this Cyber Assessment. The group will work together to ensure that Rotterdam becomes a cyber-safe environment for residents, entrepreneurs and organizations.

2. Digitally skilled and resilient Rotterdam society

A cyber resilient Rotterdam starts with the inhabitants of the city. They have a lot of different roles such as citizen, employee, entrepreneur, civil servant, student, volunteer, etc. Whatever role people play, in all roles good digital skills are indispensable today.

In Rotterdam we can't start early enough with sharing digital skills and would prefer that teaching digital skills start in children's education. Teaching digital skills should therefore be prioritized in education, including the basics of cyber resilience. Pupils and students must learn to recognize when their digital security is at stake and need to know what to do in such situations.

When students become employees, they shouldn't stop learning, after all, the developments in the field of digitization never stop. We want to keep working on digital skills through projects and campaigns in the city. Especially in the case things go wrong. When someone unexpectedly becomes the victim of a digital crime, then we must help the victim to rectify any damage suffered and offer support so that in the future someone is prepared for cybercrime.

Fortunately, there are also many residents and companies that recognize and acknowledge cybercrime and want to proactively protect themselves. They should be provided with an easy and efficient channel to ask questions and seek help, for example in the form of a virtual cyber counter. It is important not to reinvent the wheel, but seek connection with organizations that have already arranged such a counter, such as the Chamber of Commerce(KvK) and MKB-Nederland.

These actions can ensure that Rotterdam has a very digitally-skilled and resilient population. This allows the city of Rotterdam to profile itself as a digital and cyber-resilient city, led by the best mayor in the world.

3. Knowledge sharing between organizations

There is still a lot to be done in the field of knowledge sharing. Among others at municipalities. We still see that too many municipalities are reinventing the wheel and trying to fathom this complex matter. The VNG is a good place for municipalities to engage in collaboration and share results such as this CA010 2022.

We can also go further in collaborating within Rotterdam by, for example, sharing cyber resilience strategies between organizations, but also case history about current cyber incidents and crimes. The participants of CA010 2022 indicate having a great willingness and need to share these types of information and to learn from each other. However, a precondition for this is that information can be shared in a secure and confidential context, without for example, leeks to the press. The aforementioned catalyst could be the one to facilitate this safe context.

The participants in the Cyber Assessment note that cyber resilience is still very much pigeonholed within organizations. We see that specialists within the domains ICT, P&O and Facilities and Safety are working on cyber resilience issues from their own profession. Instead of tackling these challenges together and in an integral manner.

We see the same happening in strategic, tactical and operational governance layers within organizations. Each of these layers has their own perspective on digitization and cyber resilience and tries to steer towards this.

To achieve an effective increase in cyber resilience, the functional columns and the executive layers within organizations should be working much better aligned with each other.

4. Cyber supply chain collaboration in Rotterdam

We have seen that in today's network society, a large amount of collaboration occurs in supply chains by both public and private organizations. In addition, there is an increasing exchange of information and cooperation between supply chains. This development causes society to lose their insight into the way in which organizations and processes are interrelated. It is therefore necessary to gain insight into these dependencies. This can help us to prevent getting surprised by unexpected consequences when a cyber incident occurs at an organization in Rotterdam.

Creating insight into these supply chains is very complex. So choices have to be made in how we are going to approach this. The focus will therefore primarily lie on the urban functions that we have chosen and especially on the most vital processes or services that are offered by the functions to the city.

As a hub, the municipality can play a facilitating role in this analysis. They are the only party to have a role in every urban function. The municipality can fall back on the commitment of the participants in CA010 2022 laid down in the participation covenant and at the same time encourage new participants to sign up to this covenant.

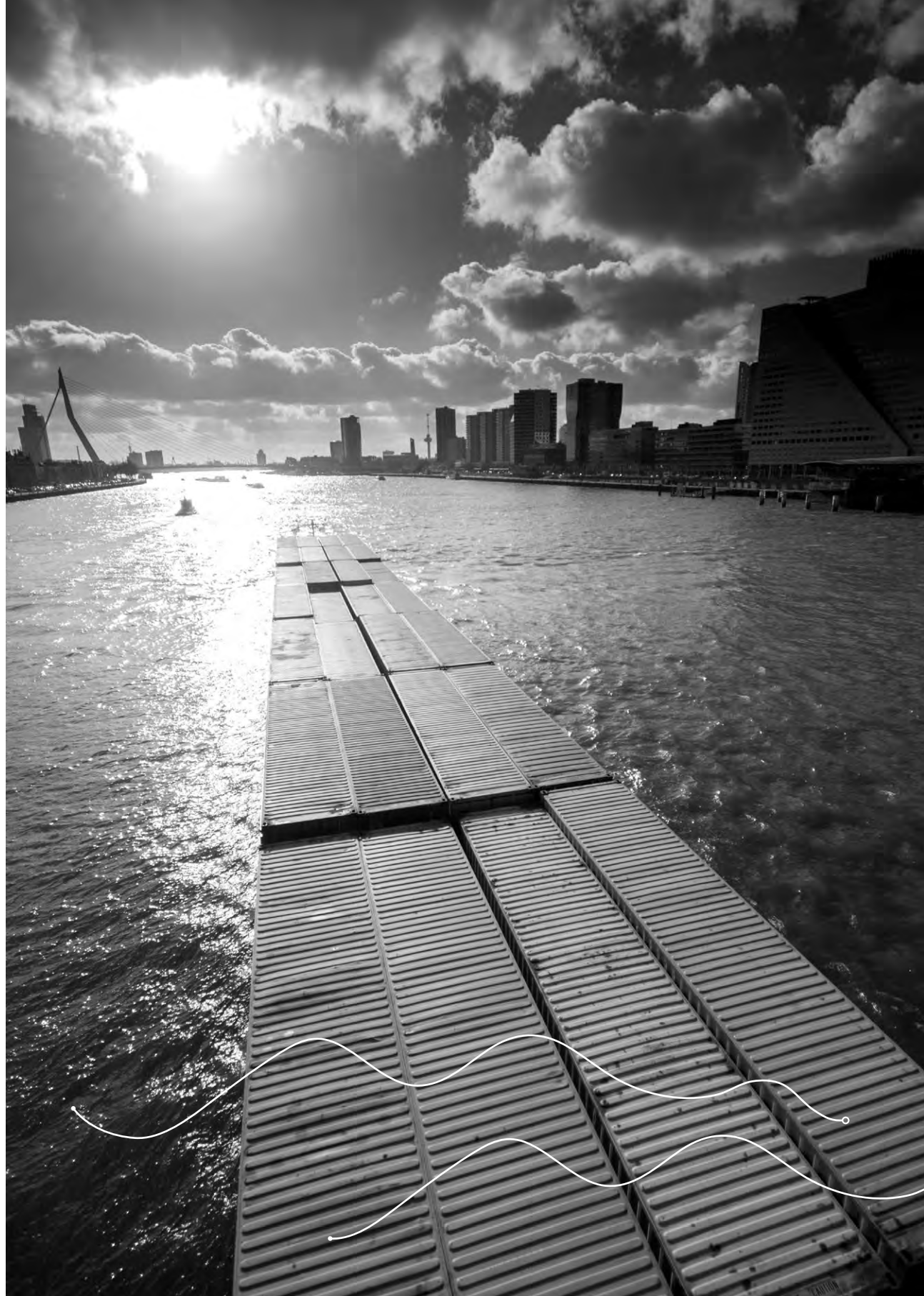
5. Cyber impact control and crisis management

All organizations participating in CA010 2022 pay a lot of attention to their cyber resilience. However, an accident is just around the corner. Before you know it you pressed a malicious link in an email or forgot to update a critical server to a secure version, with a cyber incident as a result. And as we can read in this Cyber assessment, a cyber incident can escalate very quickly to a cyber crisis, and through chain dependencies a crisis at one organization can escalate to a citywide cyber crisis.

Rotterdam already has several structures to manage a crisis. Think of the Veiligheidsregio Rotterdam Rijnmond and FERM for the port and maritime sector. Primarily, existing structures must be made more suitable to deal with cyber crises and better interconnected to fight cyber crises, as is already happening in other domains.

The three best ways to prepare for a crisis are practice, practice and practice. On an operational level, many organizations do this quite regularly. Exercises involving both directors, management and operations are performed less frequently and exercises involving multiple urban functions of the city have actually never been done. One of the ambitions of this plan is to make such exercises a reality. Again, the previously appointed catalyst can play an important coordinating and driving role.

The community around cyber resilience in Rotterdam can also lend a helping hand. Many organizations are looking for crisis protocols or perspectives for action on common cyber crises, such as ransomware, CEO fraud and DDOS attacks. We can develop these protocols together and organizations can voluntarily share the outlines of their protocols with the Rotterdam cyber community. This will help organizations to have better material faster, they can practice more effective and are better equipped against future cyber crises.



Urban Functions

Urban Functions Rotterdam

Urban functions are parts of society that are essential to make the Rotterdam region function properly. When an urban function does not function properly, economic damage can occur and other urban functions can cease to operate as a result. For this Cyber assessment Rotterdam distinguishes ten urban functions. During the sessions, these ten functions were analyzed. The summary of the results of this analysis is included below.

Mobility

The mobility function covers the facilities and processes for traffic and transport in the Rotterdam region. Within the Cyber Assessment Rotterdam 2022 the focus is on the mobility sector, the way in which the different transport systems function and how citizens and businesses are provided with (travel) information.

The Rotterdam region is praised by stakeholders for its abundant existing infrastructure. Rotterdam can be reached via motorways, roads, rail, waterways and by air via Rotterdam The Hague Airport. Downside is that the massive use and presence of these various traffic junctions poses an increased threat because it creates an interesting target for malicious actors to attack. If a successful attack occurs on the mobility sector it can create chaos among users on the one hand, and on the other hand economic damage due to locations not being easily accessible, which means for example, delays in the delivery of goods.

Resilience in the mobility function means keeping the city accessible and actively informing its travelers and other users. These are the essential elements needed if part of the mobility (systems) threatens to fall out.

To ensure the proper functioning of the mobility infrastructure several supply chain partners use a variety of ICT systems. Any of these systems has a different level of emergency facilities, which means that during a failure a possible domino effect can occur. A recognizable example is the power failure in Diemen in 2016, which resulted in a situation where the complete train traffic in the Noord-Holland region got stuck and no flights from Schiphol airport could take off or land.

Via the ICT systems of organizations in the mobility sector, companies and citizens can proactively request and use mobility information. This information allows users to anticipate situations on the road, waterway, in the air or on the track. This is seen as a strong point, because the self-reliance of citizens and companies with digital mobility information seems to grow. Although a lot of travel information is already available, stakeholders see that each mobility component (road, rail, water and air) functions on its own “island”. This results in a sector that does not yet operate as an integrated supply chain and parties aren’t always aware of each other's information and developments.

One mentioned opportunity to achieve this is better cooperation in the supply chain through active information and knowledge sharing and combining about opportunities and threats with each other, with the aim of good accessibility of the city and an informed traveler. For example if a rail connection fails as a result of a hack, certain target groups such as public order and safety personnel and healthcare workers should get priority with other transport options, such as the bus.

Conversely, early information provision can induce employers to provide alternative transport options, such as minibus taxis.

Combining and analyzing data from different forms of transport can lead to better accessibility and mobility within the city. Analysis of current data from the railway, the road network, waterways and the bus transportation can enable the traveler to avoid delays. The traveler also gets the choice to the most environmentally friendly option or a digital meeting, if there is no efficient transport option.

Mobility

Strengths

- Spacious presence of mobility infrastructure in different modes: road, rail, water and air.
- Lots of digital mobility information available to users.
- Part of the safety systems for mobility connected to emergency facilities.

Weaknesses

- The mobility sector isn’t functioning yet as a collaborative chain.
- The sector has different levels of emergency facilities, for example in the event of a power failure.
- The sector is highly dependent on ICT systems, with possible domino effects on failure and impact during prolonged outages.

Opportunities

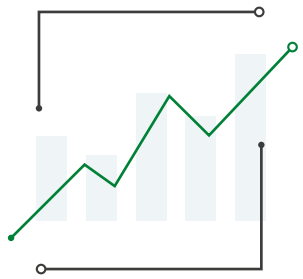
- With collaboration and information exchange in the chain and between modalities, mobility can improve further.
- Self-propelled vehicles, vessels and drones can enhance mobility and make the city accessible while keeping up with increasing mobility.

Threats

- Recognizable and critical facilities such as bridges, dams, station and the airport may be an attractive target.
- Major traffic junctions have social impact in the event of a dropout.
- Autonomous mobility increases dependency on digital infrastructure.

Actions:

- Ensure that the sector functions more as a chain and actively shares and combines information with each other, so that the city remains accessible and citizens are informed early.
- Explore whether the mobility sector as a whole can implement emergency facilities as a baseline to secure the accessibility of and within Rotterdam.
- Ensure that the sector periodically exercises jointly with failure and emergency scenarios to improve resilience in the future.



Economy

The urban economy function covers all facilities and processes for economic traffic, trade and industrial processes in the Rotterdam region.
The Cyber Assessment Rotterdam 2022 focuses on the preconditions for the proper functioning of the Rotterdam economy.

Rotterdam Rijnmond is a region with an important economic footprint. Its most prominent feature is being Europe's largest port, which is worldwide in sixth place with a handling of 441.5 million tons of goods per year. In addition, Rotterdam has a concentration of high-tech sectors in the region that act as drivers of the digital knowledge economy. Due to this position, Rotterdam has managed to create an excellent business climate and companies and organizations can find the region well.

In order to hold and strengthen this position, the city of Rotterdam wants to take a clear pioneering role. She takes on this role by being an example in the field of high-quality and reliable digital infrastructure and digital skilled potential employees.

The digitization of the urban function economy offers opportunities, but is at the same time an Achilles' heel, because a strong digital infrastructure can also be an invitation to enemy actors to disrupt or abuse its reliability. With its FERM initiative (add note: FERM is part of the Port Cyber Resilience Program. Goal of the program is to stimulate cooperation between companies at the port of Rotterdam and raising awareness regarding cyber risks in order to be the best digitally secured port in the world.) the port of Rotterdam has set a good example of self-organization for cyber resilience to face this threat.

Participants note that in recent years the physical domain has become more and more integrated with the digital domain, to the level that these two in some situations are almost indistinguishable from each other.

Economy

Strengths

- Position as a world port, including the associated physical and digital infrastructure.
- Concentration of high-tech sectors in the region as a driver for the digital knowledge economy.

Weaknesses

- Awareness of the opportunities of digitization by entrepreneurs and employees.
- Fear of sharing information about incidents and the speed with which this happens.

Opportunities

- Use the cyber resilience of the region as an opportunity to improve the business climate.
- Stimulate knowledge sharing about cyber resilience in the region to bring down costs for organizations.
- Make use of the well-organized industry associations and existing programs in Rotterdam for connecting to SMEs.
- Stimulating cyber security at suppliers and organizations through tenders, permits or incentive schemes.

Threats

- Basic ICT security for many organizations in the region not in order.
- Lack of an approach to make chains resilient, such as used in superyacht construction.
- Relatively high digital illiteracy in the region, while lower-skilled work is disappearing.
- Organizations have limited knowledge and resources on the field of cyber resilience.

With its facilities and processes, the Rotterdam economy is highly dependent on the reliable use of digital systems.

We also note that entrepreneurs sometimes find it difficult to see opportunities with digitization, and when they recognize them, they find it difficult to make them so concrete that they can take action. The MKB010>Next program has made vouchers and online training for entrepreneurs available, but the possible risks are still being insufficiently recognized. Collaboration between entrepreneurs and also returning communication campaigns could contribute to making concrete digitization initiatives.

In addition, we still have insufficient insight into the way in which organizations with economic functions within and between chains depend on each other. This results in an opaque playing field, within which a cyber incident within a completely different chain can have an unexpected effect on the functioning of your own organization.

On the other hand, the participants indicate that employees' digital skills are still falling short. This does not only apply to “older” employees, but also for young starters who come straight out of school. Too many incidents are still caused by unsafe behavior of people.

Lack of insight into chain dependencies and lagging digital skills can limit economic growth or even cause economic damage. This is evident, for example, from the recent ransomware attacks in the Netherlands and beyond. The most famous example comes from Rotterdam from June 2017, whereby a quarter of Rotterdam's container capacity was not available. The terminal company was no longer able to accept containers loading or unloading.

We note that basic ICT security in many companies stays behind. All the incidents we see confirm that this is a recalcitrant problem. Participants distinguish two opportunities to address this problem.

The first opportunity to increase cyber resilience within the urban function lies with more cooperation and knowledge sharing. The participants experience a fear of sharing information about incidents, which has a limiting effect on shared learning. By collaborating more and sharing knowledge, it should become clearer which chain dependencies exist and what level of security is required within the chain.

The second opportunity lies in joining forces as partners by jointly investing money and time in cybersecurity measures. Complicating factors that the participants recognize in putting the basic ICT security in order are the lack of resources and qualified staff.

Participants recognize this especially in small businesses although they are part of the chain. Collaboration provides organizations with advantages of scale and offers the possibility to steer together to a basic level of cybersecurity in the sector. It is also possible to join forces to manage the scarcity problem for attracting and deploying qualified cyber professionals.

Actions:

- In Rotterdam, collaborate more in chains of organizations with an economic dependence on the Cyber domain. Do this by sharing information. Consider, for example, setting up a Rotterdam CERT (Computer Emergency Response Team), in collaboration with existing bodies such as the Digital Trust Center. Use resources and experience from other sectors or regions.

- Do not just consider Cyber Resilience as an ICT challenge, but include non-ICT domains. For example, consider the physical domain and the employees of organizations.

- Support entrepreneurs in developing digital skills on organizational level and in developing the digital skills of current and future employees. To do this, seek collaboration with the urban function Education.

- Work together to attract and deploy quality cyber professionals in the scarce market. Consider, for example, setting up a pool of cyber professionals to support each other whenever possible.

Governance

Strengths

- Large companies perform relatively well in cyberspace.
- Sense of responsibility for a cyber-resilient Rotterdam is present at domain experts from many different organizations.

Weaknesses

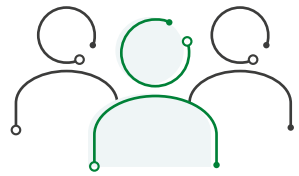
- Lack of direction, fragmentation of public and private and unclear responsibilities.
- Cyber crisis management within the Veiligheidsregio, including scenario-based exercises for executives.
- Cyber security is insufficiently part of existing processes and programs.

Opportunities

- Creating a good business climate for organizations by promoting Rotterdam as cyber resilient city.
- Integrate physical and digital crisis structures CGRIP and CERTs.
- Creating a regional platform to share information.

Threats

- Mayors mainly have powers in the physical public space within the boundaries of the municipality. There is a lot of uncertainty about whether and how these powers can be used in the online public space.
- Managerially and politically there is not enough recognition on how serious the shift from traditional crime to digital crime is.
- Organizations signal that they don't have their own house in order.
- Reinventing the "wheel".



Governance
The urban function of governance covers the facilities and processes for decision-making both in government and in private organizations. Within the Cyber Assessment Rotterdam 2022 the focus will be on the role of directors with regard to cybersecurity and the way directors make decisions.

Rotterdam has a strong attraction for companies as location to settle. There are several large companies and head offices of multinationals within the region.

Within the business community and the (semi-)government there is a wait-and-see attitude towards investments in cybersecurity. We also recognize this in the advice of the Cyber Security Council, in which the recommendation for the coming term of office is to invest 833 million euros extra in the coming four years in Cyber Resilience to catch up. Organizations wait too much on others to act and invest before they act themselves. This leads to a lack of direction, responsibilities within and outside organizations are pushed aside and initiatives remain fragmented.

The administrative and political support for investing in cybersecurity has increased in recent years, but is still inadequate. The trend is that organizations only make budgets available when there is a direct threat or (reputation) damage may occur. At the same time, the shift from traditional crime to digital crime is insufficiently recognized. In addition, Chief Information Security Officers (CISOs) in many cases have too little mandate within the organization, as a result of which they cannot be sufficiently decisive.

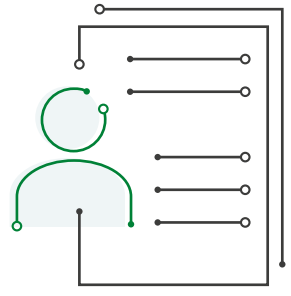
However, participants in the Cyber Assessment Rotterdam 2022 see an opportunity to increase cyber awareness and willingness to invest among executives. For example, by practicing more with each other and executing simulations on cybersecurity and cyber resilience. The results of these exercises and simulations can help CISOs provide feedback to management including advice for investment.

Through the involvement of multiple organizations and the joint results the participants in the Cyber Assessment Rotterdam 2022 expect a more proactive attitude, more awareness and better substantiation of the need for investments in cyber resilience. Additional benefit of joint action with multiple organizations is that solutions or investments can be tackled jointly and shared.

The awareness of cyber resilience and the decisiveness of organizations will be able to grow because of this. In addition, there is a chance to create a more permanent place on the agendas of executives.

Actions:

- Organize dilemma sessions and table-tops for executives involving multiple urban functions. This gives them sufficient insight into cyber resilience to conduct a thorough executive discussion on this.
- Integrate cybersecurity into all urban functions and work with cyber ambassadors who are the gateway to resources and a sparring partner for the organization. They put the subject on the map and seek cooperation within and outside their own organization.
- Create a cyber-direction meeting for the city to align all activities from this cyber assessment, prioritize and open doors where necessary.



Public services

The urban function of public services covers the facilities and processes for the provision of services to residents and businesses in the Rotterdam region. Inside the Cyber assessment Rotterdam 2022 the emphasis is on the digital facilities that replace the previously existing physical counters. For example, it concerns digital communications or services. Think of the application of permits, identity documents or subsidy details, purchasing transport tickets, planning home care and distance education.

Public service providers include both government agencies and, for example healthcare and educational institutions and public transporters. Digitization gives these public service providers the opportunity to provide more services and deliver these services faster. At the same time, the citizen gets increasingly dependent on digital means to do business with these service providers. On the one hand, this imposes requirements on the government regarding functionalities and system security. On the other hand, this also put higher demands on the skills of citizens who want to interact with the municipality or other public service providers.

In the field of public services, the Rotterdam region has long-standing collaborations with semi-public and private partners. These collaborations become easier, as more and more systems are connected to each other and can communicate with each other. However, participants note that the public services therefore become increasingly complex and more specialized at a technical level. This makes it more complex to maintain these systems by knowledgeable staff. In particular aspects such as time, rising costs and insufficiently qualified personnel are a bottleneck here.

Citizens are highly dependent on public services within the Rotterdam region for, among other things, transport, care, education and safety. Participants in the Cyber Assessment Rotterdam 2022 therefore identify the risk of social disruption as a threat, if public services cannot properly function. Precisely because of the

Public Service

Strengths

- We have gained a lot of experience with past incidents.
- Services from collaborations are becoming easier for customers.
- Large-scale communication possibilities are available when needed.

Weaknesses

- Service providers have insufficient insight into the whereabouts of all stored data.
- Sensitive data is often still insufficiently secured.
- Citizens are becoming more dependent on digital solutions and not everyone can deal with that very well.

Opportunities

- Digitization makes it possible to provide more and faster services.
- Co-creation between companies and municipalities is an opportunity for innovation and added value for customers.
- Social media makes it possible to get in touch with citizens and organizations more easily.

Threats

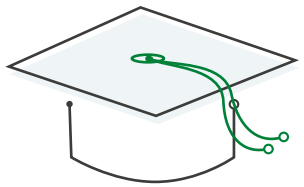
- Infrastructure is becoming more complicated and therefore needs more time and money to maintain.
- Changing laws and regulations causes non-compliance risk.
- If the digital infrastructure does not function properly, there is a risk of social disruption.

importance of continuity of public services, it is important that information security is in order.

Finally, the participants indicated that in the past the public service providers have gained a lot of experience with incidents related to misuse of data by unauthorized persons. An example of such an incident is a data breach. Public service personnel in particular are, because of these kinds of incidents, aware of the sensitivity of the data they work with. These past experiences can make them ambassadors for a digitally secure Rotterdam region.

Actions:

- Jointly develop an insight into which organizations handle which data and where they are stored. This insight should ensure that we get a better grip on information and minimize the chance of incidents. Please take into account the possible confidential nature of the data to create this understanding.
- Create public trust on data security from all involved organizations by showing that involved organizations handle information safely and take responsibility if things go wrong.
- Stimulate working in a privacy-friendly manner, for example by setting up a privacy enabling office, learning from existing initiatives, such as at the Chamber of Commerce.



Education

The urban function of education covers the facilities and processes for the delivery of education and training in the Rotterdam region. Regarding the Cyber assessment Rotterdam it concerns the function of schools in educating students and young people in digital skills and the provision of training in for example cyber security. And in Rotterdam we also know our IT Campus, which is committed to more and better IT talent for the city and for digitally proficient and agile Rotterdam citizens.

From a cyber resilience point of view, every Dutch person should reach a certain level of cyber awareness. Education is the ideal place to provide this resilience. In most cases incidents take place because of the human component, especially due to ignorance. To be resilient in the cyber domain, people should be able to recognize vulnerabilities and threats and know what they should and shouldn't do.

Within the Rotterdam region there is a wide range in primary, secondary and higher education. There are various broad courses, including studies specializing in activities within the port. The participants note that (basic) elements of cybersecurity and cyber awareness is lacking in almost all layers of education. It seems like cybersecurity within regular education has a deterrent effect. Participants indicate that this appears to be due to the complexity of the subject and the non-sexy image. Insufficient time, budget and staff within education reinforce this.

Over the past few years, we have noticed a shift in direction. Very slowly there is a realization in education that digital skills and cyber resilience are indispensable skills for the future. Where digitization now only has a place in ICT training, we see more and more training that pays attention on the digitization of their respective subject. Primary and secondary education

Education

Strengths

- Very wide range of primary, secondary and higher education in the region, including specifically for the port.
- The mindset in primary, secondary and higher education is on the change: We have to do something!
- The initiative of the Cyber workplace provides a lot of visibility and training of scarce specialists.

Weaknesses

- Insufficient learning-work opportunities to properly train young people.
- Digitization in education is not keeping up with the future.
- Parents and teachers have insufficient knowledge on cyber resilience.

Opportunities

- Deploy digitally skilled students to help the institution.
- Cybersecurity specialists in Rotterdam would like to be involved in education at schools.
- Develop digital skills starting in primary school with a Digital Resilience Diploma.

Threats

- We train for jobs that will no longer exist tomorrow.
- Little time per teacher to pay attention to it, we already have a deficit.
- Budget and priority don't get sorted in time.

are working on a revised curriculum, which will be introduced in 2023, within which six themes have been developed around digitization. Security and privacy are part of these themes.

This development is also prompted by the fact that many activities in the future can only be performed digitally supported. Without digital skills you are therefore not well equipped for the labor market. We must avoid training now for jobs that will no longer exist tomorrow.

The participants praise and encourage initiatives such as HackShield in the classroom, a free curriculum that helps students learn in a fun, educational way about cybersecurity. Since 2019, the IT Campus has also organized #hack010, in which ethical hackers from, among others, Techniek College Rotterdam, Rotterdam University of Applied Sciences and Graphic Lyceum Rotterdam work as red teams and looking for vulnerabilities in the systems of the municipality.

Not only the people who follow an education, but also the educational staff should become more cyber-alert and spread more knowledge about this domain. “Practice what you preach” is a frequently heard statement. Organize, for example, annually, per educational institution, a day at which schoolchildren or students with an excessive interest in the cyber domain train teachers and take them into the cyber world.

In line with the foregoing, many specialists within the Rotterdam region have offered to share their knowledge about cybersecurity and cyber resilience with the education sector. Not just to raise the cyber awareness level but also to introduce the new generation to dealing with cybersecurity and the job possibilities in this sector. This does require a bit of coordination.

Finally, knowledge sharing and collective purchasing of training and facilities by Kennisnet and SURF, among others, was identified as an opportunity to improve the level of cybersecurity and awareness in education.

Actions:

- Deploy specialists from profit and non-profit to develop digital skills and integrate cyber resilience into the curriculum of educational institutions.
- Stimulate cooperation between educational institutions, educational levels and the Rotterdam business community to provide good teaching materials as efficiently as possible to create and share cyber resilience. Involve institutes such as Kennisnet and SURF where possible.
- Set a good example by improving the ICT and ICT security of educational institutions and give students a role in this where possible.

Crisis mangement

Strengths

- Good cooperation on city level between public services.
- Example function of cyber resilience in the port, including the Cyber Hotline.
- Willingness to develop among all players is big.

Weaknesses

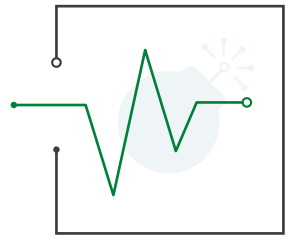
- Insufficient coordination between the urban functions.
- Unknown chain dependencies and the search for “who is the owner?".
- Insufficient basic knowledge about cyber resilience at all levels.

Opportunities

- Use new technology to make incident and crisis management faster and more effective. Think of reusing cameras, deployment of drones and location determination in phones.
- Broad support for more cyber crisis exercises in the city with more stakeholders and diversity of scenarios.
- Create a platform for smart and fast communication.

Threats

- In a crisis we see complete dependence, everything is connected together but we insufficient have oversight on the chains.
- The fast technological development results in safety and legal guarantees falling behind.
- Ransomware attacks take the form of a national crisis.
- Disruption of society by disrupting the (crisis) communication.



Crisis management (Public order and safety)
The urban crisis management function (public order and safety) concerns the facilities and processes for crisis prevention, management and aftercare. Regarding the Cyber Assessment Rotterdam 2018, the focus is on the basic knowledge of Cyber resilience and collaboration with other actors in the region.

Within the urban crisis management function, the Rotterdam go-getter mentality and the existing collaborations are praised. The cooperation between the security triangle, public order and security services (OOV), the Rotterdam-Rijnmond Security Region (VRR) is experienced as good.

Participants indicate that investments should be made in crisis management and combating cyber consequences. Various parties have a role in this, such as the Municipality of Rotterdam and the VRR. The participants signal that the evolution to a network society and the digitization of many processes change their role fundamentally. We also see that crisis management, in addition to an activity in itself, affects all other urban functions when a crisis occurs.

The participants in the Cyber Assessment Rotterdam are making a strong call for more transparency and information sharing from the Rotterdam OOV services. Not every organization receives the warnings from the NCSC, the DTC or the IBD on recent cyber threats. This oversight makes organizations vulnerable to cyber threats and thus poses a threat to the entire city and region.

The group sees a solution in a Rotterdam platform, separate from the existing and sector-specific bodies. With a Rotterdam Cyber platform, Rotterdam organizations can quickly and smartly share information about cyber incidents and threats. Where we have the fire brigade in the physical domain, this role is missed in cyber incidents. A cyber fire brigade can offer a solution to serious cyber incidents that organizations can no longer manage on their own.

Part of being cyber-resilient is fighting the consequences of cyber incidents. An approach and structure specifically for combating cyber consequences is missed in the Rotterdam region. The participants have expressed the wish to have incident structures for cyber incidents and crises to align more closely with the existing crisis structures for physical crisis. We want to better link existing structures to increase effectiveness.

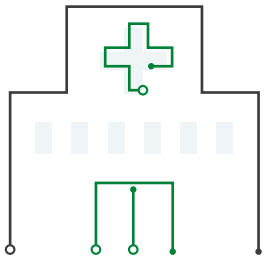
In addition to a cyber crisis organization, there is a need for regional and sector transcending practice of cyber scenarios or scenarios with cyber aspects, in order to ensure better preparation and resilience. The work scenarios can provide a lot of insights into the chain dependence of the urban functions. At the moment, organizations have limited insight into chain dependencies. Practicing can help to clarify these dependencies to jointly increase cyber resilience.

The NCTV has declared Ransomware a national crisis in the Cyber Security Assessment Netherlands 2021. It would have a lot of added value to organizations in Rotterdam to offer a standard cyber exercise Ransomware so they can prepare for this common current cyberattack.

During the sessions, the participants expressed the concern that people engaged in crisis management have too little basic knowledge of cyber resilience, for example in recognizing cyber incidents. This is in line with the observations made with the urban function education.

Actions:

- Explore the possibilities of setting up an accessible to all Cyber platform Rotterdam where knowledge and information about cyber threats can be shared. Also the clear definition of risks to be used by several parties can be developed here: The translation between digitization and organization and the effects of risks therein.
- Ensure that more regional and sector-wide exercises are practiced with cyber incidents, resulting in better preparation and resilience and insight is gained into the (digital) chain dependence.
- Organize central coordination of crisis communication, so that we have more control on crises that affect multiple organizations.



Healthcare
The urban function of healthcare encompasses the facilities and processes for care and health. Regarding the Cyber Assessment Rotterdam 2022 the focus is on ICT systems in healthcare but also the preparations that healthcare certainly takes with regard to cybersecurity.

The healthcare sector is undergoing a digitization process. More and more processes are automated or supported by technology. Digitization offers the possibility to offer more efficient, effective and also different care. For example, new technology can be used to combat loneliness. Technology also makes it possible to provide care at a distance. At the same time, the digital skills of the staff are still too low to work well with the technology and to do so in a safe manner.

Healthcare providers still make extensive use of outdated equipment, so-called legacy equipment. An example of legacy equipment is a care system that only functions on Windows XP. Windows XP is an operating system that is not supported anymore by the vendor and therefore doesn't receive security updates. When a healthcare system only functions on Windows XP, it forces system administrators to keep working with these outdated and less secure systems. Such a system poses a risk to the complete healthcare system and network of a healthcare provider.

In addition to the fact that healthcare providers use a lot of outdated equipment, they also work with a wide variety of suppliers. These suppliers have their own prioritization, budget and policy for cybersecurity. Healthcare providers have little direct influence on these suppliers, but they depend strongly on them.

Within the healthcare sector, there is a strong focus on emergency planning and backup facilities, especially the medium and large care institutions have put thought in disaster planning in the event of incidents. However, there is a lot of fragmentation in healthcare and there are also many small players, who are less able to protect themselves and make themselves resilient.

Healthcare

Strengths

- Sectoral z-CERT.
- Detailed emergency plans present.
- Expertise is present.
- Collaboration between healthcare institutions and public partners.

Weaknesses

- Lots of fragmentation and small players in the industry.
- Low digital skills with staff.
- Many different (legacy) systems present from various suppliers.

Opportunities

- Use digitization to combat loneliness.
- Offer remote care via for example the use of home automation.
- Digicoaches for healthcare.

Threats

- Threat of espionage at medical research.
- Decentrally organized and funded.
- AVG blocks the chain.

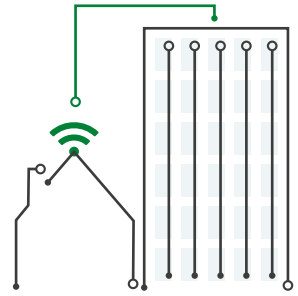
Healthcare processes are not classified as vital in the Netherlands because the threshold values are not met by the individual healthcare institutions. A disruption of a vital process, for example, has the social impact that more than 100,000 people have emotional problems or serious social survival problems.

This impact is not achieved because, for example, fallback is possible between care organizations and the number of clients per care organization is limited. The Netherlands ignores the impact that a possible disruption has on the complete healthcare sector in the Netherlands and the Rotterdam region. In recent times several national and international incidents have shown that the impact of a cyber incident at healthcare institutions can be significant and therefore also the impact on healthcare. The pressure on healthcare is so high that the extra effort that comes with managing the consequences of a cyberattack is too much, especially in the current corona period.

Digital literacy among healthcare providers is relatively low on average, because the focus is on helping and supporting clients and not on supportive processes such as digitization. In addition, healthcare institutions process per definition very privacy-sensitive data and must therefore comply with the highest GDPR requirements. The sector is still insufficiently equipped for this in terms of knowledge and expertise.

Actions:

- Investing a lot in digitally skilled human capital in healthcare. Especially in this sector, digital skills sometimes lag significantly behind, while the risk are high.
- Support chain collaboration between care organizations so that they can work together on making healthcare in Rotterdam cyber-resilient.
- Consider the healthcare sector as vital for Rotterdam, so that the sector can draw resources from the indication vital and start a lobby to achieve this nationally as well.



Housing

The urban function of Housing concerns the facilities and processes for living within the Rotterdam region. The focus within the Cyber Assessment Rotterdam 2022 is on the digital facilities that are increasingly used in homes. This is about the safety of smart systems and home automation and the vulnerability and security of the "virtual home". A risk to the safety of the home threatens the safety of the (vulnerable) resident.

The Rotterdam region is strong in the field of digital connections. Rotterdam is a connected city where experiments are increasingly taking place with home automation to facilitate remote assistance. Home automation concerns the digital systems in a building to automate processes, such as the smart thermostat or the automatic lighting of a home when you return home. Home automation has also many applications for healthcare that are being rolled out, enabling older people to live at home longer.

The downside of home automation is the security of the systems, partly because a cyberattack is less tangible and visible than a physical incident: there is a big difference between opening a physical front door and a virtual front door. Stakeholders note that organizations working and involved in housing have a sense of urgency for cybersecurity in this residential sector, but don't free up enough budget yet. Because of the wait-and-see attitude action only happens when a cyber threat becomes tangible, which is by definition too late.

During the corona crisis, the government has strongly focused on working from home for those professions in which this is possible and on distance education for pupils and students. The home and the digital resources in it therefore play a more important role in working, learning and other essential activities. As a result, citizens and entrepreneurs have become more dependent on the security of the virtual home. It is therefore even more important that the digital facilities in a home are safe and people are aware of possible risks that could affect their own personal safety.

In this context, it is important that residents also know what to do if they suspect that their cybersecurity is at risk. A cyber fire brigade could provide a solution.

Investing in and freeing up budgets for secure equipment is a challenge, because a lot of reliance is still placed on old equipment to keep services running. This equipment may contain vulnerabilities that give cybercriminals access to computer networks and digital systems in a house. It is therefore important to get the security in order, especially with the personal safety of residents in mind. Partly in light of the developments around working from home Rotterdam employers should focus on “cybersecurity-by-design”. It would be good if employers shared knowledge and experiences around this theme and that employers are stimulated to actually follow through on this.

Stakeholders say this cyber threat gives professionals the chance to apply the cybersecurity by design principles in, for example, the tender conditions. With home automation and other Internet of Things (IoT) devices, citizens assume that the equipment is secure. To improve this a process should be set up to ensure that hardware meets the latest cybersecurity requirements, is regularly provided with automated software updates and has the obligation for users to change default login names and passwords on first use.

Entrepreneurs in the Rotterdam region could respond to this by collaboration with, for example, housing associations on cyber-secure smart homes. Business and local government can start in an early stage with these kinds of initiatives, supporting the Rotterdam region to keep its "early" adopter" role and by accelerating and stimulating these kinds of new techniques.

Housing

Strengths

- Citizens and entrepreneurs in Rotterdam are flexible and can take advantage of new work from home opportunities through our strong digital infrastructure and the installation of fiber optic.
- Home automation can strongly improve the quality of living in Rotterdam, for example by remote help or care and smart sensors.

Weaknesses

- Working from home is growing, with the virtual front door often open.
- There is still old equipment in use, which is insufficiently prepared for cybersecurity.
- Residents do not have enough perspective for action when cyber incidents occur.

Opportunities

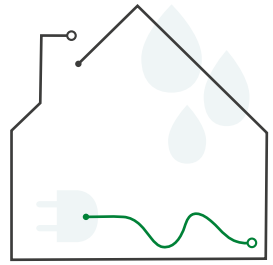
- Picking up cyber security by housing and housing associations.
- Raising demands on and awareness for cybersecurity in housing.
- A cyber fire brigade for incidents with home automation and other digital equipment in the home.

Threats

- Growing digitization of homes such as Internet-of-things makes it attractive to attackers.
- Insufficient awareness on cyber-secure living with residents and housing and equipment providers.
- Out-of-the-box digitization in housing is not always secure by default.

Actions:

- Raise awareness on cyber-secure living among residents, employers, home providers and suppliers of home automation and other equipment for in the house.
- As a housing association, ensure that cybersecurity by design principles are applied. In this way it can be ensured that implementation of home automation in homes does not introduce digital vulnerability. Consider a 'cyber-secure label' for homes, comparable to the energy label.
- Stimulate public-private partnerships aimed at cyber-secure living.



Utilities

The urban function Utilities covers the facilities and processes for primary functioning of the city of Rotterdam and all its inhabitants, companies and organizations. This concerns, for example, systems for drinking water and energy supply. The Cyber assessment Rotterdam 2022 focuses on (digital) dependence of these utilities.

Within Rotterdam there is a great diversity of organizations that provide utilities from various disciplines, such as drinking water and energy suppliers. This diversity makes being jointly cyber resilient a challenge, because parties do not sufficiently have an overview of chain dependencies and do not work on cyber resilience from a chain perspective. This challenge is amplified because the increase of chain dependencies. In addition to the dependency on utilities by all kinds of organizations, the organizations that provide these utilities are also dependent on each other. For example, the drinking water supply and mobility sector are dependent on energy supply and the healthcare sector is dependent on the mobility sector.

In addition, we see that laws and regulations are lagging behind on the digital reality. For example, various sectors are engaged during 2021 and 2022 with the Network and Information Systems Security Act (Wbni) to increase cyber resilience, while this has been a concrete threat for years.

Partnerships for information exchange between organizations that provide basic services exist, but they are too limited. That's how FERM is only accessible to port-related companies and many SMEs can't find answers when they have questions about cyber resilience, despite initiatives such as the DTC and the Platform Veilig Ondernemen. A good integration platform in Rotterdam for information exchange for the utilities sector is lacking. At the national level, we know the sectoral ISACs and the National Detection Network but SMEs are not part of these networks.

Utilities

Strengths

- A lot of experience with crisis response at the utilities sector.
- Dutch utilities are modern and multi-constructed.
- Executive attention for cyber resilience from the utilities sector.

Weaknesses

- Municipalities within the region are working too much individually.
- Insufficient setup of partnerships for SMEs.
- Regulations lag behind the reality of cyber threats.

Opportunities

- Think of the energy transition as a data transition.
- Intersectoral knowledge exchange.
- 5G regulation can increase trust in 5G.

Threats

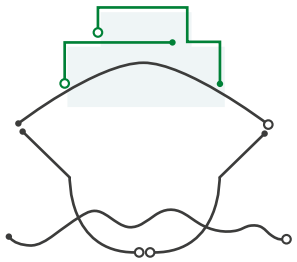
- Increase in chain dependencies means an increase of the complexity of cyber resilience within chains.
- Introduction of Internet of Things (IoT) in industrial processes.
- Stability and resilience of our energy system.

Digitization is also increasingly appearing in industrial systems, such as drinking water supply systems. For example, this development makes remote control possible and is efficient. At the same time, this innovation is a major threat. The consequence of a successful digital attack will have a big impact on the city of Rotterdam. Also, digitized industrial systems are an interesting target to state actors, therefore increasing the risk on a targeted and successful attack. The energy sector notes in this regard that the energy transition is actually a data transition, because working data-driven is applied on a large scale and the dependence that the energy processes have on data.

Participants note that cyber resilience of utilities need executive attention. This will make it possible to invest in adequate measures. On the other hand, the right expertise is scarce. It is difficult to attract and retain the people with the right knowledge. This also reinforces another dilemma. This dilemma is the choice between in-house hiring or outsourcing of cyber processes and specifically cyber security processes. In-house hiring is more expensive and complicated due to a lack of the right expertise, but outsourcing means loss of direction and control. Outsourcing also often leads to less available information to act on than when managing it in-house.

Actions:

- Organize intersectoral information exchange, in particular on the resilience side of the cyber domain.
- Municipalities must do it together, not individually, to ensure that organizations located in several municipalities do not need to enlist in multiple resilience initiatives.
- Focus in all activities on communication with a broad stakeholder group, such as from both a preventive and from a response point of view.



Port

The urban function Port comprises the facilities and processes for the primary functioning of the port of Rotterdam. Within the Cyber Assessment Rotterdam 2022 the focus is on initiatives within the port to achieve more to be cyber-resilient and prevent or limit cyberattacks.

The importance of the port of Rotterdam for the region is great, as we already have explained in the urban function Economy. Due to increasing digitization of the processes and facilities within the port an appropriate level of cyber resilience is essential. The port of Rotterdam has several initiatives in cyber resilience. These initiatives are supported by FERM. FERM is a foundation aimed at stimulating cooperation between companies in the port of Rotterdam and increasing the cyber risk awareness to become the best digitally secured port of the world.

It is important to invest in the cyber resilience of companies in the port of Rotterdam. The maturity of these companies differs greatly. It would be good if there was a better understanding of the level of cyber resilience (the degree of cyber maturity) of these companies. This can then be linked to an associated certification.

Despite the ongoing initiatives, the focus on cyber resilience is not yet enough. In the port industrial complex there are many different companies and not every company has the knowledge or capacity to increase cyber resilience. Also, resources available are too fragmented within individual organizations. The importance of the port is city transcendent, but resources are not allocated at this level.

Meanwhile, the risks are increasing, as the ways to attack also innovate.
Examples of innovation are the development of ransomware as a business model and storage spoofing. In storage spoofing non-existent storage capacities and stocks of raw materials

Port

Strengths

- Multiple initiatives in the port to amplify cyber resilience, supported by FERM foundation.
- The maritime sector makes resources available for increasing their cyber resilience.

Weaknesses

- Great diversity of organizations in the harbor making chain collaboration complex and not always obvious.
- Basic IT security at many organizations is not in order.
- Digital skills of staff are too low.

Opportunities

- Steer companies in the port more towards maturity levels instead of individual measures.
- Powers of the supervisor (ILT) on cyber area are insufficient to force organizations to change.
- Look for connection with the city and region in the field of cyber resilience.

Threats

- Interesting target for cyberattacks because of chain dependencies and the big social impact.
- Insufficient attention on cyber resilience and with it an insufficient defense against threats by state actors for example.
- Growing risks because of innovation in attacks such as ransomware as business model and storage spoofing.

and resources are sold in terminals in the Rotterdam port area. For companies, this can lead to reputational damage, because their name and reputation are damaged by cyber criminals.

The cyber risks are amplified by chain dependencies. An incident can lead to a domino effect, whereby an incident that has an effect on one organization may have impact on other organizations. The chain dependencies are not limited to the port, but extend to the city, the region and beyond. Connection between the port and the city and region can help to become stronger together.

The port of Rotterdam is the largest port in Europe. The Dutch government has designated the port of Rotterdam as one of the two main ports of the Netherlands. The main port status indicates the great importance for the Dutch economy. On the one hand, the size of the port of Rotterdam ensures for economic opportunities for the area, but on the other hand also forms a threat as an interesting target for malicious actors such as states. A cyberattack on the port can lead to major social damage.

Actions:

- Create more awareness in the port and maritime sector. Use and expand existing initiatives.
- Create more insight into chains and chain dependencies within the port and maritime sector.
- Promote transparency in the chain for cyber resilience. Think, for example, of knowledge sharing on vulnerabilities and detected attacks.
- Find the connection between the port, the city and the region in terms of cyber resilience.

Acknowledgement

This publication describes the Cyber Assessment Rotterdam 2022 (CA010 2022). Many stakeholders in the city of Rotterdam and from the Rotterdam region have contributed to the production of this publication. Without their input, knowledge and experience, this publication could never have come into existence.

We would therefore like to thank all organizations, directors, managers and specialists who made a valuable contribution with their provided experiences and knowledge in the making of this publication. We have included the logos of the participating organization on pages 6 and 7.

We hope that we can also count on these organizations and persons to take joint effort according to the actions described in this publication. Only together can we improve the chances of digitization and further increase the cyber resilience of the city of Rotterdam. We are looking forward to a valuable collaboration in making the city of Rotterdam even more digital and cyber-resilient.