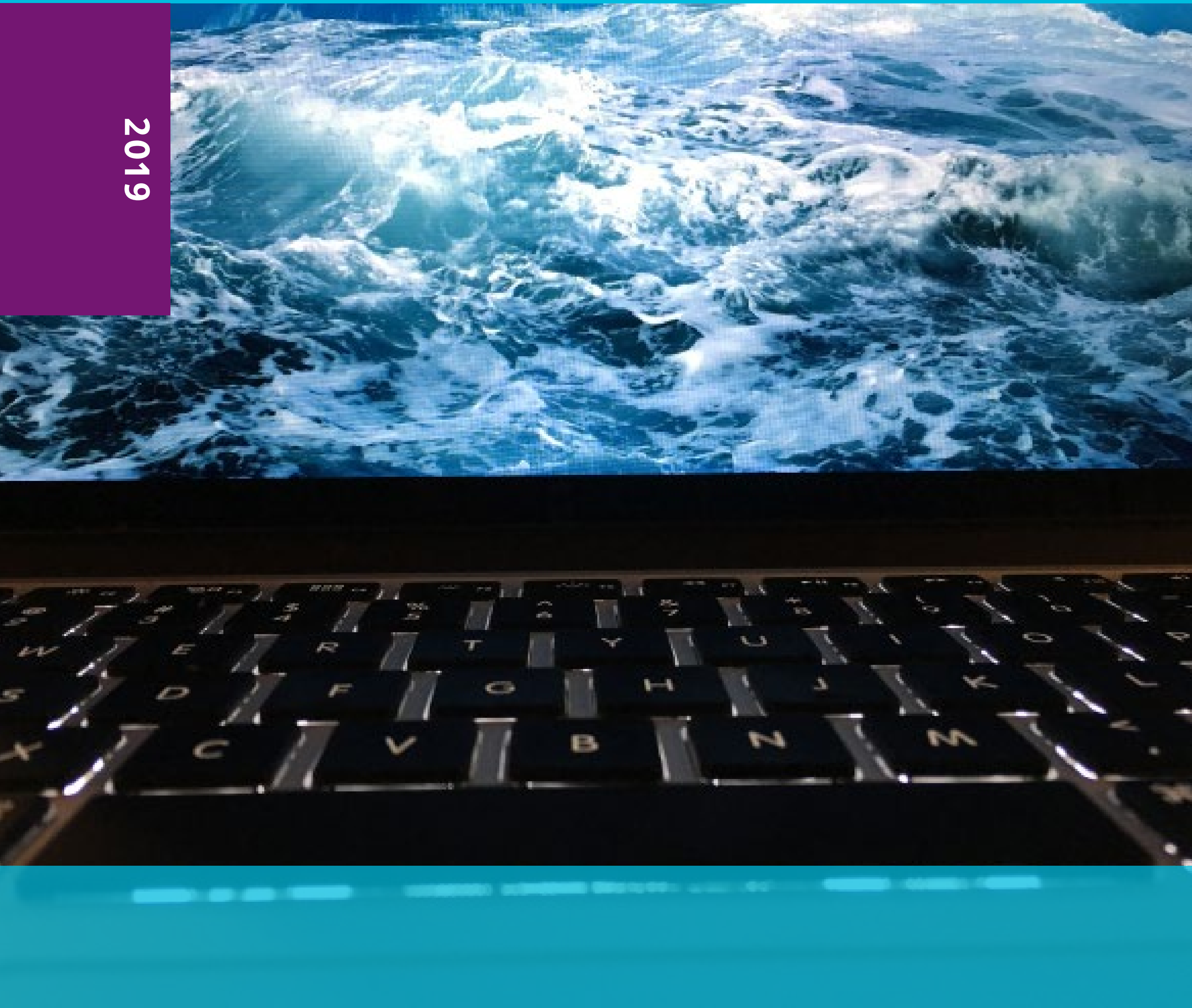
Algemene Rekenkamer

Cyber security and critical water structures

2019



Algemene Rekenkamer

Cyber security and critical water structures

The original report *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* was adopted on 11 maart 2019 and presented to the Dutch House of Representatives on 28 maart 2019.

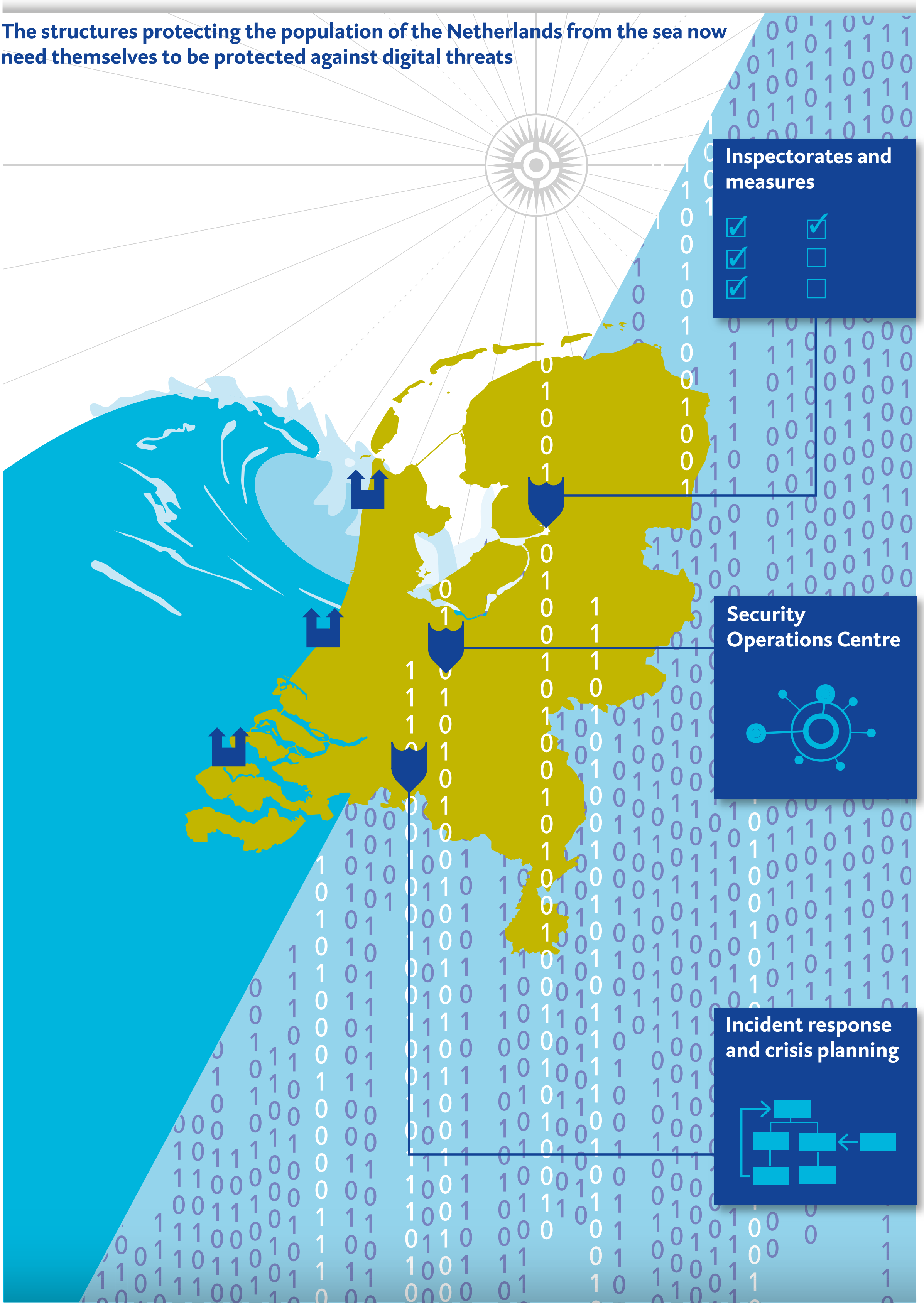

The structures protecting the population of the Netherlands from the sea now need themselves to be protected against digital threats
Inspectorates and measures
Security Operations Centre
Incident response and crisis planning

Figure 1 *Old and new threats*

Preface

Since time immemorial, the inhabitants of the Rhine-Meuse estuary have struggled to contain the water surrounding them to the west and north. By constructing mounds on which to erect buildings, dykes to enclose the land, and windmills to drain their polders, they have gradually created the country we now know as the Netherlands. Over the centuries, they have built civil engineering works to keep the water under control – works that stand as marvels of the modern world. The safety of millions of people depends on the reliability of these water structures, which are also of tremendous economic and ecological importance. Indeed, it was for this reason that the Dutch government decided that they should be regarded as constituting one of the country's 'critical sectors', in the sense that any failures or breakdowns can be socially disruptive and affect other critical sectors, such as electricity distribution.

The digital revolution now unfolding before our eyes has unleashed all sorts of new opportunities. At the same time, society has become dependent on technology and new cyber threats have arisen that until recently were completely unknown. Espionage, sabotage, terrorism and crime have all gained a digital dimension and today threaten the automated systems used for operating dykes, locks and dams. The structures that were designed to protect the population against the water now themselves need protecting against digital threats (see figure 1).

Cyber security is not the same thing as information security. Other than is the case with a failure of information security, a cyber security failure can cause damage on a scale that is potentially disruptive to society as a whole. The problem is greater than that caused by a personal data leak or a breakdown affecting organisational processes. If something goes wrong with flood defences or structures designed to control water levels, there is a risk to the physical security of the country as a whole: the battle against water is a matter of life and death.

In this audit, we examined the way in which critical water structures are protected against cyber attacks.

Contents

1 Summary

1.1 Context: cyber security and critical water structures

Cyber security is the term used to denote a wide variety of measures that are designed to prevent damage being caused by the disruption, breakdown or misuse of IT facilities[1] and to repair any damage thus caused (National Coordinator for Security and Counterterrorism, 2018a). All factors that are capable of causing damage as described above are grouped together under the umbrella term of 'cyber threats'. Certain sectors, such as those responsible for the distribution of electricity or drinking water, are so essential to Dutch society that the government has designated them as 'critical sectors'.

This audit looks at one of these critical sectors, i.e. sea defences and water management. The Minister of Infrastructure and Water Management bears political responsibility for this critical sector. The Minister is also under a statutory duty to report any serious IT incidents to the National Cyber Security Centre. The Minister has designated a number of water structures managed by the Directorate-General for Public Works and Water Management as 'critical parts' of this sector. These are referred to in this report as 'critical water structures'. Our audit examined the way in which the Directorate-General for Public Works and Water Management has prepared to deal with cyber threats to these critical water structures.

1.2 Preparing to deal with cyber threats

The operating processes at critical water structures use computer systems many of which date back to the 1980s and 1990s, a time when the term 'cyber security' was not in common use. Although these systems were originally designed to operate on a stand-alone basis, they have over the years been gradually linked up with bigger computer networks, for example in order to facilitate remote operation. However, this trend has made the systems more vulnerable to cyber threats. For the time being, it is unclear how great the threat is of a cyber attack against the sea defence and water management sector.

According to the Directorate-General for Public Works and Water Management, modernising the systems in order to eliminate any risks would be both technically challenging and costly. For this reason, the Directorate-General has decided to focus its efforts on detecting cyber attacks and mounting an adequate response in order to dispel potential threats. Although we found that the Directorate-General had made a great deal of progress in this respect, it still needs to do more in terms of both detection and response in order to meet its own cyber security targets. This main conclusion is based on the following three sub-conclusions:

1. Although the Directorate-General for Public Works and Water Management has put a great deal of effort into the implementation of a Security Programme, not all the Programme's objectives have yet been achieved.
2. While the detection and response strategy has been operationalised in the form of the creation of a Security Operations Centre (SOC), the strategy has not yet been put into full effect.
3. The Directorate-General is taking steps to deal with cyber attacks and cyber crises, but key documents are outdated. The Directorate-General makes very little use of penetration testing to test the practical effectiveness of measures taken to prevent cyber attacks.

1.2.1 Need foloow-up on the Security Programme

The Security Programme has helped the Directorate-General to make up a lot of lost ground in terms of cyber security. As part of the programme, staff from the Directorate-General inspected all tunnels, bridges, locks and other water structures and took action to offer greater resistance to a potential cyber attack.[2] We examined the measures taken as part of the Security Programme in relation to critical water structures. We found that, following the completion of the Programme, most of the measures (around 60%) had either been put in place or otherwise a deliberate decision had been taken to accept the risk in question (20%). In other cases, the measures were either in the process of adoption (11%) or had been postponed until further notice (9%). Responsibility for the remaining measures has been delegated to the Directorate-General's regional offices. Although the arrangement was that the Directorate-General would keep an eye on the progress made in relation to the remaining measures, we found that head-office staff did not have access to comprehensive information on the status of these measures. We also found that the Directorate-General had not yet achieved its ambition of including cyber security in its routine inspections.

Support audit findings

We found that, in relation to the critical water structures covered by this audit, work had been completed on the majority of the measures taken as part of the Security Programme. In the case of one particular water structure, an important measure that had been scheduled for implementation had yet to be put in place. In another case, the staff of a regional office did not know about any documents for formally transferring responsibility for the implementation of the remaining measures to the office in question.

We identified a number of reasons for the failure to adopt all the measures taken as part of the Security Programme and to ensure that cyber security becomes a permanent feature of all security activities:

- The regional offices are not under any formal obligation to adopt measures and to take part in inspections for testing cyber security.
- Old maintenance contracts prevent the Directorate-General from enforcing certain requirements in relation to cyber security. The Directorate-General is working on this problem.
- No arrangements have been made about the funding of the remaining measures and the inclusion of cyber security as a permanent aspect of inspections. This has delayed the decision-making procedure and the implementation of the measures in question.

1.2.2 Detection and response strategy not yet completed

One of the outcomes of the Security Programme was the establishment of a Security Operations Centre (SOC) whose main task is to detect and respond to cyber attacks. We found that the objective set for the end of 2017 of instantly detecting any cyber attacks directed against critical water structures had not been achieved by the autumn of 2018. This means that there is a risk of the Directorate-General failing to detect a cyber attack directed at a critical water structure, or of detecting such an attack too late.

Support audit findings

A test performed at one of the critical water structures included in our audit showed that it was possible to gain physical access to it. The SOC identified an attempt to gain digital access (by connecting a laptop computer to the network). Measures have been put in place at this particular water structure to instantly detect a cyber attack. In the case of another critical water structure included in our audit, we found that these detection measures had not yet been taken.

A number of regional offices are wary about taking measures enabling the instant detection of cyber attacks against structures managed by them. This is one of the main reasons for the failure to achieve this objective. The SOC is not empowered to oblige the regional offices to adopt such measures.

The SOC acknowledged that it did not have sufficient expertise and staff capacity to further refine and expand the detection measures. Regular talks are held with the responsible minister on the expansion of the SOC. There is a mismatch between supply and demand. As long as no information is available on the level of threat posed to the sector, it is difficult to decide on the appropriate level of investment in expertise and staff capacity.

We also found that the issue of a certificate of good conduct is the only form of screening to which SOC staff are subjected, despite the fact that they come into contact with sensitive information on the operating systems of critical water structures. It is not possible to say whether there is an inconsistency here with the level of threat, given the lack of information on the latter.

1.2.3 Outdated crisis documents and no full pen testing

The Directorate-General for Public Works and Water Management uses a crisis model to plan for a wide range of crises, including cyber crises. This model includes a number of specific crisis scenarios. We found, however, that no scenario had been constructed specifically for a crisis caused by a cyber attack. Moreover, no information was available on the cascade effects caused by a cyber crisis on other sectors. We also found that certain parts of important documents relating to the response to a cyber attack were not kept up to date. The presence of up-to-date information may prove of critical importance for a rapid and effective response to a crisis situation.

In what is known as a ‘pen test’ (penetration test), an organisation deliberately arranges for an outsider to hack into its network in order to obtain information about vulnerabilities in its information security. However, the Directorate-General makes very little use of pen tests on its critical water structures because it claims these are too risky. This means that the organisation does not have information on the ability of critical water structures to resists cyber attacks in practice.

1.3 Recommendations

We urge the Minister of Infrastructure and Water Management to take the following steps in order to form a clear picture of the action that is needed to ensure that the sector is capable of resisting cyber attacks:

1. Identify the current actual level of cyber security threat to critical water structures in order to pave the way for further decisions on the allocation of staffing and resources.

We urge the Minister of Infrastructure and Water Management to take the following steps to ensure that the measures taken as part of the Security Programme are fully implemented:

2. Instruct the Directorate-General for Public Works and Water Management to keep a uniform, centralised record of the action taken to implement the remaining measures delegated to the regional offices, and also to ensure that the remaining measures are indeed implemented in practice.
3. In addition and where necessary, improve the tools created in order to continue on the route mapped out by the Security Programme, with sufficient staffing and resources.

We recommend that the following action be taken to complete the process of detecting cyber attacks directed against critical water structures:

4. Complete the adoption of measures enabling the instant detection of cyber attacks and expand the SOC's monitoring activities (based on an objective assessment of the level of threat; see the first recommendation).
5. Review the level of screening that SOC staff are required to undergo and the classification of sensitive SOC reports (based on an objective assessment of the level of threat; see the first recommendation).

Finally, we recommend that the following action be taken to optimise the preparations for cyber crises:

6. Instruct the Directorate-General for Public Works and Water Management to design and implement a procedure for ensuring that the information on crisis maps and network reports is kept up to date.
7. Instruct the Directorate-General to ensure that the crisis model includes a crisis scenario specifically constructed for cyber security crises and that it generates information on the cascade effects.
8. Identify the risks preventing the Directorate-General from performing full pen tests on the industrial IT systems of critical water structures and use this information to map a route leading to a situation in which pen tests form an integral part of cyber security measures relating to critical water structures.

1.4 Response of the Minister of Infrastructure and Water Management

In her response, the Minister of Infrastructure and Water Management writes that she views it as her responsibility to effectively organise the digital security of the country's critical water structures. She says that she has already given her backing to a ministry-wide cyber security strategy and is seeking to reach agreements with other stakeholders on digital security in the water sector. The Minister regards our conclusion as underpinning the action she has already taken to further improve the cyber security of the water sector. She endorses our conclusions and recommendations and says she is planning to act on all our recommendations. For example, the Minister is planning to ensure that overall threat assessments and additional information obtained from interdepartmental cooperation are translated into the potential consequences for individual critical structures. The Minister believes that the threat assessments will guide the implementation of many of our recommendations. In her response, the Minister also says that the Directorate-General for Public

Works and Water Management has already made up a lot of lost ground in terms of implementing the remaining measures in the Security Programme.

1.5 Court of Audit afterword

The Minister is planning to act on our recommendations. She writes that many of them depend on whether or not the first recommendation is implemented, i.e. identifying the level of threat. However, we would like to point out to the Minister that a number of our recommendations involve the rapid completion of measures that should have been taken some time ago. This applies, for example, to the issue of connecting the critical water structures to the SOC, so that more detailed and more up-to-date information is available on the structures in question. This work should have been completed by the end of 2017 and does not therefore depend on the implementation of the first recommendation.

2 About this audit

2.1 What is the problem?

Cyber security is the term used to denote a wide variety of measures designed to prevent damage being caused by the disruption, breakdown or misuse of IT facilities and to repair any damage thus caused (National Coordinator for Security and Counterterrorism, 2018a). All factors that are capable of causing damage as described above (such as hacking, computer viruses, vandalism, etc.) are grouped together under the umbrella term of ‘cyber threats’. The focus in this audit lies on cyber attacks, i.e. deliberate attempts to cause damage.[3]

The vast majority of the operating processes used by critical sectors have been digitised, which makes them susceptible to cyber threats. In its most recent annual report, the Dutch General Intelligence and Security Service reports a heightening of activities that are intended to open the door to the digital sabotage of critical infrastructure in Europe (General Intelligence and Security Service, 2018). According to the National Cyber Security Centre (NCSC), there is a growing threat both from professional criminals active in the Netherlands and from foreign powers, i.e. state actors; and the attacks are growing increasingly sophisticated and complex (National Coordinator for Security and Counterterrorism, 2018a). The NCSC regards sabotage and disruption by state actors as posing the greatest threat to national security (National Coordinator for Security and Counterterrorism, 2018b).

2.2 Who bears political responsibility?

Writing to the Dutch Lower House of parliament in 2015, the Minister of Security and Justice identified 26 critical processes as being used by 11 different sectors (Ministry of Security and Justice, 2015). Together, these constitute the country’s critical infrastructure. Under the Data Processing and Cyber Security (Duty to Report Incidents) Act, a number of ministers were made responsible for the critical sectors and processes in question.

At the end of 2018, the Data Processing and Cyber Security (Duty to Report Incidents) Act was superseded by the Network and Information Systems Security Act, which is the name under which the Netherlands has implemented the EU Directive on the security of network and information systems (known as the ‘NIS Directive’).[4] The Dutch act describes one of the critical sectors as ‘sea defences and water management’, and designates the Minister of Infrastructure and Water Management as being responsible for it (the act refers to the Minister as the ‘critical supplier’).

Under the Network and Information Systems Security Act, the Minister remains obliged to report to the NCSC any serious IT incidents affecting water structures that she has designated as being 'critical' parts of the sector.

A number of water structures forming part of the 'sea defences and water management sector' have been designated as 'critical' by ministerial order.[5] These structures are referred to in this report as 'critical water structures'. They are managed by the Directorate-General for Public Works and Water Management, which is an executive agency operating under the aegis of the Minister of Infrastructure and Water Management and is responsible for managing the country's main water system, i.e. the major waters such as the sea and the rivers. The Minister of Infrastructure and Water Management is accountable for all action taken by the Directorate-General for Public Works and Water Management in relation to cyber security.

2.3 What are the characteristic features of the sea defences and water management sector?

In addition to making use of automated office equipment, the sea defences and water management sector also uses 'industrial IT systems', i.e. automated processes for operating locks, pumping stations and flood defences. The industrial IT systems that form part of the Netherlands' critical infrastructure may be paralysed by spyware, viruses or ransomware. In 2012, for example, alarming reports appeared in the media about a computer vulnerability that had been found to affect certain pumping stations in the province of Zeeland.[6] The reports suggested that it would be easy for internet hackers – even those without any specialist expertise – to cause flooding by using this vulnerability to switch off pumps.

In recent decades, the Directorate-General for Public Works and Water Management has used automation to make critical water structures both more reliable and more efficient. The operation of locks, pumping stations and flood defences has been automated and systems that used to operate in the old days as stand-alone systems have been linked together to form networks, so as to facilitate remote operation and inspection, for example. However, these developments took place at a time when hardly anyone had heard of the term 'cyber security'.

One of the characteristic features of industrial IT systems is that they have a much longer economic life than office systems (Agence nationale de la sécurité des systèmes d'information, 2012). This combination of obsolete technology that has become interwoven with modern technology has made such systems vulnerable to modern cyber threats (NCSC, 2016)[7]. In the light of the specific characteristics of industrial IT systems, the prevention of such attacks is both technically challenging and costly. For this reason, the Directorate-General for Public Works and Water Management has decided to focus its efforts on detecting and responding to cyber attacks.

2.4 What did we audit?

We audited the way in which the Minister of Infrastructure and Water Management has prepared to deal with cyber attacks mounted against the critical water structures managed on her behalf by the Directorate-General for Public Works and Water Management. These were our main audit questions:

1. What tools are available to the Directorate-General for Public Works and Water Management as the manager of the water structures, for detecting cyber threats and attacks and protecting itself against cyber threats to the flood defences?
2. Are the tools for detecting cyber threats and attacks effective? Do they offer sufficient protection?
3. What scenarios have been devised for a situation in which a cyber attack takes place? What action can the Directorate-General for Public Works and Water Management take in order to prevent any cascade effects, i.e. to prevent other critical sectors from being affected by the same attack?
4. How does the Directorate-General for Public Works and Water Management respond when vulnerabilities and incidents are detected

2.5 How did we perform the audit?

In order to answer the audit questions, we studied internal documents at the Ministry of Infrastructure and Water Management and the Directorate-General for Public Works and Water Management during the period between May and October 2018. We also interviewed a number of key individuals during the same period. We were interested both in whether measures had been adopted and, if so, in what these were. In order to answer the second audit question, working alongside staff from the Directorate-General, we performed an on-site audit of the effectiveness of the cyber security measures at a number of critical water structures,. At one of the structures, a team of ethical hackers tested the practical effectiveness of the cyber security measures. See Appendix 1 for more detailed information on the audit methods.

Format

Chapter 3 discusses how the Directorate-General for Public Works and Water Management made up for lost ground by mounting a cyber security programme. This is important as the programme laid the foundations for the detection of cyber attacks and painted a picture of the current level of cyber security at the Directorate-General. This information forms a partial answer to the first two audit questions.

Chapter 4 examines the way in which the Directorate-General detects cyber threats (see the first two audit questions) and how it responds to reports of vulnerabilities (the fourth audit question). Chapter 5 goes on to look at the way in which the Directorate-General has prepared to deal with cyber attacks (the third audit question) and responds to cyber security incidents (the fourth audit question). Chapter 6 sets out the conclusions and recommendations for the Minister of Infrastructure and Water Management. The Minister's response is reproduced in chapter 7, together with an afterword from us.

The chapters are interspersed with a number of case studies. Apart from illustrating our findings and conclusions, these also provide more detailed information on the practical effectiveness of the cyber security measures (in answer to the second audit question).

Confidential information

In principle, our audit reports are public documents. We are subject to very few restrictions under the 2016 Government Accounts Act on our authority to publish the findings of our audits. However, we have a policy of not publishing certain audit findings if they are capable of causing a disproportionate amount of damage to certain interests. In the case of this audit, we decided that certain information should be shared with the Upper and Lower Houses of the Dutch parliament exclusively on a confidential basis.

3 The Security Programme: making up lost ground

This chapter looks both at the organisation that manages the critical water structures on the Minister's behalf and at the multi-year Security Programme that was designed specifically for the Directorate-General for Public Works and Water Management, and which focused on cyber security. Apart from answering the first and second audit questions, the information in this chapter is also intended to create a better understanding of the context in which the Directorate-General operates. The Security Programme also forms the basis for the formulation of a series of objectives that the Directorate-General has set itself in relation to cyber security. These provided part of the framework that we used to assess our findings.

The chapter begins with a brief description of the Directorate-General for Public Works and Water Management and the organisational units and roles that are most directly relevant to the issue of cyber security. We then go on to discuss the reasons for setting up the Security Programme, its implementation and its three most important results:

1. measures to improve cyber security;
2. cyber security requirements for water structures;
3. monitoring and responding to cyber threats.

The first two of these results are examined in this chapter. A separate chapter is devoted to the third result.

3.1 Cyber security and the organisational structure of the Directorate-General for Public Works and Water Management

The Directorate-General for Public Works and Water Management is formally an agency of the Ministry of Infrastructure and Water Management and is divided into head-office departments and regional offices. A management board straddles the two. The head-office departments are responsible for formulating operating frameworks and procedures, and for supplying the regional offices with support services. The regional offices are responsible for building, managing and maintaining roads, waterways and water structures. The management board is responsible for the operation and performance of the organisation as a whole. Its main focus lies on strategic planning and decision-making.

The organisational structure of the Directorate-General for Public Works and Water Management and the main actors featuring in this audit are shown in Figure 2.

Head-office departements and regional offices work together on cyber security

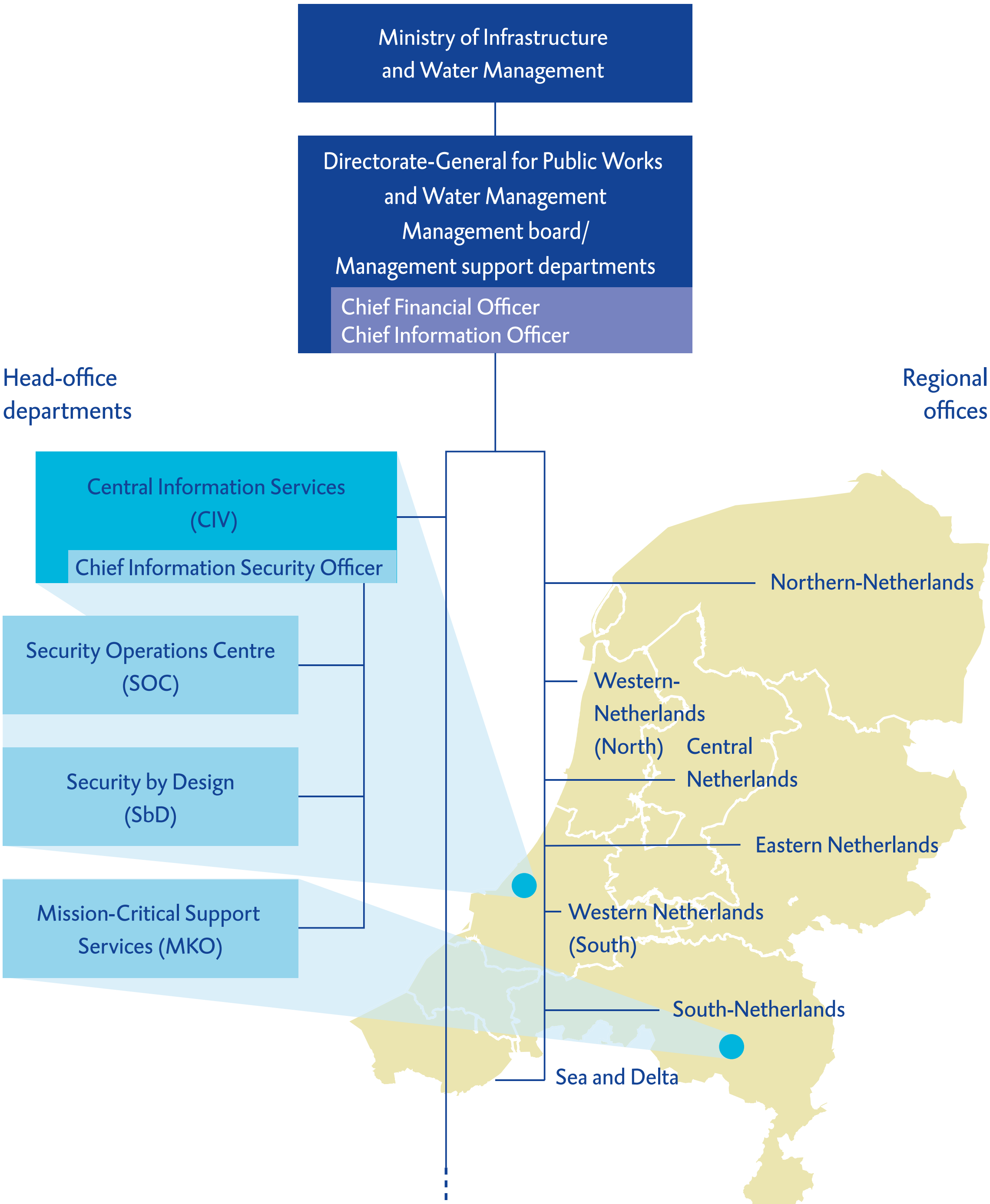

Ministry of Infrastructure and Water Management
Directorate-General for Public Works and Water Management Management board/ Management support departments
Chief Financial Officer
Chief Information Officer
Head-office departments
Regional offices
Central Information Services (CIV)
Chief Information Security Officer
Security Operations Centre (SOC)
Security by Design (SbD)
Mission-Critical Support Services (MKO)
Northern-Netherlands
Western-Netherlands (North)
Central Netherlands
Eastern Netherlands
Western Netherlands (South)
South-Netherlands
Sea and Delta

Figure 2 *Main actors at the Directorate-General for Public Works and Water Management in relation to cyber security*

Two members of the Directorate-General's management board are responsible for information security: the Chief Financial Officer and the Chief Information Officer. One of the head-office departments, Central Information Services (CIV), manages the Directorate-General's computer networks, workspaces, telephony, applications and data processing. The CIV, which employs a staff of over 1,000 people, is a key player in relation to cyber security:

- The CIV is managed by the Chief Information Officer.
- The Chief Information Security Officer, whose remit encompasses the entire Directorate-General, is a member of the CIV. Working in consultation with the Chief Information Officer, he formulates the Directorate-General's policy on information security.
- The main task of the Security by Design team at the CIV (with a staff of seven) is to ensure that cyber security requirements are incorporated in operating procedures and contracts with third parties. This aspect is discussed in greater detail in section 3.4.
- The SOC (with a staff of 11) is also based at the CIV. Its role is discussed in detail in chapter 4.
- The Mission-Critical Support Services department (with a staff of 55) is also part of the CIV. It handles all reports and warnings relating to IT incidents, including cyber incidents. Its role is examined in more detail in section 5.1.

The regional offices at the Directorate-General for Public Works and Water Management are responsible for managing and maintaining the various structures around the country, and for implementing national policy in their own regions. They are required to work in close collaboration with the CIV on all issues, including cyber security. The CIV has no authority to compel the regional offices to take certain decisions on cyber security, although the management board does have such powers. The Directorate-General has deliberately decided to give the CIV an advisory role with limited authority over the regional offices. The Directorate-General believes that this has the effect of preventing a situation from arising in which cyber security risks are dealt with at an operational level and the management board is left unaware of them. It is crucially important that information on security risks should reach the management, so that a high-level dialogue can be pursued on threats. Although the management board is entitled to impose certain cyber security measures, it generally opts for a top-down approach. Thanks to their knowledge of and proximity to the structure in question, those responsible for structures play an important role in the decision-making procedure.

3.2 The Security Programme; background, aims and resultsn

At the end of 2013, the Directorate-General for Public Works and Water Management decided to launch a Security Programme. Among the factors leading up to this decision were:

- problems with the operation of an important motorway bridge in the centre of the country; these problems had featured regularly in the news since 2009;[8]
- a report on shortcomings in information security at the local authority in the town of Veere in 2012;[9]
- a shortcoming in relation to information security[10] that we had identified during our audits in 2011 and 2012 (Netherlands Court of Audit, 2012; see box).

Previous audits (Netherlands Court of Audit, 2011–2016)

One of the findings of our 2011 accountability audit was that information security at the ministry then known as the Ministry of Infrastructure and the Environment11 and at the Directorate-General for Public Works and Water Management was not up to standard. The computer systems used by the Directorate-General were not adequately protected, leaving them vulnerable to cyber attacks. This finding prompted the Directorate-General to adopt a series of improvements in 2012, in part on the basis of the Security Programme. In our 2015 audit report, we reported that the Directorate-General had made sufficient progress in terms of solving the problems identified in our earlier report. What had previously been classified as a ‘shortcoming’ was now categorised as an ‘area for improvement’. Although we removed this item from the list of ‘areas for improvement’ the following year, we pointed to the need to ensure that the Security Programme was implemented throughout the line organisation.

The aim of the Security Programme was to ensure that ‘the infrastructure at the Directorate-General for Public Works and Water Management continues to operate in a reliable manner and that a basic level of security is assured’. The programme focused on the three ‘systems’ for which the Directorate-General is responsible, i.e. the main water system, the main waterway system and the road network. Those structures (i.e. tunnels, bridges, locks, traffic control centres, etc.) and IT systems presenting the greatest risks were the first to be taken in hand. In addition to specific structures and IT systems, the programme also covered generic facilities, such as the Directorate-General’s computer network (see section 4.1). The Directorate-General also looked at management and maintenance procedures and at the staff working with the computer systems in question.

Implementation of the Security Programme funded largely by the Minister of Infrastructure and Water Management

The Minister of Infrastructure and Water Management set aside a sum of € 114.7 million at the start of the Security Programme. Although this was intended to cover the cost of the entire programme, it became clear in the spring of 2016 that a further € 17.3 million was needed to fund various additional items, i.e. a number of structures not originally covered and various physical security measures. The Directorate-General for Public Works and Water Management came up with the additional resources by prioritising the Security Programme measures in the budgets allocated to the regional offices.

Out of the total available budget of € 132 million, a sum of € 128.2 million had been spent by the end of 2017. This left € 3.37 million worth of outstanding commitments, responsibility for which was transferred to the regional offices. The final figure for programme spending was € 3 million higher than the amount budgeted, due to extra expenditure on the main waterways. As was the case with the budget overshoot of € 17.3 million referred to above, the Directorate-General is required to fund this extra expenditure from its own budget. The final figure for the estimated cost of the programme was therefore € 134.6 million. Of this figure, the Ministry of Infrastructure and Water Management provided € 114.7 million in additional funding, while the Directorate-General paid € 19.9 million from existing budgets. Figure 3 shows the cost of the Security Programme.

The Security Programme was funded largely by the Ministry of Infrastructure and Water Management

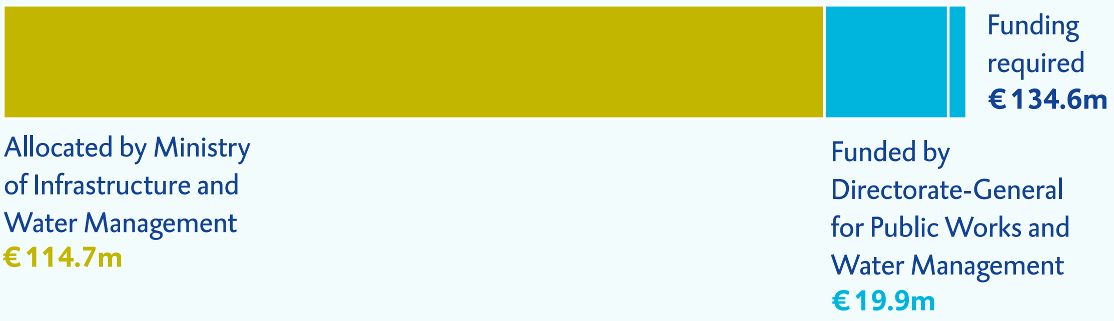


Figure 3 How the Security Programme was funded

The Security Programme had three important consequences for the cyber security of the critical water structures:

1. The Directorate-General for Public Works and Water Management defined and implemented a series of improvements as part of a sub-project known as the IMPAKT programme (standing for ‘impulse programme for tackling the critical technical infrastructure’). The Directorate-General subsequently adopted a tool known as FIT

('functional inspections and tests') to ensure that the IMPAKT programme has a lasting effect (see section 3.3).

2. Certain requirements have been formulated for integrating cyber security as a standard feature of all processes and contracts relating to the design, construction and maintenance of water structures (see section 3.4).
3. The Directorate-General has set up a Security Operations Centre (SOC) to protect the water structures from digital attacks (see chapter 4).

3.3 The IMPAKT improvement programme

3.3.1 The IMPAKT strategy: measures based on field visits

The IMPAKT strategy consisted of field visits undertaken by a team of internal and external experts to 460 structures managed by the Directorate-General for Public Works and Water Management.[12] Cyber security was the main concern (see the box). As far as the network of main waterways was concerned, the team visited 12 small structures, i.e. individual pumping stations and sluices, and 55 larger complexes, including storm-surge barriers and locks. The field visits to the water structures that formed part of the main waterway network were made in 2014 and 2015.

Criteria: multiple aspects relevant to cyber security

The IMPAKT expert teams applied a number of criteria in assessing the security of the structures. Apart from looking at cyber security, they also examined asset management processes and physical security, i.e. aspects such as key management, fencing and alarms). These have a bearing on cyber security. Asset management involves aspects such as keeping a check on which software versions and updates have been installed. A failure to update software may create a cyber security risk. Shortcomings in physical security may pose a threat to the continuity of IT services. A lack of proper physical security could not only lead to people gaining access to certain equipment, it could also enable vandals to disrupt IT services.

The IMPAKT teams also assessed the functional safety of the structures. This means the safety in and around a structure, such as the presence of fall protection and rescue equipment. As this aspect is not relevant to cyber security, we did not include it in our audit. Measures taken in relation to cyber security, physical security and asset management are referred to in this report as cyber security-related measures.

Based on the findings of the expert team, a package of measures was then proposed for the structure in question. Examples of such measures are:[13]

- Upgrade the server operating system to a version that supports data encryption.
- Ensure that no one is able to use a form of remote control without a physical switch in the vicinity of the structure being turned on.

- Make check lists detailing the issue of keys, passes, accounts, etc. giving access to the structure; make sure that those issued with means of access are required to sign for receipt.
- Remove password stickers from all keyboards and computer screens.

The regional managers were made responsible for implementing the measures. IMPAKT staff supported the managers, coordinated the work and monitored the progress made.

3.3.2 Around 60 per cent of the measures relating to critical water structures have been implemented

We used the most recent progress report to ascertain whether the Directorate-General has implemented the cyber security-related measures as planned. This progress report was updated for the last time early in 2018, shortly after the completion of the Security Programme. We concentrated on those water structures designated as critical by the Minister of Infrastructure and Water Management (see section 2.2).

Figure 4 shows the status of the cyber security-related measures for critical water structures at the end of the Security Programme. The bulk of the 218 measures have been implemented, i.e. around 60%. In the case of 43 of the proposed measures (20%), a conscious decision had been taken not to implement the measure in question and to accept the risk posed. A total of 23 measures (11%) were in the course of implementation and 20 (9%) had been postponed until further notice.

The bulk of the 218 IMPAKT measures for critical water structures have been put in place

The digital security measures taken as part of the IMPAKT programme had reached different stages by early 2018

Status early in 2018

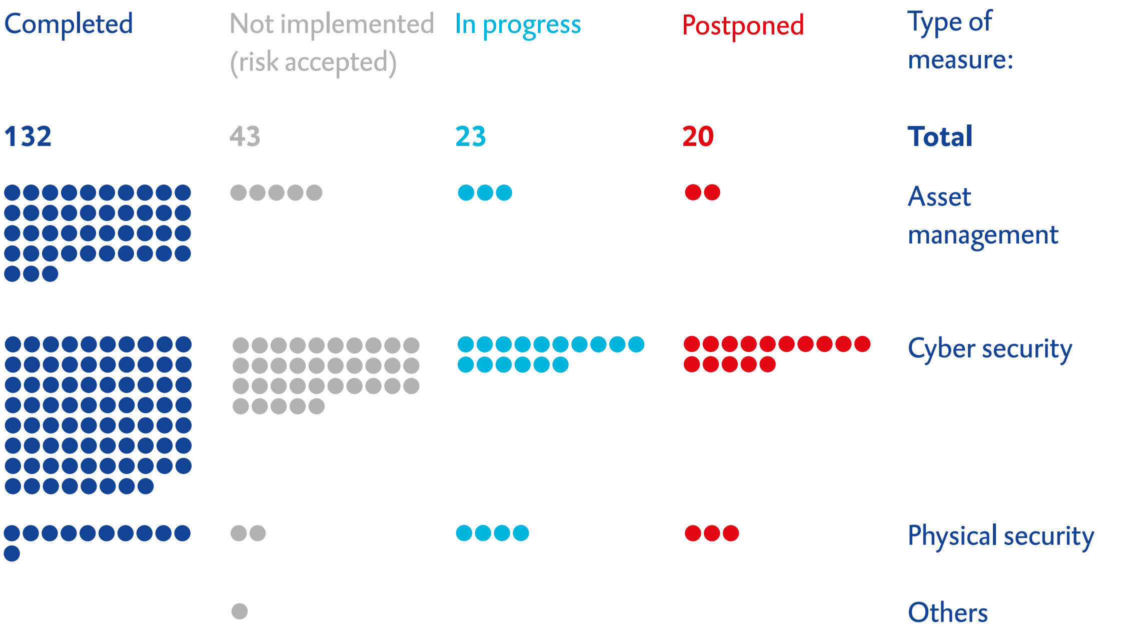


Figure 4 *Cyber security related measures in relation to critical water structures*

There are various reasons why, during the course of the Security Programme, certain measures were deferred or delayed, or why a deliberate decision was taken not to implement certain measures:

- Either the maintenance contracts with suppliers did not provide scope for making the desired adjustments in relation to cyber security, or the suppliers in question did not possess the necessary expertise.
- The implementation of the measures depended on other plans and projects. For example, staff working at one of the critical water structures included in our audit said that the physical security measures depended on the completion of an already existing project focusing on all aspects of physical security.
- The costs were not commensurate with the degree of risk. For example, at one of the critical water structures included in our audit, the level of cost involved in enabling

antiquated equipment to handle stronger passwords was excessive in the light of the level of risk involved.

Following the completion of the Security Programme, the CIV department delegated responsibility for all measures that had not yet been implemented to the regional offices managing the water structures. To this end, the CIV department sent the regional offices transfer documents with covering letters. The transfer documents contained a list of all measures identified during the course of the IMPAKT programme that still needed to be implemented. The documents stated that the regional office in question was responsible for implementing the remaining measures and that no further support would be provided by the IMPAKT programme team. The regional offices were also made responsible for funding the measures. The outstanding measures did not necessarily address security problems involving a low level of risk. At one of the water structures, for example, an important network study had not yet been performed, no proper key management procedure had been adopted, and managers had yet to attend a course in cyber security awareness.

3.3.3 No comprehensive list of outstanding measures and no fundingt

The supervision of the measures delegated to the regional offices is an aspect where there is room for improvement on the part of the Directorate-General for Public Works and Water Management. This is something for which the Chief Information Officer has been responsible since the Security Programme came to an end. The CIV department has not kept an up-to-date record of all measures and their current status since January 2018, i.e. shortly after the completion of the Security Programme. There is no comprehensive, up-to-date list of the action taken by the regional offices to address the outstanding measures. As a further point, the CIV department has no authority to compel the regional offices managing the structures to implement the outstanding measures.

Staff at the regional offices claimed that the Directorate-General failed to account for the fact that many measures involve recurring costs. An access control policy is a good example of such a measure. Clearly, such a policy cannot be implemented without devising, formalising and implementing a procedure. This is a once-only activity. Once the policy has been put in place, though, it needs to be enforced on a systematic, long-term basis. This is a process involving regular evaluations and policy refinements. However, the regional offices have not been allotted any extra funding, which means that the funding of outstanding measures is a matter of dispute.

3.3.4 Extra attention needed to pursue IMPAKT strategy in the future

The management board of the Directorate-General for Public Works and Water Management has adopted a tool known as ‘functional inspections and tests’ (FIT) to ensure that lasting lessons can be learned from the experiences gained with the IMPAKT programme. This tool supplements the inspections already performed by the Directorate-General and focuses on a number of aspects, including cyber security. It was designed as a growth model. FIT was initially part of the IMPAKT programme and was funded from the Security Programme budget. The management board of the Directorate-General expressed the wish that, following the completion of the Security Programme, FIT should be included as a standard feature of inspections of virtually all structures with movable parts.

FIT involves close collaboration between the regional offices and both the CIV department and other head-office departments. During the first year of its operation, i.e. 2017, the Directorate-General wanted local managers to use the tool on ‘a number of’ structures, with a team from head office working with the tool on a further seven structures. Based on the experiences gained from this trial, the idea was that the CIV department would draw up a proposal for giving line managers systematic responsibility for FIT. The idea was for head-office teams to inspect 21 structures in 2018, the ultimate aim being for 470 structures to undergo an annual FIT inspection by 2020.

We found that a total of seven FIT inspections were performed in 2017 (by both head-office teams and regional managers). This means that the target for 2017 was not fully met. It was not clear at the time when we performed our audit whether the target of inspecting 21 structures in 2018 would be met. At the time when the tool was launched, no funding was made available for the cost of the systematic use of FIT after 2017. The regional offices were made responsible for performing FIT inspections when the Security Programme was terminated early in 2018. As a result, the funding of FIT inspections is another topic of debate between the management board of the Directorate-General and the regional offices. A full FIT inspection costs €25,000. The management board has written to the regional offices asking them to lend their full cooperation to these inspections.

3.4 Cyber security requierements for water structures managed by the Directorate-General for Public Works and Water Management

3.4.1 Directorate-General develops standards for industrial IT systems

A second important consequence of the Security Programme for cyber security has been the formulation of cyber security requirements for computer systems used by structures managed by the Directorate-General for Public Works and Water Management. The whole sea defence and water management sector has traditionally been largely the domain of civil engineers. At the time when water structures underwent a first wave of automation in the 1980s, very little was known about the nature of today's digital threats. For a long time, the issue of cyber security was a very minor aspect of the design of water structures and their maintenance contracts. Even before the Security Programme was launched, the Directorate-General was already aware that the criteria that information security was required to meet at the time were no longer adequate for industrial IT systems.

Based on the ISO standard for information security, the Directorate-General subsequently designed its own guidelines for the cyber security of industrial IT systems. These are known as the 'cyber security implementation guidelines for structures managed by the Directorate-General for Public Works and Water Management'(or CSIR for short). The first version of these guidelines was used during the construction of the Gaasperdammer tunnel in 2012–2013.

One of the aims of the Security Programme was to incorporate cyber security requirements in maintenance contracts. The CSIR guidelines were refined and extended to this end. The Security by Design team (Sbd), which is part of Central Information Services, takes the lead in this connection on behalf of all departments at the Directorate-General.

When the IMPAKT measures were put into effect, it became clear that a number of the desired changes could not be made due to the terms of existing maintenance contracts. Moreover, the suppliers responsible for maintaining the structures were not under any contractual obligation to possess the necessary expertise. This helped to persuade the Directorate-General that cyber security should form an integral part of all products, processes and systems used by the organisation. Thus, cyber security is now a prominent aspect throughout the life cycle of all structures, from the draft design up to and including maintenance, many decades after the completion of the structure in question. The CSIR guidelines form the basis for this.

3.4.2 Cyber security requirements gradually incorporated in contracts

The Directorate-General has developed its own guidelines for cyber security in the form of the CSIR guidelines. These are sufficiently broad-based to be applicable to all water structures and industrial IT systems. We were able to see how the CSIR guidelines are structured and how requirements from the BIR (the 'baseline for information security in the civil service'), the NCSC and other guidelines and criteria have been assimilated in the CSIR guidelines. It is important to note in this connection that the Directorate-General examined all the requirements in the BIR and the NCSC's check list for industrial IT systems and, where relevant, incorporated these in the CSIR guidelines.

The requirements set out in the CSIR guidelines are now gradually being incorporated in all contracts signed by the Directorate-General. An important consideration here is that many maintenance contracts have been entered into for periods of 10 or 20 years and that it is both legally complicated and costly to alter their terms prior to their expiry. The Directorate-General has decided that it is better to wait until the contracts have come to an end and to incorporate the cyber security requirements based on the CSIR guidelines in new contracts. The idea is that, in this way, the contracts for all water structures will gradually be made 'cyberproof' over the coming years. We were informed by staff of the Directorate-General that cyber security requirements have now been included in the maintenance contracts for one of the two critical water structures that we visited as part of our audit.

3.5 Conclusions

We found that, following the termination of the Security Programme, the Directorate-General no longer had comprehensive information on the status of the remaining IMPAKT measures. This means that the Directorate-General does not have a full picture of the risk of the measures not being implemented. As a result, the Directorate-General has failed to achieve the objective it has set itself and there is a risk of certain structures remaining vulnerable to cyber attacks. The Directorate-General wishes to use FIT inspections to learn lasting lessons from the visits made as part of the IMPAKT programme. We found that this tool is not yet being used in accordance with the Directorate-General's aims.

We identified organisational problems, and problems in relation to expertise, staffing and funding in connection with both of the above conclusions.

Organisation

Neither the CIV department nor the Directorate-General's management board is entitled to compel the regional offices managing the water structures to implement the outstanding measures. The same applies to the use of FIT inspections.

Expertise and staffing

Certain IMPAKT measures were not enforceable because maintenance contracts with suppliers prevented them from being enforced, or because the suppliers in question did not possess the necessary expertise.

The Directorate-General will be incorporating the cyber security requirements from the CSIR guidelines in all contracts it is planning to sign in the coming years. Although this is a process that can still take many years due to the length of existing contracts, the Directorate-General is nonetheless trying to tackle the problem.

Funding

Following the completion of the Security Programme, the Directorate-General did not set aside any funding for the implementation of the measures it delegated to the regional offices. The regional offices now need to reprioritise their budgets in order to implement the outstanding measures. FIT inspections also need to be funded from current budgets. This has led to internal disputes about funding and reprioritisation, and has caused delays in decision-making and in the implementation of measures.

Audit of Alpha structure

Most IMPAKT measures implemented, but network studies still needed
With the aim of identifying the current status of the IMPAKT measures, we conducted fieldwork in the autumn of 2018 at a structure designated as ‘Alpha’. Figure 5 shows the status of the measures when the Security Programme came to an end, based on the data available to the Directorate-General for Public Works and Water Management.

66% of the IMPAKT measures had been implemented at Alpha by the end of the Security Programme

The digital security measures taken as part of the IMPAKT programme had reached different stages by early 2018

Status early in 2018

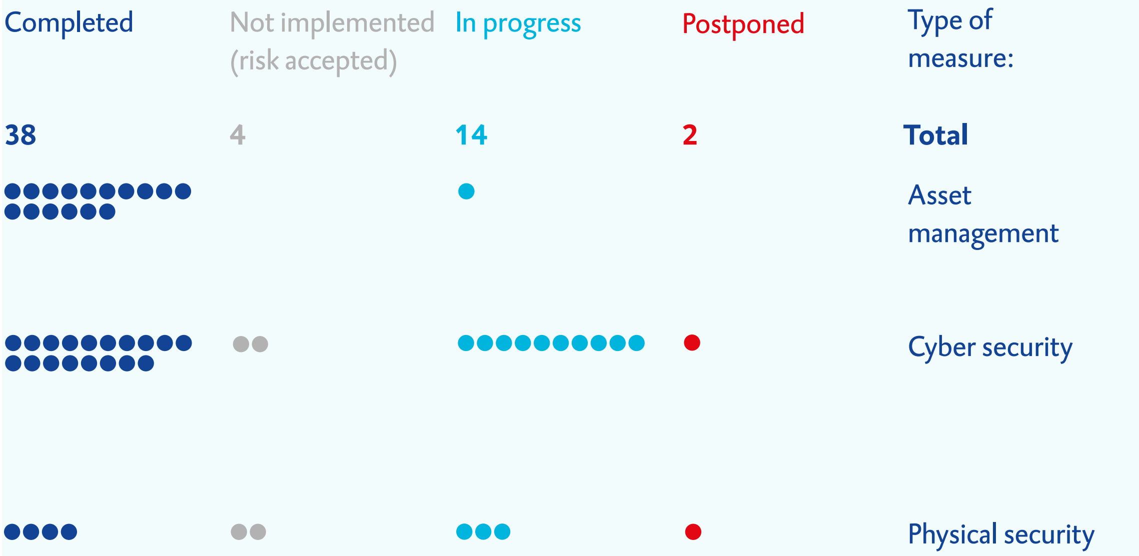


Figure 5 *Status of the IMPAKTmeasures relating to Alpha at the end of the Security Programme*

It became clear during the course of our visit that the bulk of the IMPAKT measures had been either completed (formally or virtually). One important measure was still awaiting implementation, but this could not be put into effect as part of the IMPAKT programme. As no more funds were available once the Security Programme had been completed, it remained unclear for a long time who would have to take responsibility for the measure in question. This problem was resolved in the autumn of 2018.

Vulnerability test: hackers were able to break in, but were detected by the SOC
Working in conjunction with the Directorate-General for Public Works and Water Management and an external party, we designed a test to assess the practical effectiveness of the cyber security measures taken in relation to Alpha. The test was designed to assess the following three aspects:

1. The level of resistance to unauthorised access. The hackers tried to gain physical access to the structure, as a first stage of an on-site digital attack against the digital infrastructure.
2. The SOC's detection capacity and the type of action taken when an unknown device connects with the computer network. This involved connecting a laptop computer to the computer network on-site.
3. Possible weaknesses in the infrastructure. These were assessed with the aid of an expert review of network maps and interviews with members of staff. Where there were doubts about certain weaknesses, we used a technical test to see whether these were open to exploitation.

In the case of the first part of the test, the external hackers twice managed to gain access to the structure by making use of social engineering (i.e. by misleading staff). On the first occasion, the hackers gained access to the control room, where they found themselves alone with an unlocked key cabinet and unsecured work stations. On the second occasion, the hackers managed to acquire a temporary pass allowing them to move freely around the structure. Once again, the hackers gained access to critical parts of the structure, such as servers rooms and stores were key components were stored.

In the second part of the test, a laptop computer was connected to the network from a location in the structure itself. With the exception of one member of staff, no one at the SOC was aware of this test. The hackers exhibited various forms of technical behaviour after connecting the laptop, ranging from highly secretive (i.e. without generating any traffic on the computer network) to relatively conspicuous. They were detected by the SOC in all cases. This would normally have had the effect of setting off alarm bells at the Directorate-General. However, the fact that a member of SOC staff was aware of the test meant that the first step instead involved contacting the managers of the structure, who confirmed that the break-in had been staged as part of a test.

Finally, the external party formulated seven findings based on the expert review. The findings confirmed the picture that had already emerged, i.e. that the industrial IT systems used by critical water structures are vulnerable by modern standards and that preventive measures would be both technically complex and costly.

4 Detecting cyber attacks and vulnerabilities

The Directorate-General for Public Works and Water Management has adopted a strategy of detecting and responding to cyber attacks, given that it is generally not possible to replace or fully protect industrial IT systems. For this reason, our audit focused on these particular aspects of the strategy.

This chapter discusses the third important result of the Security Programme in terms of cyber security (see chapter 3): the creation of a Security Operations Centre (SOC). This forms the remainder of our answer to the question of which tools are available to the Directorate-General for detecting cyber threats and attacks, and whether these tools offer sufficient protection (i.e. the first two audit questions). The chapter also examines the way in which the Directorate-General responds when vulnerabilities and incidents are detected (i.e. the fourth audit question), given that the SOC is also responsible for detecting vulnerabilities.

4.1 The Directorate-General's computer network and the detection strategy

4.1.1 Network offers protection; additional measures for detecting cyber attacks

The Directorate-General for Public Works and Water Management has its own glass fibre network, which forms a first line of defence against cyber attacks. Additionally, the Directorate-General has adopted a number of extra cyber security measures for detecting cyber attacks.

Our audit team found that the precise level of threat, particularly that emanating from foreign powers (i.e. state actors), was not known. The National Coordinator for Security and Counterterrorism has claimed (National Coordinator for Security and Counter-terrorism, 2018a) that the level of threat posed by professional criminals and state actors is on the rise, and that attacks are becoming increasingly sophisticated and complex.
A publication entitled Cybersecuritybeeld Nederland 2018 ('Cyber security picture for the Netherlands', National Coordinator for Security and Counterterrorism, 2018a) describes sabotage and disruption by state actors as posing the greatest threat to national security.
During the course of our audit, the SOC told us that sophisticated attackers might be able to evade detection by the Directorate-General. However, we were not able to identify the attackers' precise capacities, and their readiness to use their capacities against critical water structures.

4.1.2 Not all critical water structures covered by instant detection

The Directorate-General for Public Works and Water Management has set up a team of specialists, i.e. the SOC, to detect and respond to cyber attacks. The SOC was formed during the course of the Security Programme in accordance with a central government best practice document drawn up by experts from the Tax Administration, the IT Shared Service Centre and the Directorate-General for Public Works and Water Management.

Any cyber attacks directed against critical water structures need to be detected without delay. In order to ensure that such attacks can indeed be instantly detected, the Directorate-General needs to adopt certain measures in relation to critical water structures.

The Directorate-General had set itself the objective of ensuring, by the end of 2017, that any cyber attack directed against a critical water structure would be instantly detected. The situation in the autumn of 2018 was that instant detection was possible in the case of slightly less than half of the critical water structures.

Funding has been found to cover the cost of measures for facilitating the instant detection of cyber attacks directed against all critical water structures. The 2018 budget of the Ministry of Infrastructure and Water Management includes an allocation of € 5.4 million, which the Directorate-General claims is sufficient to cover the cost of the SOC. The main reason why instant detection has not yet been adopted at all critical water structures is the fact that certain regional offices are wary about taking the measures in question. Some of them regard the measures as posing a risk in themselves. The SOC has no authority to compel the regional offices to adopt the measures. Given that the SOC cannot undertake instant detection at all the critical water structures, the current situation is that the detection strategy is not yet fully operational.

The Minister of Infrastructure and Water Management is under a statutory obligation to report any serious IT-related incidents. The central monitoring of the critical water structures by the SOC is one of the tools available to the Minister for discharging this obligation. However, as long as no comprehensive monitoring mechanism has been put in place, the Minister does not have access to full information on the cyber security situation at all the critical water structures.

4.1.3 Detection and response by the SOC still under development

The SOC analyses large quantities of data obtained from a wide range of sources, and uses the findings generated by these analyses to detect suspicious activity. The SOC analyses the data with the aid of software designed to recognise certain situations and patterns and to emit an alert whenever such a situation or pattern arises. The software emits different types of alerts, ranging from 'low risk' (i.e. there is a relatively low risk of anything actually being wrong) to 'critical' (i.e. a digital attack is virtually certain to be taking place).

The staff of the SOC assess the alerts by examining them in more detail. This is a risk-driven activity, i.e. precedence is given to urgent alerts over low-risk alerts. Examples of suspicious situations would be unusual connections between two computers at a given structure, or a sudden change in the volume of data traffic in part of the Directorate-General's computer network. This type of suspicious situation may indicate that someone has hacked into the network, or is attempting to hack into the network. If the SOC reports, on the basis of its analysis, that there has been a cyber incident, or a possible cyber incident, a response is initiated. The first step involves reporting the incident to the Mission-Critical Support Services department (see section 5.1).

The SOC claims to have a capacity problem – in terms of both staff and expertise. This lack of capacity causes delays, for example, in analysing reports of potential threats: the SOC claims that it may take several days before any action is taken in response to low-priority alerts. The SOC staff that they would like to further refine and professionalise their detection practices, for example by refining the way in which log data are checked so as to identify any suspicious patterns. The Directorate-General says that additional funding is needed – on top of the € 5.4 million allocated for 2018 – in order to refine the detection and response strategy. Although the Directorate-General submitted a request for extra funding at the end of 2017, the Minister of Infrastructure and Water Management did not present a budget proposal for the amount in question to the Lower House.

We found that there was no clear picture at the time of our audit of the precise level of cyber security threat facing the critical water structures. This complicates the debate on the allocation of extra funding on top of the resources already allocated to the critical water structures. It is not clear whether the action taken is commensurate with the level of threat.

4.2 Reporting threats and vulnerabilities

One of the SOC's responsibilities is to alert the Ministry to vulnerabilities and to provide an effective response. A vulnerability is not the same as a cyber attack; it is a risk that has been identified and which may or may not need to be addressed. The first thing the SOC does is to gather intelligence, i.e. the SOC collects, analyses and interprets information on cyber threats. Based on this information, the Directorate-General for Public Works and Water Management can then put measures in place to eliminate the threat or mitigate its consequences.

In collecting intelligence on threats, the SOC combines its own information with information obtained from its partners. To this end, the SOC consults a number of different parties such as the General Intelligence and Security Service, the Military Intelligence and Security Service and other Security Operations Centres, including those of government entities. The NCSC, for example, is one of the SOC's external sources of information on vulnerabilities. This may be information on industrial equipment in which certain digital vulnerabilities have been discovered that a hacker could potentially exploit.
The member of SOC staff who liaises with parties such as the NCSC has been security-screened by the General Intelligence and Security Service (level A). We found that the only form of security screening to which the other members of the SOC's staff were subject, was that involved in issuing a certificate of good conduct. The Directorate-General does not impose any stricter requirements on the staff in question. This forms a barrier to information-sharing, given that not all the information obtained from the General Intelligence and Security Service can be distributed throughout the SOC. Moreover, all SOC staff come into contact with sensitive information on the IT systems of critical water structures.

The SOC also checks whether any departments or offices do not adhere to the Directorate-General's security policy. For example, SOC staff check whether all mandatory updates are installed. If the SOC identifies a divergence from standard policy, it advises the regional offices on the nature of the action they need to take in order to remedy the situation.
At the same time, the SOC is not empowered to compel the manager of a water structure to act on its recommendations. For example, a regional office may regard the risk posed by the installation of an update as being greater than that posed by not installing the update. The SOC is authorised to actively intervene only in situations constituting an acute threat, for example by quarantining suspect or infected emails, blocking high-risk IP addresses or immediately removing unauthorised equipment from the Directorate-General's network. Directorate-General staff said that sporadic use had been made of these powers.

4.3 Conclusions

In this chapter, we have sought to answer our audit question about detecting and responding to cyber attacks. The Directorate-General for Public Works and Water Management has sought to pursue a detection and response strategy by setting up the SOC. Nonetheless, the strategy is still under development and has yet to be implemented in full. The Directorate-General is not capable of instantly detecting all cyber attacks mounted against a critical water structure. As a result, the SOC does not have an up-to-date picture of the cyber security status of all critical water structures, which means that there is a risk of hackers being able to break into critical structures unnoticed. This, in turn, affects the Minister's duty to report all serious IT-related incidents affecting water structures. Whether the measures taken by the Directorate-General will prove adequate, depends on the level of threat posed. Unfortunately, no information is available on the level of threat.

Our conclusions relate to problems of an organisational nature, problems in terms of expertise and staffing, and funding.

Organisational problems

A number of regional offices are wary about taking measures to enable cyber attacks to be instantly detected. Also, the regional offices are not obliged to implement the SOC's recommendations in this respect. The SOC is not empowered to oblige the regional offices to adopt measures or implement recommendations; the management board of the Directorate-General is.

Expertise and staffing

We found that the issue of a certificate of good conduct was the only form of screening to which most SOC staff are subject, despite the fact that they come into contact with sensitive information on the operating systems of critical water structures. We cannot say whether there is an inconsistency here with the level of threat, given the absence of information on the latter.

Funding

The Ministry's budget includes an item to cover the cost of the SOC. The Directorate-General for Public Works and Water Management says that it does not have access to sufficient (additional) funding to pay for the further development of the SOC. Information on the level of threat is needed in order to make effective choices in allocating funding.

Audit of Bravo structure

IMPAKT measures fully implemented; regional office not aware of document formally transferring responsibility for remaining measures
With the aim of identifying the current status of the IMPAKT measures, we conducted fieldwork in the autumn of 2018 at a structure designated as 'Bravo'. Figure 6 shows the status of the measures when the Security Programme came to an end, based on the data available to the Directorate-General for Public Works and Water Management.

79% of the IMPAKT measures had been implemented at Bravo by the end of the Security Programme

The digital security measures taken as part of the IMPAKT programme had reached different stages by early 2018

Status early in 2018

Completed	Not implemented (risk accepted)	In progress	Postponed	Type of measure:
27	6	0	1	**Total**
●●●●●●	●●●●			Asset management
●●●●●●●●●● ●●●●●●●●●●	●●			Cyber security
●			●	Physical security

Figure 6 *Status of the IMPAKT measures relating to Bravo at the end of the Security Programme*

When we performed our fieldwork at Bravo, we found that the staff of the regional offices did not know about the IMPAKT programme documents under which they were formally made responsible for implementing all remaining measures. Similarly, they were not aware either of all the measures in question or of their current status. We did find, on the other hand, that all the measures had been taken. For example, 'hardening' had been applied at Bravo, i.e. the structure's digital resilience had been enhanced by adjusting factory settings and standard passwords and by switching off unused IT components. We also found that a server had been moved to a secure room, in accordance with a recommendation made as part of the IMPAKT programme.

A deliberate decision had been made not to act on the IMPAKT recommendation to encrypt data held on the server at Bravo. Staff at the regional office said that the data might be needed in an emergency and that the risk of not being able to decrypt the data in such a situation was more serious. This is an example of a risk that the Directorate-General has clearly analysed and consciously accepted.

Vulnerability test: stand-alone component; data difficult to manipulate
As part of our audit, we tested a component part of the Bravo structure. We paid special attention to the external links affecting the IT systems for the component in question.

The operating system at the Bravo structure is based on a 'conservative' design, i.e. manual operation. This has the advantage of reducing the cyber security risks. Nonetheless, the Bravo structure does have an IT system for helping staff to take operational decisions, as well as an IT system that automatically closes the structure in the event of a calamity (for example, if staff cannot reach the controls). Both systems receive information in the form of measurement data obtained from different sources.

Given the nature of our audit, we were particularly interested in the links between these IT systems and systems that are connected to the (public) internet. We found that there was a link between the systems: the system used to automatically close the structure in the event of a calamity 'tells' the support system that it is still operational. This is the only form of communication that is possible between the two systems. It is unidirectional, i.e. it goes from the system used to close the structure to the support system, but not in the opposite direction.

The measuring stations supplying both IT systems with crucial information on water levels are physically protected. Moreover, the support system obtains and compares data from a number of different sources, so that any discrepancies are immediately obvious. The IT system used for closing the Bravo structure in the event of a calamity is located in a separate, secure room. The Directorate-General has put in place certain measures for preventing unauthorised persons from gaining access to the system. During the test, the system was triggered by manually manipulating the data collected by the measuring stations.

No action has been taken at the Bravo structure to enable the SOC to instantly detect a cyber attack. As a result, there is a risk of a cyber security incident remaining undetected for longer than is necessary.

5 Preparing for cyber incidents and cyber crises

Alongside detection, response is one of the key aspects of the cyber security strategy adopted by the Directorate-General for Public Works and Water Management. This chapter examines the way in which the Directorate-General prepares for and responds to cyber security-related incidents and crises. The aim in doing so is to answer the fourth and fifth audit questions.

The chapter starts by showing how the Directorate-General deals with minor, more or less isolated cyber security incidents. The following section describes how the Directorate-General plans to deal with larger and more complex situations, i.e. cyber security crises. The third and final section discusses ‘pen tests’ (penetration tests).

5.1 How Mission-Critical Support Services deals with cyber security incidents

A cyber security incident is defined as an individual event that either causes actual damage or is capable of causing damage as a result of the disruption, failure or misuse of IT systems, and which may be caused by a cyber attack. An example of a cyber security incident is a warning from the SOC that a computer located in the vicinity of a critical water structure is trying to send data to a recipient located outside the structure. This is a warning that needs to be investigated as it may be symptomatic of a cyber attack.

Such potential cyber security incidents are reported and acted upon as part of the Directorate-General’s routine incident management procedure. The Mission-Critical Support Services department (MKO) at the Directorate-General is responsible for handling all reports and alerts relating to IT systems that are regarded as being critical to the Directorate-General’s mission. The MKO department receives and keeps a record of all reports of potential cyber security incidents and monitors the response to such incidents. If a member of the Directorate-General’s staff suspects that a particular structure (e.g. a bridge or a lock) is the target of a cyber security incident, they are required to report their suspicions to a regional control centre. The regional control centres together form a network of round-the-clock incident rooms. The regional control centre in question notifies the MKO department of the potential cyber security incident.

As we have already said, the SOC is also authorised to report cyber security incidents. It is quite possible that, when a potential incident is reported, the staff working at the structure in question have not yet noticed that anything is wrong. The SOC also reports cyber security incidents to the MKO department. However, before this happens, the SOC takes a closer look at the incident in question. If the SOC sees, for example, that there is a problem with the IT system used by a particular structure, the first step is to get in touch with the responsible member of staff. In practice, the problem may have been caused by scheduled maintenance activities and may not be the result of an unauthorised attempt to hack into the system. The fact is that the SOC does not receive advance notice of all maintenance work. The current situation is that SOC staff are required to manually report all software alerts to the MKO department. The Directorate-General wants to change this, so that in future all software alerts are automatically passed on to the MKO department.

The MKO departments records around 40 cyber security incidents every month and has standard procedures for dealing with cyber security incidents. It deals with all minor incidents itself: its staff have attended specialist internal training courses that are designed to equip them with the necessary expertise.

In more complex situations, a ‘task force’ is set up to deal with the incident. The task force, which may include staff from the SOC, investigates the causes of the incident and advises on how to solve the problem and prevent any escalation. If a particular incident cannot be solved by the standard procedure, the next step is to scale-up, which means that it becomes subject to the Directorate-General’s crisis management procedure (see section 5.2).

It became clear from interviews with staff of the SOC and the MKO department that the Directorate-General regards all cyber security incidents reported to date as being false alarms. According to our interviewees, not a single cyber attack has been found to have been mounted against a flood defence.

5.2 Crisis-readiness

5.2.1 No cyber security scenario in crisis management model used by Directorate-General for Public Works and Water Management

A cyber crisis may be defined as a prolonged and/or complex disruption of IT systems caused by a cyber attack. A cyber security incident may evolve into a cyber crisis, for example, where ransomware infects a single computer, which then spreads it over the entire network.

Scaling-up and scaling-down are two important parts of the response to a crisis. Depending on how the crisis develops, different organisations may be asked to help in controlling and fighting the crisis. The Directorate-General for Public Works and Water Management uses a crisis management model consisting of three scaling-up stages, with a different crisis response team for each stage. If one team does not manage to contain the situation, the response is scaled-up to the next stage. The crisis management model describes how the teams are supposed to operate and sets out the criteria used for scaling-up the response.

The Directorate-General's crisis management model includes a number of scenarios for responding to specific types of crisis. There are scenarios, for example, for a collision on a waterway and for a situation in which surface water has been contaminated. A crisis scenarios contains detailed scaling-up criteria. However, the Directorate-General has not devised a scenario specifically for a cyber security crisis.

In the event of a cyber security crisis, the Directorate-General makes use of a chart known as the 'Cyber Security Network Map'. This shows:

- which parties should be involved in dealing with a cyber security crisis;
- which parties need to liaise with each other in order to agree on the technical aspects of the response;
- which parties need to contact each other in order to coordinate the response.

Although the Cyber Security Network Map shows which parties are involved in dealing with a cyber security crisis, it does not indicate a hierarchic structure or the scaling-up lines running between them. In other words, the map does not show exactly what is supposed to happen during a crisis, the sequence of events and each party's responsibility.

The Ministry of Infrastructure and Water Management is involved in responding to a crisis if the crisis is regarded as being 'government-wide', e.g. if airlines or railways are also affected. A Departmental Crisis Centre at the Ministry coordinates the entire crisis decision-making process at the Ministry and passes on all necessary information to the inter-departmental crisis response teams.

As we have already mentioned, the Network and Information Systems Security Act obliges the Minister to report, inter alia to the NCSC, any IT-related incidents that are sufficiently serious as to be capable of disrupting society at large. The NCSC can then proceed to assess the risk of social disruption and help either to prevent or to contain it. The NCSC can also warn other critical sectors about the potential threat in good time and thus prevent it from spreading any further afield.

The line ministers are responsible for the threshold values applying to the reporting of incidents to the NCSC. The Minister of Infrastructure and Water Management is the minister responsible for the sea defences and water management sector. A threshold value could be, for example, the maximum time limit for notifying a cyber security incident. The threshold values applying to the Directorate-General for Public Works and Water Management were adopted in November 2018. Staff of the Directorate-General said that, before then, they did not know when an incident affecting a critical water structure needed to be reported to the NCSC.

5.2.2 Key crisis documents at the SOC outdated

In the event of a calamity, the SOC needs to gain rapid access to key data on the critical water structures. The SOC uses crisis maps and network reports for this purpose.

Crisis maps

Crisis maps show important features of the industrial IT systems used for the water structures. They contain, among other information, the contact details of each structure's manager, as well as those of all relevant contractors and other stakeholders. It follows from the nature of these documents that this information must be both complete and accurate. We found that some of the information given on the crisis maps was either outdated or incomplete. This problem affected, for example, the contact details of people who were supposed to be contacted in the event of a calamity. The resultant risk materialised when, in the summer of 2018, the SOC tried to get in touch with the systems manager of one of the two critical water structures included in our audit. The SOC wanted to talk to him about a report that part of the network was down. However, it proved that the member of staff named on the crisis map had left on holiday the previous day. It would therefore be better to link the contact details on the map to a role instead of to an individual. During the exercise undertaken at one of the water structures included in our audit, the information on the crisis map was used to contact a member of staff who subsequently proved not to be responsible for remedying IT problems at the structure in question.

The crisis maps are no more than snapshots made when the IMPAKT programme team visited the water structures, and in some cases are over one year old. A crisis map is updated only when a member of the SOC visits a structure, or happens to notice that a particular item is outdated. At the time of our audit, no procedure had been put in place for keeping the crisis maps up to date.

Network reports

The network reports used by the SOC during a crisis describe the component parts making up a local network of water structures. They show the connections between the component parts, the open ports and the protocols used for communicating through the ports in question. In other words, the network reports show the entry points that a hacker might use to gain entry to an IT system. They also show how a hacker could penetrate deeper into the network. Such reports have been compiled for many of the structures inspected by the IMPAKT programme team and depict the situation pertaining at the time of the programme. This means that some of the reports are already several years old.

The Directorate-General for Public Works and Water Management claimed, in relation to the network reports we were shown, that little or nothing had changed in the composition of the network during the intervening period. Nevertheless, there is a risk that a regional office may have made certain alternations to the network without the SOC being aware of these alterations. By installing a network sensor at a water structure, the SOC can ensure that it has constant access to up-to-date information on the status of the network.

5.2.3 Very little known about cascade effects

If a crisis in a critical sector affects other critical sectors such as transport or energy, this is known as a ‘cascade effect’. The National Coordinator for Security and Counterterrorism takes a particular interest in these interdependencies, and is currently looking at ‘chain dependencies’ between multiple critical sectors, for example, as part of a joint study with the Netherlands Organisation for Applied Scientific Research. The parties involved in the chain can use this type of information to reach agreements with each other so as to facilitate a rapid response to an actual or imminent crisis. Our audit team did not find any document at the head office of the Directorate-General for Public Works and Water Management with information on the possible cascade effects exerted either on or by the sea defences and water management sector.

There is currently a cooperation agreement in force between the SOC and the district water boards, enabling the SOC to respond quickly to incidents that are capable of having certain effects on the sector (but only within the sector). Staff from the water boards work at the SOC on a day-to-day basis, thus enabling information to be shared on security incidents and the responses to such incidents.

In addition, the Minister of Infrastructure and Water Management endorsed a number of additional plans supplementing the 2011 Administrative Agreement on Water Affairs on 31 October 2018 (Association of Regional Water Authorities, Association of Provincial Authorities, Vewin (association of Dutch water companies), Ministry of Infrastructure and Water Management, Association of Dutch Local Authorities, 2018). One of these additional plans involves performing a sector-wide dependency and vulnerability test for cyber security in 2020, so as to identify any chain interdependencies.

5.3 Pen tests at the Directorate-General for Public Works and Water Management

A penetration test ('pen test' for short) is an authorised attempt undertaken by an organisation to circumvent or break through its own security system. It gives the target organisation a good idea of the system's effectiveness and the potential security risks pertaining to it, and enables it to identify any areas in which improvements need to be made (GOVCERT, 2010). The Directorate-General for Public Works and Water Management can use pen tests to test the practical effectiveness of cyber security measures taken in relation to critical water structures and to improve them where necessary. Such tests are a valuable tool that could help the Directorate-General to prepare for any cyber attacks.

In practice, the Directorate-General does not perform any significant pen testing on its industrial IT systems. The Directorate-General claims that the specialist software that is required in order to perform such tests is intended for 'standard' IT systems and not for industrial IT systems. The Directorate-General admitted that it did not know much about the pen testing of industrial IT systems. Moreover, only a relatively small percentage of water structures have a test environment. Full pen tests cannot be performed on critical water structures while they are in operation as this would be too risky.

A practical example raised on a number of occasions during our contacts with staff from the Directorate-General shows that these risks are by no means hypothetical. During the course of a test, a laptop computer was connected to a water structure that was in operation at the time, in a manner that was in accordance with the procedure described in the documentation. This led to a malfunction in the water structure, which staff were no longer able to control. Fortunately, the emergency switch was still working, so that staff could regain control of the structure. It is not inconceivable, however, that this incident might have led to physical accidents or damaged the structure in question.

Under the ‘baseline for information security in the civil service’ (BIR), government organisations are supposed to subject their IT systems to regular pen tests. The Directorate-General for Public Works and Water Management has transposed the BIR into its own set of guidelines for its industrial IT systems (known as the ‘cyber security implementation guidelines for structures managed by the Directorate-General for Public Works and Water Management’ (CSIR); see section 3.4). In doing so, it has made the obligation to perform pen tests dependent on the limitations of the systems in question, which means in practical terms that they are optional. What the Directorate-General does, and has done as part of the IMPAKT programme, may be described as ‘vulnerability scans’. These involve exposing potential points of entry into a system, without these actually being used to gain entry to the system. The fact that the Directorate-General does not perform any pen tests means that it does not have any information on the ability of critical water structures to resist cyber attacks in practice.

5.4 Conclusions

This chapter discusses the audit questions about the preparations made by the Directorate-General for Public Works and Water Management for dealing with cyber security incidents and crises, and the way in which it responds to such incidents and crises. We found that the Directorate-General has not formulated a scenario specifically for cyber security as part of its crisis management model, even though it has formulated scenarios for many other situations. We also found that certain vital crisis documents were either outdated or inaccurate and that there was no procedure for updating these on a regular basis. This means that, in the event of a crisis, the Directorate-General cannot assume that the information available to it is full, up to date and reliable. Finally, we found that the Directorate-General does not subject its industrial IT systems to regular pen testing, which means that it fails to observe the instructions given in the ‘baseline for information security in the civil service’ (BIR).

In terms of the preparations made by the Directorate-General for dealing with cyber crises, we found there were problems in two areas.

Organisation

At the time of our audit, the Directorate-General had not adopted a procedure for regularly updating the crisis maps and network reports in consultation with the regional offices.

Expertise and staffing

The Directorate-General does not have enough expertise to perform pen tests on the IT systems used for critical water structures, in accordance with the ‘baseline for information security in the civil service’ (BIR). Without such pen tests, the Directorate-General cannot assess the practical effectiveness of the cyber security measures taken in respect of its water structures.

6 Conclusions and recommendations

Our audit team examined one of the country's critical sectors, i.e. sea defences and water management, and the critical water structures in particular. Political responsibility for this sector is vested in the Minister of Infrastructure and Water Management. The critical water structures are managed by the Directorate-General for Public Works and Water Management. The Minister of Infrastructure and Water Management is accountable for the action taken by the Directorate-General to enhance the cyber security of the critical water structures. The relevant objectives must be achieved with the aid of the currently available manpower and resources.

Previous chapters have shown, starting from the audit questions, the nature of the action taken by the Directorate-General to protect the country's sea and river defences from cyber threats and how effective this action is in practice. We also examined how the Directorate-General responds to cyber security incidents and cyber crises. We explained that the IT systems used by the critical water structures were designed at a time when no one had heard of cyber security. As the IT systems themselves have grown more and more interconnected with other systems both within and beyond the Directorate-General, so they have become more vulnerable to a cyber attack. The Directorate-General has to use conventional tools to counter an age-old threat, i.e. water, at a time when the same tools are faced by new threats of the modern age. This is the nature of challenge now facing the Directorate-General.

Supporting audit findings

As part of our audit, a team of external testers assessed the IT systems used by one of the critical water structures we had selected. Their test demonstrated the vulnerability of these structures by modern standards.

The strategy adopted by the Directorate-General is geared mainly towards detecting and responding to cyber attacks. This is because the specific characteristics of industrial IT systems mean that it would be both expensive and technically complex to try and prevent all such attacks. Our main conclusion is that, while the Directorate-General has done well since 2014 in making up for lost ground, it has nonetheless not succeeded in achieving its own security objectives.

This chapter sets out the secondary findings supporting the above conclusion. These are followed by our recommendations.

6.1 Information on the level of threat

At the time of our audit, we were unable to identify the precise level of threat of a cyber attack directed against the sea defences and water management sector. However, this information is vitally important in order to assess whether the right action has been taken. Such information also helps to decide how the appropriate action should be resourced, in terms of both staffing and funding. The same applies to the level of expertise required, and to the intensity of staff screening procedures. We found that the absence of this information leads in practice to a degree of uncertainty surrounding these aspects. For this reason, our first recommendation to the Minister of Infrastructure and Water Management is as follows:

1. Identify the actual current level of cyber security threat to critical water structures in order to pave the way for further decisions on the allocation of staffing and resources.

6.2 Completion of the Security Programme

The Security Programme for the Directorate-General for Public Works and Water Management has helped the Directorate-General to make up for lost ground in terms of the cyber security of critical water structures. We found that, following the completion of the Security Programme, many of the proposed measures had been adopted. Responsibility for the implementation of the remaining measures had been transferred to the regional offices responsible for managing the objects. There is no comprehensive, up-to-date list of the action taken by the regional offices to address the outstanding measures. The Directorate-General has adopted a tool known as ‘functional inspections and tests’ (FIT) to ensure that lasting lessons can be learned from the Security Programme. However, we found that the Directorate-General had not yet met the targets set for the use of the tool.

The Central Information Services department (CIV) has no powers to compel the regional offices to implement the remaining measures and to make use of the FIT tool. Although the management board does have such powers, it has not used them to date. The question of the funding of the remaining measures and the FIT tool has led to internal disputes, which have caused delays in decision-making and in the implementation of measures.

Supporting audit findings

We found that work had been completed on the majority of the measures relating to the critical water structures covered by this audit. In the case of one particular water structure, an important measure had yet to be put in place. As no more funding was available once the Security Programme had been completed, it remained unclear for a long time who would have to take responsibility for adopting the measure. At another critical water structure, the staff of a regional office did not know about any documents for formally transferring responsibility for the implementation of the remaining measures to the office in question.

We make the following recommendations to the Minister:

2. Instruct the Directorate-General for Public Works and Water Management to keep a uniform, centralised record of the action taken to implement the remaining measures delegated to the regional offices, and also to ensure that the remaining measures are indeed implemented in practice.
3. In addition and where necessary, improve the tools created in order to continue on the route mapped out by the Security Programme (including FIT inspections), by allocating sufficient staffing and resources.

6.3 Completion of the detection and response strategy

The main task of the Security Operations Centre (SOC) is to detect and respond to cyber attacks. In order to instantly detect cyber attacks directed against water structures designated by the Minister as ‘critical’, the Minister decided to adopt a number of measures specifically for the critical water structures. The aim was for all these measures to be in place by the end of 2017. This aim has not been achieved: the situation in the autumn of 2018 was that instant detection was possible in the case of slightly less than half of all critical water structures. This means that there is a risk of the Directorate-General failing to detect a cyber attack directed at a critical water structure, or of detecting such an attack too late.

Supporting audit findings

A test performed at one of the critical water structures included in our audit showed that it was possible to gain physical access to the structure. The SOC identified an attempt to gain digital access (by connecting a laptop computer to the network). Measures have been put in place at this particular water structure to instantly detect a cyber attack. In the case of another critical water structure included in our audit, we found that these detection measures had not yet been taken. This means that there is a risk of the Directorate-General failing to detect a cyber attack or of detecting such an attack too late.

The SOC says that it uses its available resources largely to analyse reports of potential cyber attacks. As a result, no resources are available for further refining the detection measures and for sharing information. As long as no information is available on the level of threat posed to the sector, it is difficult to decide on the appropriate level of investment in expertise and staff capacity.
We also found that the issue of a certificate of good conduct is the only form of screening to which SOC staff are subjected. It is unclear whether this is adequate for staff required to work with sensitive information on cyber threats.

In order to finalise and, where necessary, further professionalise the measures for detecting cyber attacks directed against critical water structures, we urge the Minister to:

4. Complete the adoption of measures enabling the instant detection of cyber attacks and expand the SOC's monitoring activities (based on an objective assessment of the level of threat; see the first recommendation).
5. Review the level of screening that SOC staff are required to undergo and the classification of sensitive SOC reports (based on an objective assessment of the level of threat; see the first recommendation).

6.4 Up-to-date crisis documents and full pen tests

The Directorate-General for Public Works and Water Management uses a crisis model to prepare for a wide range of crises, including cyber crises. This model includes a number of specific crisis scenarios. We found, however, that no scenario had been constructed specifically for a crisis caused by a cyber attack. Moreover, no information was available at head office on the cascade effects caused by a cyber attack on the critical water structures.
We also found that certain important documents relating to the response to a cyber attack (i.e. crisis maps and network reports) were not kept up to date. This means that there is a risk that the response to a cyber crisis may be neither sufficiently rapid nor sufficiently effective.

The Directorate-General performs very few pen tests on its critical water structures to prepare for cyber attacks. This means that the organisation does not have access to information on the ability of critical water structures to resists cyber attacks in practice.

Our recommendations to the Minister are as follows:

6. Instruct the Directorate-General for Public Works and Water Management to design and implement a procedure for ensuring that the information on crisis maps and network reports is kept up to date.
7. Instruct the Directorate-General to ensure that the crisis model includes a crisis scenario specifically devised for cyber security crises.
8. Identify the risks preventing the Directorate-General from performing full pen tests on the industrial IT systems of critical water structures and use this information to map a route leading to a situation in which pen tests form an integral part of cyber security measures relating to critical water structures.

7 Minister’s response and Court of Audit afterword

The Minister of Infrastructure and Water Management responded to our report on 5 March 2019. A summary of her response follows below. The full text is available on our website (www.rekenkamer.nl; in Dutch only). The chapter concludes with our own afterword.

7.1 Response of the Minister of Infrastructure and Water Management

In her response, the Minister of Infrastructure and Water Management (referred to in the remainder of this section as ‘the Minister’) writes that she agrees with our conclusions and views herself as being responsible for the digital security of the country’s water structures. The Minister regards our conclusions and recommendations as underpinning the action she has already taken to further improve the cyber security of the water sector. She says that the recently completed ministry-wide cyber security strategy will help her to make the right choices in this respect.

The Minister says she is planning to act on all our recommendations. For example, she is planning to ensure that the overall threat assessments and the additional information obtained from interdepartmental cooperation are translated into the potential consequences for individual critical structures (the first recommendation).
The Minister believes that the outcomes of these threat assessments will guide the implementation of many of our other recommendations. For example, the Minister is planning to take the level of threat as the basis on which to prioritise the remaining Security Programme measures, and also to use it as a starting point for the possible strengthening of the FIT programme, thereby ensuring that the Security Programme has a lasting effect (the second and third recommendations). The Minister also writes that the structure-related threat information will be incorporated in the decision-making process on the setting of criteria and the requisite allocation of manpower and resources (the fourth recommendation).
Finally, the Minister is planning to look into the possibilities, again based on the level of threat and in consultation with the National Coordinator for Security and Counter-terrorism, for a more appropriate form of staff screening (the fifth recommendation).
The Minister also writes that she will be adopting our recommendations on the response to cyber attacks (the sixth and seventh recommendations). The terms of the Administrative Agreement on Water Affairs signed last October take account of the need for information on the cascade effects. In order to gain a broader impression of the cascade effects, the Minister writes that the Ministry of Infrastructure and Water Management will be

adopting the strategy of intersectoral interdependencies pursued by the Ministry of Justice and Security. The Minister is also planning to investigate, in accordance with our recommendation, the risks and opportunities for conducting pen tests on existing systems (the eighth recommendation).

In her response, the Minister also says that the Directorate-General for Public Works and Water Management has already made up a lot of lost ground in terms of implementing the remaining measures in the Security Programme. The Minister claims that a comprehensive list has now been drawn up of the measures that still need to be taken in order to meet the target set in the Security Programme.

7.2 Court of Audit afterword

The Minister accepts our finding that further action needs to be taken in relation to the cyber security of the country's critical water structures. These are needed first of all in order to meet the targets set by the Minister herself and in the second place to ensure that the level of cyber security is commensurate with the current level of threat (once the latter has been assessed).

At the same time, in order to implement our recommendations, the Minister must first act on the first of these, i.e. identify the level of threat. Although this sounds logical, we would like to point out to the Minister that it is also important to ensure that certain measures that should have been taken some time ago are taken in the near future. This applies, for example, to the issue of connecting the critical water structures to the SOC, so as to generate more detailed and more up-to-date information on the structures in question. This work should have been completed by the end of 2017 and does not therefore depend on the implementation of the first recommendation.

The Minister refers in her response to the recently adopted ministry-wide cyber security strategy, the contents of which were not available at the time of our audit. We will closely monitor the progress made with the aid of this strategy, as we will the implementation of the measures the Minister has promised to take.

Appendix 1 Audit methods

This report seeks to answer the following audit questions:

1. What tools are available to the Directorate-General for Public Works and Water Management as the manager of the water structures, for detecting cyber threats and attacks and protecting itself against cyber threats to the flood defences?
2. Are the tools for detecting cyber threats and attacks effective? Do they offer sufficient protection?
3. What scenarios have been devised for a situation in which a cyber attack takes place? What action can the Directorate-General for Public Works and Water Management take in order to prevent any cascade effects, i.e. to prevent other critical sectors from being affected by the same attack?
4. How does the Directorate-General for Public Works and Water Management respond when vulnerabilities and incidents are detected?

In order to answer the audit questions, we studied various internal documents drawn up by the Directorate-General for Public Works and Water Management and the Ministry of Infrastructure and Water Management. These documents included, apart from policy papers and memoranda, specific information relating to the visits made as part of the IMPAKT programme (i.e. the scores awarded to each structure against the predefined assessment criteria; a description of the vulnerabilities detected at selected structures; the measures formulated to address these vulnerabilities; and the status of the various measures on the date when the Security Programme came to an end).
We also interviewed members of staff from the Directorate-General for Public Works and Water Management (both from Central Information Services and from the regions where we visited water structures) and from the Ministry of Infrastructure and Water Management. We also spoke with a number of other stakeholders, i.e. the National Coordinator for Security and Counterterrorism, the NCSC, the Association of Regional Water Authorities and the Water Management Centre. We also interviewed a number of cyber security experts, notably on the question of how to test the effectiveness of measures.

The second audit question, viz. about the effectiveness of cyber security measures, formed the focal point of our visits to a number of selected critical water structures. The IMPAKT inspections and the measures taken as a result of these inspections provided a framework for our visits. We then looked at how the measures in question worked in practice. In the case of one of the critical water structures we audited, we did so by performing a routine test. At another critical water structure, we assessed the effectiveness of the measures with the aid a pen test that we had devised in collaboration with the Directorate-General for Public Works and Water Management.

We ourselves selected the structures we wished to visit, in close consultation with the staff responsible for managing them. The criteria we used in selecting the structures were as follows:

- the structure must appear on the list of critical structures;
- a mix of structures, some of which had adopted measures for instant detection and others of which had not;
- the age of the structure;
- possible cascade effects caused by the failure of the structure.

We found that no water structure had been affected by a cyber security incident to date. For this reason, it was not possible to reconstruct the response to such an incident, as we had hoped to do. We nonetheless did our best to obtain the information we wanted by studying the results of past exercises (affecting the critical water structures included in our audit) as well as the results of the pen test we performed at one of the critical water structures in conjunction with the Directorate-General for Public Works and Water Management and an external party.

Appendix 2 Audit criteria

The Minister of Infrastructure and Water Management is responsible for the cyber security of the country's critical sea defences and water management sector and, as part of this sector, for those water structures she has designated as being 'critical'. One of the aspects of this responsibility involves reporting any security incidents (for which the Minister has set a threshold value). The Directorate-General for Public Works and Water Management manages the structures the Minister has designated as 'critical water structures' and is the contracting authority for the necessary cyber security measures.

One of the key issues in our audit was our general criterion for ministerial responsibility and efficiency, i.e. if a third party collects, manages or spends public money and/or performs a public task, the responsible minister must ensure at all times, by exercising effective supervision, that the third party in question acts both lawfully and efficiently. The Minister of Infrastructure and Water Management must at all times be able to report (to the Lower House of the Dutch parliament) on the measures that the Directorate-General for Public Works and Water Management has taken in the past, and is planning to take in the future, in order to enhance the cyber security of water structures. In order to do so, the Minister has to know what action the Directorate-General has taken and what effect this action has had. The objectives must be achieved with the manpower and other resources that are already available. We would expect the Minister of Infrastructure and Water Management to have consulted the Directorate-General in order to determine whether her policy plans are feasible (and the deadlines realistic) and enforceable, and whether the action taken will have the desired effect.

Alongside this general criterion, our audit also made use principally of criteria based on the objectives set by the Minister and the Directorate-General for ensuring that the cyber security of the country's critical water structures is up to standard. One of these objectives, for example, states that all measures formulated as a result of the Security Programme for the Directorate-General for Public Works and Water Management (known as the 'Security Programme' for short) should be applied to existing vulnerabilities (and that, if not, a conscious and well-founded decision should have been taken to accept the risk in question). After all, a failure to adopt the measure in question (or else an acceptance of the risk) implies that the structure in question remains vulnerable to cyber threats. This objective, and the resultant criterion, are particularly relevant to our first sub-conclusion.

Another objective, again resulting from the Security Programme, is to take measures facilitating the instant detection of cyber attacks directed against all water structures designated as ‘critical’ by the Minister of Infrastructure and Water Management (and to do so by the end of 2017). We linked this criterion in particular to our second sub-conclusion. We also included a criterion relating to the availability of the right people (in terms of quality, screening, responsibilities and multi-deployability) for the purpose of detection and response (based on ISO standard 27002).

Finally, the criteria applied in relation to our third sub-conclusion related to the availability, completeness, reliability and up-to-dateness of standards, procedures, plans and tests for such aspects as incident and crisis management. In working on this sub-conclusion, we also took account of criteria and guidelines for industrial IT systems, as developed by the Directorate-General for Public Works and Water Management. We found that, in translating the ‘baseline for information security in the civil service’ (BIR) into its own baseline standards for industrial IT systems, the Directorate-General had reformulated certain requirements in the BIR as optional guidelines. This applied to the performance of pen tests. The Directorate-General took this decision in the light of the characteristics (and age) of its systems.

Appendix 3 Key to abbreviations and technical terms

Asset management
Asset management is a wide-ranging term. In the context of this audit, it is about managing software, software updates, and maintenance and breakdown processes, and working together with contractors and subcontractors on critical water structures.

BIR
Baseline for information security in the civil service: a system of general security measures that applies to all information and data systems used by the civil service.

Security Programme
Security Programme for the Directorate-General for Public Works and Water Management: a programme covering a wide range of aspects, including cyber security at the Directorate-General.

CIV
Central Information Services department.

CSIR
Cyber security implementation guidelines for structures managed by the Directorate-General for Public Works and Water Management.

FIT
Functional inspections and tests. A FIT inspection is an inspection of critical components of structures and includes an assessment of cyber security.

IMPAKT
Impulse programme for tackling the critical technical infrastructure. This was a sub-project of the Security Programme. It involved (inter alia) defining cyber security measures and putting them into effect at water structures managed by the Directorate-General for Public Works and Water Management.

NCSC
National Cyber Security Centre.

Pen test
Short for ‘penetration test’, in which an organisation tests the practical effectiveness of its digital security by getting a team of ethical hackers to hack into its own IT systems.

Ransomware
A type of malicious software that is designed to block access to an IT system. The victim can regain access to the system only by making a payment.

SOC
Security Operations Centre.

Social engineering
Method used by hackers, including ethical hackers, in which the latter seek to gain access to IT systems by misleading users. This may involve, for example, manipulating users to divulge their passwords.

Stand-alone
Separate, i.e. operating independently of any external hardware or software.

Appendix 4 Bibliography

Publications

Agence nationale de la sécurité des systèmes d'information (2012). *Managing Cyber security for Industrial Control Systems*. Paris: own publication.

Netherlands Court of Audit (2011). *Rapport bij het Jaarverslag 2010 Ministerie van Infrastructuur en Milieu* ('Audit report on the 2010 annual report of the Ministry of Infrastructure and Water Management'). The Hague: own publication.

Netherlands Court of Audit (2012). *Rapport bij het Jaarverslag 2011 Ministerie van Infrastructuur en Milieu* ('Audit report on the 2011 annual report of the Ministry of Infrastructure and Water Management'). The Hague: own publication.

Netherlands Court of Audit (2013). *Rapport bij het Jaarverslag 2012 Ministerie van Infrastructuur en Milieu* ('Audit report on the 2012 annual report of the Ministry of Infrastructure and Water Management'). The Hague: own publication.

Netherlands Court of Audit (2014). *Rapport bij het Jaarverslag 2013 Ministerie van Infrastructuur en Milieu* ('Audit report on the 2013 annual report of the Ministry of Infrastructure and Water Management'). The Hague: own publication.

Netherlands Court of Audit (2015). *Rapport bij het Jaarverslag 2014 Ministerie van Infrastructuur en Milieu* ('Audit report on the 2014 annual report of the Ministry of Infrastructure and Water Management'). The Hague: own publication.

Netherlands Court of Audit (2016). *Rapport bij het Jaarverslag 2015 Ministerie van Infrastructuur en Milieu* ('Audit report on the 2015 annual report of the Ministry of Infrastructure and Water Management'). The Hague: own publication.

[-][14]

GOVCERT (2010). *Pentesten doe je zo*. The Hague: own publication.

NCSC (2016). *Uw ICS/SCADA- en gebouwbeheersystemen online*. The Hague: own publication.

National Coordinator for Security and Counterterrorism (2018). *Nederlandse Cyber security Agenda, Nederland digitaal veilig*. The Hague: own publication.

National Coordinator for Security and Counterterrorism (2018). *Cyber securitybeeld Nederland 2018*. The Hague: own publication.

Civil Service (2017). *Vertrouwen in de toekomst: Regeerakkoord 2017–2021*. The Hague: own publication.

Association of Regional Water Authorities, Association of Provincial Authorities, Vewin (association of Dutch water companies), Ministry of Infrastructure and Water Management, Association of Dutch Local Authorities (2018). *Aanvullende Afspraken Bestuursakkoord Water*. The Hague: own publication.

Ministry of Security and Justice (2105). *Brief aan de Tweede Kamer van de Minister of Security and Justice d.d. 12 mei 2015, over herziening van de Strategie Nationale Veiligheid, herijking vitale infrastructuur en verbetering crisisbeheersing* ('Letter of 12 May 2015 from the Minister of Security and Justice to the Dutch House of Representatives, on a review of the National Security Strategy, a recalibration of critical infrastructure and the improvement of crisis management'). House of Representatives, 2014-2015 session, 30821, no. 23.

Legislation

Cyber Security (Duty to Report Incidents) Decree. Decree of 4 December 2017 designating suppliers, products and services obliged to report serious IT-related incidents.[15]

Network and IT Systems (Security) Decree. Decree of 30 October 2018 regulating the enforcement of the Network and IT Systems (Security) Act.

Decree issued by the Minister van Infrastructure and Water Management on 21 December 2017 (ref. RWS-2017/49666) designating critical water structures or parts thereof, in connection with the entry into force of the Cyber Security (Duty to Report Incidents) Decree.

Civil Service Data Security Regulations Decree 2007, Special information 2013 (VIRBI 2013). Decree of the Prime Minister, Minister of General Affairs, of 1 June 2013, no. 3124134, containing Civil Service Data Security Regulations 2007, Special information 2013.

Government Accounts Act 2016. Act of 22 March 2017 regulating the management of, the distribution of information on, the auditing of and the reporting on central government finances, on the management of public liquid assets held outside the Kingdom, and on the supervision of the management of public liquid assets and public financial assets held outside the Kingdom.

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Network and IT Systems (Security) Act. Act of 17 October 2018 regulating the implementation of Directive (EU) 2016/1148.[16]

Data Processing and Cyber Security (Duty to Report Incidents) Act. Act of 25 July 2017 regulating the processing of data to enhance security and the integrity of electronic data systems that are critical to Dutch society, and imposing a duty to report serious incidents.[17]

Appendix 5 Endnotes

1 ICT (information and communication technology) and IT (information technology) are more or less interchangeable terms. We have decided to use the latter in this report.

2 Cyber security was one of the aspects of covered by the audit guidelines. We also examined other aspects closely related to cyber security. These are discussed in detail in section 3.3 of the report.

3 Strictly speaking, damage caused to a computer as a result of a lightning strike or an instance in which data is deleted by mistake are also examples of cyber security risks. This audit concentrates, however, on those threats emanating from deliberate human behaviour. It is worth bearing in mind that the Directorate-General for Public Works and Water Management does not necessarily need to be deliberated targeted in a cyber attack and that such an attack may also involve 'innocent' third parties. For example, a computer virus may have been written to infect computers at random and may be spread unwittingly by an official at the Directorate-General who is himself or herself acting in good faith.

4 This is Directive (EU) 2016/1148, better known as the NIS Directive (Network and Information Systems Directive).

5 Please note that the (as yet unpublished) decree that we inspected still refers to the Data Processing and Cyber Security (Duty to Report Incidents) Act, which has now been repealed but is yet to be superseded by a new version.

6 This formed the topic of an item on a current affairs programme on Dutch TV: https://eenvandaag.avrotros.nl/item/sluizen-gemalen-en-bruggen-slecht-beveiligd/ It should be borne in mind that the picture painted in the report, which concerned industrial IT systems with a direct connection to the internet, does not apply to the water structures managed by the Directorate-General for Public Works and Water Management. This is, however, the implication in the report, which contains images of the Maeslandt and Eastern Scheldt sea defences.

7 The NCSC document refers to ICS/SCADA. This is an example of jargon that we have sought to avoid in this report. In practice, the term is synonymous with 'industrial IT systems'.

8 See for example: https://www.computable.nl/artikel/ict_topics/security/3814774/1276896/softwarefout-veroorzaakte-ongeluk-ketelbrug.html The incident at an important motorway bridge in the centre of the country illustrates the importance of efficient industrial IT systems and the knowledge gap affecting the organisations that deal with them.

9 See endnote 6.

10 The term 'shortcoming' is used by us to refer to a situation in which a ministry's operational management is either poorly planned or poorly executed. In order to qualify as a shortcoming, a problem identified by us must be more than just an incident and must be of some financial significance.

11 This ministry underwent a change of name and is now called the Ministry of Infrastructure and Water Management. For the sake of clarity, this is the name used in the rest of this report, even where we are writing about a point in time in which the ministry was still using its former name.

12 In addition to water structures forming part of the main water system, this also concerned structures in the main waterway system and the road network.

13 The examples are intended merely as illustrations for the reader. They have not been reproduced verbatim; jargon and technical details have been removed.

14 The draft version of the report contained a reference here to the report on the vulnerability test on the Alpha structure. This reference named the party responsible for performing the test. This is confidential information that has been removed from the final version of the report.

15 Repealed on 9 November 2018.

16 For a long time, this act was referred to under its original short title, i.e. the Cyber Security Act.

17 Repealed on 9 November 2018.

Information

Netherlands Court of Audit
Communication Department
P.O. Box 20015
2500 EA The Hague
The Netherlands
+31 70 342 44 00
voorlichting@rekenkamer.nl
www.courtofaudit.nl

Cover

Design: Corps Ontwerpers
Photo: HH/EyeEm Mobile GmbH

Translation

Tony Parr Business Translation

The Hague, March 2019