National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

Nationwide Crisis Response Plan for Digital Crises

Cover image: IJtunnel Amsterdam

Critical and non-critical processes are highly dependent on digital networks and systems. Outages and disruptions will directly impact our society. The control room has a key role in both preparation and response to an incident and (potential) crises.

Contents

Allowed distribution TLP: WHITE
(Traffic Light Protocol)

This document is labeled TLP: WHITE. The NCTV uses the Traffic Light Protocol to unambiguously define how information may be distributed. A TLP label indicates the applicable sharing boundaries. More information about the TLP standard can be found on the Forum of Incident Response and Security Teams: www.first.org/tlp.

This is a publically accessible document. Recipients may share the information in this document within and outside their organisation.

For questions and feedback please contact info@nctv.minjenv.nl.

Foreword

The importance of digital systems to our society cannot be overstated. Whether in relation to living, working, travel, payment or face-to-face interaction: our lives are enabled through a digital infrastructure. This infrastructure provides an ocean of opportunities and possibilities, but not without risks. After all, a crisis in the digital domain will not be limited to the universe of bits and bytes but will very rapidly become visible and palpable in the real world. Society could be disrupted within a short period of time.

Digital threats are now a permanent challenge to our national security. As the Cyber Security Assessment Netherlands 2022 shows, there is an asymmetry between the increasing digital threat landscape and the development of our resilience. This asymmetry increases the risk of disruption. Even if the gap between our resilience and these threats is reduced, it should be noted that there is no such thing as 100% security. Digital processes can always fail due to technical or human errors. The increasing activities of state actors and criminal organisations in the digital domain add another layer of uncertainty.

In practice, we are observing successive cyber attacks and incidents, with increasingly significant consequences. Noted examples include the Citrix incident, which forced the Medical Center Leeuwarden and the Central Government to take far-reaching measures, the attack on the North and East Gelderland Security Region, where cyber criminals were able to hack into and shut down key systems using ransomware, and the vulnerability in Apache Log4J, which exposed and alerted our crisis management structures to supply chain dependencies. These are examples of digital incidents that (could) have had an impact on the physical domain. Luckily, the effects – however much of a nuisance to those involved – were relatively limited. However, what would happen if cyber incidents like these were to seriously disrupt society and lead to major societal unrest? In light of such a threat, a well-organised crisis management approach is a prerequisite to providing an adequate response.

The National Cybersecurity Strategy 2022-2028 emphasises the importance of rapid and adequate response to cyber incidents and crises. Efficient cooperation between government agencies, the private sector, the scientific community and civil society is crucial to any such approach – including across local, regional and national domains. The Nationwide Crisis Response Plan for Digital Crises provides a framework for an organised response to cyber incidents and crises. Our national plan contains a great deal of information about crisis management in the digital domain, including the link to physical impact management at both the national and regional level. All of this is useful for the translation of our national digital crisis approach to the more operational crisis management documents in use with individual organisations.

Effective crisis management requires practice in addition to joint preparation. The flexibility of the building-blocks method in this plan provides an opportunity for you to create crisis scenarios appropriate for your organisation, which will allow you tokick-start this process. The Nationwide Crisis Response Plan for Digital Crises constitutes an excellent foundation for the development of individual plans and exercises. We kindly invite you to use it for these purposes and thus contribute to a digitally secure nation.

We are proud that the Nationwide Crisis Response Plan for Digital Crises was realised in close collaboration between the Central Government and the Security Regions, alongside private partners. After all, in a rapidly changing digital landscape, safeguarding our national security is a shared and joint responsibility.

Pieter-Jaap Aalbersberg
National Coordinator for Counterterrorism and Security

Gerhard van den Top
Mayor Hilversum, Cyber portfolio holder on behalf of the Security Regions Council

National Coordinator for Counterterrorism and Security
Ministry of Justice and Security

Veiligheids beraad

The sluice complex in Lelystad plays an important part in water distribution from the IJsselmeer.

1. Introduction

Present-day society has become largely dependent on digital technology. The Cyber Security Assessment Netherlands (CSAN) (Cybersecuritybeeld Nederland, CSBN) provides annual insight into digital threats, potential harm to various interests, the state of our resilience and, finally, the risks to cyber security in the Netherlands. The increasing threat, as outlined in several editions of the CSAN, demonstrates the importance of thorough preparation for digital crises causing societal disruption.

Our dependence on digitised processes and systems is so great that any harm to either of these has the potential to lead to societal disruption. Both critical and non-critical processes are highly dependent on network and information systems. The failure and disruption of these systems, or of key digital processes within the cooperating supply chains, will very rapidly affect a number of critical processes – likely within hours.

Objective

The Nationwide Crisis Response Plan for Digital Crises (Hereafter; NCRP-Digital) (*Landelijk Crisisplan Digitaal, LCP-Digitaal*) is a set of guidelines aimed at providing insight and clarity regarding the existing agreements and legislation concerning the management of digital incidents and (potential) crises at a national level.[1] The plan sets out the joint approach to a digital crisis at a national level, as well as the cooperation and alignment with the relevant crisis response partners in the public and private sectors and cooperation with networks at an international level. The plan is therefore a cyber-specific elaboration of the generic approach to crises, outlined in the Decree establishing the Ministerial Crisis Management Committee and the National Crisis Management Handbook (only available in Dutch).

The most significant added value of the NCRP-Digital is in the preparatory phase. This plan is the overarching framework for the individual operational plans and documents of the various actors and organisations involved in digital crisis management. The NCRP-Digital does not supersede or otherwise supplant these plans. The operational plans and documents of the actors and organisations involved in digital crisis management must, however, where applicable, be aligned with the NCRP-Digital.

The information set out in this plan answers the following questions:

- Which organisations are and could be involved in a(n) (imminent) large-scale cyber crisis, and what are the responsibilities of the various parties?
- How does information dissemination take place in a cyber crisis, and how are functional (cyber specific) and generic crisis management structures linked?
- What are the principal distinctive elements or building blocks within cyber crisis management?
- Which specific dilemmas and key decisions are relevant to decision makers during a(n) (imminent) large-scale cyber crisis?

1. Incidents can be considered a crisis or potential crisis as soon as they have a significant impact. According to the Network and Information Systems Security Act (Wet beveiliging netwerk- en informatiesystemen, Wbni), an incident relates to any event with an actual harmful effect on the security of network and information systems.

Target groups

The target groups of this plan are the actors and organisations within or directly linked with the scaled-up national, local and regional crisis response structure that play a role in managing (potential) digital crises. This includes employees, CISOs, managers and administrators of all actors and organisations that may play a role within activated national, local and regional crisis management structures. These actors and organisations include the relevant ministries and organisations that operate within the digital sphere, such as the National Cyber Security Centre, the CIO system, the intelligence and security services, the police and the Public Prosecution Service. The plan is equally intended for local and regional authorities, such as the security regions, water authorities and the municipal CISO organisation. In addition, it is intended for institutions in, for example, the health care and education sectors and for private sector partners in order to align their own preparations and planning accordingly.

Adoption and implementation procedure

- In addition to a version intended for public disclosure, the NCRP-Digital also has a version classified as TLP: Amber. This means that this publication is intended for organisations involved in cyber crisis management and that the information may only be distributed within the organisation on a need-to-know basis.
- The National Crisis Management Directors' Committee (*Rijksbrede Directeurenoverleg Crisisbeheersing*, DOCB), in which the Security Regions and providers of critical processes are likewise represented, is the official commissioning party of the NCRP-Digital.
- The NCRP-Digital was drawn up by a drafting group consisting of representatives of the National Coordinator for Security and Counterterrorism, the National Cyber Security Centre, the National Crisis Centre, and the security regions, in close consultation with the Ministries of the Interior and Kingdom Relations, Foreign Affairs, Defence, Economic Affairs and Climate Policy, Finance, and Infrastructure and Water Management, the police, the General Intelligence and Security Service (AIVD) and the Public Prosecution Service. The NCRP-Digital was submitted for consultation to the Critical National Infrastructure Committee and the Public-Private Cyber Security Directors' Consultation Committee.
- The NCRP-Digital was coordinated with the Council of Commanders and Directors of the Security Regions (*Raad van Commandanten en Directeuren Veiligheidsregio*, RCDV) and with the Security Regions Council.
- At a national level, the NCRP-Digital was coordinated by the Crisis Management Directors' Committee(DOCB) and the Cyber Security Directors' Committee and was subsequently adopted in the Ministerial Committee for Defence, International, National and Economic Security and in the Council of Ministers.

Management cycle

The National Coordinator for Security and Counterterrorism and the security regions, represented by the Security Regions Council, are the owners of and are responsible for managing and updating the NCRP-Digital. Each year, in consultation with the relevant ministries, security regions and other relevant actors and organisations, the National Coordinator for Security and Counterterrorism will review whether the NCRP-Digital, or components thereof, requires an update.

The next (extensive) update of this plan is expected to follow the implementation of the systemic changes announced in the National Cyber Security Strategy (*Nederlandse Cybersecurity Strategie*, NLCS) and the associated action plan. Chapter 2, Summary, includes a brief overview into the future development of the cyber security system under the NLCS.

Use

- The NCRP-Digital is used for crisis preparation purposes.
- The NCRP-Digital is used as a basis for cyber crisis response exercises at regional and national level, such as ISIDOOR.
- The NCRP-Digital is used as a source of information during cyber crises.

The evaluations that are drawn up as a result of national and other exercises and crises are used as input for subsequent updates of the NCRP-Digital.

2. Summary

Scope

The domain to which this crisis response plan applies is defined as the 'digital sphere' in the 2019 National Security Strategy. This refers to the conglomerate of digital technology and services and includes permanent, temporary and local (digital) connections and data, with no geographical restrictions. All entities in society can be connected in the digital sphere.[2]

Within the digital sphere, the NCRP-Digital focuses on managing crises with significant societal impact related to the security of networks and information systems, and related cascading effects. The plan is applicable to crises where the (presumed) cause likewise lies in the digital sphere.

Various conceivable incidents could lead to an activation of the crisis structure as outlined in this plan. This may relate to both highly discernible situations characterised by a failure of networks and information systems with a significant societal impact and situations that are not visible to the outside world but may constitute a major (digital) threat.

The CSAN 2022 has identified four key risks to national security that may be relevant to an activation of the national crisis structure:

- Unauthorised access to information and data extraction (and possibly the publication of information and data), through espionage in particular. Examples include espionage targeting communications within the central government or the development of innovative technologies.
- Inaccessibility of processes, due to sabotage and/or the use of ransomware or preparations to this end. Examples include cyber infiltration in processes that ensure the distribution of electricity.
- Breaches of cyberspace and cyberspace security, such as through the abuse of global IT supply chains.
- Large-scale outage of digitised processes: a situation in which one or more processes are disrupted due to technical causes or as a result of unintentional human actions.[3]

If one or more of the above mentioned risks manifest themselves on a large scale or in key social (digital) processes and systems, this may impact national security interests.[4]

2. National Security Strategy 2019.
3. The CSAN 2022 also refers to natural causes. This type of cause does not necessarily have to lead to activation of the crisis structure under the National Digital Crisis Plan. The organisations described in this plan can play an active or advisory role in a scenario of this nature as well.
4. The national security interests as outlined in the National Security Strategy 2019 are: territorial security, physical security, economic security, ecological security, social and political stability and the international rule of law.

Regionaal risicoprofiel

In addition to nationally defined risks, the risks defined at a regional level are equally relevant to the NCRP-Digital. In accordance with the Security Regions Act (Section 15), the executives of a security region must determine a regional risk profile. The regional risk profile is an inventory and assessment of high-risk situations and the types of crises that may arise from these situations. The regional risk profile is revised at least[5] once every four years. The executives of the security region make strategic policy decisions on risk and crisis management . These objectives are defined in the policy plan of the security regions.

Part of the security regions' risk profiles focuses on cyber-related developments and risks. An increasing degree of social dependence on and interdependence of digital systems is designated as a significant risk. The risk profiles set out that a cyber crisis and/or digital disruption is a risk but that it may equally be attributed to a failure and/or disruption of ICT and telecommunications and/or voice and data communications. In addition, almost all security regions emphasise the risk of so-called cascade and supply chain effects.

Characteristics, risk assessment and impact

Crises in the digital domain differ from other types of crises in a number of ways:

- The speed with such crises manifest themselves. A digital crisis can arise instantly, or first develop akin to a peatmoor fire with a series of incidents, which collectively constitute or lead to a crisis. The same holds true for the recovery time following a disruption: it can either befrom extremely short or extremely long.
- Due to dependencies within the supply chain, a digital crisis can have an impact on several critical processes simultaneously. This can quickly lead to societal disruption – especially if the crisis persists for a longer period of time.
- Due to complex dependencies within the supply chain, the source of a digital crisis can sometimes be difficult to trace, complicating the crisis response. Due to interdependence among organisations involved in supply chains, incidents with suppliers or customers can lead to societal disruption. The critical interests of the Netherlands and its allies stand to be affected as a result of espionage in relation to confidential data and information, theft of such data (data extraction) or sabotage.
- The crisis management organisations themselves and their functioning may also be seriously impacted. Failure and limited availability of the ICT resources of crisis management organisations have a direct effect on response capacity, such as internal and external communications.
- In tackling the source of the crisis, the government partly depends on the actions of private sector parties, which means that close public-private partnerships are crucial. Virtually all digital infrastructure and digital services are in the hands of parties in the private sector.
- It can be a complex endeavour to determine where a particular incident has originated, who is responsible for a potential attack and ascertain what the potential objective of an attack is.. That is why the investigation services involved will assume malicious intent until it is proven that this is not the case. Both state and criminal actors operate within the digital sphere and can be responsible for a crisis.
- A crisis affecting the network and information systems rarely affects only the digital domain. In most cases, undesired effects will also occur in the physical domain.
- Networks and information systems will often transcend borders. It can be assumed that any crisis relating to network and information systems will be international in nature, with the cause of the crisis potentially being abroad, affecting several countries simultaneously. The origin of a crisis may also (partly) be in the Netherlands, but with the impact taking effect elsewhere.
- There is a shortage of specialised experts, particularly within the digital domain, who are able to take on source and impact control.
- The digital domain is cross-jurisdictional in nature, which means that the options available for enforcement and investigation at national level are limited, and international cooperation is required where appropriate.
- A crisis in the digital domain may be part of a hybrid conflict, which refers to a conflict taking place between states, involving integrated use of resources and actors with the aim of achieving specific strategic objectives.

The effects of a crisis in the digital domain can permeate all layers of society. This plan therefore focuses on an all-hazard approach to the societal consequences and impact of a crisis in the digital domain.

5. Section 14 in conjunction with Section 15 of the Security Regions Act.

Overarching issues

In any crisis in the digital domain, a distinction can be made between eight overarching issues, or 'building blocks'. The building blocks of a digital crisis are relevant to identifying the consequences and effects, to the organisation and approach of the crisis response and to the involvement of various actors and organisations. The following building blocks are always relevant to any digital crisis:

- whether the incident or crisis was intentional or unintentional;
- technical failure inside or outside the Netherlands;
- the involvement of a state or other actor;
- the impact on important (non-critical) social facilities and services;
- the impact on critical processes;
- cross-regional impact (including physical impact);
- the impact of the crisis abroad;
- the (un)availability a potential technical solution.

In a crisis situation, it will not always be possible to provide answers or to or gain certainty about any of these overarching issues. Identifying all or part of the building blocks during a crisis will, however, immediately contribute to insight into the necessary crisis management activities. In order to effectively understand the significance of the building blocks, it is vital that organisations not only refer them during a crisis but also principally use the building blocks to set up exercise scenarios and crisis response processes in line with national, local and regional crisis response structures and agreements. Chapter 4: Building blocks provides an extensive outline of each individual issue, with an overview of potential consequences and effects to each building block and an indication of the actors and organisations that could be involved in the response.

Digital crisis response in a nutshell

Digital crisis response or crisis management is typified by intensive collaboration between different sectors, networks and public and private actors. They can simultaneously be involved in the management of the digital and physical consequences and impact of a crisis. An extensive web of information flows exists between all of these partners – a web that transcends borders – in which definitions, action prospects, technical and non-technical information, which are vital to crisis management, are shared as much as possible.

In the event of a(n) (imminent) crisis, the National Coordinator for Security and Counterterrorism is able to activate the national crisis response structure through the National Crisis Centre, in which crisis management coordination (and decision making) takes place between all the relevant ministries, other relevant administrative bodies and private sector partners. The precise composition of the partners involved within the national crisis management organisation depends on the crisis, with the above mentioned building blocks providing an indication of the relevant actors.

The National Cyber Security Centre is the national CERT that provides assistance to the Central Government and critical entities in relation to digital threats and incidents. In addition, the National Cyber Security Centre acts as the operational coordinator in the context of managing digital crises. The National Cyber Security Centre is connected to a network of computer crisis response teams and other intermediary organisations in the Nationwide Network (*Landelijk Dekkend Stelsel*, LDS), each of which bears responsibility for providing assistance to their respective sectors. Key partners on the government side, such as the Government Chief Information Officer, the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD), work closely with the NCSC and are, corresponding to their respective responsibilities, involved in crisis management, as well as in the national crisis response structure. For the purposes of its duties, the National Cyber Security Centre also liaises with international partners and private security companies that may play a significant role in crisis management.

Critical and non-critical companies, institutions and organisations affected by a digital crisis remain responsible for the continuity of their own processes and services. In certain cases, there may be a statutory obligation to report an incident. In addition, notifying partners within the crisis management or supply chain is useful and necessary. Please see Chapter 3: Cyber system and crisis processes, Section C – Crisis processes for a visualisation of the applicable reporting centres.

Any subsequent effects on public order and safety are tackled by way of the security regions and the local triumvirate, using recognisable structures such as GRIP, the coordinated regional procedure for combating incidents. Various operational organisations (such as the Directorate-General for Public Works and Water Management), public bodies and independent administrative bodies may, on the basis of their areas of responsibility, be directly involved in physical crisis management. In the event of a digital crisis with national impact, the National Crisis Centre and the national crisis response structure form the pivot between physical and digital crisis management.

In the national crisis response structure, public communications about any digital crisis are coordinated by or with the National Crisis Communication Core Team (*Nationaal Kernteam Crisiscommunicatie*, NKC). The core communications of the National Crisis Centre are able to support communications officers from locally or regionally competent authorities and any relevant departmental directorates with advice, resources and a network of hands-on experts.

Chapter 3: Cyber-system and crisis processes also provide an extensive description of all the various organisations and actors involved, the crisis processes and communications agreements and guidelines during a cyber crisis.

Recovery phase

In the recovery phase of a crisis in the digital domain, attention must in any case be devoted inter alia to restoring the continuity of processes and services, forensic investigation, evaluation of the crisis and any psychological aftercare for the staff involved. It should be emphasised that, after the initial crisis response, organisations, institutions and companies themselves bear primary responsibility for ensuring the continuity of services and for any necessary repair or reconstruction of digital environments. Please see Chapter 3: Cyber system and crisis processes, Section C for an outline of the recovery phase of a cyber crisis.

Insight into the National Cyber Security Strategy and the future cybersecurity system

On October 10th, 2022, the National Cyber Security Strategy 2022-2028 (NLCS) and the corresponding action plan were published.[6] This strategy includes pillars, goals, sub-goals and actions that inter alia will affect the management of digital crises in the Netherlands. As stated in the National Cyber Security Strategy, it is vital that organisations work together effectively in the event of any national or other digital crises, in line with (supra) regional, national and international crisis response mechanisms.

One of the principal changes to the cybersecurity system relates to the continued development of the National Cyber Security Centre into the national CERT. To that end, the NCSC, the Digital Trust Centre (DTC) and the CSIRT for digital services (CSIRT-DSP) will be merged into a single national cyber security authority, as set out in the National Cyber Security Strategy and announced in a Letter to Parliament on this matter in September 2022.[7] In addition, greater cohesion will be created between other intermediary organisation by stimulating integration where necessary. Among other actions, this means that a review will be carried out to determine whether it has added value to merge other sectoral computer crisis teams with the NCSC.

In addition to the creation of a single national CERT, the government will draw up a roadmap with the business community for the implementation of a public-private platform for reciprocal cyber security information and knowledge sharing, in order to provide all parties involved with relevant technical and non-technical information, clarification and perspective for action in a timely manner. This will take place in line with the maturity level and the needs of various target groups.

Furthermore, in the second half of 2024, the European Network and Information Security Directive 2 (NIS2) and the Critical Entity Resilience Directive (CER) will be transposed into national legislation. As a result of the NIS2, many sectors and organisations within the EU will be faced with statutory obligations for the security of network and information systems. The duties of organisations, such as the NCSC and sectoral regulators, will also be expanded considerably as a result of the implementation. The CER focuses on the physical safety and security of critical processes. Together, the NIS and the CER provide a framework for the digital and physical resilience of critical entities.

In the area of incident response, the National Response Network (NRN) will be developed further into a national incident response network. It will also be reviewed whether the current set of legal instruments for intervention in a national crisis (including emergency legislation) is sufficient for a crisis involving digital elements.

Finally, there will be more intensive efforts in the area of joint preparation, exercises and crisis management by the Central Government, on an interdepartmental basis, with the security regions and private partners. The publication of this NCRP-Digital, which will be used for the preparation of the national cyber exercise ISIDOOR IV, is the first step in this direction. As an initiative of the National Cyber Security Strategy, an administrative cooperation agreement on the topic of digital security will be drawn up with the Association of Netherlands Municipalities, through which joint efforts in the area of municipal cybersecurity will be developed in greater detail.

During the lifecycle of the National Cyber Security Strategy, an annual review will be carried out to ascertain whether the NCRP-Digital should be updated, based on new lessons learned.

6. National Cyber Security Strategy 2022-2028 | National Coordinator for Security and Counterterrorism (nctv.nl).
7. tk-uitvoerder-programmaplan-sporen-integratie-csirt-dsp-dtc-ncsc.pdf (overheid.nl).

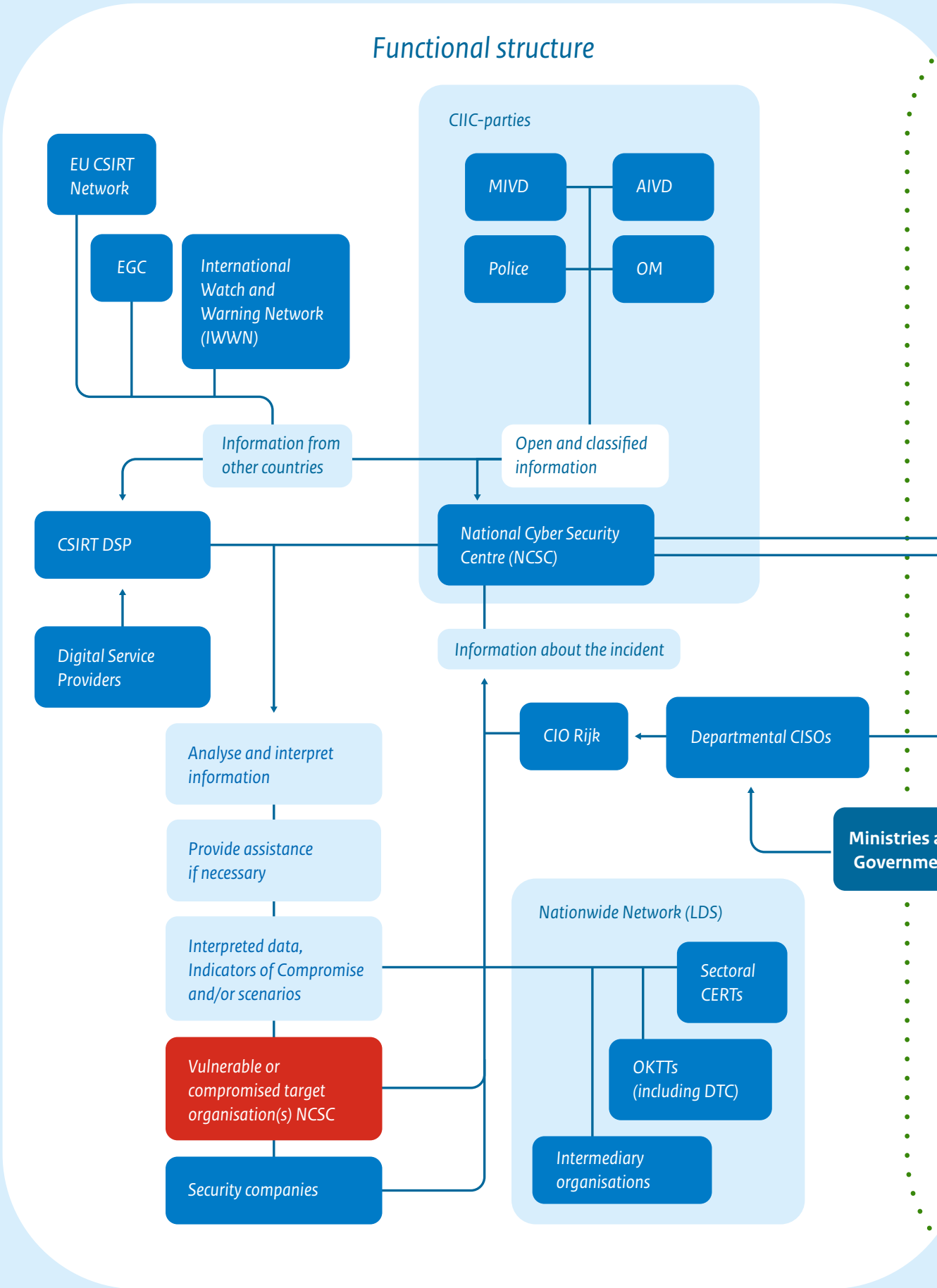
The Eemshaven power station is the largest and (one of three) newest coal-fired power stations in the Netherlands.

3. Cyber system and crisis processes

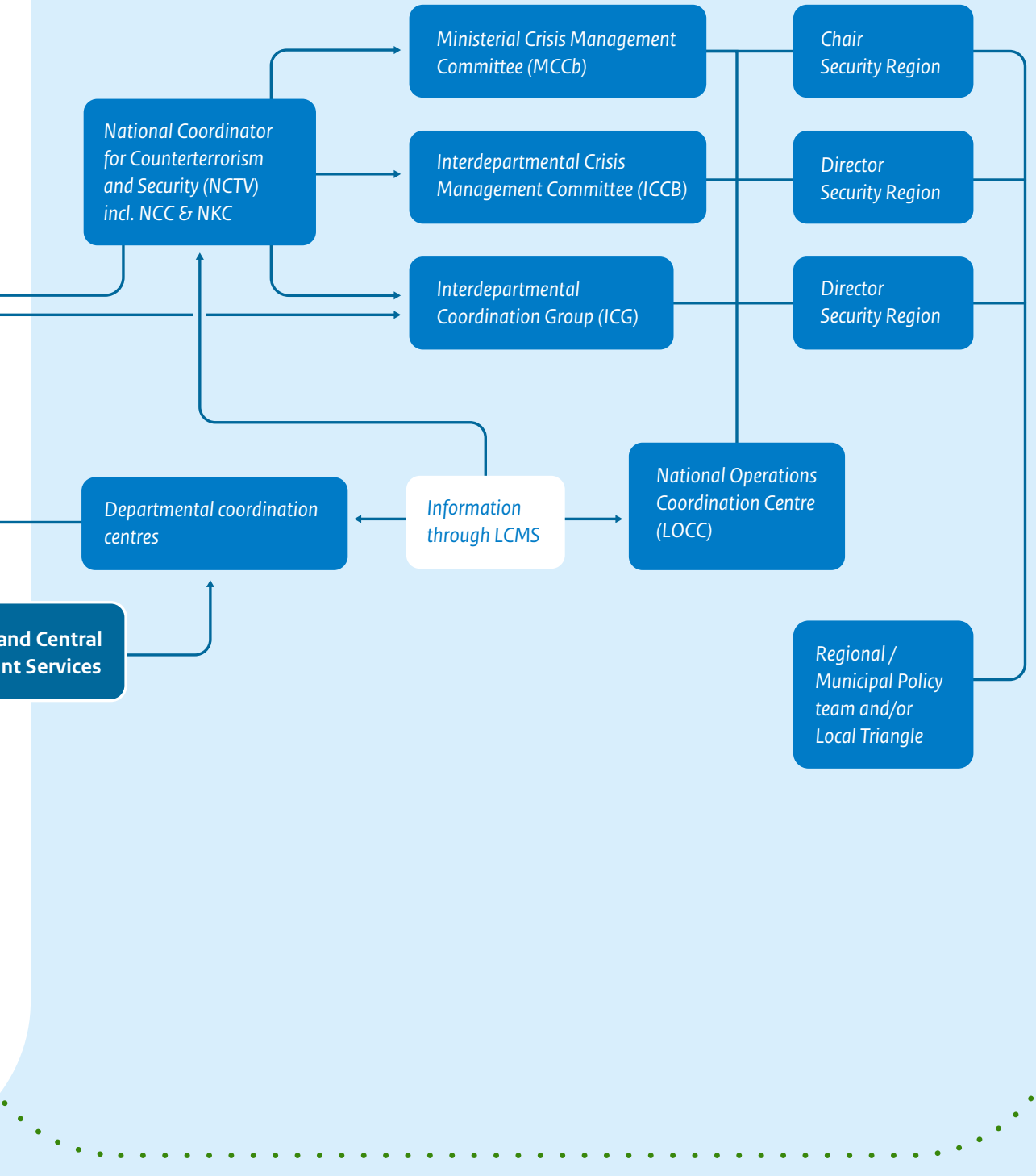
In many cases a digital crisis will not be an isolated incident and will impact many facets within our society. A large number of players are involved in managing a digital crisis – in both the digital and the physical domain. In addition, both public and private sector parties are involved, which have their own responsibilities during a digital crisis but equally work closely together with one another. That is why it is vital to have accurate insight into how all these parties are connected, how they interact and which duties they perform.

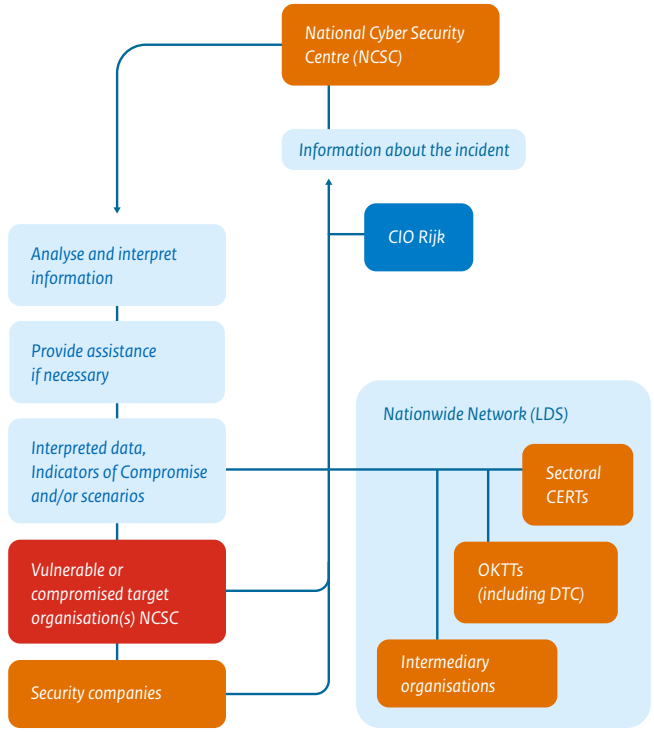
The visual representations in this chapter show how the cyber-specific crisis response structure aligns with the regular crisis response structures in the Netherlands. A distinction, in this case, is made between sectoral crisis response structures and the alignment of these structures at both national and regional level. This chapter will focus on the cyber-specific crisis response structure (Section A), which addresses operational coordination, incident analysis, attribution and detection, responding to the cause and international cooperation. The next section will provide an outline of the connection of the cyber-specific crisis response structure to the general crisis management structure (Section B), with a focus on administrative coordination, follow-up and impact control and information management. This chapter also contains role descriptions of organisations that are involved in digital crisis management, as well as information on relevant crisis processes, including notification, alerting, scaling up and crisis communications (Section C).

Information flows during a (potential) crisis



General structure





A. Functional Crisis Management Structure (the cyber-specific system)

National Cyber Security Centre (NCSC)

The NCSC is the central information hub and expertise centre for cyber security in the Netherlands. The NCSC is the national CERT, which provides the Central Government and critical entities with assistance in the event of digital threats and incidents. In the event of a large-scale digital crisis, or a threat thereof, the NCSC has an operational coordinating role. For the benefit of its responsibilities, the NCSC has up-to-date situational awareness, is in close contact with (target-group) organisations, establishes connections with parties in the cyber system and provides as much advice and perspective for action as possible to tackle or prevent digital incidents. The NCSC itself provides assistance where necessary, for example, by providing incident response capacity.

The NCSC forms the operational hub in the cyber system of the Netherlands. The NCSC's remit inter alia consists of:

- Providing government organisations and critical entities with assistance in taking measures to ensure or restore the continuity of services.
- Notifying and advising these organisations and entities on threats and incidents related to their network and information systems.
- Conducting analyses and technical investigations into digital threats and incidents in order to assist, inform and advise these entities.
- Notifying or advising other organisations about threats and incidents at these entities.
- Notifying intermediary organisations (CERTs and OKTTs (organisations with a duty to inform the public or other organisations regarding threats and incidents that are relevant to them) designated under the Network and Information Systems Security Act (*Wbni*)) or in certain cases other individual entities, regarding threats and incidents relating to their network and information systems.
- In order to prevent cyber incidents and increase resilience, the NCSC provides resilience advisories on cyber security risks and mitigation.
- Advising the general public on digital threats and incidents in general.
- Under the Network and Information Systems Security Act, critical entities are obliged to report incidents with a significant impact on their services to the NCSC.
- Other providers and organisations outside of the Central Government can also voluntarily report to the NCSC in the event of an incident with a significant impact on their services. In such cases, the extent to which assistance can be provided is reviewed for each report.
- In accordance with the Network and Information Systems Security Act (Wbni), the NCSC is the single point of contact (SPOC) for the security of network and information systems, as referred to in the European NIS Directive. To this end, the NCSC maintains close contact with national authorities and authorities in other Member States.
- In addition, the NCSC takes part in international partnerships. All of these partnerships have crisis response plans in place

(standard operating procedures), which come into effect in the event of a large-scale cross-border incident or threat thereof.

In order to carry out these duties, the NCSC works closely with a large number of national and international organisations and partnerships, including:

- The National Response Network (NRN). The NRN is a partnership between the Tax and Customs Administration, the Directorate-General for Public Works and Water Management, SURFcert, the Information Security Service (IBD), the Ministry of Defence, Z-CERT and the NCSC. The aim of the NRN is to jointly increase the digital resilience of Dutch society in general and the resilience of network and information systems. The NRN also provides collective contribution during large-scale cyber security incidents by pooling capacities in order to strengthen the response to incidents. Finally, the NRN contributes to strengthening the knowledge and information position of the participating organisations and to the prevention or timely countering of cyber threats.
- In the context of the National Detection Network (NDN), the NCSC, like the AIVD and the MIVD, shares acute and other threat information with affiliated organisations in order to protect these organisations against cyber threats.
- Within the Cyber Intel Info Cell (CIIC), the NCSC, the AIVD, the MIVD, the National Police and the Public Prosecution Service gather information about cyber incidents and threats in order to achieve a more accurate national situational overview and to arrive at perspectives for action more rapidly.
- It is vital that the NCSC is able to collaborate with security companies effectively. The method of cooperation varies on a case-by-case basis, for example, with the aim of arriving at a national situational overview or coordinated incident response.
- The NCSC encourages and facilitates cooperation within critical infrastructure and in the Central Government through Information Sharing and Analysis Centres (ISACs), in which organisations can exchange information about incidents, threats and mitigating measures.
- Under the coordination of the NCSC, information about incidents and threats is shared within a nationwide network of partnerships, consisting of sectoral CERTs and other intermediary organisations.

Nationwide Network and cyber security partnerships

In order to be able to recognise threats rapidly, the exchange of knowledge, information and expertise is crucial. The Nationwide Network of cyber security partnerships meets this need, as more information is shared more widely, more efficiently and more effectively between public and private sector parties. The NCSC can exchange information with intermediary organisations that are designated as CERTs and OKTTs under the Wbni.

The designation of an intermediary organisation under the Wbni allows the NCSC to share threat and incident information relating to the systems of entities in the target group of that intermediary organisation, including data that can be traced to individuals (such as IP addresses) and, under certain additional conditions, confidential information that can be traced to an entity.

The NCSC website provides an up-to-date overview of the CERTs and OKTTs within the Nationwide Network.[8]

Digital Trust Center (DTC)

The Ministry of Economic Affairs and Climate Policy contributes to enhancing the cyber security of non-critical businesses through the use of the Digital Trust Centre (DTC). The DTC's remit includes, among other duties, providing proactive assistance in prevention. The DTC focuses on the non-critical business community, promotes a generic message with regard to increasing resilience/cyber security and is responsible for providing general information.

The DTC works closely with the NCSC.

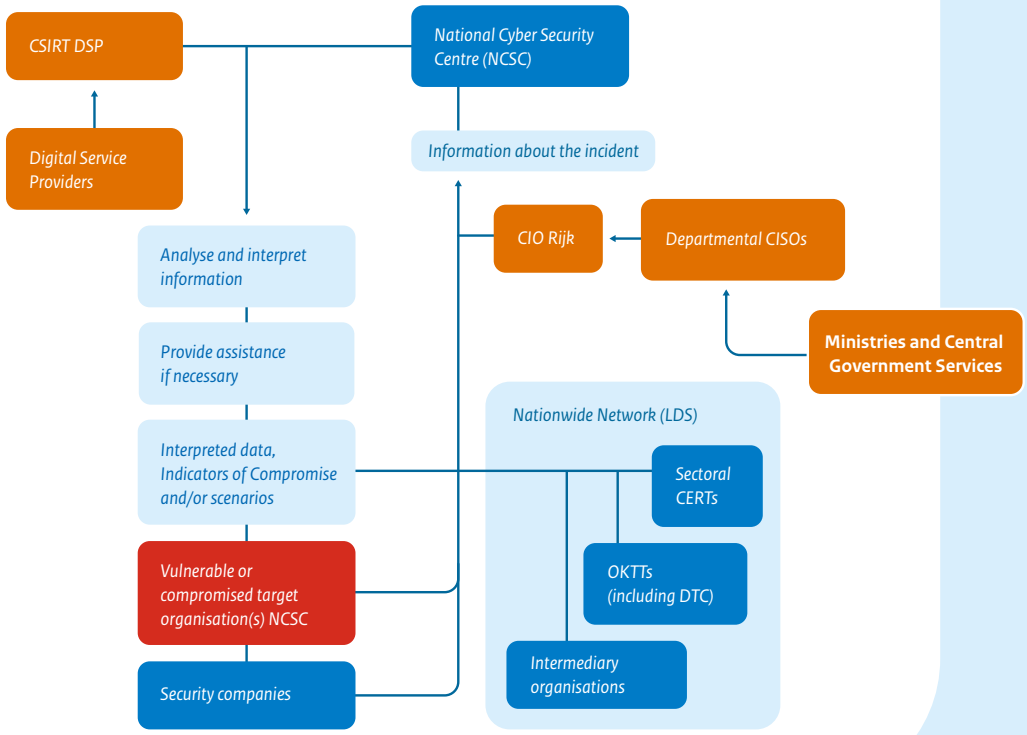
Critical entities

Critical entities are parties that operate, manage or make available a service the continuity of which is of critical importance to Dutch society. Critical entities themselves are primarily responsible for the uninterrupted provision of their services within processes designated as critical (such as electricity, Internet access, drinking water and payment transactions). Together, these processes make up the critical infrastructure.

In addition to the Central Government, critical entities belong to the target group of the NCSC and are entitled to assistance, information and advice, in accordance with the Wbni. Various critical entities are required to report incidents with a significant impact on their services to their regulator and are required to report security breaches in network and information systems that can have a significant impact to the NCSC. Specific critical entities (OESs) also have a duty of care to their own network and information systems (please see Ch 5: Responsibilities in greater detail).

Critical entities often have their own CISO organisation and/or are assisted by private security companies for the security of the organisation's (digital) systems and the management of incidents in IT/OT systems.

8. Connection to the Nationwide Network (LDS) | Becoming a partner | National Cyber Security Centre (ncsc.nl).



CSIRT-DSP

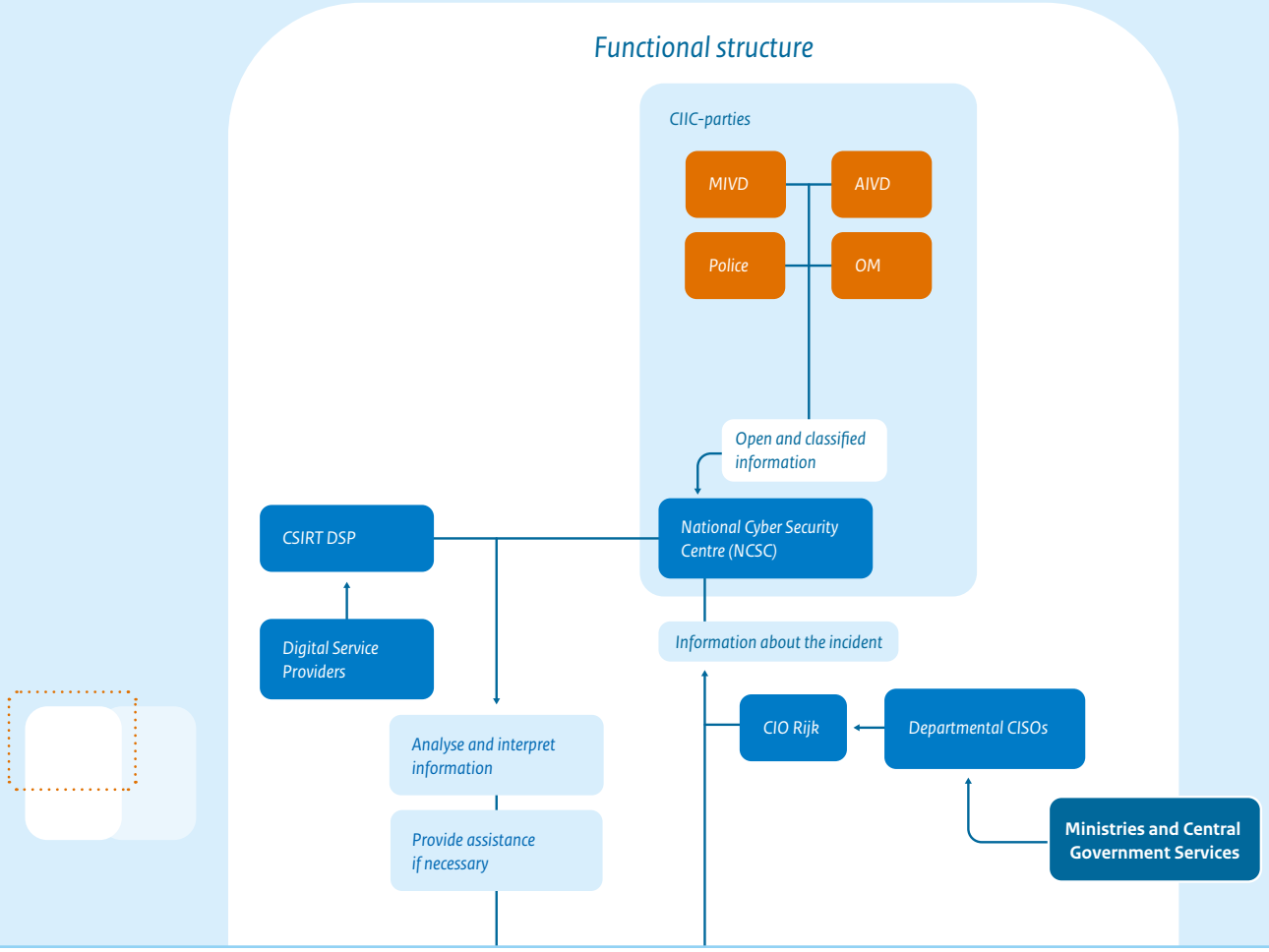
The CSIRT-DSP is the national Computer Security Incident Response Team for digital service providers. Due to the implementation of the European NIS Directive, the responsibilities of the CSIRT-DSP are regulated in the Network and Information Systems Security Act (Wbni).

Digital service providers are required to report incidents with a significant impact to their network and information systems. They also have a duty of care (taking security measures in respect of their network and information systems). These digital service provides include online market places, online search engines and cloud computer services. In addition to being this reporting centre, the CSIRT-DSP supports its target group by monitoring incidents at a national level, by providing relevant information regarding risks and incidents, by providing assistance in the event of incidents and by providing risk and incident analyses. The CSIRT-DSP will alert its target group under various circumstances, for example in cases where vulnerable systems are known, and regarding vulnerabilities in software. The CSIRT-DSP works with digital service providers to make the Netherlands more digitally resilient. To this end, there is close cooperation with the NCSC, the DTC and the EU CSIRT network.

Departmental CIOs, CISOs, the Central Government's CIO, The Central Government's CISO and the Central Government's Security Authority

Under the coordination of the Ministry of the Interior and Kingdom Relations, departmental CIOs and the office of the Central Government's Chief Information Officer (*CIO Rijk*) play a key role in the area of information security under the CIO System Decree (*Besluit CIO Stelsel*). The departmental CISO can issue instructions to any civil servant, external employee and visitor on behalf of the Secretary General and the departmental CIO, in coordination with the Ministry's security authority, insofar as this is necessary for the implementation of departmental information security policies and compliance with information security regulations. The office of the Central Government's Chief Information Security Officer (CISO Rijk) has an interdepartmental coordinating role in relation to cross-governmental information security incidents and emergencies. In the event of a potential, serious, acute and cross-departmental breach of the security of information systems or the risk thereof, the Central Government's Chief Information Security Officer is authorised inter alia to issue instructions and put measures in place (or have them put in place) on behalf of the Secretary General of the Ministry of the Interior and Kingdom Relations. The Central Government's CISO will continuously coordinate with the Central Government's CIO, the Central Government's security authority, and with relevant ministries about any (potential) breach or the risk thereof and the measures put in place to mitigate that breach or risk, and will have direct access to the secretaries-general of the ministries if necessary, in consultation with the departmental CISOs.

In the event of a(n) (imminent) cyber incident, the departmental crisis management organisations are the point of contact for the National Crisis Centre (NCC). In cases where a(n) (imminent) cyber incident affects several ministries and specific coordination is needed, the office of the Central Government's CIO will be the relevant point of contact, as it chairs the CISO council. The Central Government's CISO can, having consulted the CISO council, escalate to the administrative/political executives of the Ministry of the Interior and Kingdom Relations. When the crisis response structure is activated, the Central Government's CISO takes part in the Interdepartmental Coordination Group (ICG). The Director General for Digitalisation and the Public Sector (DGDOO), to whom the Central Government's CISO reports, will take part in the Interdepartmental Crisis Management Committee (ICCB).



General Intelligence and Security Service (AIVD)

The AIVD investigates digital attacks that pose a potential threat to national security. The AIVD can detect and mitigate attacks of this nature, inform victims and provide awareness to potential targets. The AIVD carries out these duties in direct contact with targeted organisations as well as in collaboration and coordination with the NCSC, other CIIC participants and other parties within the Central Government. Moreover, the AIVD has the essential task of informing policy officers and executives, enabling them to implement effective ICT security policies. In addition, the AIVD provides the Central Government and other stakeholders, such as critical entities, with bespoke information security advice to counter state actors. The purpose of this advice is to increase resilience to digital attacks committed by state actors and to limit or prevent (digital) damage. The AIVD works closely with the NCSC. In addition, the AIVD works closely with other national and international partners. For example, the AIVD, the MIVD and the NCSC share relevant threat information within the National Detection Network (NDN) so that affiliated organisations are able to put in place mitigating measures.

Military Intelligence and Security Service (MIVD)

The MIVD conducts investigations into actors that pose a potential threat to national security, with a particular focus on threats to the interests of the Ministry of Defence. The MIVD detects and mitigates attacks committed by state actors and informs (potential) victims. This takes place in close cooperation with the NCSC. In addition, the MIVD provides awareness to potential targets. In this context, the MIVD maintains a special relationship with the defence industry. In addition, as a result of its intelligence position, the MIVD is able to contribute to the attribution of digital attacks.

Furthermore, on behalf of the security authority the MIVD carries out the General Security Requirements for Defence Contracts Act (*Algemene Beveiligingseisen voor Defensie Opdrachten*, ABDO) by advising on this issue and supervising its enforcement and oversight.

Public Prosecution Service (OM)

In the event of a(n) (imminent) incident and/or crisis in the digital domain, the Public Prosecution Service (OM) is responsible for maintaining the rule of law and enforcing the rule of law under criminal law. This means that the Public Prosecution Service:

- has authority over the (legal) investigation into the circumstances of the emergency or crisis and the securing of (digital) evidence, or is involved in the exchange of relevant information (e.g. from/to private parties or the intelligence and security services);
- is committed to preventing or stopping criminal offences by means of criminal law or by having measures taken in the context of the 'guarding and security' system;
- maintains the rule of law by conducting criminal investigations and prosecuting natural persons or legal entities for criminal offences and makes use of alternative intervention methods in that context, such as notifying victims, disrupting criminal activities or preventing new victims or perpetrators. In that context, the Public Prosecution Service works closely with international and private partners.

Police

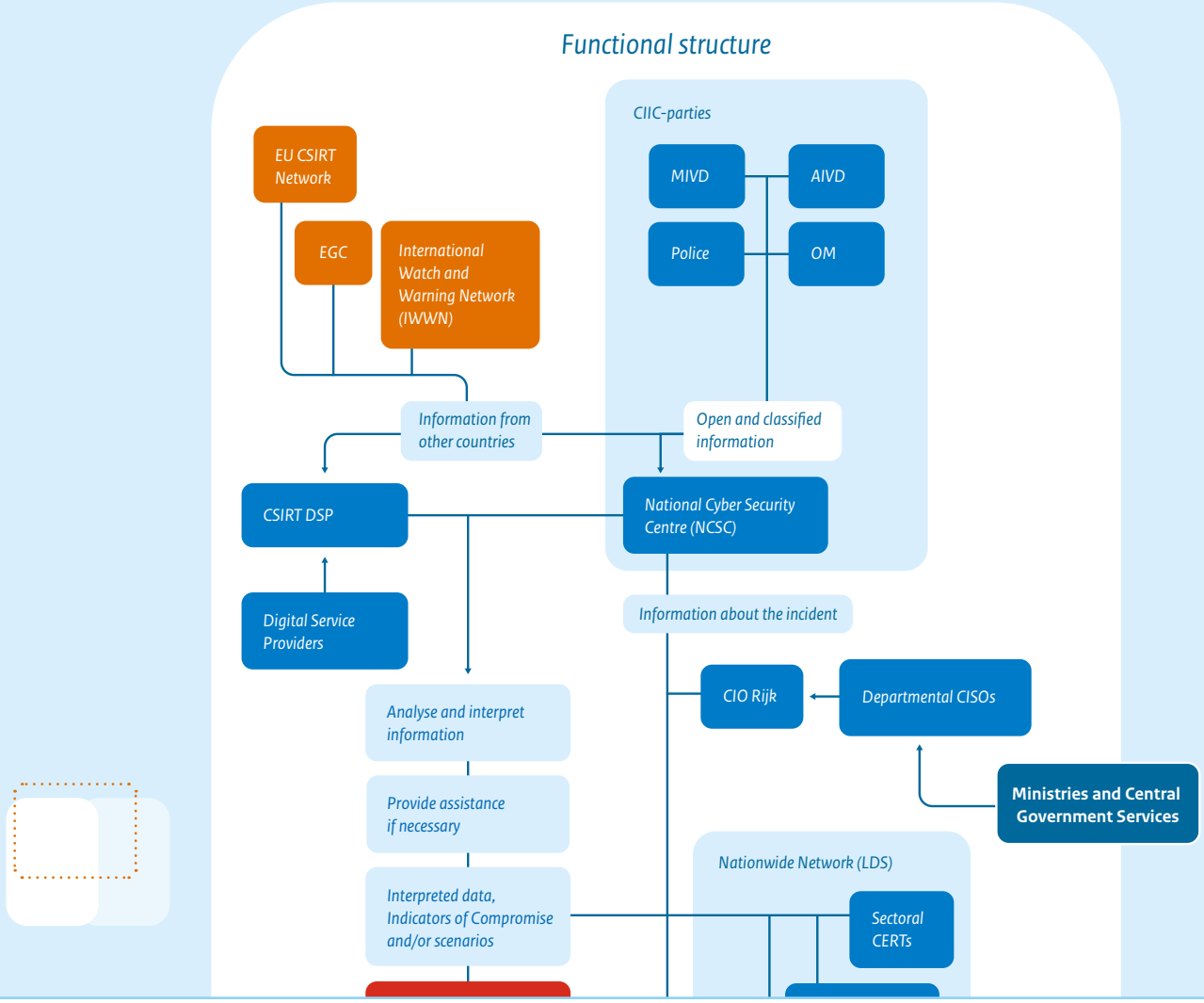
Special investigative powers can be used to trace potential suspects of cyber crime (especially cyber crime leading to a crisis), to stop and prevent criminal offences (where possible) and to dismantle criminal infrastructures. This can lead to the prevention/disruption of these criminal activities and/or to the arrest of suspects in the Netherlands or abroad. Depending on the context and the options available, the most suitable approach (one or more intervention methods) is chosen: prevention, notification, disruption and investigation (and prosecution). If there are any side effects and consequences in the physical domain (such as social unrest, riots and looting), the police similarly have an (enforcement) responsibility in that context. In addition to the cyber crime teams in the police units and in the Team High Tech Crime (THTC), other teams (such as standard teams, the real-time intelligence team and the riot police) are likewise consulted.

At an international level, the police can exchange information through INTERPOL, Europol and various 24/7 networks. Some of these channels may not be useable in the event that the crisis is or might be military in nature or is caused by a state actor. In principle, investigations will in such cases not be able to be carried out through organisations like INTERPOL. The police are also responsible for the technical management of the 112 control rooms.

Cyber Intel/Info Cell (CIIC)

The AIVD, the MIVD, the Police, the NCSC and the Public Prosecution Service collaborate with one another within the Cyber Intel/Info Cell, as referred to in the CIIC Cooperation Agreement (*Convenant samenwerking* CIIC[9]). The aim of the Cyber Intel/Info Cell is to strengthen the national situational awareness in respect of cyber threats and incidents, to enable parties to better carry out their statutory duties in relation to those threats and incidents, to more rapidly provide other stakeholder organisations with a broader range of perspectives for action in relation to cyber threats and thereby increase the digital capabilities of the CIIC partners and to improve security in the digital domain. To this end, the participating organisations collect information about cyber threats and incidents, with the information jointly assessed by employees of the participating organisations. Any relevant analyses and information can be provided to stakeholder organisations.

9. Government Gazette 2020, 30702 | Government.nl > Official publications (officielebekendmakingen.nl).



International partners and partnerships

European Union

The 2016 European Network and Information Security Directive (NIS) established a European network of national CSIRTs and CERT-EU (the CSIRT network). Within this CSIRT network, the CSIRTs are able to exchange operational information quickly and effectively. The CSIRT network is actively supported by the European Network and Information Security Agency (ENISA).

ENISA focuses on the issue of network and information security for Member States and the European Commission and provides these parties with support in this regard. The objective of ENISA is to increase the security and resilience of communications and information systems. ENISA holds a biennial exercise cycle entitled Cyber Europe, during which the design of a so-called Standard Operating Procedure (SOP) is tested. This is a tool for the CERTs in Europe to exchange information in a safe and effective manner in the event of an international crisis in the digital domain.

CERT-EU acts as a response organisation for incidents in the digital domain for the European institutions.

At a European level a blueprint[10] has been published that helps Member States deal with digital incidents. This blueprint applies to incidents that cause such a degree of disruption that Member States are unable to cope with an incident themselves or if the incident has consequences for several Member States or EU institutions. This may involve incidents with a large-scale or significant impact or technical or political relevance, requiring timely coordination and response at the European political level.

The response protocol also gives Europol (EC3) more of an operational remit for large-scale cross-border incidents and crises. In such cases Europol principally works together with police services and ENISA in the area of information sharing and focuses on its investigative remit.

In cases where tackling a cross-border crisis involves a criminal component, Eurojust (the agency for cooperation between judicial authorities) has likewise been provided a role. Eurojust's involvement takes place at the initiative of Europol. Within the judicial domain, Eurojust is able to consult with the European Judicial Cybercrime Network (EJCN) for specific cyber expertise.

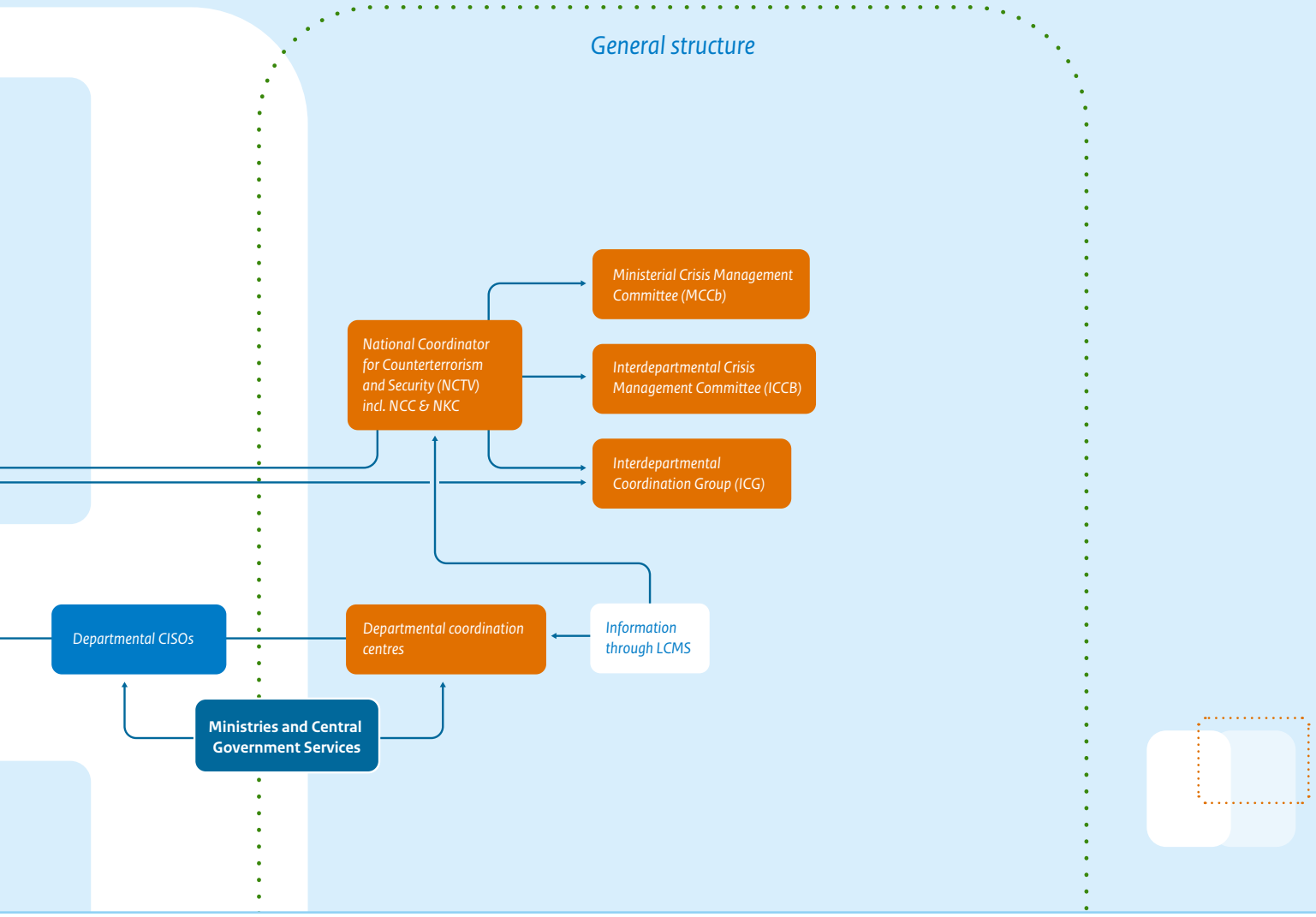
10. Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises, 13 September 2017 (L239/36).

International Watch and Warning Network

The International Watch and Warning Network (IWWN) is a(n) (informal) worldwide network of government representatives from 15 countries (including the Netherlands) for operational collaboration and crisis management in the field of cyber security. The IWWN maintains links with the functional points of contact which carry a national responsibility, has developed Standard Operating Procedures (SOP) for major threats and crisis, organises exercises, advances cooperation and encourages information sharing.

European Government CERTs group

The European Government CERTs group (ECG) is a highly trusted, informal association of government CERTs in Europe. Its participants work together on the basis of mutual trust and understanding. Together, they work on mitigating measures, information sharing in relation to incidents, knowledge development and joint policies. EGC is an operational group with a technical approach, focused on incident response and information sharing.



B. General Crisis Management Structure (national crisis response structure)

The National Coordinator for Security and Counterterrorism

The National Coordinator for Security and Counterterrorism (NCTV), which is part of the Ministry of Justice and Security, protects the Netherlands against societally disruptive threats and coordinates cyber security policy in the Netherlands, including the organisation of the cyber security system. The NCTV instructs the NCSC and provides the Minister of Justice and Security with strategic guidance and advice in the event of a(n) (imminent) cyber crisis. The NCTV also has an overarching administrative and coordinating role in relation to national crisis escalation and is therefore involved in both the functional and the general crisis management structures. The NCTV facilitates and supports interdepartmental decision-making at the director and political-executive level through the National Crisis Centre (NCC). The Minister of Justice and Security acts as the coordinating minister for crisis management and cyber security.

In cases where the national crisis response structure, or parts thereof, is escalated due to a(n) (imminent) cyber crisis, the functional crisis management structure (cyber-specific) and the general crisis management structure (national crisis response structure) must be connected. In the event of a(n) (imminent) cyber crisis, existing agreements are used in accordance with the Decree establishing the Ministerial Crisis Management Committee (*Instellingsbesluit Ministeriële Commissie Crisisbeheersing*) and the National Crisis Management Handbook (*Nationaal Handboek Crisisbeheersing*). Optimal flexibility is the key principle that underpins the organisation, structure and working method of the national crisis response structure. All components and consultations within that structure are deployed as needed and are set up and composed in a flexible manner. A tailored approach is taken for each individual situation and, if necessary, in relation to each individual meeting

.

The **Ministerial Crisis Management Committee** (*Ministeriële Commissie Crisisbeheersing*, **MCCb**) is responsible for the coordination and decision-making regarding response measures at the political-executive level, including the application of ministerial powers. The implementation of the response measures, including the application of ministerial powers, takes place in accordance with the decisions taken in the MCCb. The decisions of the MCCb make up the framework for implementation by public and private sector partners.

The **Interdepartmental Crisis Management Committee** (*Interdepartmentale Commissie Crisisbeheersing*, **ICCb**) is a coordinating and decision-making body at a senior level of the civil service (director, Directors-General) chaired by the NCTV. If necessary, the decisions taken by the ICCb are submitted to the MCCb for approval.

The MCCb and the ICCb are supported and advised by an **Interdepartmental Coordination Group** (ICG) (*Interdepartmentaal Afstemmingsoverleg*, **IAO**) chaired by the NCTV. In a(n) (imminent) national cyber crisis, representatives of the ministries with the relevant policy remit, relevant departmental crisis centres, the NCSC and other relevant partners will participate in the ICG. Within the ICG, a national situational assessment is aggregated, potential measures are coordinated and decisions for the ICCb and the MCCb are prepared.

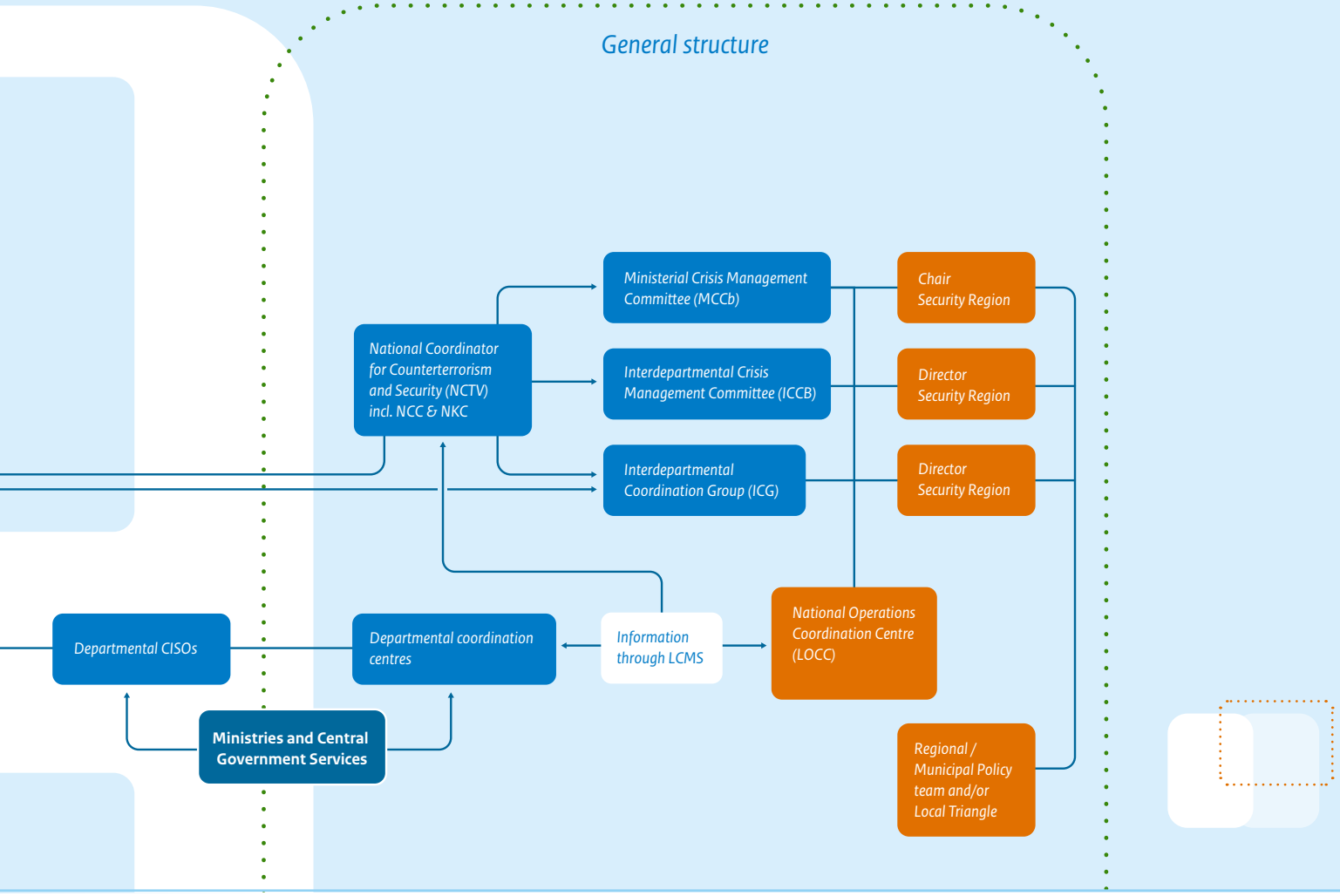
The **National Crisis Centre** (NCC) is part of the NCTV and the interdepartmental coordination centre and is the hub of and for information provision to directors and ministers and crisis communications. The NCC provides the supporting or executive staff and facilitates the (preparation of) interdepartmental decision-making, at both the director and the political-executive level:

- The division of roles between the local/regional and national level during digital incidents and crises is in line with the regular responsibilities and structures.
- The key principle is to align as much as possible and to make use of the regular structures, supplemented if necessary with specific knowledge or expertise in the field of cyber and the digital domain.
- At the national level, the agreements and structures of the National Crisis Management Handbook (NHC, 2022) form the foundation in this regard.

The NCC is the 24/7 information hub and point of contact of the Central Government, and is in direct contact with the NCSC and the National Operations Coordination Centre (Landelijk Operationeel Coördinatie Centrum, LOCC) during incidents with a digital component that impact local authorities or security regions.

The **Departmental Coordination Centres** (DCCs), or another unit within the relevant ministry with the same remit as a DCC, are responsible for the implementation and coordination of the departmental response activities within their own sectors. This similarly applies to a digital crisis/crisis with a digital component, in which they are the link between the affected or involved ministry, their own sectors and the national crisis response structure.

The **National Crisis Communications Core Team** (*Nationaal Kernteam Crisiscommunicatie*, **NKC**) advises the ICCb and the MCCb on the communications strategy and the communications impact of decisions either proposed or taken. The NKC develops and coordinates the communications of the National Government and the Central Government and, where necessary, will coordinate those communications with other public and private sector partners involved.



The **National Operations Coordination Centre** (*Landelijk Operationeel Coördinatie Centrum*, **LOCC**) is part of the Ministry of Justice and Security, is part of the national crisis response structure and takes part in the ICG. The LOCC is staffed by experienced employees from various organisations in the security domain, such as the security regions, the national police, the fire services, the Ministry of Defence, the Netherlands Municipal Public Health Services and Medical Assistance in Accidents and Disasters (GGD/GHOR), the National Institute for Public Health and the Environment (RIVM) and the Red Cross. This makes the LOCC a multidisciplinary organisation in terms of organisation and implementation.

The duties of the LOCC are as follows:

- ensuring the provision of the multidisciplinary National Operational Assessment and operational advice in the event of national and international incidents, crises, disasters and major events;
- coordinating regional, national and international assistance, including assistance as referred to in the Security Regions Act (Wet veiligheidsregio's) and the Police Act 2012 (Politiewet 2012);
- providing support and assistance at the request of relevant partners in the event of regional and supra-regional incidents, crises, disasters and major events; and
- ensuring the coordination, training and deployment of the Dutch experts in the context of the EU Civil Protection Mechanism in its capacity as the National Training Coordinator.

Security regions (regional crisis management organisation)

Within any security region, the **regional crisis management organisation** fundamentally consists of the emergency services (fire brigade, police and medical assistance) and the municipalities, under the authority of the mayor or the chair of the security region. Security Regions are responsible for ensuring the organisation and setup of the regional crisis management organisation, including, depending on the situation at hand, linking up with the necessary crisis management partners.

In cases where an incident in the digital domain has an impact on public order and safety, the security regions are responsible for ensuring the continuity of society and its inhabitants by limiting the impact on public order and security and providing residents with perspectives for action. The focus of the security regions is on addressing the impact of the (physical) effects in society, preventing societal disruption, and on protecting and informing citizens and participating organisations and institutions. This involves providing care for the population, fire services, medical health care, leadership and coordination, information management and crisis management as defined in the Security Regions Act (*Wet Veiligheidsregio's*, Wvr).

The security regions will assess the potential societal impact of any digital incident in their region in consultation with relevant partners, taking into account any potential cascade effects. Insight into the incident and the potential risks and cascade effects is essential to crisis management and to communication with the

civilian population and affected organisations and for the normalisation of society following an incident.

Alongside their partners, the security regions invest in universal instruments, such as a solid information position, assessment, awareness and a scenario mindset in the event of digital disruptions. In addition, the security regions encourage high-risk objects and partners in their region to ensure proper digital resilience and recovery capacity.[11] The NCC is the security regions' national point of contact for the Central Government.

In the event of a cyber crisis in the geographical area of a municipality, the mayor or the chair of the security region, as the competent authority, is able to make use of the crisis management structure. The GRIP structure can then be escalated to rapidly form a crisis response team and create clear information and decision-making lines. The mayor, or the chair of the security region, will seek advice from the Municipal Policy Team (*Gemeentelijk Beleidsteam*, GBT) or the Regional Policy Team (*Regionaal Beleidsteam*, RBT), about the impact of the digital disruption on social life and the measures to be taken to tackle the impact. This escalation will inter alia take place if the impact of the cyber crisis leads to a broader impact on society and (major) deployment of the emergency services. If it appears that the crisis also has (major) effects on public order and safety or that there is a need for additional investigative powers to trace the responsible actor, the *triumvirate* will convene.[12] The police are subject to dual authority: with regard to maintaining public order and providing assistance, authority lies with the mayor, whereas with regard to criminal enforcement, authority lies with the Public Prosecution Service. This consultation between the police, the mayor and the Public Prosecution Service is the local triumvirate of authority. Where relevant to crisis management, the information from the triumvirate consultations will be shared with the policy team on a need-to-know basis.

11. Section 7(3) of the Security Regions Act wetten.nl – Regulations – Security Regions Act – BWBR0027466 (overheid.nl).
12. Section 13 Police Act 2012. wetten.nl – Regulations – Police Act 2012 – BWBR0031788 (overheid.nl).

C. Crisis processes

This section contains a description of the relevant crisis response processes in the event of a digital incident, including reporting, alerting and escalating, and crisis communications. This description will be general in nature. Depending on the sector in which an organisation operates, sector-specific dynamics or agreements may still apply, and it is vital that these are clearly understood in their own operationally developed crisis response plans.

1. Report, alert and escalate

In the case of incidents affecting digital processes and systems, the process of reporting, alerting and escalating goes through various organisations, depending on the nature and scope of an incident and statutory roles and duties. When reporting an incident, the impact on the digital organisation, the impact on the continuity of services and potential effects on physical safety and public order must be taken into account.

Under the Wbni, most critical entities have a duty to report to the NCSC any incidents that has or could have a significant impact for the continuity of the service they provide. Critical entities designated as providers of an essential service also have a duty to report incidents with a significant impact to their sectoral regulators. Digital service providers also have a duty to report to both the CSIRT-DSP and the Radiocommunications Agency Netherlands (Agentschap Telecom).

Other entities may report a digital incident to their sectoral computer crisis team that is part of the Nationwide Network (if the entity is part of the target group of the respective crisis team).

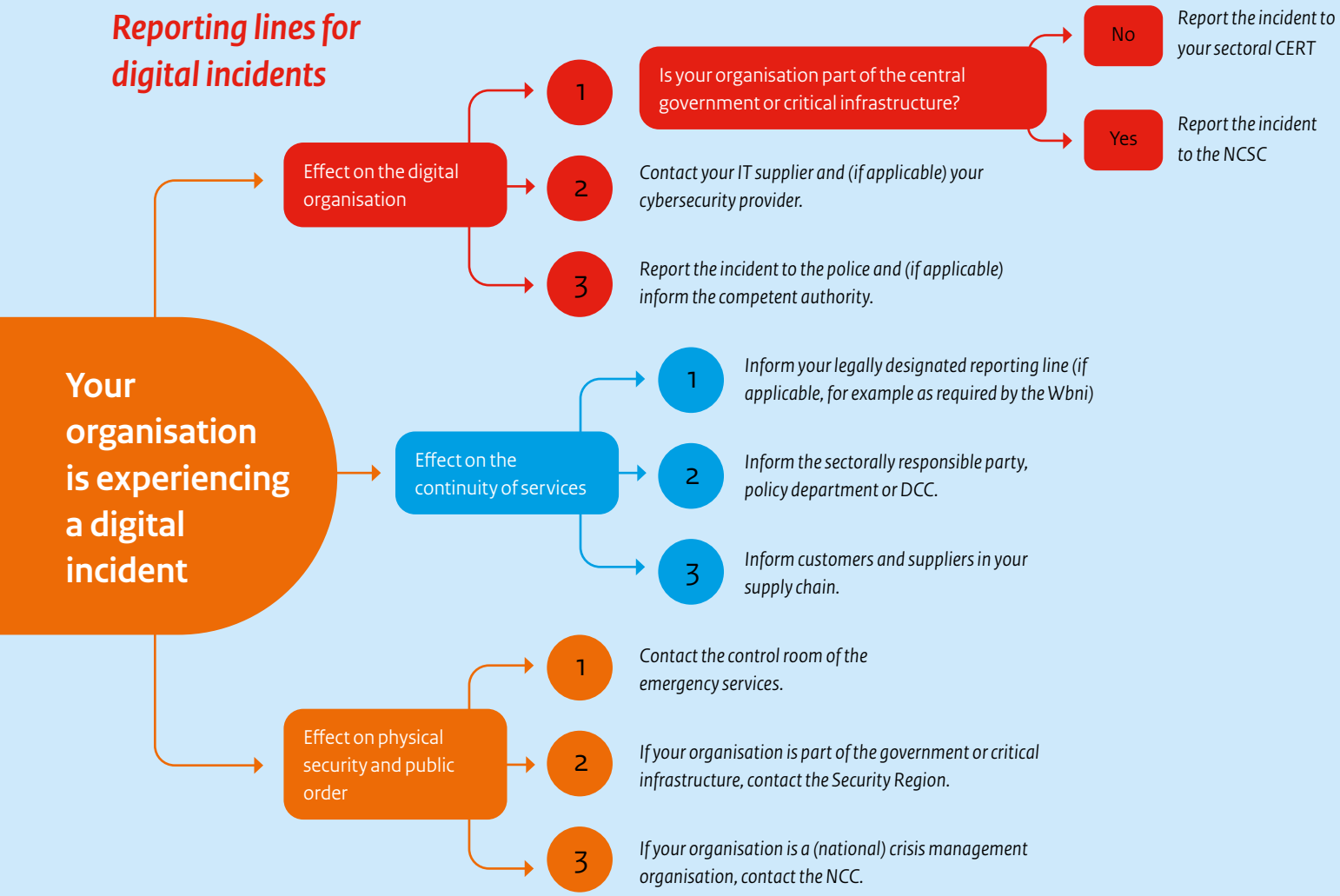
Depending on the nature and scope of an incident, a sectoral computer crisis team involved in crisis management organisation and/or the NCSC may decide to escalate internally. In the event of a(n) (imminent) major digital incident, the NCSC will advise the NCTV on the potential use of the national crisis response structure or parts thereof. The escalation of (parts of) the national crisis response structure will take place in accordance with the National Crisis Management Handbook.

If an incident has an impact on the continuity of services, the affected organisation must notify its statutory reporting centre (if applicable) and the party with system-level responsibility or the departmental crisis centre as well as keep it up to date on developments. In addition, it is vital that partners and providers in the supply or crisis management chain are informed.

Due to the (potential) impact of a digital incident, there may also be an impact on physical security and public order. In case of major (imminent) crises, the NCC will inform the relevant security regions and/or competent local authority of incidents with potential cascade and subsequent effects in the physical domain, if there is reason to do so. In addition, incidents with an impact on physical security and public order can be reported directly to the relevant (emergency) services and/or regional or local authorities, including the security region. Information regarding an incident with a (potential) physical impact within the regional or local domain can be communicated to other local and regional authorities (municipalities, provinces and water authorities) by the security region. In terms of controlling the physical impact, the security region can escalate using existing and recognised structures, such as within the GRIP structure at regional level.

In the event of a(n) (imminent) cyber crisis, the affected organisations themselves bear primary responsibility for resolving the digital disruption within their own organisations. The NCSC will support and assist the Central Government and critical entities in taking measures in order to safeguard the continuity of services or restore continuity (in the event of an incident).

Please refer to the figure below for an overview of the relevant points of contact in the event of a digital incident.



2. Crisis communications

Crisis communications are aimed at responding to the social need for information, at mitigating damage and at providing signification. At a time when information (whether true or false) can be shared in minutes using social media, clear communication principles are critical.

The high degree of complexity of digital incidents and the intertwining of the digital with the physical domain make it difficult to determine the effects of potential cyber crises in a timely manner. Societal disruption as a result of incidents in the digital domain is often characterised by a rapid spread and multiple cascade effects. The crisis will arise independently of geographical boundaries and may be protracted, and there will often be uncertainty regarding the cause, scope and impact for a lengthy period of time. In the case of a cyber crisis, the most critical aspect is translating complex technical/technological problems into general communications that are easy to understand. Bringing together the functional and general crisis management structures also takes place within the NKC (for external communications purposes), with an important role played by the NCSC. This is also were the public-private sector connection takes place.

Uncertainty should not prevent parties from communicating. On the contrary, during a crisis, visibility, clarity and timeliness in communications are of crucial importance. In the event of a crisis or the threat thereof in the digital domain with significant societal consequences, all relevant parties will therefore coordinate the timing and content of their communications as much as possible. The point of departure is that existing structures, roles and methods should be maintained, with a view to the unique and particular nature of the digital domain.

The updated Umbrella Memorandum Crisis communications in the digital domain (*Koepelnotitie Crisiscommunicatie in het digital domein*) (NCTV, 2022) specifies the responsibilities, communications principles and methods of coordination in detail. The memorandum also includes the division of communications roles between the various partners at regional, national and international level, as well as key messages. The document does not only focus on crisis communications in the event of a digital crisis with a societally disruptive impact; after all, crisis response communication and national coordination will also often be required for digital threats or digital incidents with a limited (regional) impact. The Umbrella Memorandum was drawn up in consultation with various partners: NCSC, the Ministries of the Interior and Kingdom Relations, Economic Affairs and Climate Policy, and Infrastructure and Water Management, the police, representatives of the security regions and the Public Prosecution Service.[13]

13. The Umbrella Memorandum is available on www.nctv.nl.

National

Once the national crisis response structure has been activated, the NKC is established, with communications professionals of the NCC and of the involved ministries. The NKC will coordinate press briefings and briefings for the general public by the Central Government and advise the crisis response consultations in the Central Government on the communications strategy to be followed and the communications impact of any proposed or taken decisions. The NKC will issue communications about visible measures or about the threat that has not yet materialised and will provide process information about what the government is doing and why. In addition, it will formulate communications frameworks and core messages where national powers are concerned and will coordinate those messages with partners outside the Central Government, such as the involved security regions/municipalities, organisations and institutions.

Even if the national crisis response structure has not (yet) been activated in the event of a threat or incident in the digital domain, it is often recommended that communications coordination should take place whether at interdepartmental level or between the Central Government and the regions. The Communications Department of the NCC will organise this coordination and, if necessary, will support the communications officers from locally or regionally competent authorities and any involved Communications directorates with advice, resources and a network of hands-on experts.

Regional

The Security Regions Act stipulates that the executive of the security region is responsible for providing citizens within the region with information regarding disasters and crises, regarding the measures taken by the government to prevent, address or control them and about the course of action to be followed. Within the municipalities, final responsibility for crisis communications at a local level is delegated to the mayor of an affected municipality or to the chair of the security region. In addition, it is the responsibility of the relevant minister to provide specific information about potential crises within their domain.

In the event of a cyber crisis, the chair of the security region or the mayor will focus on their own region/municipality in their communications, taking into account what is being communicated in any neighbouring municipality/region or by the Central Government. This will require a great deal of coordination with the parties involved within both the functional and the general crisis management structures. The NKC is a key partner in crises with a supra-regional impact. In addition, coordination will always have to take place with the Public Prosecution Service regarding communication in relation to the investigation process. This is no different from other types of crises involving intentional acts and attribution.

International

During incidents that cross national borders, the NKC will coordinate crisis communications with other European Member States through the Crisis Communications Network, consisting of representatives of all EU Member States and EU bodies, and with the Benelux Crisis Communication Centre.

Responsibilities

Crisis communication in the digital domain takes place in accordance with regular powers and responsibilities. Each party involved will communicate regarding its own issues under its own responsibility but will coordinate the timing and content of the message in a centralised manner (usually within the NKC).

The table below sets out the regular communication responsibilities as they always apply. They set out the key points of who communicates about what. This division of labour will continue to apply when the national crisis structure is escalated. The commitment to coordinating the content and timing of messages will continue to apply in all cases.

Key areas of focus for crisis communication

The objective of crisis communication is to provide clear and timely communications (for the general public). This requires a proactive way of communication that is considerate, open, timely and consistent – even if very little information is available. In that case, the focus will be on process communication: outlining what information is and is not available and what steps are being taken. This is how the government maintains visibility. Communications from officials connect society and appeal to the resilience of individual citizens and of Dutch society as a whole.

As long as there is uncertainty as to whether a crisis is the result of an intentional act, references to possible causes, duration and scope are avoided as much as possible. The public will be informed about visible measures and, where desirable/possible, about invisible measures as soon as possible. Within each phase, where possible, it is crucial that an answer be provided to the question: what can people do? How can citizens take action and help others? This advances the self-reliance of those affected and those involved.

Any crisis will see the dissemination of a lot of information at a high frequency – this includes incorrect information. It is crucial to be aware of disinformation, to confirm what is true and at the same time to debunk false rumours or let it be known that the relevant parties are aware of any rumours and that they are being investigated.

Onderwerp	Organisatie
National Crisis Communication Core Team	Coordinating press briefings and public communication on the digital incident and the visible impact
Emergency services (police, fire brigade)	Local/regional impact Perspectives for action in the physical domain for citizens
Mayor, chair of the security region	Maintaining public order and safety Security measures and local/ regional assessments
Public and private sector parties	Effects on the organisation and employees in question, direct impact on customers or suppliers
NCSC	Analysis & assessment, mitigating measures and perspectives for action
DTC, CERTs and SOC organisations	Technical/operational mitigating measures for relevant individual target groups
NCTV, Minister of Justice and Security as coordinating minister for cyber security and responsible for crisis management	Threat assessment from a national security perspective
Police/Royal Netherlands Marechaussee	Physical security measures (general)
AIVD/MIVD	Assessment of activities and threats by state actors and attribution.
Public Prosecution Service, National Public Prosecutor's Office	Criminal investigation (in the case of a deliberate act)
Relevant minister	Facts and assessment Perspectives for action at national level (in consultation with other relevant ministries)

3. Recovery phase (aftercare and recovery)

The recovery phase of a(n) (imminent) digital crisis entails various challenges. It will for example be difficult to assess when a cyber disruption is truly over, and it may not be clear whether systems are 'clean' once again. It is also difficult to determine whether and when systems will work properly and responsibly again. This makes it even more complicated to test whether all problems (and corresponding effects) have been resolved and which costs have been incurred and can be recovered in the recovery phase.

In any case, attention should be devoted to:

- Assessing the social and psychological impact of the incident at a national level.
- Restoration of continuity where it has been disrupted. Recovery can be an intensive and lengthy process if major damage has been done to IT or if large parts of systems need to be replaced. Recovery from failure of critical processes can equally be intensive, including regarding the scarcity of required expertise or other resources.
- Monitoring the situation, developments in the threat and new related incidents.
- Forensic and criminal investigation, inter alia to determine as accurately as possible the perpetrator, the circumstances and the extent of the digital crisis. Please be aware that (technical) forensic expertise must often be purchased privately. Even before a crisis, it would be prudent to contact security companies that offer these services and possibly enter into contracts with them.
- Evaluation of both the (technical) approach to the disruption and the process-based approach to crisis management (critical processes of crisis management).
- Embedding the lessons learned in the planning (crisis plans, guidance and continuity plans).
- Aftercare for personnel involved. Despite the fact that there may be no physical victims, the impact on an organisation'semployees may be significant.
- In the event of a cyber crisis with a major impact on society, decisions will have to be made in the method of organisation. The national crisis management organisation may transition to a specific crisis management organisation or a project organisation. Collaboration between various sectors may similarly be required in this context. This will form part of the decision-making process during the crisis.

Building block		Building block value
Cause		**Unintentional:** The incident (a malfunction, failure or leak) is caused by a technical or human error, not involving harmful intent.
		**Intentional:** The incident is caused intentionally.
Source		**Within the Netherlands:** The cause of the incident is within the Netherlands.
		**Outside the Netherlands:** The cause of the incident is (entirely or partially) in a foreign country. The source can be in one or several countries, including the Netherlands.
Actor		**Non-state actor:** An incident has been caused by a non-state actor.
		**State actor:** The incident was intentionally caused by a state actor or a party closely associated with a state.
Affected domain		**Only in the digital domain:** The effects of the incident are only noticeable in the digital domain; there are no consequences in the physical world.
		**Socially important services (non-critical):** Critical processes have not been affected. However, the effects may be noticeable in public transport, healthcare, petrol stations, supermarkets, schools or in the private sector. Citizens, the private sector and/or government are experiencing significant disruption due to the incident.
		**Critical processes:** Critical entities are affected by the incident. One or multiple critical processes are experiencing (significant) disturbance. One of the critical processes that could be disrupted is the response capacity of actors in the national and regional crisis management organisations. Citizens, the private sector and/or government are experiencing significant disruption.
Affected area		**One (Security) Region:** The incident is affecting one (security) region in the Netherlands.
		**Multiple (Security) Regions:** The incident is affecting multiple (security) regions in the Netherlands. The affected regions may be far apart geographically.
		**Multiple countries:** The incident is affecting foreign countries. One or multiple countries may be affected, possibly including the Netherlands..
Technical solution		**Technical solution is available:** It is or will soon be clear how to technically address the incident or vulnerability. The necessary actions to implement a technical solution can be taken.
		**Technical solution is not available:** It isn't clear how the incident r vulnerability can be technically addressed. The only possible actions are mitigating in nature.

4. Building blocks

Due to the fact that there are countless conceivable scenarios when it comes to incidents and imminent crises in the digital sphere – especially in combination with a potential impact on the physical domain – this crisis response plan has selected an approach based on building blocks. The building blocks have been defined in terms of key differences that are significant to the crisis response. The building blocks are as follows: cause, source, actor, impacted domain, affected area and prospect of a technical solution. The following chapter will specify eight potential scenarios in greater detail: a deliberate act, technical failure outside of the Netherlands, state actor, facilities that are important to society (non-critical), critical processes, supra-regional impact, impact abroad and unknown technical solution.

The nature and course of the incident will partly determine the structure of the desired response. A broad-strokes inventory has been drawn up for each individual building block of how consequences/effects and the necessary measures can have an impact on the design and approach of the crisis response.

In practice, a given crisis will constitute a combination of various building blocks. It is primarily intended as a tool that the target groups of this document can use in their own preparation and in an actual situation. By examining which building blocks are or could be involved, an assessment can be made of the task at hand and of the choices that can be made in terms of organisation and the involvement of partners.

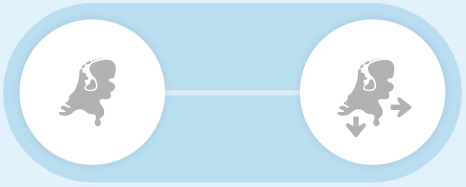
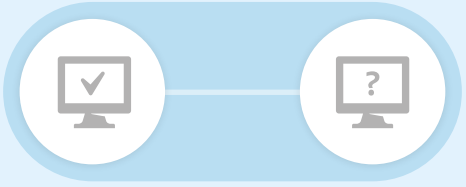
Situational awareness, monitoring and information provision are regular duties of the NCSC, the NCTV (NCC) and the security regions on a 24/7 basis. All organisations are therefore involved in all situations.

The police, intelligence and security services and the Public Prosecution Service will be involved from the outset, given that one can expect prolonged lack of clarity on whether the building blocks of 'deliberate act' and 'state actor' apply. The Ministries of Foreign Affairs and Defence will similarly be involved from the outset as long as it is unclear whether the 'state actor' building block applies. In addition, various ministries may be involved, depending on the nature of the incident and the associated departmental policy responsibility.

Building block	Building block value		
Cause	Unintentional	Intentional	
Source	Within the Netherlands	Outside the Netherlands	
Actor	Non-state actor	State actor	
Affected domain	Only in the digital domain	Socially important services (non-critical)	Critical processes
Affected area	One (Security) Region	Multiple (Security) Regions	Multiple countries
Technical solution	Technical solution is available	Technical solution is not available	

Building block values

A situation can be outlined based on the defined building blocks and building block values. By examining which building blocks are or could be relevant, an assessment can be made of the task at hand and decisions can be made regarding the method of organisation. Insight can also be obtained into partner involvement.

Building block	Building block value
Cause	 Unintentional / **Intentional**
Source	 Within the Netherlands / Outside the Netherlands
Actor	 Non-state actor / State actor
Affected domain	 Only in the digital domain / Socially important services (non-critical) / Critical processes
Affected area	 One (Security) Region / Multiple (Security) Regions / Multiple countries
Technical solution	 Technical solution is available / Technical solution is not available

Cause

Deliberate act

An incident has taken place due to a deliberate act perpetrated in the Netherlands, with the impact equally being limited to the Netherlands.

Consequences, effects and involved organisations

Consequences and effects	People and institutions are extorted (e.g. financially, blackmail, defamation, reputational damage)
	Decrease in trust in digital services
	Information integrity is compromised
	Social unrest, public disorder
	The effects could worsen due to cascading effects or repeating incidents.
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised (critical) processes
	Suppliers and customers in the supply chain of the (critical) processes
	Security companies
	Intermediary organisations and sectoral CERTs
	Police, Royal Marechaussee
	Public Prosecution Service
	Investigative and forensic organisations
	Ministries responsible for the compromised sectors or organisations
	NCSC and NCTV

In the case of a suspected criminal offence, the Public Prosecution Service will lead the investigation, and the police will carry out the investigation.

It will generally not immediately be clear whether a digital crisis was caused intentionally. From an investigative perspective, the fact that there may be an attributable act at play will always be taken into account until this has been explicitly ruled out. In an incident response context, the NCSC will assist (target group) organisations (central government and critical entities) in taking measures to restore the continuity of the affected service.

Conscious choices must be made in the incident response between the importance of the investigation on the one hand and the importance of recovery and mitigating (societal) impact on the other. If the digital incident is evidently unintentional, there may still be criminal offences involved (e.g. due to negligence), as a result of which investigative powers may remain a possibility.

Building block	Building block value
Cause	Unintentional / Intentional
Source	Within the Netherlands / **Outside the Netherlands**
Actor	Non-state actor / State actor
Affected domain	Only in the digital domain / Socially important services (non-critical) / Critical processes
Affected area	One (Security) Region / Multiple (Security) Regions / Multiple countries
Technical solution	Technical solution is available / Technical solution is not available

Source

Technical failure outside the Netherlands

An incident has taken place in the Netherlands as a result of technical failure outside the Netherlands.

Consequences, effects and involved organisations

Consequences and effects	Disruption of business processes could worsen because the source of the incident is outside The Netherlands.
	Attribution could be difficult because the source is outside The Netherlands.
	Limited or no influence from The Netherlands on the (technical) solution.
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised (critical) processes
	Intermediary organisations and sectoral CERTs
	Ministry of Foreign Affairs
	AIVD, MIVD
	NCSC and NCC (international networks)
	Ministries responsible for the compromised sectors or organisations
	NCTV

In itself, the interpretation of this building block will not immediately lead to escalation of (parts of) the national crisis structure, but it will create a dynamic with parties outside the Netherlands, which may require closer cooperation with international partners.

The NCSC will coordinate the collaborative effort with international (cyber) partners and will work closely with an extensive national and international network of computer crisis teams, such as the European CSIRT network, the International Watch and Warning Network (IWWN) and the European Government CERTs group (EGC). The NCSC is able to conduct technical investigations in consultation with these international partners.

Depending on the situation, the Ministry of Foreign Affairs will be able to take on a diplomatic coordinating role with the country where the source of the incident is located. The intelligence services and the police will be able to investigate, potentially in consultation with their international counterparts, in order to determine the source of the incident.

Building block	Building block value		
Cause	Unintentional	Intentional	
Source	Within the Netherlands	Outside the Netherlands	
Actor	Non-state actor	**State actor**	
Affected domain	Only in the digital domain	Socially important services (non-critical)	Critical processes
Affected area	One (Security) Region	Multiple (Security) Regions	Multiple countries
Technical solution	Technical solution is available	Technical solution is not available	

Actor

State actor

An incident has taken place involving a state actor. This can have various purposes: (economic) espionage, (preparation for) sabotage, influence as part of a larger or international conflict, retaliation, etc.

Consequences, effects and involved organisations

Consequences and effects	Disruption (critical) processes
	Compromised integrity of (information)systems
	Diplomatic/international unrest
	Social unrest
	Political unrest/pressure
	Possibly increased risks for Dutch citizens, organisations and business abroad.
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised (critical) processes
	Intermediary organisations and sectoral CERTs
	Ministries of AZ, BZ, BZK, DEF, JenV
	Police, Royal Marechaussee
	AIVD, MIVD
	NCSC and NCC (international networks)
	Ministries responsible for the compromised sectors or organisations
	NCTV

In severe cases involving casualties, disruptive damage or disruption of essential government processes, an armed attack may be involved and the War Act (Oorlogswet) may be invoked to declare a state of emergency. In addition, the right to self-defence will arise under Article 51 of the UN Charter. Furthermore, it will be possible to invoke the NATO treaty and the EU treaty. However, most actions committed by state actors will not immediately cross the threshold into armed conflict. As such, decision-making on the use of the crisis structure is prudent.

In cases where a state actor is involved, the intelligence and security services have independent statutory duties: the AIVD will investigate persons and organisations that pose a threat to the critical interests of the state, and the AIVD and the MIVD will conduct investigations into other countries. In addition, the role and involvement of the Ministries of Defence, Foreign Affairs and General Affairs will change. In operational terms, the NCSC will continue to carry out its coordinating role with regard to the cyber incident, including in the event of an attack originating from a state actor. Depending on the nature of the attack, some decisions will take place in parallel in several bodies, as agreed in the national crisis response structure if escalation is expedient in the relevant case (the Cabinet Committee for Security and Intelligence (*Raad Veiligheid en inlichtingen*), the Cabinet Committee for Defence and International Affairs (*Raad Defensie en Internationale Aangelegenheden*), the Ministerial Core Group for Special Operations (*Ministeriële Kerngroep Speciale Operaties*), etc.). There is a chance that the international dimension will also require a response from international organisations such as the EU, OSCE, NATO or the UN.

Building block	Building block value		
Cause	Unintentional		Intentional
Source	Within the Netherlands		Outside the Netherlands
Actor	Non-state actor		State actor
Affected domain	Only in the digital domain	**Socially important services (non-critical)**	Critical processes
Affected area	One (Security) Region	Multiple (Security) Regions	Multiple countries
Technical solution	Technical solution is available		Technical solution is not available

Impacted domain

Facilities that are important to society (non-critical and non-essential services)

An incident has taken place in which non-critical facilities that are nevertheless important to society have been affected, such as public transport (including traffic signals), supermarkets, petrol stations, schools, support services, non-critical business and municipalities.

Consequences, effects and involved organisations

Consequences and effects	Disruption business processes of compromised businesses and organisations
	Compromised integrity of systems
	Disruption of public safety and security
	Social unrest
	Political unrest/societal upheaval
	Economic damage
	Reputational damage and loss of trust
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised processes
	Suppliers and customers in the supply chain of the compromised processes
	Security companies
	Digital Trust Center, Intermediary organisations and sectoral CERTs
	Police
	Public Prosecution Service
	Ministries responsible for the compromised sectors or organisations
	Security regions, LOCC
	Local Triangle
	Security Regions Council
	NCTV, NCSC

In cases where non-critical facilities are affected, this does not by definition mean that national or regional crisis management organisations need to be involved. Businesses, institutions and organisations remain primarily responsible for the continuity of their own processes.

If social unrest/impact and effects in the physical world were to arise, this can, however, lead to escalation of crisis response structures. Under the coordination of the NCSC, information about incidents and threats is shared within a nationwide system of cyber security partnerships, including sectoral CERTs and other intermediary organisations. The cumulative effect of disruptions must be taken into account: if several facilities and services are impacted at the same time, this can have an effect on the potential ensuing societal disruption, which will lead to a faster response from national and regional crisis response structures.

Building block	Building block value
Cause	Unintentional / Intentional
Source	Within the Netherlands / Outside the Netherlands
Actor	Non-state actor / State actor
Affected domain	Only in the digital domain / Socially important services (non-critical) / **Critical processes**
Affected area	One (Security) Region / Multiple (Security) Regions / Multiple countries
Technical solution	Technical solution is available / Technical solution is not available

Affected domain

Critical processes and essential services

An incident has taken place that has affected one or more critical processes in the Netherlands.

Consequences, effects and involved organisations

Consequences and effects	Disruption/outage of essential digital services for the continuïty of critical processes.
	Possible cascading effects to non-critical services.
	Disruption of business processes of compromised companies and organisations.
	Compromised integrity of (information)systems
	Disruption of public safety and security
	Social unrest
	Political unrest/societal upheaval
	Economic damage
	Reputational damage and loss of trust
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised critical processes
	Suppliers and customers in the supply chain of the compromised (critical) processes
	Security companies
	Police
	AIVD, MIVD
	Public Prosecution Service
	Ministries responsible for the compromised critical processes
	Security regions, LOCC
	Local Triangle
	Security Regions Council
	NCTV, NCSC

Critical processes in the Netherlands are increasingly dependent on digitised processes, the underlying (information) systems and supply chain dependencies. These processes and systems make up the foundation of our society. An incident of this nature will rapidly affect national security interests, with cascade effects that may lead to the activation of the national crisis response structure.

Critical entities will always continue to be responsible for ensuring their own continuity and services. In the event of a disruption or failure, the NCSC is able to provide support where necessary, for example, by giving advice and carrying out a technical analysis for this purpose.

Building block	Building block value
Cause	Unintentional / Intentional
Source	Within the Netherlands / Outside the Netherlands
Actor	Non-state actor / State actor
Affected domain	Only in the digital domain / Socially important services (non-critical) / Critical processes
Affected area	One (Security) Region / **Multiple (Security) Regions** / Multiple countries
Technical solution	Technical solution is available / Technical solution is not available

Affected area

Supra-regional impact

An incident has taken place that has led to consequences and effects in several security regions and/or other regionally classified sectors or areas.

Consequences, effects and involved organisations	
Consequences and effects	Increased complexity because of scarcity of crisis response capacity and interregional differences
	Disruption of business processes of compromised companies and organisations.
	Compromised integrity of (information)systems
	Possible cascading effects to non-critical services.
	Disruption public safety and security
	Social unrest
	Political unrest/societal upheaval
	Economic damage
Organisations involved	Reputational damage and loss of trust
	Providers of compromised critical processes
	Suppliers and customers in the supply chain of the compromised (critical) processes
	Security companies
	Police
	AIVD, MIVD
	Public Prosecution Service
	Ministries responsible for the compromised critical processes
	Security regions, LOCC
	Local Triangle
	Security Regions Council
	NCTV, NCSC

If the incident affects more than one security region in the Netherlands (due to the fact that the source and impact are situated in different regions or because several regions have been affected), cooperation must take place among the relevant security regions with regard to impact control, primarily in relation to the physical impact and any societal unrest.

The NCC acts as the National Government's 24/7 information desk and point of contact for the security regions and acts as the link with the other ministries and the NCSC, in close cooperation with the LOCC.

Building block	Building block value
Cause	Unintentional / Intentional
Source	Within the Netherlands / Outside the Netherlands
Actor	Non-state actor / State actor
Affected domain	Only in the digital domain / Socially important services (non-critical) / Critical processes
Affected area	One (Security) Region / Multiple (Security) Regions / **Multiple countries**
Technical solution	Technical solution is available / Technical solution is not available

Affected area

Impact abroad

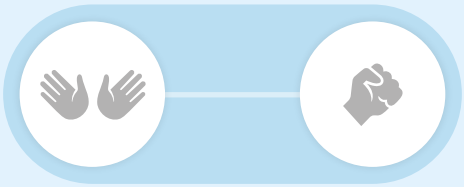
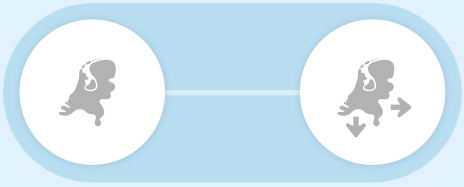
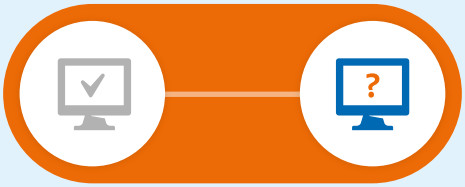
An incident has taken place in the Netherlands that has had an impact abroad.

Consequences, effects and involved organisations

Consequences and effects	Reputational damage for The Netherlands
	International pressure on The Netherlands
	Disruption of business processes of compromised companies and organisations.
	Compromised integrity of (information)systems
	Disruption public safety and security
	Political unrest
	Economic damage
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised (critical) processes
	Suppliers and customers in the supply chain of the compromised (critical) processes
	Security companies
	International networks
	Public Prosecution Service
	AIVD, MIVD
	NCSC and NCC (as single point of contact)
	Ministries of AZ, BZ, DEF, JenV and possibly other ministries responsible for the compromised sectors or organisations.
	NCTV

This building block involves the activation of international cooperation to determine the source and cause of the incident and to mitigate the effects thereof as much as possible (please also see the building block 'source outside the Netherlands'). The difference lies in the fact that, in the case of this building block, the source may be located in the Netherlands. If this is the case, it makes tackling the source somewhat easier, given that there is no need to take into account the jurisdiction of other countries.

If it is confirmed that the source is located in the Netherlands, with effects that are noticeable in several countries, the (international) pressure on the Netherlands to provide a solution, and on the Dutch government in particular, will increase. This can also lead to escalation of (parts of) the national crisis structure. The NCSC will conduct technical analyses into the incident insofar as it can and will share all relevant technical information within its extensive network of international computer crisis teams as much as possible.

Building block	Building block valuez
Cause	 Unintentional — Intentional
Source	 Within the Netherlands — Outside the Netherlands
Actor	 Non-state actor — State actor
Affected domain	 Only in the digital domain — Socially important services (non-critical) — Critical processes
Affected area	 One (Security) Region — Multiple (Security) Regions — Multiple countries
Technical solution	 Technical solution is available — **Technical solution is not available**

Solution prospects

Unknown technical solution prospects for a protracted period

An incident has taken place for which the technical solution prospects remain unknown for a protracted period of time and the response is mainly focused on impact mitigation.

Consequences, effects and involved organisations

Consequences and effects	Social unrest because of absence of a solution or solution perspective.
	Uncertainty. Crisis response shifts to coping with/ managing a protracted problem.
	Disruption of business processes of compromised companies and organisations.
	Compromised integrity of (information)systems
	Disruption public safety and security
	Political unrest
	Economic damage
Organisations involved	Digital service providers of the compromised parties
	Providers of compromised (critical) processes
	Suppliers and customers in the supply chain of the compromised (critical) processes
	Security companies
	Security regions, LOCC
	Ministries responsible for the compromised sectors or organisations.
	NCSC and NCTV

The NCSC, working alongside its national and international partners, will push for technical solutions to become available as soon as possible. In addition, the NCSC will be able to advise (target group) organisations (government and critical entities) on a potential course of action or mitigating measures.

All reports to the emergency services in the Nijmegen region are handled by the control room for the police and fire brigade.

5. Responsibilities (laws and regulations)

The key existing statutory duties and powers that allow information to be shared or, in extreme cases, allow intervention in the digital resilience of the Central Government, critical entities and non-critical organisations have been identified and catalogued in consultation with the relevant ministries. This overview was submitted to the House of Representatives on 3 February 2020.[14]

The chapter below will briefly discuss the Network and Information Systems Security Act and the Telecommunications Act (Telecommunicatiewet.

Network and Information Systems Security Act

The Network and Information Systems Security Act (Wbni) aims to increase the digital resilience of critical entities, the Central Government and digital service providers. In respect of several of these organisations, the Wbni provides for an obligation to notify and report incidents with a significant impact on the continuity of the services, and a duty of care to put in place the correct security measures and is aimed at mitigating the effects of cyber incidents and preventing societal disruption. The Wbni additionally specifies the circumstances of a notifiable incident.

Under the Wbni, all critical entities and components of the Central Government are entitled to information, advice and other assistance from the National Cyber Security Centre (NCSC) with which they can guarantee the continuity of the services they provide.

In addition to the right to assistance, most critical entities also have obligations under the Wbni. In this context, a distinction is made between two types of entities: 'providers of an essential service' (*aanbieders van een essentiële dienst*, AEDs) and 'other designated critical entities' (*andere aangewezen vital aanbieders*, AAVAs):

1. AEDs have a duty to report incidents with a significant impact on the continuity of services to the sectoral regulator and the NCSC, alongside a duty (of care) to take appropriate technical and organisational measures to control the risks to the security of their network and information systems. In addition, these parties are obliged to take appropriate measures to prevent incidents that affect the security of the network and information systems used for the provision of services as well as to limit the effects of such incidents as much as possible. Compliance with these obligations by AEDs is monitored by various sectoral regulators. The duty of care is specified in greater detail in the Network and Information Systems Security Decree (*Besluit beveiliging netwerk- en informatiesystemen*, Bbni).[15]

14 Available for download at: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity.

15. The Network and Information Systems Security Decree (Bbni) came into force alongside the Wbni. Critical providers are designated in the Bbni, which therefore fall under the obligations of the Wbni.

2. 2. AAVAs are critical entities that do not operate in sectors referred to in the Annex to the European Network and Information Security(NIS) Directive but that are considered critical in the Netherlands and are designated as other critical entities in the Bbni. These parties are obliged to report incidents with a significant impact on the continuity of their services to the NCSC.

If, for example, AEDs do not sufficiently comply with the duty of care, a regulator may intervene by taking administrative enforcement action or by administering fines.

Telecommunications Act

The key statutory provisions with regard to telecommunications are included in chapters 11a, 14 and 18.

Risk and crisis management measures (Chapter 11a)

In a general sense, providers of public electronic communications networks and public electronic communications services are obliged to put in place appropriate technical and organisational measures in order to manage the risks to the security and integrity of their networks and services. In addition, they must take all necessary measures to ensure, in the event of a technical malfunction or failure of the electricity network, the greatest possible availability of public telephone services using the public electronic communications network.

Furthermore, providers of public electronic communications networks and public electronic communications services are obliged to notify the Minister forthwith of any breach of security or loss of integrity as a result of which the continuity of public electronic communications networks and public electronic communications services is significantly interrupted.

Exceptional circumstances (Chapter 14)

In the event that exceptional circumstances have been declared, the Minister of Economic Affairs and Climate Policy has extensive powers to issue instructions to every provider of public electronic communications networks and public electronic communications services, namely in respect of:

- the maintenance and operation of public telecommunications networks and services, which includes, for example, the prioritisation or, conversely, the limitation of communication; the potential disabling of services or a modified form of provision (e.g. temporary free calls or allowing persons other than subscribers to make use of services, as well as prioritising or limiting certain forms of communication);
- the maintenance and operation or limitation or termination of the use of radio transmitters (e.g. enabling or disabling transmitters or radio links); and
- guaranteeing the accessibility of the 112 emergency number to the greatest extent possible through the obligation to install a facility to prevent congestion in the accessibility of 112.

For the purpose of preparing for exceptional circumstances, the Minister of Economic Affairs and Climate Policy may designate providers of public electronic communications networks and public electronic communications services that are obliged to make preparations to be able to carry out instructions during exceptional circumstances. These preparations lie in the area of:

- participation in exercises and/or consultations. The National Telecommunications Continuity Group (*Nationaal Continuïteitsoverleg Telecommunicatie*, NCO-T) is a consultative body that is subject to this;
- implementation of continuity planning and crisis management; and
- reporting on preparations.

During a crisis or incident, in which no exceptional circumstances have been declared, the Minister of Economic Affairs and Climate Policy can consult with the providers of the relevant critical processes through the NCO-T. The companies designated as members thereof may be requested to cooperate in any response actions.

Designation power
(Chapter 18)

Chapter 18 contains additional provisions for the Telecommunications Act, including provisions relating to the designation power of the Minister of Economic Affairs and Climate Policy to collect intelligence (18.7) as well as instructions relating to the maintenance and operation of communications networks and the provision and use of their public electronic communications services, if this is necessary for the termination of criminal behaviour against a person (in consultation with the Minister of Justice and Security) or if this is necessary in the interest of the security of the state (in consultation with the Minister of the Interior and Kingdom Relations) (18.9).

The ECT terminal for container handling in the Maasvlakte is fully automated.

Annexes

1. **Duties and responsibilities of the ministries and other relevant organisations**
2. **Relevant sources and literature**
3. **Abbreviations**

Annex 1

Duties and responsibilities of the ministries and other relevant organisations

Ministry of the Interior and Kingdom Relations

Departmental CIOs, CISOs, The Central Government's Chief Information Officer, The Central Government's Chief Information Security Officer and the Central Government's Security Authority

Under the coordination of the Ministry of the Interior and Kingdom Relations, departmental CIOs and the office of the Central Government's Chief Information Officer (*CIO Rijk*) play a key role in the area of information security under the CIO System Decree (*Besluit CIO Stelsel*). The departmental CISO can issue instructions to any civil servant, external employee and visitor on behalf of the Secretary General and the departmental CIO, in coordination with the Ministry's security authority, insofar as this is necessary for the implementation of departmental information security policies and compliance with information security regulations.

The office of the Central Government's Chief Information Security Officer (*CISO Rijk*) has an interdepartmental coordinating role in relation to cross-governmental information security incidents and emergencies. In the event of a potential, serious, acute and cross-departmental breach of the security of information systems or the risk thereof, the Central Government's Chief Information Security Officer is authorised inter alia to issue instructions and put measures in place (or have them put in place) on behalf of the Secretary General of the Ministry of the Interior and Kingdom Relations. The Central Government's CISO will continuously coordinate with the Central Government's CIO, the Central Government's security authority, and with relevant ministries about any (potential) breach or the risk thereof and the measures put in place to mitigate that breach or risk, and will have direct access to the secretaries-general of the ministries if necessary, in consultation with the departmental CISOs.

DG for Digitalisation and the Public Sector (DGDOO) and the Digital Society Department

In the event of a(n) (imminent) crisis, the DG for Digitalisation and the Public Sector (*DG Digitalisering en Overheidsorganisaties*, DGDOO, which the Government CIO and the Digital Society Department report to) acts as a point of contact for government organisations for issues that fall within its policy remit (including computerisation and Government ICT, the digital government and the digital society). The DGDOO contributes to the situational assessment of the government, in coordination with crisis partners such as the NCSC and the IBD. Among other things, as the party with system-level responsibility for digitalisation, the DGDOO is responsible for communications with stakeholders and the Minister of the Interior and Kingdom Relations.

In the event of a(n) (imminent) government-wide crisis, the Digital Society Department will be in close contact with the various Computer Emergency Response Teams (CERTs)/information hubs of the other authorities, such as the municipalities, provinces and water boards.

General Intelligence and Security Service (AIVD)

The AIVD carries out investigations into digital attacks that pose a potential threat to national security, for example, in the event of suspicion of the involvement of a state actor. The AIVD can detect and mitigate attacks of this nature, inform victims and provide awareness to potential targets. The AIVD carries out these duties in direct contact with victim and target organisations as well as in cooperation and coordination with the NCSC, CIIC participants and other parties within the Central Government. In addition, the AIVD has the task of informing policy officers and officials, allowing them to implement effective digital security policies. Furthermore, the AIVD provides the Central Government and other stakeholders, such as critical entities, with bespoke information security advice. The purpose of this advice is to increase resilience to digital attacks committed by state actors and to limit or prevent (digital) damage.

The AIVD works closely with the NCSC. In addition, the AIVD works closely with other national and international partners. The AIVD, the MIVD and the NCSC share relevant threat information within the National Detection Network (NDN) so that affiliated organisations are able to put in place measures in line with their own responsibilities.

Ministry of Foreign Affairs

The Minister of Foreign Affairs is responsible for the diplomatic and political response to cyber attacks and will coordinate the diplomatic and political response of the Netherlands in a like-minded, EU, OSCE and NATO context. The attribution of cyber attacks is likewise coordinated by Foreign Affairs, in consultation with relevant domestic and foreign partners.

In addition, the Ministry of Foreign Affairs and the embassies in particular have a vital monitoring and signalling function aimed at enhancing situational awareness.

Where appropriate, the Security Policy Department will be the first point of contact for international incidents in the digital domain. Once the national crisis response structure has been activated, the crisis coordinator of the Ministry of Foreign Affairs will be the first point of contact.

Ministry of Defence

The Catalogue of National Operations (*Catalogus Nationale Operaties*) lists various Defence capabilities and their availability for deployment in the civilian domain. Where appropriate, these capabilities are also available for the management of incidents in the digital domain.

The Ministry of Defence has military advisers in each security region, who are the primary point of contact for the security regions regarding requests for military assistance and support and for the desired impact to be achieved.

In the event of activation of the national crisis structure, the Central Staff will in principle take part in the ICG. The Secretary General will in principle take part in the ICCb in preparation for the MCCb. The Secretary General, HChief of Defence Staff, Directors General for the Policy or Legal Affairs Departments will advise the Minister on their contributions in the MCCb.

The Defence Cyber Security Centre (DCSC) is tasked with identifying, analysing and executing coordinated mitigation or elimination of cyber threats against and/or disruptions of Defence IT resources. In addition, the DCSC focuses on partnerships with other departments in the context of the government-wide mitigation of cyber threats.

The DCSC works closely with other organisation such as the NCSC, the NATO Computer Incident Response Capability (NCIRC) and CERT organisations from all over the world. It is also a member of the EU PESCO project Cyber Rapid Response Teams. Agreements have been made with the NCSC through the NRN regarding mutual support and assistance in the cyber domain in the interest of a joint overview of digital threats and the optimal coordination of operational activities.

The Defence Cyber Command (DCC) is responsible for the development and deployment of military action capability in the cyber domain. This digital capability consists of its own operational capacity and a knowledge institute (Cyber Warfare and Training Centre). In addition, the DCC has a number of cyber reservists that can be called up in case of an emergency. In the event of a cyber incident, the DCC can provide military assistance to civil authorities at their request. In extreme cases, the DCC can use its offensive cyber capability to carry out a cyber attack. With regard to its regular duties, the DCC maintains contacts and partners (interdepartmental) with partners and actors within and outside of the Ministry of Defence in the context of information provision surrounding cyber incidents and personnel exchanges for the exchange of knowledge and experience.

Royal Netherlands Marechaussee (KMar)

In the event of a (cyber) incident/disruption in one of the assigned areas of responsibility, the Royal Netherlands Marechaussee will conduct an investigation into any criminal offences under the authority of the Public Prosecution Service. To this end, KMar has cyber resources of its own at its disposal in order to conduct its own investigations or will collaborate with the police.

Military Intelligence and Security Service (MIVD)

The MIVD conducts investigations into actors that pose a potential threat to national security, with a particular focus on the interests of the Ministry of Defence. The MIVD can detect and mitigate attacks committed by state actors and inform (potential) victims. This takes place in close cooperation with the NCSC. In addition, the MIVD provides awareness to potential targets. In this context, the MIVD maintains a special relationship with the defence industry. In addition, as a result of its intelligence position, the MIVD is able to contribute to the attribution of digital attacks.

Furthermore, on behalf of the security authority the MIVD carries out the General Security Requirements for Defence Contracts Act (*Algemene Beveiligingseisen voor Defensie Opdrachten*, ABDO) by advising on this issue and supervising its enforcement and oversight.

NATO

Due to the fact that civilian and military networks and systems in the cyber domain are closely intertwined, there is a chance that NATO could become involved in a potential cyber crisis. In such cases, cooperation with and through NATO can take place in various ways. The NATO Cyber Security Centre (NCSC) is responsible

for the security of NATO networks. Allies and various NATO units also share threat information and other intelligence through NATO, for example, through the NATO MISP. If desired, assistance from allies can also be requested through NATO in the form of NATO Rapid Response Teams. In addition, NATO also has various platforms for operational cooperation between public and private sector parties, in which the DCSC and the MIVD are represented.

Ministry of Economic Affairs and Climate Policy

The Minister of Economic Affairs and Climate Policy, as the party with system-level responsibility for the telecom sector, is responsible for maintaining the national digital infrastructure. During an incident in the digital domain, it is primarily up to the parties in the sector themselves to put in place measures to help resolve the crisis: the Minister does not bear operational responsibility. Under exceptional circumstances, the Minister may issue instructions to providers of electronic communications services and networks under Section 14 of the Telecommunications Act.

The Telecommunications Act provides for the option of designating providers of public telecommunications services and/or infrastructure to make preparations to maintain telecommunications during exceptional circumstances. One of the preparations is to participate in the consultation group established by the government, the National Telecommunications Continuity Group (NCO-T). The purpose of the NCO-T is for the government to work with the providers to:

- draw up preventive measures in order to prevent serious disruption or outages of public communications networks and services; and
- put in place measures to remedy any disruption or failure as quickly as possible with as little damage as possible to critical interests.

Within the NCO-T, agreements are made on the obligations of these providers that follow from the Telecommunications Act. These are obligations in the area of continuity planning and crisis management.

The Minister of Economic Affairs and Climate Policy is also responsible for the trusted services of the eIDAS Regulation. Trusted services are services that guarantee the proper and authenticated exchange of data via the Internet. Examples include electronic signatures, seals, time stamps, registered electronic delivery services and certificates for the authentication of websites. Trusted services are provided by commercial parties but are also used within the government itself. They are part of the critical national telecommunications infrastructure.

In addition, the Ministry of Economic Affairs and Climate Policy is responsible for policy with regard to the Energy sector. Pursuant to the Wbni, providers of essential services (AEDs) have been designated in the electricity, gas and oil subsectors. AEDs are subject to a notification obligation and duty of care regarding cyber security. The Radiocommunications Agency Netherlands supervises compliance with the duty of care of these AEDs on behalf of the Ministry of Economic Affairs. In addition, sectoral legislation is currently being drafted, imposing additional requirements in relation to cyber security and crisis management within the energy sector.

Radiocommunications Agency Netherlands

The Radiocommunications Agency Netherlands (AT) engages in expanding, distributing and optimising the electronic communications domain. Although its principal focus is on the frequency spectrum, alongside the Netherlands Authority for Consumers & Markets (*Autoriteit Consument en Markt*), Radiotelecommunications Agency Netherlands also supervises compliance with many provisions in the Telecommunications Act, such as the obligations resting on providers of public telephony services to provide continuous access to the 112 emergency number. In addition, under the Telecommunications Act, the Radiotelecommunications Agency Netherlands is the organisation to which any failure in services must be reported.

The duties of the Radiocommunications Agency Netherlands during crises include:

- proactive monitoring and providing advice on site. This is to ensure the continuity of the networks and services and to support crisis management operations;
- assessing the immediate and long-term impact;
- assessing other processes in relation to the Electronic Communications Domain, such as, for example:
  - advising on the continuity of the networks;
  - terminating radio links (e.g. illegal links);
  - seizing and/or disabling transmission and other equipment;
  - requisitioning equipment and information;
  - taking administrative enforcement action;
  - preparing measures to allocate frequencies during exceptional circumstances.

Ministry of Justice and Security

The Minister of Justice and Security is the coordinating minister for crisis management and cyber security. The NCTV, which is part of the Ministry of Justice and Security, is the commissioning authority of the NCSC, which, as an operational organisation, also falls under the responsibility of the Minister of Justice and Security. In addition, the Minister is responsible for the critical communications services 112, C2000 and NL-Alert.

Public Prosecution Service

In the event of a(n) (imminent) incident in the digital domain, the Public Prosecution Service is responsible for maintaining the rule of law and enforcement under criminal law. This means that the Public Prosecution Service:

- has authority over the (legal) investigation into the circumstances of the emergency or crisis and the securing of (digital) evidence or is involved in the exchange of relevant information (e.g. from/to private parties or the intelligence and security services);
- is committed to preventing or stopping criminal offences by means of criminal law or by having measures taken in the context of the 'guarding and security' system;
- maintains the rule of law by conducting criminal investigations and prosecuting natural persons or legal entities for criminal offences and makes use of alternative intervention methods in that context, such as notifying victims, disrupting criminal activities or preventing fresh victims or perpetrators. In that context, the Public Prosecution Service works closely with international and private partners.

Police

Special investigative powers can be used to trace potential suspects of cyber crime (especially cyber crime leading to a crisis), to stop and prevent criminal offences (where possible) and to dismantle criminal infrastructures. This can lead to the prevention/disruption of these criminal activities and/or to the arrest of suspects in the Netherlands or abroad. Depending on the context and the options available, the most suitable approach (one or more intervention methods) is chosen: prevention, notification, disruption and investigation (and prosecution). If there are any side effects and consequences in the physical domain (such as social unrest, riots and looting), the police similarly have an (enforcement) responsibility in that context. In addition to the cyber crime teams in the police units and in the Team High Tech Crime (THTC), other teams (such as standard teams, the real-time intelligence team and the riot police) are likewise consulted.

At an international level, the police are able to liaise and act through INTERPOL, Europol and various 24/7 networks. Some of these channels may not be useable in the event that the crisis is or may be military in nature or is caused by a state actor. In principle, in such cases, it will not be possible to carry out investigations through organisations like INTERPOL. The police are also responsible for the technical management of the 112 control rooms.

Ministry of Finance

Tripartite Crisis Management Operational Committee (TCO)

The Tripartite Crisis Management Operational Committee (*Tripartiet crisismanagement operationeel*, TCO) will become operational in the event of intelligence on (imminent) operational disruptions to the payment and securities transactions in the core financial infrastructure, e.g. as a result of a cyber attack. The TCO serves as a decision-making body and has the following duties:

- to take measures in the event of an imminent, cross-institutional disruption of payment and securities transactions; and
- to communicate with stakeholders.

The participants in the TCO are the Ministry of Finance, the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, AFM), and De Nederlandsche Bank (DNB). All three of these parties play a key role in the functioning of payment and securities transactions. In this context, the Minister of Finance bears political responsibility for the financial system, with the AFM supervising conduct as well as securities transactions and DNB exercising integrity supervision and acting as the central bank, including under the Wbni, and enhancing the proper functioning of payment transactions. DNB chairs the TCO.

Ministry of Infrastructure and Water Management

The Ministry of Infrastructure and Water Management is responsible for policy in a large number of sectors that are vital to keeping the Netherlands safe, liveable and accessible. Within these sectors, at present, nine critical processes have been identified. Within that group, the following providers of an essential service (AEDs) have been designated under the Wbni:

- for transport by water: Harbour Master's Division of the Port of Rotterdam Authority (*Havenbedrijf Rotterdam N.V.*);
- for transport by air: Royal Schiphol Group N.V., Air Traffic Control The Netherlands (*Luchtverkeersleiding Nederland*), Maastricht Upper Area Control Centre (MUAC), Aircraft Fuel Supply B.V., the Royal Netherlands Marechaussee and any airline with at least 25% of the total number of aircraft movements at Schiphol in a calendar year;
- for transport by rail: designated infrastructure operators and railway companies;
- for transport by road: designated road authorities and operators of intelligent transport systems;
- for drinking water: the drinking water companies.

Within the nuclear sector and the control and management sector (*keren en beheren*), a number of other critical entities have been designated as such (AAVAs) under the Wbni.

For the purposes of the Wbni, the Minister of Infrastructure and Water Management has designated the Human Environment and Transport Inspectorate (Inspectie voor de Leefomgeving en Transport, ILT) as the regulator for compliance with the obligations of the Wbni by AEDs. The stand-by number of the Ministry of

Infrastructure and Water Management's Departmental Crisis Management Coordination Centre (Departmentaal Coördinatiecentrum Crisisbeheersing IenW, DCC-IenW) serves as the 24/7 Wbni reporting centre for the ILT.

At the Directorate-General for Public Works and Water Management (RWS), the operational organisation, a Security Centre has been established for the three networks of the Main Water System (*Hoofdwatersysteem*), the Main Road Network (*Hoofdwegennet*) and the Main Waterway Network (*Hoofdvaarwegennet*). The Security Centre has a broad remit, including advising on projects to implement the correct security requirements, the development of cyber security standards for the entire sector (primarily in the area of IA) and actively monitoring the networks of the Directorate-General for Public Works and Water Management. This takes place both for Industrial Automation and for the office environment. The Security Centre collaborates with other government agencies, such as the NCSC, Joint-SOC (J-SOC, a partnership between SOC RWS, the Tax and Customs Administration, SSC-ICT, DICTU, the Education Executive Agency and the Ministry of Justice and Security), the AIVD and the water authorities on a daily basis. In addition, the Directorate-General for Public Works and Water Management is part of the National Response Network (NRN). The SOC RWS is able to escalate to a higher level in the event that a situation becomes more complex and crisis response decision-making must take place at a more senior level. If the digital disruption has a physical impact on the network of the Directorate-General for Public Works and Water Management, escalation can take place to the Directorate-General's national crisis organisation.

Other relevant organisations within the cyber system

The **Cyber Security Council (CSR)** is a national and independent advisory body to the government and is composed of senior representatives from public and private sector organisations and the scientific community. The CSR advises the government on the implementation of the cyber security strategy.

Annex 2

Relevant sources and literature

Agenda and final letter Risk and Crisis Management 2018-2021, Letter to Parliament 12 November 2018 and 30 April 2020.

Netherlands Court of Audit, *Digitale dijkverzwaring: cyber security en vitale waterwerken*, 2019, and response from the Minister of Infrastructure and Water Management, 25 February 2019.

W. Bantema et al., *Burgemeesters in cyberspace*, 2018.

Cyber Security Assessment Netherlands, 2022.

Defence Cyber Strategy 2018.

M. van Eeten, *Blussen met nullen en enen* (Van Slingerlandt Lecture, 31 October 2019).

Evaluation of ISIDOOR 2021.

Inspectorate of Justice and Security, *Evaluatie rijkscrisisorganisatie tijdens de DigiNotar-crisis*, July 2012.

Decree establishing the Ministerial Crisis Management Committee 2022.

Netherlands Institute for Safety (IFV), *Bestuurlijke Netwerkkaarten Crisisbeheersing en bijbehorende bevoegdhedenschema's.*

Netherlands Institute for Safety (IFV), *Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring)*, April 2022.

Netherlands Institute for Safety (IFV), *Crisiscommunicatietips voor uitval van vitale voorzieningen*, December 2018.

Netherlands Institute for Safety (IFV), *Verbinden van werelden? Een analyse van de aanpak van zeven bovenregionale crisistypen*, Arnhem 2019.

Netherlands Institute for Public Safety (NIPV), *Cyber scenario's voor veiligheidsregio's.*

Netherlands Institute for Public Safety (NIPV), *Bestuurlijke bevoegdheden cyber. Verkenning van bevoegdheden en overige interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio's bij (dreigende) digitale incidenten*, 2022.

Landelijk convenant voor samenwerkingsafspraken tussen Veiligheidsregio's, Politie en Telecom.

H. Modderkolk, *Het is oorlog, maar niemand die het ziet*, 2019.

National Crisis Management Handbook 2016.

National Security Strategy 2019.

National Cyber Strategy 2022-2028.

Dutch Safety Board (OVV), *Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix*, 2021.

Recommendation EU on coordinated response to largescale cyber security incidents and crises, 13 September 2017 (L239/36).

National Institute for Public Health and the Environment (RIVM), *Rijksbrede risicoanalyse Nationale Veiligheid*, 2022.

National Institute for Public Health and the Environment (RIVM), *Themarapportages cyberdreigingen*, 2022.

Security Regions Council, *Bestuurlijk routeboek digitale ontwrichting*

WRR, *Voorbereiden op digitale ontwrichting*, 2019 and government response 2021.

Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten 2020.

Annex 3

Abbreviations

AED	Provider of Essential Services
AIVD	General Intelligence and Security Service
BZK	Ministry of the Interior and Kingdom Relations
CERT	Computer Emergency Response Team
CSIRT	Cyber Security and Incident Response Team
DCC	Defence Cyber Command/Departmental Coordination Centre
DOCB	Crisis Management Directors' Consultation
DTC	Digital Trust Center
EGC	European Government CERTs group
ENISA	European Network & Information Security Agency
EU CyCLONe	European Union Cyber Crises Liaison Organisation Network
EU CSIRT's Network	European Union Cyber Security Incident Response Teams Network
EZK	Ministry of Economic Affairs and Climate Policy
FIRST	Forum of Incident Response and Security Teams
ICCb	Interdepartmental Crisis Management Committee
IGC	Interdepartmental Coordination Group
ISAC	Information Sharing & Analysis Center
IWWN	International Watch and Warning Network
JenV	Ministry of Justice and Security
LDS	Nationwide Network
LOCC	National Operations Coordination Centre
MCCb	Ministerial Crisis Management Committee
NATO	North Atlantic Treaty Organization
NCC	National Crisis Centre
NCO-T	National Telecommunications Continuity Group
NCSC	National Cyber Security Centre
NLCS	National Cybersecurity Strategy 2022-2028
NCTV	National Coordinator for Security and Counterterrorism
NCV	Emergency Communications Network
NHC	National Crisis Management Handbook
NKC	National Crisis Communication Core Team
NRN	National Response Network
NVS	National Security Strategy
OKTT	Organisations with an objective manifest duty to inform the public or other organisations
OM	Public Prosecution Service
SOP	Standard Operating Procedure
TCO	Tripartite Crisis Management Operational Committee
THTC	Police High Tech Crime Team
VNG	Association of Netherlands Municipalities
VR	Security region

Distribution
Distribution
National Coordinator for
Counterterrorism and Security (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

More information
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

December 2022