RAND EUROPE

Digitale weerbaarheid van Nederlandse organisaties

Mogelijkheden en uitdagingen voor de meetbaarheid

Fook Nederveen, Erik Silfversten, Maria Chiara Aquilino, Scott Warnier

For more information on this publication, visit www.rand.org/t/RRA3700-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

Voorwoord

Mede door de toenemende afhankelijkheid van technologie en de groeiende impact van cyberincidenten op de maatschappij, is er steeds meer aandacht in beleid voor de digitale weerbaarheid van organisaties. Digitale weerbaarheid is het vermogen om middels technische, procedurele of organisatorische maatregelen cyberincidenten te voorkomen of, wanneer cyberincidenten zich toch voordoen, deze te weerstaan, te absorberen, zich ervan te herstellen of een nieuw evenwicht te bereiken. Het meten en vergroten van digitale weerbaarheid is echter buitengewoon ingewikkeld door, onder andere, de dynamiek en verwevenheid van digitale systemen en het ontbreken van een samenhangende, gestandaardiseerde meetaanpak op organisatieniveau. Het doel van dit onderzoek is inzichtelijk te maken of, en zo ja hoe en onder welke randvoorwaarden, de digitale weerbaarheid van Nederlandse organisaties meetbaar gemaakt kan worden op een breed toepasbare manier door de NCTV.

Dit onderzoek is uitgevoerd door onderzoeksbureau RAND Europe in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) en op aanvraag van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). RAND Europe is een onafhankelijk not-for-profit-beleidsonderzoeksbureau, met als doel beleid en besluitvorming te verbeteren. Dit rapport is onderworpen aan peerreview, conform de kwaliteitsstandaarden van RAND voor kwalitatief hoogstaand onderzoek. We willen onze collega's Henri van Soest en Rebecca Lucas bedanken voor hun opbouwende commentaar. Daarnaast bedanken we de leden van de wetenschappelijke begeleidingscommissie voor dit onderzoek voor hun gedegen onderzoeksbegeleiding en het waardevolle commentaar op conceptversies van het rapport. Deze commissie bestond uit voorzitter prof. dr. Roland van Rijswijk-Deij (Universiteit Twente), dr. Sascha van Schendel (Erasmus Universiteit Rotterdam), dr. Marcel Spruit (Haagse Hogeschool), drs. Casper van Nassau (WODC) en een medewerker van het ministerie van Justitie en Veiligheid. Ten slotte danken we de geïnterviewde deskundigen voor het delen van hun inzichten. De auteurs zijn verantwoordelijk voor de inhoud van dit rapport. Voor meer informatie over RAND Europe of dit document kunt u contact opnemen met Stijn Hoorens (hoorens@randeurope.org).

RAND Europe	RAND Europe	RAND Europe
Gardens Business Centre New Babylon	Rue de la Loi 82	Eastbrook House
Anna van Buerenplein 41	Bus 3	Shaftesbury Rd
2595 DA Den Haag	1040 Brussel	Cambridge CB2 8DR
Nederland	België	Verenigd Koninkrijk
Tel. +31 10 899 5916	Tel. +32 2669 2400	Tel. +44 1223 353 329

Samenvatting

Bij overheden is het besef steeds verder ingedaald dat niet alle incidenten voorkomen kunnen worden. Om die reden wordt steeds vaker de term 'weerbaarheid' gebruikt in beleidsdocumenten. Waar in het verleden vooral aandacht was voor preventie, wordt met 'weerbaarheid' meer aandacht gegeven aan de continuïteit van een systeem, ook als een dreiging tóch tot een incident leidt. Bij digitale systemen wordt er gesproken van digitale weerbaarheid of cyberweerbaarheid. Digitale weerbaarheid is van groot belang aangezien samenlevingen en organisaties steeds afhankelijker zijn van technologie.

Het bevorderen van digitale weerbaarheid van organisaties is een van de speerpunten van de Nederlandse Cybersecuritystrategie (NLCS) 2022-2028. De inzet is om daarbij de vastgestelde scheefgroei tussen digitale dreigingen enerzijds, en de mate van digitale weerbaarheid van organisaties anderzijds, zo klein mogelijk te maken en te houden. Er bestaat echter nog geen geschikte weerbaarheidsmaat waaraan de overheid de mate van digitale weerbaarheid van organisaties kan aflezen. Door het gebrek aan dergelijke informatie is het lastig om vast te stellen of de weerbaarheid daadwerkelijk is toegenomen en om te beoordelen waar investeringen en inspanningen effectief en efficiënt zijn geweest.

Het doel van dit onderzoek was inzichtelijk maken of de digitale weerbaarheid van Nederlandse organisaties meetbaar gemaakt kan worden op een breed toepasbare manier door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De hoop is dat het op den duur mogelijk wordt voor de overheid om veranderingen in de mate van digitale weerbaarheid van organisaties, al dan niet als gevolg van beleidsinterventies gericht op de verhoging ervan, te kunnen volgen.

Dit onderzoek is een verkenning van de mogelijkheden voor het meten van (aspecten van) digitale weerbaarheid van organisaties, welke – bij voorkeur kwantitatieve (waarbij alles met een ordinale schaal als kwantitatief opgevat wordt) – indicatoren daarvoor gebruikt of ontwikkeld kunnen worden, en wat deze data kunnen zeggen over de staat van de digitale weerbaarheid van organisaties. Deze open insteek betekent ook dat dit onderzoek niet is gericht op het opleveren van een uitgewerkte meetmethode waar de NCTV vervolgens mee aan de slag kan gaan. In plaats daarvan worden de voor- en nadelen van verschillende benaderingen uiteengezet, evenals de overwegingen die bepalend zullen zijn voor de opzet van een mogelijk toekomstig meetinstrument.

Dit onderzoek is gestoeld op A) een bescheiden literatuuronderzoek, waarbij gezocht is naar studies gericht op het meten van digitale weerbaarheid, B) interviews met deskundigen, gericht op hun praktijkervaringen met het meten van digitale weerbaarheid en C) interne workshops waarin de bevindingen van dit onderzoek werden bediscussieerd en implicaties geanalyseerd.

Hoe kan 'digitale weerbaarheid' worden afgebakend?

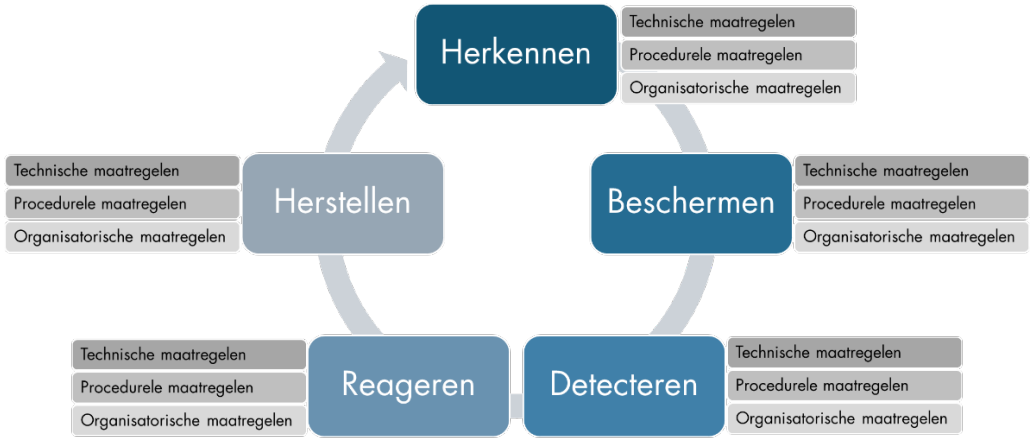
De NCTV definieert digitale weerbaarheid in Nederlandse Cybersecuritystrategie 2022-2028 als:

> Het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging. Die risico-afweging kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen.

Deze definitie is als uitgangspunt genomen voor dit onderzoek om zoveel mogelijk aan te sluiten bij de Nederlandse beleidsomgeving. De Nederlandse overheid maakt geen onderscheid tussen 'digitale weerbaarheid' en 'cyberweerbaarheid'. Ook die laatste term wordt soms gebruikt, en de twee begrippen worden beschouwd als synoniemen. In de literatuur bestaat echter nog geen duidelijke consensus over het gebruik en de definities van cyber- en digitale weerbaarheid. Sommige auteurs hanteren bijvoorbeeld een nauwere kijk op weerbaarheid door hun definities te beperken tot het vermogen van een systeem om te blijven functioneren of technisch te herstellen na aanvallen (louter de 'warme' fase). In de Nederlandstalige literatuur wordt voor de engere opvatting ook wel de term 'veerkracht' gebruikt. Maar de definities van menig andere auteur, evenals opvattingen in het bredere vakgebied van weerbaarheid, sluiten meer aan op de bredere zienswijze van de NCTV, waarin weerbaarheid gezien wordt als een continu, cyclisch proces dat zowel preventieve als reactieve en lerende elementen omvat. Doorgaans wordt deze cyclus opgedeeld in fasen als herkennen, beschermen, detecteren, reageren en herstellen, of variaties hierop.

Verschillende strategieën, wetten en beleidsdocumenten vertalen dit brede concept naar interventies, waaronder technische maatregelen (zoals firewalls en back-ups), procedurele maatregelen (zoals risicobeoordelingen en incidentresponsplannen) en organisatorische maatregelen (zoals training en governance). Literatuur en beleidsdocumenten beschouwen de fasen van de weerbaarheidscyclus als samenhangende deelprocessen, die elk een combinatie van technische, procedurele en organisatorische maatregelen vereisen.

Figuur 1. De kernonderdelen van digitale weerbaarheid



Wat leert de literatuur over bestaande meetinstrumenten van digitale weerbaarheid van organisaties?

Ondanks de toegenomen aandacht voor het verhogen van digitale weerbaarheid, blijkt het inzichtelijk maken van de mate van weerbaarheid buitengewoon ingewikkeld. Verschillende technische, procedurele, organisatorische en externe kenmerken spelen hierbij een rol. Technologieën en bedreigingen veranderen bijvoorbeeld constant en snel. Daarnaast zijn technische systemen vaak te complex voor mensen om volledig te kunnen begrijpen, of om te kunnen testen op alle kwetsbaarheden in het systeem. Tevens zijn er veel aspecten die een rol spelen bij digitale weerbaarheid die lastig te vangen zijn in indicatoren, zoals de rol van sociale relaties tussen werknemers en de werkcultuur. Ten slotte zijn digitale processen in hoge mate verbonden en verweven met processen buiten de controle van de organisatie, waardoor bijvoorbeeld via afhankelijkheden van toeleveranciers incidenten buiten de organisatie direct de digitale weerbaarheid kunnen aantasten.

Op al deze terreinen zijn data nodig om zeker te weten in welke richting de mate van digitale weerbaarheid van een organisatie zich beweegt. Er bestaan momenteel geen methoden die een dergelijk compleet beeld opleveren. Niettemin zijn er methoden ontwikkeld die toegepast kunnen worden om inzichten te vergaren over aspecten van de digitale weerbaarheid van organisaties. In dit onderzoek hebben we 18 benaderingen geïdentificeerd en geanalyseerd. Deze vervullen verschillende functies: ze stellen organisaties in staat om hun ontwikkeling in de loop van de tijd systematisch te volgen, huidige sterke en zwakke punten te identificeren en/of specifieke gebieden aan te wijzen waar verdere verbetering nodig is. Maar enkele van deze benaderingen omvatten echter alle vijf eerdergenoemde fasen van digitale weerbaarheid én alle drie typen maatregelen. De meeste benaderingen richten zich op kwalitatieve in plaats van kwantitatieve indicatoren, waarbij de nadruk ligt op beschrijvende beoordelingen en subjectieve evaluaties in plaats van numerieke of datagestuurde meetcriteria. Ze kunnen weliswaar waardevolle contextuele inzichten en operationele adviezen opleveren, maar vaak zijn het eerder flexibele raamwerken die grotendeels op conceptueel niveau blijven en toepasbaar zijn op organisaties in verschillende sectoren en verschillende grootten dan dat het gedetailleerde methodologieën betreffen. De resultaten zijn doorgaans inzichtelijk specifiek voor een organisatie, maar kunnen niet eenvoudig worden vergeleken met de resultaten van andere organisaties. Hoewel de meeste van deze benaderingen niet expliciet ingaan op welke wijze rekening gehouden wordt met nog niet gekende dreigingen, wordt er in verschillende instrumenten nadruk gelegd op een proactieve strategie om met dergelijke onzekerheden om te gaan.

Er is weinig bekend over de validiteit en betrouwbaarheid van deze 18 benaderingen. Voor geen van de instrumenten vonden we bewijs dat ze nauwkeurig meten wat ze beogen, of dat ze consistent zinvolle resultaten opleveren in verschillende organisatorische contexten. Dit roept vragen op over de werkelijke waarde die deze kaders bieden en de mate waarin ze bijdragen aan het verbeteren van de digitale weerbaarheid. Bovendien is het onduidelijk door welke specifieke mechanismen de weerbaarheid beïnvloed zou worden, waardoor het moeilijk is om hun effectiviteit te bepalen.

Wat leert de beantwoording van bovenstaande vragen over de wijze waarop digitale weerbaarheid meetbaar kan worden gemaakt?

Op dit moment is er geen bestaande methode beschikbaar om de specifieke gegevens te genereren die nodig zijn voor het meten van digitale weerbaarheid. De methoden die in deze studie zijn geïdentificeerd en geanalyseerd, benadrukken de inherente afwegingen en spanningen die gepaard gaan met het conceptualiseren en meten van digitale weerbaarheid op organisatieniveau. Geen van deze methoden wordt op het moment van schrijven door een overheid ingezet met als doel de mate van digitale weerbaarheid te meten. De geïdentificeerde methoden worden überhaupt zelden alleen hiervoor gebruikt. Andere doeleinden zijn bijvoorbeeld risicobeheer, het waarborgen van basisbeveiligingsmaatregelen of naleving ervan, wat indirect kan bijdragen tot een beter begrip van weerbaarheid, ook al is dat niet hun primaire doel. Alle in de literatuur geïdentificeerde benaderingen hebben voor- en nadelen en verschillende sterke en zwakke punten voor het meten van digitale weerbaarheid. Empirische gegevens die nodig zijn om de validiteit van de huidige meetmethoden te toetsen ontbreken echter, en het is dus lastig te zeggen of een methode inherent beter presteert dan een andere.

Niettemin bieden de geanalyseerde benaderingen nuttige aanknopingspunten om een toekomstige meetmethode vorm te geven, afhankelijk van het uiteindelijke doel ervan. Als het doel is om digitale weerbaarheid op organisatieniveau op te bouwen en de implementatie van basismaatregelen voor digitale weerbaarheid te meten, kan het Britse Cyber Essentials-programma een nuttig uitgangspunt bieden. Als het doel is om gegevens te verzamelen en de gereedheid van organisaties om cyberincidenten te identificeren, te beschermen, te detecteren, erop te reageren en ervan te herstellen, gedetailleerder te meten, dan is een uitgebreider beoordelingskader op basis van de NIST- of ISO-raamwerken wellicht geschikter. En ten slotte, is het algemene doel van de benadering voor het meten van digitale weerbaarheid om uitgebreide en sectorspecifieke gegevens te verzamelen en te analyseren over hoe organisaties presteren in reallife digitale weerbaarheidscontext? Dan is waarschijnlijk een benadering nodig die vergelijkbaar is met raamwerk dat TNO ontwikkeld heeft voor organisaties in de financiële dienstverlening.

Al deze drie gebruiksscenario's hebben belangrijke uitdagingen gemeen. Zo doen ze niet volledig recht aan de organisatorische context waarin digitale weerbaarheid bestaat. Risicobereidheid en investeringsdrempels van de organisatie spelen bijvoorbeeld een belangrijke rol voor de digitale weerbaarheid. Een andere uitdaging is dat 'volledige' digitale weerbaarheid – of het handhaven van volledige functionaliteit in de loop van de tijd – geen statisch gegeven is. Dit kan veranderen naarmate dreigingen, eisen en verwachtingen evolueren. Bovendien hangt de effectiviteit af van het type en de kwaliteit van de informatie die organisaties bereid zijn te delen.

Implicaties voor de NCTV

Hoewel het ontwikkelen van een praktische aanpak voor het meten van digitale weerbaarheid op organisatieniveau gepaard gaat met uitdagingen – zoals het gebrek aan bewijs voor de effectiviteit van bestaande methoden, de beperkte mogelijkheden voor geautomatiseerde of kwantitatieve metingen, en twijfels bij de haalbaarheid van de ambitie om veranderingen in de mate van digitale weerbaarheid van organisaties als gevolg van beleidsinterventies te kunnen vaststellen – kan het verzamelen van aanvullende

gegevens nieuwe inzichten opleveren in specifieke aspecten van de digitale weerbaarheid van organisaties in Nederland. De NCTV kan daarbij het best stapsgewijs te werk gaan door te beginnen met het ontwikkelen van een vergelijkbare maatstaf voor een bepaald onderdeel, bijvoorbeeld het herstelvermogen van een organisatie na een cyberincident, en dit vervolgens uit te bouwen door ook andere aspecten te gaan beoordelen.

In de huidige situatie is er echter geen wettelijk mandaat voor de NCTV om organisaties te verplichten om dergelijke gegevens te verstrekken. Tegen deze achtergrond is het van belang dat de NCTV terughoudend blijft met het creëren van nieuwe rapportageverplichtingen zonder duidelijke juridische basis of beleidsnoodzaak, gezien de kosten die dit voor organisaties kan veroorzaken. Eventuele nieuwe dataverzameling zal vooral op vrijwillige basis moeten plaatsvinden. Om ervoor te zorgen dat nieuwe dataverzameling aansluit op bestaande wettelijke mechanismen, een aanvulling vormt op bestaande initiatieven en tastbare voordelen biedt, zoals bruikbare inzichten of gerichte ondersteuning, is het van belang om na te denken hoe deelname en betrokkenheid gestimuleerd kunnen worden. Ook is het belangrijk om een evenwicht te vinden tussen het type en de hoeveelheid informatie die van organisaties wordt gevraagd en hun beperkte middelen.

Een van deze bestaande mogelijkheden betreft de meldplicht onder de Cyberbeveiligingswet. Dit is de Nederlandse omzetting van de Europese NIS2-richtlijn, en biedt een kader om informatie te verzamelen over significante cyberincidenten die de continuïteit of veiligheid van zogenoemde ‘essentiële’ en ‘belangrijke’ entiteiten kunnen beïnvloeden. Deze meldingen zullen leiden tot nieuwe gegevens over de digitale weerbaarheid van organisaties, die tot dusver niet direct beschikbaar waren voor de overheid. Deze meldplicht biedt dus kansen om – voor zover wettelijk toegestaan en uitvoerbaar binnen de bestaande rapportageverplichtingen – beter inzicht te krijgen in bepaalde aspecten van digitale weerbaarheid die richting kunnen geven aan toekomstig beleid gericht op het versterken van de digitale weerbaarheid in Nederland.

Summary

Governments are becoming increasingly aware that incidents cannot always be prevented. Because of this, the term 'resilience' is being used more frequently in policy documents. Whereas in the past the focus was mainly on prevention, 'resilience' places greater emphasis on the continuity of a system even when a threat does lead to an incident. In the case of digital systems, the term 'digital resilience' or 'cyber resilience' is used. Digital resilience is of great importance, as societies and organisations are becoming increasingly dependent on technology.

Promoting the digital resilience of organisations is one of the priorities of the Dutch Cybersecurity Strategy (NLCS) 2022-2028. The aim is to minimise the identified imbalance between digital threats on the one hand and the degree of digital resilience of organisations on the other. However, there is currently no suitable resilience measure that the government can use to assess the degree of digital resilience of organisations. The lack of such information makes it difficult to determine whether resilience has actually increased, or to assess where investments and efforts have been effective and efficient.

The aim of this study was to provide insight into whether the digital resilience of Dutch organisations can be made measurable in a broadly applicable way by the National Coordinator for Security and Counterterrorism (NCTV). The hope is that, in time, it will become possible for the government to monitor changes in the degree of digital resilience of organisations, whether as a result of policy interventions aimed at increasing it or not.

This study is an exploration of the possibilities for measuring (aspects of) the digital resilience of organisations, which indicators can be used or developed for this purpose (preferably quantitative ones, in which everything with an ordinal scale is considered quantitative), and what these data can say about the state of the digital resilience of organisations. This explorative approach also means that this study does not seek to produce a detailed measurement method that the NCTV can then use. Instead, the advantages and disadvantages of different approaches are outlined, as well as the considerations that will determine the design of a possible future measurement tool.

This research is based on A) a small literature review, searching for studies focused on measuring digital resilience, B) interviews with experts, focusing on their practical experiences with measuring digital resilience, and C) internal workshops in which the findings of this research were discussed and implications analysed.

How can 'digital resilience' be defined?

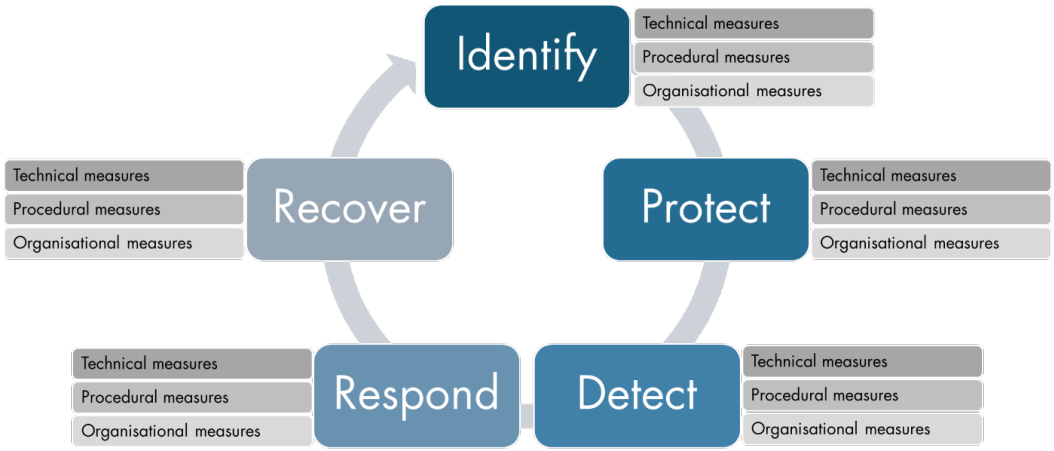
The NCTV defines digital resilience in the Dutch Cybersecurity Strategy 2022-2028 as:

> The ability to reduce relevant risks to an acceptable level by means of a set of measures to prevent cyber incidents and, if they do occur, to detect them, limit the damage and facilitate recovery. What constitutes an acceptable level of resilience is determined by a risk assessment. This can help with the selection of the right technical, procedural or organisational measures.

This definition has been taken as the starting point for this study to align with the Dutch policy environment. The Dutch government does not distinguish between 'digital resilience' and 'cyber resilience.' The latter term is also sometimes used by them, and the two terms are considered synonyms. However, there is still no clear consensus in the literature on the use and definitions of cyber and digital resilience. Some authors, for example, take a narrower view of resilience by limiting their definitions to the ability of a system to continue its functioning or to recover technically after attacks. In Dutch-language literature, the term '*veerkracht*' is also used for this narrower interpretation. However, the definitions of many other authors, as well as views in the broader field of resilience literature, are more in line with the broader view of the NCTV, in which resilience ('*weerbaarheid*') is seen as a continuous, cyclical process that includes both preventive and reactive and learning elements. This cycle is usually divided into phases such as identify, protect, detect, respond and recover, or variations thereof.

Various strategies, laws, and policy documents translate this broad concept into interventions, including technical measures (such as firewalls and backups), procedural measures (such as risk assessments and incident response plans), and organisational measures (such as training and governance). Literature and policy documents consider the phases of the resilience cycle to be interrelated sub-processes, each of which requires a combination of technical, procedural, and organisational measures.

Figure 1. The core components of digital resilience



What does the literature teach us about existing instruments for measuring the digital resilience of organisations?

Despite the increased focus on improving digital resilience, gaining insight into the degree of resilience is proving to be extremely complicated. Various technical, procedural, organisational, and external characteristics play a role. For example, technologies and threats are constantly and rapidly changing. In addition, technical systems are often too complex for people to fully understand or to test for all possible vulnerabilities in the system. There are also many aspects that play a role in digital resilience that are difficult to capture in indicators, such as the role of social relationships between employees and the workplace culture. Finally, digital processes are to a high degree connected and interdependent on processes outside of the organisation's control, meaning that incidents outside the organisation can directly affect digital resilience, e.g. through dependencies on suppliers.

Data is needed in all these areas to determine with certainty the direction in which an organisation's digital resilience is moving. There are currently no methods that provide such a complete picture. Nevertheless, methods have been developed that can be used to gain insights into aspects of the digital resilience of organisations. In this study, we identified and analysed 18 approaches. These fulfil various functions: they enable organisations to systematically monitor their development over time, identify current strengths and weaknesses, and/or pinpoint specific areas where further improvement is needed. However, only a few of these approaches cover all five aforementioned phases of digital resilience and all three types of measures. Most approaches focus on qualitative rather than quantitative indicators, emphasising descriptive assessments and subjective evaluations rather than numerical or data-driven measurement criteria. While they can provide valuable contextual insights and operational advice, they are often flexible frameworks that remain largely at a conceptual level and are applicable to organisations in different sectors and of different sizes, rather than detailed methodologies. The results are usually specific to an organisation but cannot be easily compared with the results of other organisations. Although most of these approaches do not explicitly address how unknown threats are taken into account, several instruments emphasise a proactive strategy for dealing with such uncertainties.

Little is known about the validity and reliability of these 18 approaches. No evidence proving that they accurately measure what they intend to measure or that they consistently produce meaningful results in different organisational contexts was found for any of these tools. This raises questions about the real value these frameworks offer and the extent to which they contribute to improving digital resilience. Furthermore, it is unclear which specific mechanisms would influence resilience, making it difficult to determine their effectiveness.

What do the answers to the above questions teach us about how digital resilience can be made measurable?

At present, there is no existing method readily available to generate the specific data desired to measure digital resilience. The methods identified and analysed in this study highlight the inherent trade-offs and tensions associated with conceptualising and measuring digital resilience at the organisational level. None of these methods are at the time of writing being used by a government for the purpose of measuring the

degree of digital resilience. Moreover, the methods identified are rarely used for this purpose alone. Other purposes include risk management, ensuring basic security measures, or compliance, which can indirectly contribute to a better understanding of resilience, even if that is not their primary purpose. All approaches identified in the literature have advantages and disadvantages and different strengths and weaknesses for measuring digital resilience. However, empirical data needed to test the validity of current measurement methods are lacking, making it difficult to say whether one method inherently performs better than another.

Nevertheless, the approaches analysed offer useful starting points for designing a future measurement method, depending on its ultimate purpose. If the goal is to build digital resilience at the organisational level and measure the implementation of basic digital resilience measures, the UK's Cyber Essentials program may offer a useful starting point. If the goal is to collect data and measure in more detail the readiness of organisations to identify, protect, detect, respond to, and recover from cyber incidents, then a more comprehensive assessment framework based on the NIST or ISO frameworks may be more appropriate. Finally, if the overall goal of the approach to measuring digital resilience is to collect and analyse comprehensive and sector-specific data on how organisations perform in real-life digital resilience contexts, an approach similar to the framework developed by TNO for organisations in the financial services sector is likely to be necessary.

All three of these use cases share important challenges. For example, they do not fully reflect the organisational context in which digital resilience exists. The organisation's risk appetite and investment thresholds, for example, play an important role in digital resilience. Another challenge is that ‘complete’ digital resilience – or maintaining full functionality over time – is not a static given. This can change as threats, demands, and expectations evolve. Moreover, effectiveness depends on the type and quality of information that organizations are willing to share.

Implications for the NCTV

Although developing a practical approach to measuring digital resilience at the organisational level presents challenges – such as the lack of evidence for the effectiveness of existing methods, the limited possibilities for automated or quantitative measurements, and doubts about the feasibility of the ambition to determine changes in the degree of digital resilience of organisations as a result of policy interventions - new insights into specific aspects of the digital resilience of organisations in the Netherlands could be gathered by collecting additional data. The NCTV would be best advised to proceed step by step, starting by developing a comparable benchmark for a specific component, such as an organisation's resilience after a cyber incident, and then expanding on this by assessing other aspects as well.

In the current situation, however, there is no legal mandate for the NCTV to require organisations to provide such data. Against this background, it is important that the NCTV remains cautious about creating new reporting obligations without a clear legal basis or policy necessity, given the costs this may entail for organisations. Any new data collection will primarily have to be carried out on a voluntary basis. To ensure that additional data collection complements is in line with existing legal mechanisms, existing initiatives and offers tangible benefits, such as useful insights or targeted support, it is important to consider how participation and involvement can be encouraged. It is also important to strike a balance between the type and amount of information requested from organisations and their limited resources.

One of these existing options concerns the reporting obligations under the Dutch Cybersecurity Act, which transposes the EU's NIS2 Directive. This law provides a framework for collecting information about significant cyber incidents that could affect the continuity or security of so-called 'essential' and 'important' entities. These reports will provide new data on the digital resilience of organisations that was not previously directly available to the government. Therefore, this reporting obligation offers an opportunity – to the extent permitted by law and feasible within the existing reporting obligations – to gain better insight into certain aspects of digital resilience that could guide future policy aimed at strengthening digital resilience in the Netherlands.

Inhoudsopgave

Tabellen, Figuren en Kaders

Tabellen

Figuren

Kaders

1. Introductie

1.1. Achtergrond

Bij overheden is het besef steeds verder ingedaald dat niet alle incidenten voorkomen kunnen worden. Om die reden wordt steeds vaker de term 'weerbaarheid' gebezigd in beleidsdocumenten.[1] Weerbaarheid duidt op het vermogen van een systeem om voorbereid te zijn op een ongunstige gebeurtenis of verstoring, deze te weerstaan, te absorberen en/of een nieuw evenwicht te bereiken (Nederveen et al. 2024). Waar in het verleden vooral aandacht was voor preventie, wordt met 'weerbaarheid' meer aandacht gegeven aan de continuïteit van een systeem, ook als een dreiging tóch tot een incident leidt. De maatschappij – een voorbeeld van een systeem – dient weerbaar gemaakt te worden tegen dreigingen tegen de nationale veiligheid. Dit gaat verder dan het beschermen van bijvoorbeeld kritieke infrastructuur en de bevolking. Het betreft naast het vermogen van maatschappelijke actoren om voorbereid te zijn op maatschappelijke ontwrichtende ontwikkelingen, ook capaciteiten om deze te absorberen, ervan te herstellen, en vervolgens de maatschappij aan te passen om in de toekomst beter voorbereid te zijn. Weerbaarheid is dus een cyclisch fenomeen.

Bij digitale systemen wordt er gesproken van digitale weerbaarheid of cyberweerbaarheid. De Nederlandse overheid gebruikt deze termen als synoniemen. Digitale weerbaarheid omvat cybersecurity – de bescherming van systemen en het voorkomen van cyberaanvallen – maar door de term 'weerbaarheid' te gebruiken, komt er wederom meer nadruk te liggen op de continuïteit van deze systemen wanneer incidenten zich onvermijdelijk toch zullen voordoen. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV 2022a, 9) definieert digitale weerbaarheid in Nederlandse Cybersecuritystrategie 2022-2028 als:

> Het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

Digitale weerbaarheid is van groot belang aangezien samenlevingen en organisaties steeds afhankelijker zijn van technologie. Terwijl de ontwikkelingen in digitale processen, producten, diensten en netwerken de samenleving veel hebben opgeleverd – zoals hogere arbeidsproductiviteit en efficiëntie, versimpelde

[1] Bijvoorbeeld in nationale veiligheidsstrategieën, zoals de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (NCTV 2023a), weerbaarheid actieplannen, zoals dat van het VK (Cabinet Office 2025), en in internationale fora zoals de NAVO en de G7 (NATO 2024a; NATO 2024b; The White House 2023).

administratieve processen en het toegankelijker maken van kennis – gaat de digitalisering gepaard met nieuwe dreigingen en kwetsbaarheden.

Waar bij cybersecurity de nadruk wordt gelegd op de bescherming van systemen en het voorkomen van cyberaanvallen (de 'voorkomen'-fase van weerbaarheid), wordt er met digitale weerbaarheid óók nadruk gelegd op het kunnen blijven functioneren van een organisatie en het beperken van de schade (de 'absorberen'-fase van weerbaarheid), het herstel ('herstelfase') en het leren en aanpassen wanneer een incident plaatsvindt (de 'transformatie- en adaptatiefase').

De totale schade van cyberincidenten loopt op

Cyberaanvallen op het Nederlandse bedrijfsleven zijn volgens een onderzoek van ABN Amro aan de orde van de dag: een op de vijf bedrijven rapporteerde in 2024 schade te hebben ondervonden (Krauwer 2025). De Autoriteit Persoonsgegevens stelde op basis van wettelijk verplichte datalekmeldingen vast dat in 2023 in ieder geval 178 ransomwareaanvallen hadden plaatsgevonden in Nederland (NCTV 2024a). Een van deze aanvallen leidde al tot een lek van de persoonsgegevens van ongeveer 2,5 miljoen Nederlanders (NCTV 2024a). Volgens een recent rapport van cybersecurity bedrijf Check Point Software Technologies zou het aantal cyberaanvallen in Nederland in het eerste kwartaal van 2025 met 53 procent zijn toegenomen, meer dan de gemiddelde stijging van 47 procent wereldwijd (Hoeffnagel 2025). Bedrijven lijken zich echter steeds beter te weren tegen aanvallen van buitenaf. Zo neemt volgens de Cybersecuritymonitor van het CBS (2025) het aantal cybersecurityincidenten bij bedrijven dat ten minste één type incident (uitval ICT-systeem, vernietiging data, onthulling data) heeft gehad door een aanval van buitenaf al jaren af.

Wereldwijd lijkt de (financiële) impact van cyberincidenten niettemin toe te nemen. In 2019 werden de jaarlijkse kosten van cybercriminaliteit voor de wereldeconomie geschat op €5,5 biljoen (5.500.000.000.000) door de Europese Commissie (2019), een bedrag dat volgens het Global Risks Report van het World Economic Forum (2023) zal toenemen tot $10,5 biljoen in 2025 (Murphy 2024). Desondanks laat recent onderzoek (Conradie & Kellij 2024) zien dat het aantal kleinere Nederlandse mkb-bedrijven (<10 medewerkers) dat geen enkele maatregel lijkt te nemen, is toegenomen naar een op de drie, een toename ten opzichte van 2023 toen 19 procent van de kleine bedrijven geen actie ondernam. Ook blijft de hoeveelheid meldingen die men doet van (pogingen tot) cybercrime nog heel laag omdat ondernemers, bijvoorbeeld, stellen geen schade te hebben geleden of de verwachting hebben dat een melding indienen geen concrete gevolgen heeft (Conradie & Kellij 2024).

Kortom, de veiligheid van digitale systemen van organisaties wordt steeds crucialer voor hun functioneren. Bovendien is digitale weerbaarheid essentieel voor de nationale veiligheid – zeker in tijden van toenemende hybridedreigingen en waarin steeds meer systemen met elkaar verbonden zijn (NCTV 2023b). De gevaren hierbij variëren van potentiële aantasting of verstoring van vitale infrastructuur en processen, maar kunnen ook sociale cohesie en politieke processen schaden, bijvoorbeeld door het vertrouwen in de politiek, de rechtstaat en diens instituties aan te tasten. Een van de vier pijlers van de Nederlandse Cybersecuritystrategie (NLCS) 2022-2028 is daarom het bevorderen van de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties (NCTV 2022a). De inzet is om daarbij de vastgestelde scheefgroei tussen digitale dreigingen enerzijds, en de mate van digitale weerbaarheid van organisaties anderzijds, zo klein mogelijk te maken en te houden.

Het bepalen of initiatieven gericht op het vergroten van digitale weerbaarheid doeltreffend zijn, is een complexe aangelegenheid

Ondanks de toegenomen aandacht voor het verhogen van digitale weerbaarheid blijft het inzichtelijk maken van de mate van weerbaarheid ingewikkeld. Kenmerken van de digitale ruimte die volgens Snyder et al. (2022) het meten van de technische aspecten van digitale weerbaarheid uitdagend maken, zijn bijvoorbeeld het dynamische karakter – zowel de technologieën als het bedreigingslandschap veranderen constant en in een hoog tempo, wat een grote mate van onvoorspelbaarheid voor de toekomst met zich meebrengt – en de complexiteit: veel softwaresystemen zijn te complex voor mensen om volledig te kunnen begrijpen of om te kunnen testen op alle kwetsbaarheden in het systeem.

Daarnaast zijn er organisatorische kenmerken die het digitaal weerbaar maken van organisaties verder bemoeilijken. Veel vormen van cyberaanvallen richten zich niet zozeer op het exploiteren van technologische openingen, maar op het uitbuiten van menselijke kwetsbaarheden door bijvoorbeeld informatie te vergaren via phishing (Neri et al., 2025). Digitale weerbaarheid bereiken met louter technologische middelen is volgens verschillende auteurs (Neri et al, 2025; Grøtan et al. 2022; Baskerville et al. 2014) bijgevolg niet mogelijk en moet altijd aangevuld worden met organisatorische aspecten. Organisatorische factoren bestaan uit een reeks kenmerken van een organisatie die invloed hebben op de werkplek, zoals de structuur van een organisatie, het beleid binnen de organisatie, sociale relaties en communicatie, besluitvormingsprocessen, kennis en vaardigheden van werknemers, werkcultuur en vele andere elementen (Bagheri et al., 2023; Goodman & Haisley 2007). Dit maakt digitale weerbaarheid een veelzijdig en complex concept waarbij veel aspecten betrokken zijn.

Doordat digitale processen in hoge mate met elkaar verbonden en verweven zijn, vormen zij gezamenlijk een digitaal ecosysteem waarbij incidenten in een deel van dit systeem kunnen doorwerken naar andere organisaties (NCTV 2024a). Het grote aantal actoren dat verantwoordelijkheid draagt voor digitale weerbaarheid bemoeilijkt dit verder. Ook de verbondenheid van risico's speelt hierin mee. Zo staan digitale risico's niet op zichzelf maar worden ze beïnvloed door vele verschillende factoren. Verschillende situaties kunnen een potentieel gevaar vormen voor de nationale veiligheid en digitale weerbaarheid van de samenleving. Denk hierbij aan aanvallen op toeleveranciers die vervolgens problemen opleveren voor andere bedrijven in de keten of denk aan situaties waarin gegevens van burgers verhandeld worden en vervolgens misbruikt worden door kwaadwillenden, maar ook een tekort aan cybersecuritydeskundigen kan tot grote risico's leiden (NCTV 2024a). Gezamenlijk kunnen deze factoren leiden tot cascade-effecten, waarbij kleine gaten in digitale weerbaarheid bij organisaties kunnen leiden tot problemen die vele malen groter zijn in omvang zoals, in extreme gevallen, de uitval van vitale infrastructuur (Panda & Bower 2020; Pescaroli et al. 2018).

Deze verbondenheid zorgt er ook voor dat steeds meer mensen betrokken moeten worden bij het digitaal weerbaar maken van organisaties en de samenleving. In vrijwel iedere organisatie werken mensen met digitale middelen en dragen zij een gedeelde verantwoordelijkheid voor het beschermen van de digitale systemen van hun organisatie, aangezien hackers ook via hen toegang kunnen krijgen tot organisatiebrede systemen.

De overheid hanteert (nog) geen coherente aanpak voor het meten van digitale weerbaarheid

Het belang van digitale weerbaarheid is herhaaldelijk benadrukt in het overheidsbeleid van de afgelopen jaren, bijvoorbeeld in de Nederlandse Cybersecuritystrategie 2022-2028 (NCTV 2022a) en de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (NCTV 2023a). Daarnaast zijn er verschillende initiatieven opgezet zoals het Cyberweerbaarheidsnetwerk (NCTV 2024c) waarin ook best practices voor digitale weerbaarheid worden geïdentificeerd. Echter, er wordt geen weerbaarheidsmaat gehanteerd waaraan de overheid de digitale weerbaarheid van organisaties kan aflezen. Door het gebrek aan dergelijke informatie is het lastig om vast te stellen of de weerbaarheid daadwerkelijk is toegenomen, en op welke wijze en ten aanzien van welke aspecten. Hierdoor blijft de asymmetrie tussen de dreiging en digitale weerbaarheid alomtegenwoordig en slecht begrepen (Jansen 2023). Daarnaast maakt het gebrek aan concrete inzichten in de mate van weerbaarheid, zowel binnen Nederlandse organisaties als binnen de samenleving in zijn geheel, het moeilijk om te beoordelen waar investeringen en inspanningen effectief zijn geweest, evenals het destilleren van goede praktijken die kunnen worden gerepliceerd en om de kosten en effectiviteit van verschillende benaderingen met elkaar te vergelijken.

Uit onderzoek voor het WODC uit 2021 bleek al dat cybersecuritybeleid zeer moeilijk meetbaar te maken is – vooral in termen van doelbereik en effectiviteit – door, onder andere, het ontbreken van duidelijke termijnen, normen en referentiepunten (Brennenraedts et al. 2021). Tevens werd de praktische haalbaarheid van het verkrijgen en verwerken van de benodigde data in twijfel getrokken. De onderzoekers benoemen hierbij dat er vaak grote methodologische uitdagingen liggen in het aantonen van causale relaties in een beleidscontext vanwege de complexiteit van de context waarin beleid wordt uitgevoerd waardoor het vaak lastig is om één dimensie te isoleren.

Vervolgonderzoek uit 2023 heeft ook aangetoond dat hoewel veel concrete voorstellen voor activiteiten van de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) goed meetbaar zijn, de meetbaarheid van de beleidsimpact of beleidseffecten nog moet worden uitgewerkt om deze operationeel bruikbaar te maken in evaluaties (Driesse et al. 2024: 106). Tabel 1 toont de generieke meetinstrumenten die in deze nulmeting van de NLCS worden opgesomd voor Pijler 1 (‘Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties’). Deze zouden volgens de auteurs gebruikt kunnen worden om ontwikkelingen in de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties in kaart te brengen en om te helpen bij contextualisering en strategische keuzes en prioritering (Driesse et al. 2024). Tegelijkertijd erkennen zij dat deze indicatoren geen uitspraken opleveren over de impact van de NLCS. Deze indicatoren kunnen weliswaar indicaties geven van de digitale weerbaarheid van de samenleving, maar voor het meten van digitale weerbaarheid van organisaties levert het weinig data op. De indicatoren liggen namelijk niet op het organisatieniveau (bijvoorbeeld ‘het aantal cyberincidenten in Nederland’). Daarnaast ontbreekt een gedeeld begrip van digitale weerbaarheid, en is het een incompleet en inconsistent overzicht.

Tabel 1. Bestaande generieke meetinstrumenten digitale weerbaarheid genoemd in de NLCS-nulmeting

Meetinstrument	Relevante indicator(s)
Basisbeveiliging.nl van de Internet Cleanup Foundation	• Aantal organisaties & ministeries dat slaagt voor de uitgevoerde beveiligingstesten
Cybersecuritybeeld Nederland van de NCTV	• Aantal cyberincidenten in Nederland
Cybersecuritymonitor van het CBS	• Percentage genomen cybersecuritymaatregelen door bedrijven • ICT-veiligheidsincidenten • Aantal ransomware- en DDoS-aanvallen op Nederlandse organisaties
Nationaal Cybersecurity Bewustzijnsonderzoek van Alert Online (NCTV)	• Mate waarin Nederlanders/overheden/bedrijven zich zorgen maken over een cyberaanval • Gemiddelde cijfer dat Nederlanders/overheden/ bedrijven zichzelf geven voor het veilig omgaan met onlinerisico's
Het samenhangend inspectiebeeld cybersecurity vitale processen, een samenwerking van verschillende overheidsdepartementen	• Aantal cybersecurity-incidenten gerapporteerd aan de toezichthouders die de drempelwaarde overschrijden

Bron: Driesse et al. 2024, 106.

Hoewel er nog geen geïntegreerde, samenhangende, samenlevingsbrede aanpak is voor het meten van weerbaarheid, zijn er wel instrumenten ontwikkeld die aspecten van digitale weerbaarheid deels in kaart brengen binnen bijvoorbeeld overheidsorganisaties. Zo heeft de Tweede Kamer onlangs ingestemd met een voorstel om binnen de overheid aan de slag te gaan met een gestandaardiseerde vorm van penetratietesten, zoals de Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW). Deze gestandaarde methodiek heeft als doel het vergroten van de controle op de zogenoemde pentest-opdrachten aangezien deze methodiek voorzienbare beveiligingsfouten die momenteel nog over het hoofd worden gezien, beter kan aanpakken door een auditor toe te voegen die controleert of dit proces goed is doorlopen (Van Trigt 2024). In Annex A wordt een reeks andere relevante initiatieven ter versterking van de digitale weerbaarheid van Nederlandse organisaties besproken.

Niettemin zijn consistente en gestandaardiseerde ‘meetlatten’ voor digitale weerbaarheid in organisaties nodig om inzicht te krijgen in veranderingen in de mate van weerbaarheid, en om uiteindelijk de effecten van initiatieven te kunnen beoordelen en te kunnen vaststellen of de doelstellingen van de NLCS bereikt zijn. Een gedeeld begrip van de indicatoren van digitale weerbaarheid zou organisaties beter in staat moeten stellen om hun tijd en middelen effectiever te investeren en vast te stellen waar die investering al dan niet succesvol is geweest in het verbeteren van hun weerbaarheid. Bovendien zou het de Nederlandse overheid in staat kunnen stellen om een beter beeld te krijgen van hoe het met de bredere digitale weerbaarheid

gesteld is onder Nederlandse organisaties en zo te begrijpen waar aanvullende maatregelen nodig kunnen zijn.

1.2. Doelstelling en onderzoeksvragen

Het doel van dit onderzoek is inzichtelijk te maken of, en zo ja hoe en onder welke randvoorwaarden, de NCTV de digitale weerbaarheid van Nederlandse organisaties meetbaar kan maken op een breed toepasbare manier. De hoop is dat het op den duur mogelijk wordt voor de overheid om veranderingen in de mate van digitale weerbaarheid van organisaties te kunnen volgen, al dan niet als gevolg van beleidsinterventies gericht op de verhoging ervan.

Vooraf werd geen onderscheid gemaakt naar grootte, sector of type organisatie. Ook werden er geen specifieke eisen gesteld aan welke informatie een meetmethode zou moeten opleveren, welke middelen er mogelijk beschikbaar voor gemaakt kunnen worden en wie een meting uiteindelijk zou moeten gaan uitvoeren. Ook hebben we ons niet beperkt tot aspecten van digitale weerbaarheid waarvoor de NCTV reeds een rechtsgrondslag heeft om organisaties te verplichten deze te verstrekken. De voorliggende vraag is in eerste instantie namelijk: welke relevante gegevens zouden verzameld kunnen worden? Het onderzoek heeft dus een sterk verkennende aard: de focus ligt op het verkennen van de mogelijkheden voor het ontwikkelen van een meetinstrument op basis van bestaande of te ontwikkelen kwantitatieve indicatoren voor aspecten van digitale weerbaarheid van organisaties, en in hoeverre een dergelijk instrument iets kan zeggen over de staat van de digitale weerbaarheid van organisaties. Deze open insteek betekent ook dat dit onderzoek niet is gericht op het opleveren van een uitgewerkte meetmethode waar de NCTV vervolgens mee aan de slag kan gaan. In plaats daarvan zullen we de voor- en nadelen uiteenzetten van verschillende benaderingen, en zullen we de overwegingen toelichten die bepalend zullen zijn voor de opzet van een mogelijk toekomstig meetinstrument. Tabel 2 toont de onderzoeksvragen en deelvragen die centraal staan in dit onderzoek.

Tabel 2. Onderzoeksvragen

1.	**Hoe kan 'digitale weerbaarheid' worden afgebakend?**
1.1.	Wat wordt in bestaande wetenschappelijke en grijze literatuur verstaan onder digitale weerbaarheid?
1.2.	Wat zijn de kernelementen van digitale weerbaarheid en hoe worden deze in het Nederlandse cybersecuritybeleid nader uitgewerkt?
2.	**Wat leert de literatuur over bestaande meetinstrumenten van digitale weerbaarheid van organisaties?**
2.1.	Op welke elementen van digitale weerbaarheid hebben deze instrumenten betrekking?
2.2.	Op welke wijze wordt in bestaande meetinstrumenten rekening gehouden met nog niet gekende dreigingen?[2]
2.3.	Wat is er bekend over de validiteit en betrouwbaarheid van bestaande meetinstrumenten van digitale weerbaarheid?
2.4.	Zijn er elementen van weerbaarheid die ontbreken in bestaande instrumenten voor het meten van de digitale weerbaarheid in Nederland?
3.	**Wat leert de beantwoording van bovenstaande vragen over de wijze waarop digitale weerbaarheid meetbaar kan worden gemaakt?**
3.1.	Welk type uitspraken[3] wordt mogelijk geacht bij de wijze waarop digitale weerbaarheid meetbaar kan worden gemaakt?
3.2.	Welke randvoorwaarden kunnen worden onderscheiden bij het meten van digitale weerbaarheid?
3.3.	Hoe vertalen deze bevindingen zich naar een praktisch meetinstrument dat periodiek inzicht kan bieden in de digitale weerbaarheid binnen verschillende organisaties in Nederland?

Om de bruikbaarheid van de bevindingen te optimaliseren, is er vanuit de opdrachtgever gevraagd om de definitie van 'digitale weerbaarheid' van de NCTV te hanteren. Onderzoeksvraag 1 is dus voornamelijk bedoeld ter contextualisering van het onderzoek en om de kernelementen van digitale weerbaarheid in kaart te brengen.

[2] Om Nederland digitaal veilig te maken, richt de NCTV zich op het identificeren en duiden van dreigingen en risico's, waaronder nog niet gekende dreigingen. Voor de NCTV houdt een meetinstrument dus idealiter ook rekening met nog niet gekende dreigingen.

[3] Bijvoorbeeld: 'de digitale weerbaarheid van organisatie X is met Y% gestegen ten opzichte van een vorige meting', of 'organisatie X scoort 'groen' op digitale weerbaarheidsaspect Y'.

1.3. Methodologie

In dit onderzoek zijn verschillende methoden toegepast: een literatuuronderzoek (Paragraaf 1.3.1), interviews met deskundigen (Paragraaf 1.3.2) en interne workshops waarin de bevindingen van dit onderzoek werden besproken en bediscussieerd om nader tot een praktisch meetinstrument te komen.

1.3.1. Literatuurstudie

We hebben Engelstalige gestructureerde zoekopdrachten uitgevoerd op Google Scholar voor resultaten vanuit de periode 2019-2024, met behulp van de zoektermen die in Tabel 3 zijn weergegeven. Google Scholar verzamelt een breed scala aan onderzoeken uit academische tijdschriften en daarbuiten, waardoor er een uitgebreid overzicht van de beschikbare literatuur wordt geboden.

We besloten ons te beperken tot literatuur uit de afgelopen vijf jaar (2019 tot januari 2025) om te voorkomen dat we ons zouden baseren op verouderde methoden in dit snel veranderende vakgebied dat voortdurend wordt bijgewerkt en herzien. Zo duurt het vaak lang, soms meerdere jaren, voordat de effecten van beleids- en wetswijzigingen duidelijk worden. Methoden die voor 2019 ontwikkeld zijn en nog steeds van waarde zijn, konden daarnaast ofwel genoemd worden in recentere literatuur, ofwel door geconsulteerde deskundigen aangedragen worden. Daarnaast hebben we expliciet raamwerken opgenomen van buiten de zoekresultaten wanneer deze prominent in de literatuur werden genoemd of door collega's werden voorgesteld en in overeenstemming waren met de reikwijdte van het onderzoek.

De eerste zoekopdracht, zoals te zien in Tabel 3 hieronder, leverde een breed scala aan resultaten op die nuttig waren voor theoretische inzichten, maar niet specifiek gericht waren op de metrische en organisatorische aspecten van cyberweerbaarheid. De resultaten van de vierde zoekopdracht, daarentegen, waren uitgebreider en brachten deze bronnen aan het licht die ontbraken bij eerdere zoekopdrachten.

Hoewel de eerste 100 resultaten per zoekopdracht gescreend zijn op relevantie voor het onderzoek op basis van de titel en abstract, las het onderzoeksteam in totaal 18 bronnen volledig vanwege hun hoge relevantie voor het onderzoek. Dit waren voornamelijk wetenschappelijke artikelen (16) en rapporten (2). Nadat er 4 toch niet bruikbaar bleken, bleven er uiteindelijk 14 over voor de analyse van dit onderzoek. Een laatste aanpassing van de zoekopdracht, waarbij het deel (digital OR cyber) AND (resilience) vervangen werd door (digital resilience OR cyber resilience OR information resilience) leverde nog 4 extra relevante resultaten op. Uiteindelijk zijn er dus 18 resultaten geselecteerd die in dit rapport besproken zullen worden. Om voor elk geïdentificeerd raamwerk evaluaties te vinden over de respectieve validiteit en betrouwbaarheid ervan, hebben we ten slotte enkele simpele zoekopdrachten uitgevoerd op Google. De gebruikte zoekterm was "[naam van het raamwerk]" AND (validity OR reliability) AND evaluation.

Tabel 3. Zoekopdrachten

Zoekopdracht	Database	Periode
1. (digital OR cyber) AND (resilience) AND (measure* OR indicator OR metric* OR assess* OR estimat* OR quantif* OR evaluat*)	Google Scholar	2019-2024
2. (organisational) AND (digital OR cyber) AND (resilience) AND (measur* OR address* OR evaluat* OR indicator* OR metric* OR assess* OR framework*)	Google Scholar	2019-2024
3. (organisation*) AND (digital OR cyber) AND (resilience) AND (measur* OR address* OR evaluat* OR indicator* OR metric* OR assess* OR framework*)	Google Scholar	2019-2024
4. (cyber) AND (security) AND (maturity model* OR maturity framework*) AND (valid*) AND (reliab*)	Google Scholar	2019-2024
5. (organisation* OR organization*) AND (digital OR cyber) AND (resilience) AND (measur* OR address* OR evaluat* OR indicator* OR metric* OR assess* OR framework*) AND (valid*) AND (reliab*)	Google Scholar	2019-2024
6. (organisation* OR organization*) AND (digital OR cyber) AND (resilience) AND (element* OR sector*) AND (measur* OR address* OR evaluat* OR indicator* OR metric* OR assess* OR framework*) AND (valid*) AND (reliab*)	Google Scholar	2019-2024

Voor een optimale inzet van de beschikbare middelen, is de literatuurstudie binnen dit onderzoek bewust nauw begrensd. Deze aanpak heeft een aantal beperkingen: dat we ons hebben beperkt tot één academische database (Google Scholar), we hebben alleen gezocht op organisaties en niet op andere termen als 'bedrijven', 'firms', 'companies' of 'businesses', we hebben niet expliciet gezocht op literatuur die gericht is op specifieke aspecten van digitale weerbaarheid zoals gedrag en governance, en we sluiten mogelijk interessante meetmethoden van buiten het veld uit. Met de uitgevoerde zoekopdrachten en de consultaties van de geïnterviewde deskundigen, de begeleidingscommissie en onze collega's, beoogden wij niettemin de voornaamste methoden te identificeren.

1.3.2. Interviews

Tijdens dit onderzoek zijn acht interviews uitgevoerd met academische en praktijkexperts op het gebied van digitale weerbaarheid uit verschillende sectoren. Deze interviews waren semigestructureerd rondom de interviewvragen. De specifieke expertise en ervaringen van de deskundigen waren leidend voor het gesprek, maar er werd ook gevraagd naar hun interpretatie van digitale weerbaarheid, hun ervaringen met het meten van (aspecten) van digitale weerbaarheid, inclusief de wijzen waarop en welke informatie het hun oplevert, en hun reacties op en ideeën voor het ontwikkelen van een meetinstrument voor de NCTV. De interviews hadden dus verschillende doelen. Ze zijn ingezet om nieuwe literatuur en instrumenten te vinden die niet in de literatuurstudie geïdentificeerd werden. Daarnaast zijn ze gebruikt om voorlopige bevindingen te valideren en potentiële oplossingen/ideeën te bespreken. In overeenstemming met de begeleidingscommissie is besloten om vooral deskundigen te benaderen met praktische ervaring en expertise over het versterken en monitoren van digitale weerbaarheid binnen organisaties, zoals Chief Information Security Officers

(CISO's). De aantekeningen die tijdens de interviews zijn gemaakt, zijn verwerkt in de analyse in de komende hoofdstukken. In bronvermeldingen zijn de interviews willekeurig genummerd.

Tabel 4. Lijst met geïnterviewden

Beems, Karin	Teamleider Keurmerken, Centrum voor Criminaliteitspreventie en Veiligheid
Bernard, Vaisha	Chief Hacker, Eye Security
Boshuizen, Godfried	CISO, Mourik B.V.
De Jong, Arjan	Specialistisch Inspecteur, Rijksinspectie Digitale Infrastructuur (RDI)
Koeroo, Oscar	CISO, Ministerie van Volksgezondheid, Welzijn en Sport
Slot, Raymond	Lector Cybersecurity, Hogeschool Utrecht
Wissink, Wouter	Senior Principal Cyber Engineer, Verbond van Verzekeraars
Anoniem	CISO bij een Nederlandse universiteit

1.4. Leeswijzer

Hoofdstuk 2 schetst een beeld van hoe het begrip digitale weerbaarheid gebruikt wordt in academische en grijze literatuur, hoe de term gehanteerd wordt en uitgewerkt is in het Nederlandse beleid, en uit welke kernonderdelen het begrip bestaat. In lijn met de definitie van de NCTV onderscheiden we vijf verschillende fasen van digitale weerbaarheid. Verschillende strategieën, wetten en beleidsdocumenten vertalen dit brede concept naar interventies, waaronder technische maatregelen (zoals firewalls en back-ups), procedurele maatregelen (zoals risicobeoordelingen en incidentresponsplannen) en organisatorische maatregelen (zoals training en governance).

Hoofdstuk 3 biedt een overzicht van bestaande benaderingen om (bepaalde kernonderdelen van) digitale weerbaarheid in kaart te brengen. Hierbij zullen de deelvragen onder onderzoeksvraag 2 de rode lijn vormen door verder in te gaan op de wijze waarop deze instrumenten van elkaar verschillen, welke kernonderdelen wel en niet worden meegenomen, en wat er bekend is over de validiteit en betrouwbaarheid van deze instrumenten. Na een individuele analyse van iedere benadering zetten we uiteen welke lessen getrokken kunnen worden uit de literatuur over het meetbaar maken van digitale weerbaarheid.

Ten slotte richt **Hoofdstuk 4** zich op de mogelijkheden voor het meetbaar maken van aspecten van digitale weerbaarheid door de NCTV, en de implicaties en beperkingen hiervan.

2. Gebruik en afbakening van de term 'digitale weerbaarheid'

Dit hoofdstuk zet uiteen wat er verstaan wordt onder digitale weerbaarheid in zowel wetenschappelijke als grijze literatuur (Paragraaf 2.1) als in de Nederlandse beleidscontext (Paragraaf 2.2). We nemen de definitie van digitale weerbaarheid van de NCTV en het gebruik van het begrip in het beleid als uitgangspunt voor dit onderzoek om zoveel mogelijk aan te sluiten bij de Nederlandse beleidsomgeving. Paragraaf 2.3, ten slotte, geeft een overzicht van de kernelementen van digitale weerbaarheid van organisaties. In Hoofdstuk 3 analyseren we in hoeverre de bestaande methoden die digitale weerbaarheid van organisaties meten deze kernonderdelen afdekken.

2.1. Definities van digitale weerbaarheid

Zoals reeds aangehaald definieert de NCTV (2022a, 9) digitale weerbaarheid als:

> Het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging. Die risico-afweging kan helpen om de juiste technische, procedurele of organisatorische maatregelen te kiezen.

Hoewel in de Nederlandse beleidscontext er redelijk consequent gesproken wordt over 'digitale weerbaarheid', wordt ook in bepaalde gevallen 'cyberweerbaarheid' gebruikt.[4] Ook in de communicatie naar burgers en organisaties wordt er gesproken over zowel cyberweerbaarheid, met bijvoorbeeld de Tool Cyberweerbaarheid van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV 2025), en digitale weerbaarheid, bijvoorbeeld de vijf basisprincipes van digitale weerbaarheid opgezet door het Nationaal Cyber Security Centrum (NCSC 2025) (de basisprincipes worden verder toegelicht in Annex A.2). De Nederlandse overheid gebruikt de termen dus als synoniemen.

Bij het onderzoeken van het concept van digitale weerbaarheid vonden we in de wetenschappelijke literatuur een reeks definities en beschrijvingen van 'cyberweerbaarheid' (*cyber resilience*) en 'digitale weerbaarheid' (*digital resilience*). Tabel 5 geeft een illustratie van de conceptualisering van digitale- en cyberweerbaarheid in zowel academische als toegepaste contexten. Op deze manier ontstaat een beeld van wat er onder 'digitale weerbaarheid' verstaan wordt, en uit welke kernonderdelen het bestaat. Dit is geen uitputtende lijst van

[4] Ook binnen NCTV-rapporten, met name wanneer er gesproken wordt over initiatieven van andere organisaties. Zie bijvoorbeeld *Voortgangsrapportage 2024 Nederlandse Cybersecuritystrategie* (NCTV 2024b, 10, 14, 19, 23, 24 & 27).

definities of beschrijvingen van het concept, noch hebben we gezocht op andere termen dan digitale of cyberweerbaarheid. Er volgt dus geen analyse van termen als 'cybersecurity' en 'information security' die voor de opkomst van de term 'weerbaarheid' gebruikt werden om eenzelfde fenomeen te duiden.

Tabel 5. Definities van digitale- en cyberweerbaarheid

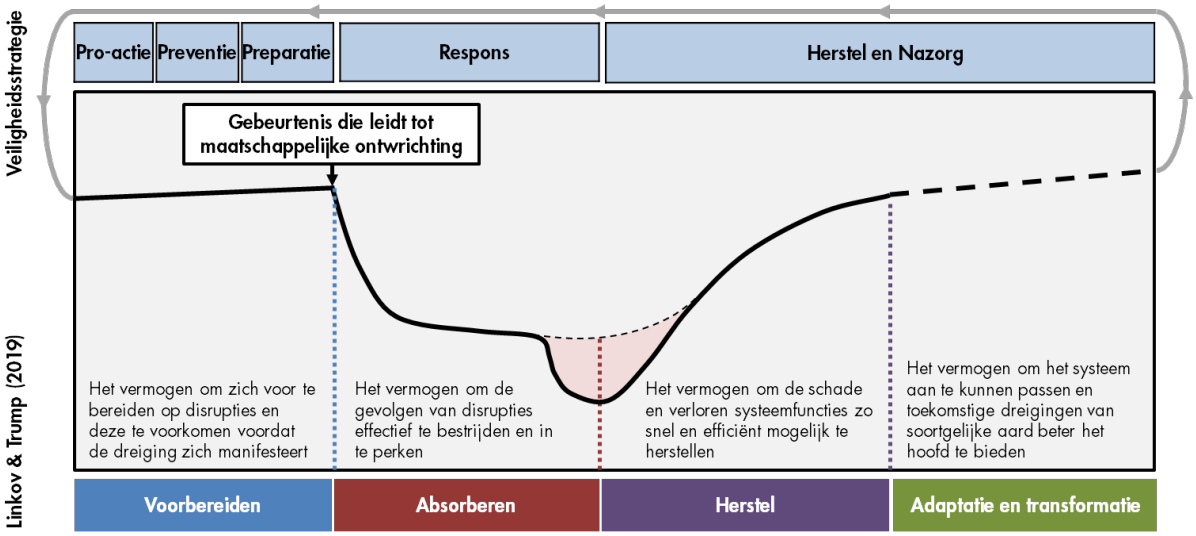
Definitie	**Bron**
'Resilience includes the ability to resist and recover from intentional attacks, accidents, threats and natural disasters. Cyber resilience requires the integration of the risk management process and the resilience management process. Risk management selects and prioritizes potential measures to prevent or mitigate impacts, whereas resilience seeks to improve the system's inherent ability to respond to inevitable changes, both long and short, thus adopting a time perspective.'	Annarelli et al. 2020, 3
'Cyber resilience (or resiliency) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. Cyber resiliency can be a capability of a system, a system-of-systems, a mission, a business function, an organisation, or a cross-organisational mission; the term can also be applied to an individual, household, group, region, or nation.'	Bodeau & Graubart 2016, 1
[Cyber] 'resilience is broader in scope and "is essential when risk is incomputable, such as when hazardous conditions are a complete surprise or when the risk analytic paradigm has been proven ineffective". Resilience takes over from risk management when the latter has been ineffective at shielding an organisation from disruptive threats and implies a constant cycle of activities and responses––starting well ahead of an adverse event and concluding well after the event has ended—to implement the adaptive measures needed to counter the next unpredictable shock.'	Dupont 2019, 1
'Digital (i.e. cyber) resilience in healthcare is considered as an expansion of higher order/institutional resilience. In other words, the exploration of digital resilience should reflect the increasing scope of digitalisation as a primary enabler (and respectively, a vulnerability vector) for healthcare system performance.'	Garcia-Perez et al. 2023, 3
'The ability of a process, business, organisation, or nation to anticipate, withstand, recover, and evolve in order to improve their capabilities in face of adverse conditions, stress, or attacks to the cyber resources it needs to function.'	INCIBE, 2019 in Carías et al. 2020, 2
'Cyber resilience has recently emerged as a strategy that complements security efforts and contributes to cyber risk management. In the event of an attack, cyber resilience efforts aim to ensure essential operations; maintain critical function levels; and rapidly recover. Given that it is impossible to guarantee a network can never be penetrated, cyber resilience efforts frequently do not focus on whether an attack can happen and instead focus on how to react when they do occur.'	Jacobs et al. 2018, p.38

Definitie	Bron
'Cyber resilience refers to the ability of systems to resist and recover from, or adapt to, a cyber compromise. The ability to restore a system's functionality after a cyber-compromise is important for a broad range of systems. Cyber resilience is focused on recovery.'	Kott & Linkov 2021, 81
'The concept of the [digital] resilience of the digital platform ecosystem has been developed to cope with exogenous shocks and become resistant to future disruptions.'	Mehedintu & Soava 2022, 6
'Despite slight variations in definitions, the concept of cyber resilience remains vital as the ability of a system to defend against cyberattack incidents, maintain critical functionality, and restore the quality of services to pre-incident levels. Overall, the main aim of cyber resiliency can be defined as the ability of the organisation to prepare, defend, recover, adapt, and learn from cyber events.'	Munusamy & Khodadadi 2023, 61
'A cyber system's ability to function properly and securely despite disruptions to that system. Disruptions can be cyber or physical; they can also be intentional, accidental, or random.'	Vugrin & Turgeon 2015, p.76

Sommige opvattingen van weerbaarheid zijn beperkt tot het vermogen van een systeem om te blijven functioneren of te herstellen na aanvallen, terwijl andere auteurs ook het verdedigen tegen aanvallen of het beperken daarvan meenemen in hun definitie. In de Nederlandstalige literatuur wordt voor de engere opvatting ook wel de term 'veerkracht' gebruikt. Deze term gebruiken wij niet in deze rapportage omdat de term 'weerbaarheid' breder opgevat wordt: het omvat het vermogen van een samenleving om schokken en verstoringen te absorberen, zich aan te passen en te herstellen (veerkracht), maar ook de preventieve component: proberen de impact van dreigingen te verkleinen voordat ze zich voordoen (Nederveen et al. 2024). Bovendien volgen wij de terminologie van de NCTV, die consistent het begrip weerbaarheid gebruikt.

Uit de omschrijvingen in Tabel 2 blijkt dat er onder professionals en in de literatuur nog geen duidelijke consensus bestaat over het gebruik en de definities van 'cyberweerbaarheid' en 'digitale weerbaarheid'. Terwijl de NCTV risicobeoordeling als een integraal onderdeel van digitale weerbaarheid beschouwt, wordt dit door enkele auteurs eerder als een extern, ondersteunend proces gezien die weerbaarheidsstrategieën mogelijk maakt en onderbouwt (Jacobs et al. 2018; Dupont, 2019). Sommige auteurs zijn nóg restrictiever en beschouwen digitale weerbaarheid als uitsluitend gericht op het reageren op en herstellen van cyberincidenten (Kott & Linkov, 2021). Niettemin sluiten de meeste auteurs zich aan bij de bredere zienswijze van de NCTV, waarbij aandacht uitgaat naar de volledige levenscyclus van een incident, met maatregelen vóór (de 'koude' fase), tijdens en na een incident (de 'warme' fase) (Annarelli et al. 2020, Bodeau & Graubart 2016, Garcia-Perez et al., 2023, INCIBE 2019 in Carías et al. 2020, Mehedintu & Soava 2022, Munusamy & Khodadadi 2023, Vugrin & Turgeon 2015). Hierin komen alle fasen in de cyclus die doorgaans worden onderscheiden in literatuur over weerbaarheid in het algemeen terug: 1) Voorbereiden/Anticiperen, 2) Absorberen, 3) Herstel en 4) Adaptatie en Transformatie. Figuur 2 toont hiervan een voorbeeld gebaseerd op Linkov & Trump (2019) uit een eerder WODC-onderzoek naar het meten van maatschappelijke weerbaarheid.

Figuur 2. Conceptualisering van weerbaarheidsfasen in literatuur en de Veiligheidsstrategie



Bron: Nederveen et al. (2024).

In literatuur over digitale weerbaarheid worden daarbij vaak variaties gebruikt die specifieker zijn voor het digitale domein, zoals de fasen in het NIST-raamwerk[5]: 1) Herkennen, 2) Beschermen, 3) Detecteren, 4) Reageren, en 5) Herstellen. In de definitie van de NCTV worden daarnaast drie categorieën van maatregelen genoemd op basis waarvan de digitale weerbaarheid in de verschillende fasen of ten aanzien van verschillende capaciteiten versterkt kan worden:

1. **Technische maatregelen**, zoals anti-malware en anti-tampersoftware, onderhoud van software, applicatiebeveiliging, en het isoleren van geïnfecteerde systemen (zowel preventief als reactief). Dergelijke maatregelen zijn gericht op het versterken van onder andere de integriteit, betrouwbaarheid, beschikbaarheid en veiligheid van informatiesystemen. Ook het uitvoeren van penetratietesten en cyber-wargaming vallen hieronder.
2. **Procedurele maatregelen**, zoals procedures rond het identificeren, mitigeren, monitoren en evalueren van risico's: risicobeoordelingen, risicobeperking, continue monitoring, feedbackloops en incidentresponseplannen; evenals identiteits- en toegangsbeheer, rapportageprotocollen en businesscontinuitymanagement.
3. **Organisatorische maatregelen**, zoals de inzet van middelen, training van personeel, management van toeleveringsketens, organisatiestructuren, en verantwoordelijkheden en leiderschap. De sector waarin een organisatie actief is, speelt hierbij een belangrijke rol.

Een kanttekening hierbij is dat de te nemen maatregelen divers van aard zijn, en zich niet altijd gemakkelijk laten indelen in een van deze drie categorieën, of beperkt kunnen worden tot een van eerdergenoemde fasen.

2.2. Digitale weerb14aarheid in het Nederlandse cybersecuritybeleid

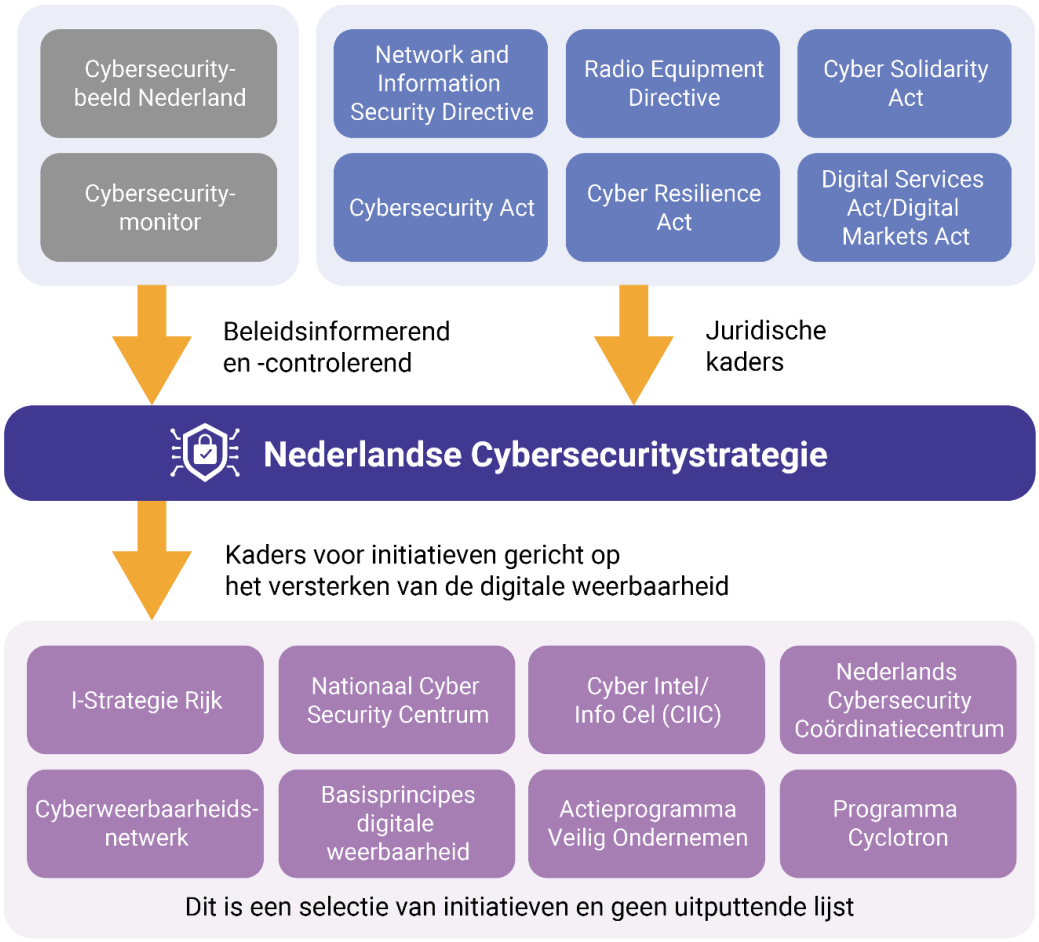
Er zijn veel verschillende initiatieven en wetgevende stukken die relevant zijn voor digitale weerbaarheid van Nederlandse organisaties. Het grootste deel van de wetgevende stukken die hierbij belangrijk zijn,

[5] Zie: https://www.nist.gov/cyberframework

bestaan uit Europese wet- en regelgeving, terwijl de meeste initiatieven een nationale focus hebben binnen Nederland. In dit deel onderzoeken we hoe de term 'digitale weerbaarheid' wordt toegepast in een aantal van deze beleidsstukken en initiatieven en we analyseren wat eronder wordt verstaan, welke eisen er worden gesteld, welke maatregelen worden gestimuleerd, en wat dit alles ons leert over hoe deze aspecten van digitale weerbaarheid gemeten kunnen worden.

De Cybersecuritystrategie is het overkoepelende beleidsstuk op dit terrein van de Nederlandse beleidscontext. Figuur 3 geeft een grafische weergave van hoe de verschillende stukken en initiatieven zich tot de NLCS verhouden. De grijze vlakken linksboven tonen documenten die een informerende en controlerende functie hebben voor het beleid rondom digitale weerbaarheid. De blauwe vlakken rechtsboven tonen de Europese verordeningen en richtlijnen die tezamen het juridische kader vormen voor het Nederlandse digitale weerbaarheidsbeleid. De belangrijkste hiervan in de context van digitale weerbaarheid van organisaties is de *Network and Information Security* (NIS2)-richtlijn, die in de Nederlandse wetgeving getransponeerd zal worden als de Cyberbeveiligingswet (Cbw). De paarse vlakken onder de strategie tonen enkele van de vele, uiteenlopende 'initiatieven' die zijn opgezet om digitale weerbaarheid te vergroten in verschillende ketens, branches of regio's.

Figuur 3. Visualisatie van hoe 'digitale weerbaarheid' vorm krijgt in de Nederlandse beleidscontext



Bron: RAND Europe analyse van de beleidscontext.

In Annex A worden de stukken en initiatieven genoemd in Figuur 3 in detail besproken en analyseren we wat zij betekenen voor de digitale weerbaarheid van organisaties. Hieruit blijkt dat de Nederlandse beleidscontext rondom digitale weerbaarheid wordt gekenmerkt door een combinatie van strategische doelstellingen, juridische kaders en een breed scala aan initiatieven.

De NLCS formuleert algemene doelen, zoals het vergroten van inzicht in digitale dreigingen, het stimuleren van beschermende maatregelen en het bevorderen van adequate reactie(s) op incidenten. De nadruk ligt hierbij op publiek-private samenwerking, informatie-uitwisseling en het versterken van organisatorische en procedurele maatregelen. In het Actieplan van de NLCS zijn vervolgens concrete uitvoeringsstappen uitgewerkt. De juridische kaders, vooral bestaande uit Europese wet- en regelgeving, stellen minimumeisen aan cybersecurity voor vitale sectoren en verplichten organisaties tot het nemen van passende technische en organisatorische maatregelen, het uitvoeren van risicoanalyses en het melden van incidenten. Andere wetgeving, zoals de CSA, RED, CRA, CSOA, draagt bij aan het verhogen van het beveiligingsniveau van producten, diensten en platformen, en richt zich vooral op de fase 'beschermen' in de weerbaarheidscyclus.

Naast beleid en wetgeving zijn er tal van initiatieven en samenwerkingsverbanden die de digitale weerbaarheid in ketens, sectoren en regio's versterken. Deze initiatieven zijn essentieel voor het vergroten van bewustwording, het delen van kennis en het stimuleren van gedragsverandering, met bijzondere aandacht voor het mkb, waar een achterstand in digitale weerbaarheid bestaat. Mogelijk kan er ook gekeken worden naar de effectiviteit van deze maatregelen, zowel individueel als wat betreft de onderlinge coördinatie tussen initiatieven om te voorkomen dat er overlap of versnippering plaatsvindt.

Een belangrijke uitdaging in de Nederlandse beleidscontext is de versnippering van initiatieven en het ontbreken van gestandaardiseerde meetmethoden om de effectiviteit van beleid en maatregelen te evalueren. Dit bemoeilijkt het verkrijgen van een integraal overzicht en het meten van voortgang. De ontwikkeling van het Cyberweerbaarheidsnetwerk (CWN) en de integratie van bestaande samenwerkingsverbanden bieden kansen voor meer coördinatie, duidelijkheid en samenwerking. Mogelijk biedt wetgeving, zoals de normen in de Cyber Resilience Act, of commerciële certificeringen, zoals ISO-standaarden, een kans om kwantitatieve factoren te formuleren die kunnen bijdragen aan het evalueren van beleidsinstrumenten. Met behulp van deze gestandaardiseerde methoden zou het weerbaarheidsniveau van organisaties gemeten en vergeleken kunnen worden. Tegelijkertijd blijft het van belang om sectorspecifieke behoeften te erkennen en maatwerk te bieden, zodat zowel grote organisaties als het mkb effectief ondersteund worden.

Daarnaast is het belangrijk te erkennen dat ketenafhankelijkheden ervoor zorgen dat het belang van digitale weerbaarheid op alle niveaus en schaalgroottes speelt. Wanneer wetgeving zich alleen richt op grote organisaties en niet op alle schakels binnen een keten kunnen deze afhankelijkheden leiden tot zwakke punten en een afname van digitale weerbaarheid voor de gehele keten. Door risicoanalyses of certificeringen uit te breiden tot een overzicht van de complete keten zouden kosten gedrukt kunnen worden, juist voor kleinere partijen, en zou de digitale weerbaarheid hierin kunnen stijgen.

2.3. Kernelementen van digitale weerbaarheid

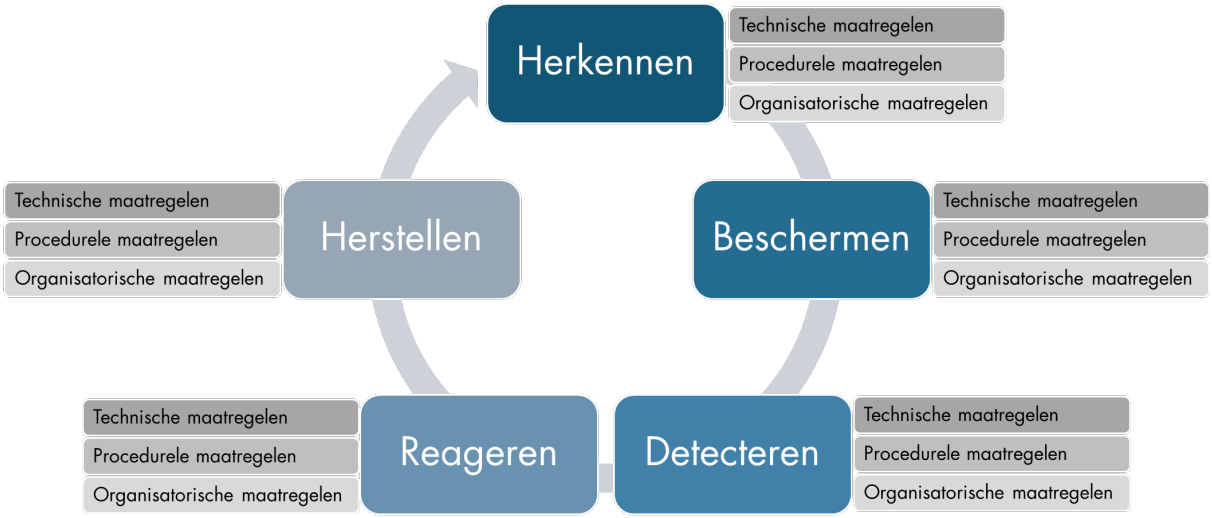
De kern van digitale weerbaarheid, zoals uiteengezet aan het einde van Paragraaf 2.1, is dat het een breed en cyclisch concept betreft dat verder gaat dan alleen het technisch kunnen herstellen van systemen na een

incident. In de literatuur en het Nederlandse beleid wordt digitale weerbaarheid opgevat als het vermogen van organisaties om risico's te identificeren, dreigingen te voorkomen, incidenten te detecteren, adequaat te reageren en vervolgens te herstellen en te leren. Dit sluit aan bij de bredere definitie van de NCTV, die weerbaarheid positioneert als een continu proces dat zowel preventieve als reactieve en lerende elementen omvat.

In de Nederlandse context wordt deze brede conceptualisering vertaald naar een mix van strategische doelen, juridische kaders en praktische initiatieven. De NLCS en de implementatie van richtlijnen zoals de Cyberbeveiligingswet operationaliseren digitale weerbaarheid door sommige organisaties te verplichten en te stimuleren om in alle fasen van de cyclus maatregelen te nemen. Dit gebeurt via een combinatie van technische (zoals firewalls, monitoring en back-ups), procedurele (zoals risicobeoordelingen, incident-responseplannen en rapportageprotocollen) en organisatorische maatregelen (zoals training, governance en publiek-private samenwerking). De vijf basisprincipes van het NCSC en DTC bieden een handzaam kader dat deze multidimensionale aanpak concretiseert. Tegelijkertijd wordt in het beleid erkend dat de effectiviteit en impact van deze maatregelen moeilijk te meten zijn, mede door het ontbreken van gestandaardiseerde meetinstrumenten en de grote verschillen in weerbaarheidsniveaus tussen sectoren en organisaties. Dit leidt tot een spanningsveld tussen de ambitie om digitale weerbaarheid breed te versterken en de praktische uitdaging om deze daadwerkelijk te monitoren en te sturen.

De verschillende fasen van de weerbaarheidscyclus – herkennen, beschermen, detecteren, reageren en herstellen – worden in de literatuur en beleidsdocumenten als samenhangende deelprocessen gezien, waarbij elk van deze fasen vraagt om een combinatie van technische, procedurele en organisatorische maatregelen. In het volgende hoofdstuk zullen deze fasen gebruikt worden om te zien welke van deze fasen gedekt worden door bestaande meetinstrumenten om digitale weerbaarheid in kaart te brengen.

Figuur 4. De kernonderdelen van digitale weerbaarheid



3. Bestaande instrumenten voor het meten van digitale weerbaarheid

In dit hoofdstuk analyseren we de bestaande instrumenten die organisaties kunnen gebruiken om hun digitale weerbaarheid te monitoren en te meten. We kijken daarbij onder andere in hoeverre deze methoden de kernonderdelen van digitale weerbaarheid, zoals besproken in het vorige hoofdstuk, afdekken. De verschillende raamwerken die zijn geïdentificeerd in de literatuur vervullen verschillende functies: ze stellen organisaties in staat om hun ontwikkeling in de loop van de tijd systematisch te volgen, huidige sterke en zwakke punten te identificeren en/of specifieke gebieden aan te wijzen waar verdere verbetering nodig is. In dit hoofdstuk zullen achtereenvolgens 18 raamwerken voor het meten van digitale weerbaarheid worden geanalyseerd door te kijken naar, onder andere, de inputs, outputs, beperkingen en validiteit van deze raamwerken.

3.1. Aanpak bij het beoordelen van benaderingen

Uit de literatuur over digitale weerbaarheid blijkt dat er verschillende methodologieën, raamwerken en best practices zijn ontwikkeld om digitale weerbaarheid in kaart te brengen. In totaal hebben we 18 raamwerken gevonden die in de literatuur werden voorgesteld als van toepassing zijnde op de digitale weerbaarheid van organisaties, ook wanneer dit niet expliciet vermeld werd door de auteurs van die raamwerken. Voor veel van deze raamwerken is het dan ook niet expliciet een doel om digitale weerbaarheid te meten. Naast het (mogelijk) van toepassing zijn op digitale weerbaarheid van organisaties, zijn er geen andere selectiecriteria toegepast.

Voor ieder raamwerk hebben we onderzocht welke elementen van digitale weerbaarheid aan de orde komen (Onderzoeksvraag 2.1), hoe er omgegaan wordt met onbekende dreigingen (Onderzoeksvraag 2.2) en wat de validiteit en betrouwbaarheid is van de aanpak (Onderzoeksvraag 2.3). De validiteit en betrouwbaarheid van bestaande meetinstrumenten voor digitale weerbaarheid zijn cruciaal voor het beoordelen van hun effectiviteit. Validiteit zorgt ervoor dat deze instrumenten nauwkeurig meten wat ze beogen te meten, en de ware essentie van digitale weerbaarheid in verschillende contexten en populaties weergeven. Betrouwbaarheid garandeert de consistentie en reproduceerbaarheid van resultaten in de loop van de tijd en in verschillende contexten. Samen bepalen deze eigenschappen de bruikbaarheid van de resultaten (Windle et al. 2011). Het is belangrijk op te merken dat we de betrouwbaarheid en validiteit van deze raamwerken niet zelf hebben getest of geëvalueerd. Standpunten die in de literatuur worden geuit, ook door de bedenkers van de methode, zijn opgenomen in de verschillende tabellen hieronder. Waar geen evaluaties van de methoden te vinden waren, hebben we dit aangegeven.

Organisaties voeren zelden post mortem weerbaarheidsanalyses uit na verstoringen, waardoor het moeilijk is om processtoringen in verband te brengen met specifieke gehanteerde raamwerken. Bovendien worden in de literatuur de uitdagingen bij het kwantificeren van en het evalueren van de prestaties van dergelijke benaderingen benadrukt. Ligo et al. (2021) stellen dat de effectiviteit van een cyberfysisch systeem het best kan worden beoordeeld aan de hand van de mate waarin het zijn missie of bedrijfsdoelstellingen bereikt, en niet op basis van technische indicatoren zoals het aantal gebruikers of de transactiesnelheid. Het beoordelen van digitale weerbaarheid aan de hand van het volbrengen van de missie weerspiegelt het belang van het systeem en zijn afhankelijkheden. Tegelijkertijd is dit nog uitdagender dan het meten van technische functionaliteit door de complexe en indirecte afhankelijkheden die het moeilijk maken om de werkelijke impact op de missie of het bedrijf te identificeren en te kwantificeren (Ligo et al. 2021).

Daarnaast ligt de focus van dit onderzoek op het verkennen welke kwantitatieve indicatoren voor aspecten van digitale weerbaarheid in organisaties beschikbaar zijn of ontwikkeld zouden kunnen worden, en op de aard van de inzichten in het niveau van digitale weerbaarheid die deze indicatoren zouden kunnen bieden. Daarom hanteren we een bredere definitie van wat kwantitatieve indicatoren zijn dan gebruikelijk is, aangezien we elke vorm van ordinale schaal, zoals rood-amber-groen-beoordelingen, als kwantitatief beschouwen voor onze analyse. Deze inclusieve benadering stelt ons in staat om een breder scala aan meetpraktijken te verzamelen.

In dit hoofdstuk beschrijven we voor elke geïdentificeerde methode: de verzamelde inputgegevens, de methoden voor gegevensverzameling, de outputs, de beperkingen en specifieke aspecten van digitale weerbaarheid waarop elk raamwerk zich richt, waarbij we waar mogelijk kwantitatieve indicatoren onderzoeken. De volledige lijst van de verschillende aspecten die we hebben onderzocht, staat in de eerste kolom van Tabel 6. Daarnaast leiden we iedere methode kort in, gaan we in op de toegankelijkheid van het raamwerk, inclusief eigendom, lichten we de sector toe waarop het zich richt, indien van toepassing ('Sectorale focus'), geven we aan welke kernelementen en maatregelen van digitale weerbaarheid in het raamwerk worden meegenomen (Herkennen, Beschermen, Detecteren, Reageren, Herstellen, Technische maatregelen, Procedurele maatregelen, Organisatorische maatregelen), bespreken we of en hoe het raamwerk rekening houdt met onbekende bedreigingen, en bespreken we wat er bekend is over de validiteit en betrouwbaarheid volgens bestaande evaluaties. Voor iedere methode hebben we een kolom toegevoegd met een kleurgecodeerde beoordeling van de sterke punten en beperkingen van dergelijke aspecten in verhouding tot de wensen van de NCTV. De onderstaande tabel laat zien wat de rood-amber-groene codering onder elk aspect betekent.

Tabel 6. Kleurcoderingkader

	Groen	Amber	Rood
Beschrijving	-	-	-
Toegankelijkheid	Gratis gebruik van alle documentatie en vrij om aan te passen	Toegang moet worden aangevraagd of is betaald	Niet toegankelijk
Sectorale focus	Digitale weerbaarheid voor elke organisatie	Specifiek voor een sector	Niet gericht op organisaties/onduidelijk
Welke elementen van digitale weerbaarheid worden onderzocht?	Alle kernelementen en maatregelen komen aan bod	Sommige aspecten van kernelementen en maatregelen worden behandeld	Geen van de kernelementen of maatregelen worden behandeld
Inputgegevens (wat wordt verzameld en hoe)	De verzameling en aard van de gegevens zijn toegankelijk en het proces lijkt functioneel	Verschillen in verzameling en aard van gegevens, en/of onduidelijkheid over de functionaliteit van het proces	Gegevens (verzameling) van een andere aard dan verwacht voor dit onderzoek
Kwantitatieve indicatoren van digitale weerbaarheid	Kwantitatieve indicatoren zijn vermeld	Kwantitatieve indicatoren mogelijk, maar niet vermeld	Aanpak maakt geen gebruik van kwantitatieve indicatoren
Output	Een kwantificering van het niveau van digitale weerbaarheid van organisaties	Relevante inzichten in het niveau van digitale weerbaarheid, maar geen enkele vorm van scoring	Geen duidelijke inzichten in het niveau van digitale weerbaarheid van organisaties
Onbekende bedreigingen	Er wordt aangegeven hoe de methode omgaat met onbekende dreigingen	Niet vermeld, maar kunnen waarschijnlijk worden meegenomen	Niet (aannemelijk) meegenomen
Beperkingen	De beperkingen t.a.v. de doelstellingen van dit onderzoek zijn duidelijk	Beperkingen zijn niet vermeld en/of onduidelijk	De aard van de beperkingen, de aanpak en de outputgegevens betekenen dat de aanpak niet goed aansluit bij de doelstellingen van deze studie
Betrouwbaarheid	Onafhankelijk bevestigd	Waarschijnlijk	Onzeker
Validiteit	Onafhankelijk bevestigd	Waarschijnlijk	Onzeker

Bron: Analyse van RAND Europe op basis van de onderzoeksvragen.

3.2. Samenvatting van bestaande benaderingen

In dit gedeelte geven we een overzicht van de 18 in de literatuur geïdentificeerde raamwerken. De reikwijdte van de raamwerken is niet altijd geworteld in de context van digitale weerbaarheid. Sommige van de bronnen die tijdens het literatuuronderzoek zijn geanalyseerd, suggereerden raamwerken die bijvoorbeeld uit de financiële of gezondheidszorgsector voortkomen en die mogelijk de behoeften en doelstellingen op het gebied van digitale weerbaarheid kunnen dekken indien ze hierop praktisch zouden worden toegepast. Dergelijke raamwerken zijn eveneens meegenomen in dit hoofdstuk. Achtereenvolgens komen de volgende raamwerken aan bod:

1. Ambidextrous Cybersecurity Approach (AMBI CYBER)
2. Het conceptuele raamwerk van Blanchet et al.
3. De criteria van Bradford Hill
4. CERT Resilience Management Model (CERT-RMM)
5. Common Vulnerability Scoring System (CVSS)
6. Cyber Essentials
7. Cyber Physical Systems Security Framework (CPSS)
8. Cyber Resilience Framework (CAF)
9. Cyber Resilience Quantification Framework (CRQF)
10. Cyber Resilience Recovery Model (CRRM)
11. Cyber Resilience Self-Assessment Tool (CR-SAT)
12. Cyber Resiliency Engineering Framework (CREF)
13. Cybersecurity Maturity Model Certification (CMMC)
14. International Organization for Standardization (ISO) 27000-series
15. Linkov's Resilience Matrix Framework
16. National Institute of Standards and Technology (NIST) Framework
17. NIAC- Resilience Model
18. TNO-raamwerk

1. Ambidextrous cybersecurity approach (AMBI CYBER)

Beschrijving	AMBI-CYBER focust op het beveiligen van gegevens, systemen en netwerken en faciliteert gelijktijdig de snelle integratie van nieuwe technologieën. Het definieert de 'Cybersecurity Efficient Frontier' door een combinatie van organisatorische, technologische en culturele competenties (Carayannis et al., 2021).	
Toegankelijk-heid	Het eigendom van het theoretische kader berust bij de auteurs of de uitgever. Het artikel is vrij toegankelijk.	G
Toepassings-gebied	Digitale weerbaarheid voor elke organisatie.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Het maakt gebruik van een *balanced scorecard* en een 7P's stage gate-model – *Patient, Persistent, Persevering, Proactive, Predictive, Preventive, and Pre-emptive* – om veiligheid, beveiliging en privacy te optimaliseren binnen een dynamische prestatiegrens. Daarnaast is er behoefte aan een juiste kwalificatie, kwantificering en weging van de 7P's- en 5V's-variabelen in een *multicriteria decision-making analysis* (MCDMA). Het raamwerk omvat alle elementen en maatregelen die in deze studie zijn vastgesteld.	
Inputgegevens (wat wordt verzameld en hoe)	AMBI-CYBER verzamelt gegevens met betrekking tot organisatorische, technologische en culturele competenties, waarbij de nadruk ligt op de bescherming van gegevens, systemen en netwerken, de integratie van nieuwe technologieën en het optimaliseren van veiligheid, beveiliging en privacy.	G
Kwantitatieve indicatoren van digitale weerbaarheid	De kwantitatieve indicatoren van AMBI-CYBER voor digitale weerbaarheid omvatten maatstaven voor veiligheid, beveiliging en privacy, technologie-integratiepercentages en prestaties langs de Cybersecurity Efficient Frontier. Het meet ook proactief gedrag en biedt een uitgebreide beoordeling van de weerbaarheid van een organisatie.	A
Output	De AMBI-CYBER-architectuur, gebaseerd op het 7P-model, biedt meer inzicht in de mentaliteit, het analytisch gedrag en de prestatiekenmerken van een organisatie. Cybersecurity-ambidexteriteit maakt een leerproces mogelijk dat leidt tot een verbeterd absorptievermogen op het gebied van cybersecurity (Carayannis et al., 2021).	A
Onbekende bedreigingen	De proactieve en voorspellende aspecten van het raamwerk kunnen zich vertalen in de integratie van AI of zelfverdedigende apps om organisaties in staat te stellen bedreigingen te detecteren en erop te reageren.	G
Beperkingen	De beperkingen van de aanpak omvatten een gebrek aan empirische, op bewijs gebaseerde bevindingen die nodig zijn om de belangrijkste factoren van de effectiefste AMBI-CYBER-configuraties te identificeren, te verklaren en te voorspellen. Deze leemte suggereert dat toekomstig onderzoek zich op deze gebieden moet richten om de theorie, het beleid en de praktijk beter te onderbouwen en de robuustheid en toepasbaarheid van de bevindingen te verbeteren.	G
Betrouwbaar-heid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties van de validiteit van het raamwerk gevonden.	R

2. Blanchet et al. (2017) conceptueel raamwerk

Beschrijving	Het raamwerk identificeert vier kernconcepten – kennis, onzekerheden, onderlinge afhankelijkheid en legitimiteit – als drijvende krachten achter de weerbaarheid van gezondheidszorgstelsels, hoewel legitimiteit als een concept van hogere orde wordt beschouwd en daarom niet in het model is opgenomen. De overige concepten zijn aangepast om de nadruk te leggen op veiligheid binnen de digitale transformatie van de gezondheidszorg: kennis en middelen beoordelen het begrip van bedreigingen en de respons op cyberincidenten; risicobewustzijn evalueert het begrip van interacties tussen digitale activa en operationele continuïteit; en partnerschappen & toeleveringsketen onderzoeken de betrokkenheid bij de dynamiek van de waardeketen en de veiligheid van de toeleveringsketen. Veiligheid in transformatie geeft het veiligheidsaspect weer van het digitale transformatievermogen van zorgorganisaties (Garcia-Perez et al., 2023). Het huidige raamwerk is alleen toegepast op de sector gezondheidszorg.	
Toegankelijkheid	Het eigendom van het theoretische kader berust bij de auteurs (Blanchet et al.) of de uitgever. Het artikel is vrij toegankelijk.	G
Reikwijdte	Gezondheidszorg.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	Blanchet et al. onderzoeken elementen van digitale weerbaarheid, zoals kennis en middelen, risicobewustzijn, partnerschappen en onderlinge afhankelijkheden in de toeleveringsketen, en veiligheidsintegratie in digitale transformatie. Het raamwerk omvat alle elementen die in deze studie zijn vastgesteld, maar richt zich op procedurele en organisatorische maatregelen en laat technische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	In het conceptuele raamwerk van Blanchet et al. wordt digitale weerbaarheid in de gezondheidszorg beoordeeld aan de hand van enquêtes onder leidinggevenden, risicobeoordelingen, evaluaties van partnerschappen en beveiligingsbeoordelingen om inzicht te krijgen in bedreigingen, risicobewustzijn, onderlinge afhankelijkheden en transformatiebeveiliging.	A
Kwantitatieve indicatoren van digitale weerbaarheid	Niet vermeld.	A
Output	De output van de toepassing van het conceptuele raamwerk van Blanchet op digitale weerbaarheid in de gezondheidszorg is bedoeld als een uitgebreide evaluatie van de gereedheid en capaciteit van een organisatie om cybersecuritybedreigingen aan te pakken, de operationele continuïteit te handhaven, onderlinge afhankelijkheden effectief te beheren en robuuste beveiligingsmaatregelen te integreren in initiatieven voor digitale transformatie (Garcia-Perez et al., 2023).	A
Onbekende bedreigingen	Niet (aannemelijk) vastgelegd.	R
Beperkingen	Wat betreft digitale weerbaarheid: er wordt verwacht dat de gezondheidszorgsector de relatie tussen onzekerheid en digitalisering in beide richtingen zal moeten navigeren. Een goed begrip en beheer van de onzekerheden die voortvloeien uit deze bidirectionele relatie verhoogt de veiligheid tijdens de digitale transformatie. Om dit te bereiken is niet alleen interne expertise nodig, maar ook kennis die is opgedaan door samenwerkingen binnen de gezondheidszorgsector en de wereldwijde waardeketen daarvan (Garcia-Perez et al. 2023).	A
Betrouwbaarheid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden. De betrouwbaarheid hangt ook af van de kwaliteit en nauwkeurigheid van de verzamelde gegevens en de context waarin het wordt toegepast.	R
Validiteit	Er zijn geen evaluaties van de validiteit van het raamwerk gevonden.	R

3. De criteria van Bradford Hill

Beschrijving	Geïnspireerd door de criteria van Bradford Hill, oorspronkelijk ontwikkeld voor het beoordelen van causaliteit in epidemiologische studies, is deze methode aangepast om de consistentie bij het evalueren van weerbaarheidsmaatstaven te verbeteren. De negen aspecten die Hill bespreekt – sterkte van associatie, consistentie, specificiteit, temporaliteit, biologische gradiënt, plausibiliteit, coherentie, experiment en analogie – dienen als een uitgebreid raamwerk voor het beoordelen van digitale weerbaarheid (Kott & Linkov, 2021).	
Toegankelijkheid	Er zijn geen beperkingen of eigendomsclaims die het gebruik ervan beperken of speciale toestemming vereisen, aangezien ze deel uitmaken van de fundamentele publieke kennis op het gebied van epidemiologie.	G
Toepassingsgebied	Raamwerk uit de epidemiologie dat geschikt kan zijn voor het meten van de digitale weerbaarheid van organisaties, mits op de juiste wijze aangepast.	R
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	R
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	De Bradford-Hill-criteria onderzoeken digitale weerbaarheid door de sterkte van de associatie, consistentie en specificiteit van weerbaarheidsmaatregelen te beoordelen, evenals hun timing (tijdelijkheid) en effectiviteit (biologische gradiënt) (Kott & Linkov, 2021). Het raamwerk heeft geen betrekking op de elementen die in deze studie zijn vastgesteld, maar richt zich alleen op procedurele maatregelen en laat technische en organisatorische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	De aangepaste Bradford-Hill-criteria voor het beoordelen van digitale weerbaarheid omvatten het verzamelen van gegevens door middel van statistische analyses, longitudinale studies en gerichte beoordelingen om respectievelijk de sterkte van de associatie, de consistentie en de specificiteit te evalueren. Aanvullende input omvat tijdlijnen van gebeurtenissen voor tijdelijkheid, gecontroleerde experimenten voor biologische gradiënten en experimenten, literatuuronderzoek en raadpleging van deskundigen voor plausibiliteit en coherentie.	A
Kwantitatieve indicatoren van digitale weerbaarheid	Niet vermeld.	A
Output	Het toepassen van de criteria van Bradford Hill op digitale weerbaarheid kan inzicht verschaffen in herhaalbaarheid, consistentie met betrekking tot missies, monotoniciteit met betrekking tot verdedigingsmechanismen (vermoedelijk betere verdediging kan nieuwe zwakke punten met zich meebrengen en verder onderzoek mogelijk maken), monotoniciteit van aanvallen (vermoedelijk sterkere aanvallen kunnen ineffectief zijn tegen bestaande verdedigingssystemen) (Kott & Linkov, 2021).	A
Onbekende bedreigingen	Niet (aannemelijk) vastgelegd.	R
Beperkingen	De criteria zijn nog steeds gebaseerd op epidemiologie en zouden moeten worden aangepast om specifiek de digitale weerbaarheid te meten (Kott & Linkov, 2021).	A
Betrouwbaarheid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties van de validiteit van het raamwerk gevonden.	R

4. CERT Resilience Management Model (CERT-RMM)

Beschrijving	Het CERT-RMM, ontwikkeld door het Carnegie Mellon Software Engineering Institute, streeft naar integratie en institutionalisering van digitale weerbaarheid door een evenwicht te vinden tussen technische en organisatorische maatregelen. Het legt de nadruk op het behouden van een hoog contextueel en situationeel bewustzijn, het ontwikkelen van netwerkgerichte en geoefende vaardigheden op het gebied van dreigingsbeheer en het verbeteren van het aanpassingsvermogen (Dupont, 2019).	
Toegankelijk-heid	De eigendomsrechten berusten bij SEI/CMU en alleen de Amerikaanse overheid heeft een royaltyvrij recht voor intern gebruik door de overheid. Anderen moeten de geautoriseerde documentatie aanschaffen en toestemming vragen voor gebruik buiten persoonlijke of educatieve doeleinden.	A
Toepassings-gebied	Digitale weerbaarheid voor elke organisatie.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	Het CERT RMM onderzoekt digitale weerbaarheid door middel van technische en organisatorische maatregelen, waarbij de nadruk ligt op contextbewustzijn, vaardigheden op het gebied van dreigingsbeheer en aanpassingsvermogen. Deze elementen versterken gezamenlijk het vermogen van een organisatie om haar digitale infrastructuur te beschermen en in stand te houden tegen steeds veranderende dreigingen. Het raamwerk omvat alle elementen die in deze studie zijn vastgesteld, maar richt zich op technische en organisatorische maatregelen en laat procedurele maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens omvatten informatie met betrekking tot technische en organisatorische maatregelen, contextueel en situationeel bewustzijn, vaardigheden op het gebied van dreigingsbeheer en aanpassingsvermogen. Deze gegevens worden doorgaans verzameld door middel van beoordelingen en evaluaties van de bestaande cybersecuritypraktijken, het beleid en de infrastructuur van een organisatie. Dit kan het verzamelen van gegevens uit beveiligingsaudits, incidentrapporten, netwerkmonitoring, opleidingsgegevens van werknemers en feedback van belanghebbenden omvatten, om een uitgebreid inzicht te krijgen in de weerbaarheid van de organisatie.	A
Kwantitatieve indicatoren van digitale weerbaarheid	Kwantitatieve indicatoren van digitale weerbaarheid in CERT RMM omvatten de responstijd bij incidenten, systeemuitval, efficiëntie van patchbeheer, detectiegraad van bedreigingen en naleving van opleidingsvereisten voor werknemers. Deze maatstaven beoordelen gezamenlijk het vermogen van een organisatie om cyberdreigingen te weerstaan en daarvan te herstellen.	G
Output	Inzicht in de effectiviteit van zowel technische als organisatorische maatregelen, waarbij sterke punten worden benadrukt en hiaten worden geïdentificeerd die verbetering behoeven. Daarnaast biedt het model aanbevelingen voor het vergroten van contextueel en situationeel bewustzijn, het verbeteren van vaardigheden op het gebied van bedreigingsbeheer en het vergroten van het aanpassingsvermogen. Het uiteindelijke resultaat zou zijn dat organisaties worden begeleid bij het institutionaliseren en integreren van digitale weerbaarheidspraktijken om zich beter voor te bereiden op en te reageren op verstoringen (Dupont, 2019).	A
Onbekende bedreigingen	Niet vermeld.	A
Beperkingen	De beperkingen van het CERT Resilience Management Model (RMM) bestaan uit de moeilijkheid om complexe onderlinge afhankelijkheden tussen organisaties, systemen en kritieke infrastructuren aan te pakken, wat een effectieve beoordeling van de weerbaarheid kan belemmeren. Bovendien heeft het model te maken met uitdagingen bij het in kaart brengen van aanzienlijke verschillen in paraatheids- en responsstrategieën voor verschillende soorten verstoringen. Deze complexiteit vereist meer genuanceerde en aanpasbare beoordelingsmethoden (Dupont, 2019).	A
Betrouwbaar-heid	Hoewel er geen evaluaties van de betrouwbaarheid van het raamwerk zijn gevonden, beschouwen Caralli et al. (2013) de kwantitatieve indicatoren in het CERT Resilience	A

	Management Model (RMM) als betrouwbaar en geschikt om te worden toegepast in verschillende beoordelingen, zoals gepresenteerd in hun studie, waardoor stabiele en herhaalbare resultaten worden gegarandeerd.	
Validiteit	Er zijn geen evaluaties van de validiteit van het raamwerk gevonden.	R

5. Common Vulnerability Scoring System (CVSS)

Beschrijving	Dit scoresysteem is een veelgebruikt hulpmiddel in cybersecurity voor het beoordelen van de ernst van ontdekte kwetsbaarheden, waardoor prioriteiten kunnen worden gesteld bij het toepassen van patches en het nemen van mitigerende maatregelen. Het combineert vooraf gedefinieerde wegingsfactoren met het oordeel van experts om de exploiteerbaarheid en impact te evalueren, wat resulteert in een totale score die de kriticiteit van de kwetsbaarheid aangeeft (Jacobs et al., 2018).	
Toegankelijk-heid	CVSS is vrij beschikbaar voor gebruik. Het raamwerk kan gratis worden aangepast voor gebruik door organisaties; publicatie met bronvermelding en naleving van de richtlijnen is vereist. Alle documentatie, inclusief de officiële specificatie, is gratis beschikbaar op de website van het Forum of Incident Response and Security Teams (FIRST).	G
Toepassings-gebied	Digitale weerbaarheid voor elke organisatie.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	A
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	De uitslag wordt afgeleid uit de evaluatie van de exploiteerbaarheid en impact van de kwetsbaarheid, met behulp van vooraf gedefinieerde wegingsfactoren en deskundig oordeel. De CVSS-score helpt bij het prioriteren van patch- en mitigatie-inspanningen door aan te geven welke kwetsbaarheden het kritiekst zijn en als eerste moeten worden aangepakt. Het raamwerk kijkt naar de elementen 'detecteren' en 'reageren' die in deze studie zijn vastgesteld, en richt zich op procedurele maatregelen, waarbij technische en organisatorische maatregelen buiten beschouwing worden gelaten.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens voor het CVSS omvatten informatie over de exploiteerbaarheid en impact van ontdekte kwetsbaarheden. Deze invoergegevens worden verzameld door middel van een combinatie van vooraf gedefinieerde wegingen en het oordeel van materiedeskundigen. De gegevens worden gekwantificeerd om de ernst en kriticiteit van elke kwetsbaarheid te beoordelen, wat resulteert in een totale score die helpt bij het prioriteren van patch- en mitigatie-inspanningen. Specifiek voor de Impact Subscore (ISC) worden numerieke waarden toegekend aan elke impactbeoordeling, die vervolgens worden gebruikt om de ISC te berekenen en de impact van verschillende scenario's op de systeembeveiliging te beoordelen.	G
Kwantitatieve indicatoren van digitale weerbaarheid	Het CVSS-model maakt gebruik van kwantitatieve indicatoren, zoals exploiteerbaarheidsmetriek (aanvalsvector, complexiteit) en impactmetriek (vertrouwelijkheid, integriteit, beschikbaarheid) om een totale score te genereren die prioriteit geeft aan maatregelen om kwetsbaarheden aan te pakken. Deze indicatoren helpen bij het beoordelen van de digitale weerbaarheid door kritieke kwetsbaarheden te benadrukken.	G
Output	Totale score die de kritieke aard van een kwetsbaarheid kwantificeert. Daarnaast biedt ISC een specifieke maatstaf voor de potentiële impact van een kwetsbaarheid, die kan worden gebruikt om de veiligheidsimplicaties van verschillende scenario's te vergelijken en te beoordelen.	G
Onbekende bedreigingen	Niet vermeld.	A
Beperkingen	Niet vermeld.	A
Betrouwbaar-heid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties van de validiteit van het raamwerk gevonden.	R

6. Cyber Essentials

Beschrijving	Cyber Essentials is een door de Britse overheid gesteund certificeringsprogramma dat is ontworpen om organisaties te helpen zichzelf te beschermen tegen veelvoorkomende cyberdreigingen. Het richt zich op de implementatie van vijf basisbeveiligingsmaatregelen: firewalls, veilige configuratie, gebruikerstoegangscontrole, bescherming tegen malware, en software-updates. Volgens de Britse overheid kunnen deze maatregelen ongeveer 80% van de veelvoorkomende cyberaanvallen voorkomen. Het programma biedt twee certificeringsniveaus: Cyber Essentials, waarbij zelfevaluatie plaatsvindt, en Cyber Essentials Plus, waarbij onafhankelijke validatie door een externe auditor plaatsvindt (NCSC, 2025).	
Toegankelijk-heid	Het raamwerk is eigendom van de Britse overheid en wordt beheerd via het NCSC. Het is openbaar beschikbaar en kan vrij worden gebruikt. Officiële richtlijnen en documentatie met vereisten zijn vrij toegankelijk en bruikbaar.	G
Toepassings-gebied	Cyber Essentials richt zich op de IT-infrastructuur die een organisatie gebruikt om haar bedrijfsactiviteiten uit te voeren. Dit omvat alle apparaten die toegang hebben tot organisatorische gegevens of diensten, zoals e-mails, klantgegevens, websites en clouddiensten.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen / Beschermen / Detecteren / Reageren / Herstellen	A
	Technische maatregelen / Procedurele maatregelen / Organisatorische maatregelen	A
	Cyber Essentials onderzoekt de belangrijkste elementen van digitale weerbaarheid aan de hand van vijf technische controles: firewalls, veilige configuratie, toegangscontrole, bescherming tegen malware en beheer van beveiligingsupdates. Deze controles beschermen organisaties tegen veelvoorkomende cyberdreigingen door kwetsbaarheden aan te pakken en het risico op succesvolle aanvallen te verminderen, waardoor de algehele digitale weerbaarheid wordt verbeterd. Het raamwerk omvat de elementen 'identificeren' en 'beschermen' die in deze studie zijn vastgesteld, en richt zich uitsluitend op de technische maatregelen, waarbij procedurele en organisatorische maatregelen buiten beschouwing worden gelaten.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens voor Cyber Essentials worden verzameld via een gestandaardiseerde vragenlijst (NCSC, 2025).	G
Kwantitatieve indicatoren van digitale weerbaarheid	Cyber Essentials maakt voornamelijk gebruik van kwalitatieve indicatoren om de naleving van de vijf belangrijkste controles te beoordelen.	R
Output	De output van Cyber Essentials is een certificering die bevestigt dat een organisatie de nodige beveiligingsmaatregelen heeft geïmplementeerd om zich te beschermen tegen veelvoorkomende cyberdreigingen. Deze certificering is er in twee vormen: Cyber Essentials voor zelfbeoordeling en Cyber Essentials Plus voor onafhankelijke verificatie. Beide vormen bieden belanghebbenden zekerheid over de cybersecurity van de organisatie.	A
Onbekende bedreigingen	Cyber Essentials detecteert niet specifiek onbekende bedreigingen. Het richt zich op het implementeren van basisbeveiligingsmaatregelen ter bescherming tegen veelvoorkomende cyberdreigingen.	R
Beperkingen	De Cyber Essentials-certificering heeft beperkingen, waaronder het feit dat er alleen een momentopname wordt gemaakt, waarbij de nadruk ligt op basisbeveiligingsmaatregelen.	A
Betrouwbaar-heid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties van de validiteit van het raamwerk gevonden.	R

7. Cyber Physical Systems Security Framework (CPSS)

Beschrijving	Het Cyber-Physical Security System (CPSS)-raamwerk identificeert tien essentiële gebieden om tot een grondige beoordeling van de 'gezondheidstoestand' van cybersecuritysystemen te komen. Deze gebieden omvatten gegevens- en informatiebeveiliging om veilig delen en rapporteren te garanderen, evenals fysieke beveiliging om toegangscontrole te beheren. Het raamwerk omvat ook tactieken tegen mogelijke cyberaanvallen, forensische en prognostische evaluaties en uitgebreide herstelplannen om de weerbaarheid en integriteit van het systeem te versterken (DiMase et al., 2015).	
Toegankelijkheid	Het eigendom van het theoretische kader berust bij de auteurs (DiMase et al.) of de uitgever. Het artikel is vrij toegankelijk.	G
Toepassingsgebied	IT-infrastructuur van elke organisatie en technische sector.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	Het CPSS-raamwerk onderzoekt elementen van digitale weerbaarheid, zoals gegevensbeveiliging, fysieke toegangscontrole, anti-vervalsingsstrategieën, forensische en prognostische evaluaties en herstelplanning. Het raamwerk omvat alle elementen die in deze studie zijn vastgesteld, maar richt zich op technische en procedurele maatregelen en laat organisatorische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	Het CPSS-raamwerk verzamelt inputgegevens uit beveiligingsaudits, toegangscontrolelogboeken, forensische analyses en herstelplannen om de cybersecurity te beoordelen. Deze gegevens omvatten meetgegevens over gegevensbeveiliging, toegangsbeheer, tegenmaatregelen voor mogelijke cyberaanvallen en strategieën voor systeemherstel. Het raamwerk maakt ook gebruik van een ontwerpscorekaart om het resterende risico van CPSS te meten. De gegevens die worden gebruikt in de CPS-samenvattende beoordelingsscorekaart zijn afkomstig van scorekaarten die een meer gedetailleerde evaluatie van het CPSS-ontwerp weergeven en omvatten elk niveau van systeemengineering (DiMase et al., 2015).	G
Kwantitatieve indicatoren van digitale weerbaarheid	Het CPSS-raamwerk definieert niet expliciet kwantitatieve indicatoren, maar organisaties kunnen gebruikmaken van statistieken zoals de frequentie van datalekken, pogingen tot ongeoorloofde toegang, detectiepercentages van vervalsingen, doorlooptijd van forensische analyses en hersteltijddoelstellingen.	A
Output	CPSS levert belangrijke output die helpt bij het aanpakken van de uitdaging van het beheren van bedreigingen in grootschalige CPS met een uitgebreide dekking. Deze aanpak biedt richtlijnen voor de ontwikkeling van beveiligingsmaatregelen die nodig zijn om kritieke CPS-middelen en commando- en controlefuncties te beschermen. Dit wordt bereikt door het verstrekken van uitgebreide documentatie, modellering en een raamwerk voor traceerbaarheid, inspecteerbaarheid en duurzaamheidsbeheer van het CPSS gedurende de gehele levenscyclus van het CPS (DiMase et al., 2015).	G
Onbekende bedreigingen	Niet vermeld.	A
Beperkingen	Niet vermeld.	A
Betrouwbaarheid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

8. Cyber Assessment Framework (CAF)

Beschrijving	Het raamwerk is ontworpen voor gebruik door organisaties die onder de Network and Information Systems (NIS) Regulations vallen en in de hele particuliere sector, waaronder sectoren als energie, gezondheidszorg en transport. Het raamwerk is opgebouwd rond vier hoofddoelstellingen: het beheren van veiligheidsrisico's, het beschermen tegen cyberaanvallen, het detecteren van cybersecurity-incidenten en het minimaliseren van de impact van incidenten. Het omvat 14 cyberbeveiligingsprincipes met ondersteunende resultaten en indicatoren van goede praktijken. Het CAF wordt gebruikt voor zowel zelfbeoordeling als voor beoordelingen door regelgevende instanties en biedt een systematische aanpak voor het beheren van cybersecurityrisico's en het waarborgen van naleving van relevante regelgeving.	
Toegankelijk-heid	Hoewel het raamwerk vrij toegankelijk is en kan worden aangepast voor intern gebruik binnen een organisatie of sector, is de officiële documentatie auteursrechtelijk beschermd door de Britse overheid (Crown Copyright).	G
Toepassings-gebied	Het Cyber Assessment Framework (CAF), ontwikkeld door het Britse National Cyber Security Centre (NCSC), is ontworpen om de digitale weerbaarheid van organisaties te verbeteren, met name van de organisaties die essentiële diensten en kritieke nationale infrastructuur exploiteren.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Het onderzoekt digitale weerbaarheid aan de hand van vier hoofddoelstellingen: het beheren van veiligheidsrisico's, het beschermen tegen cyberaanvallen, het detecteren van veiligheidsincidenten en het minimaliseren van de impact van incidenten. Deze elementen versterken het vermogen van een organisatie om cyberdreigingen te weerstaan en zich daarvan te herstellen. Het raamwerk omvat alle elementen en maatregelen die in deze studie zijn vastgesteld.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens worden verzameld door middel van een evaluatie van de mate waarin een organisatie een specifiek principe naleeft, wat wordt bepaald door alle bijdragende resultaten te beoordelen met betrekking tot dat principe. Ter ondersteuning van deze beoordelingen wordt elk bijdragend resultaat gekoppeld aan een reeks indicatoren voor goede praktijken (IGP's). En aan de hand van deze relevante IGP's worden de criteria voor het beoordelen of een resultaat 'bereikt', 'niet bereikt' of, indien van toepassing, 'gedeeltelijk bereikt' is, duidelijk gedefinieerd (NCSC, 2024).	G
Kwantitatieve indicatoren van digitale weerbaarheid	Het Cyber Assessment Framework (CAF) maakt gebruik van kwalitatieve indicatoren, zoals indicatoren voor goede praktijken, om de digitale weerbaarheid te beoordelen. Er worden geen kwantitatieve maatstaven beschreven.	R
Output	De output van het CAF wordt gegenereerd door de resultaten te identificeren die als cruciaalst worden beschouwd voor het beheer van veiligheidsrisico's voor de essentiële functies van een organisatie. Deze geprioriteerde resultaten bieden een eerste perspectief op wat passende en evenredige cybersecurity voor die organisatie inhoudt. De geselecteerde subset van belangrijke resultaten vormt een voorbeeld van een CAF-profiel, dat kan dienen als benchmark of doelstelling voor organisaties bij hun inspanningen op het gebied van cybersecurity.	A
Onbekende bedreigingen	Hoewel het niet expliciet tools bevat voor het detecteren van onbekende bedreigingen, kunnen organisaties die het CAF gebruiken het aanvullen met andere methodologieën die technieken bevatten voor het identificeren van onbekende bedreigingen, zoals *threat hunting* en gedragsanalyse.	R
Beperkingen	Niet vermeld.	A
Betrouwbaar-heid	Er zijn geen evaluaties gevonden van de betrouwbaarheid van het raamwerk.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

9. Cyber Resilience Quantification Framework (CRQF)

Beschrijving	Het raamwerk biedt een gestructureerde aanpak voor het evalueren, prioriteren en verbeteren van digitale weerbaarheid in organisaties door de fasen, capaciteiten en beïnvloedende factoren van digitale weerbaarheid te integreren. Het aanpasbare raamwerk is ontworpen om het vermogen van IT-infrastructuren om cyberaanvallen te weerstaan, te herstellen en te beoordelen, en omvat vier fasen: plannen/voorbereiden, absorberen, herstellen en aanpassen. Elke fase vertegenwoordigt een stadium in het reageren op cyberdreigingen en het verbeteren van de weerbaarheid.	
Toegankelijk-heid	Het eigendom van het raamwerk berust bij de auteurs of de uitgever. Het artikel is gratis toegankelijk.	G
Toepassings-gebied	IT-infrastructuur van elke organisatie.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Het CRQF onderzoekt digitale weerbaarheid aan de hand van absorptievermogen, aanpassingsvermogen en vitale capaciteiten, waarbij de nadruk ligt op het weerstaan van, aanpassen aan en herstellen van cyberincidenten. Het onderzoekt ook complexiteitsbeheer, netwerktopologie, toewijzing van middelen, IT-preconfiguratie en buffercapaciteit om de algehele weerbaarheid te verbeteren. Het raamwerk omvat alle elementen en maatregelen die in deze studie zijn vastgesteld.	
Inputgegevens (wat wordt verzameld en hoe)	Het CRQF is gebaseerd op simulaties voor het kwantificeren van digitale weerbaarheid. De invoerparameters voor elk simulatiescenario hebben betrekking op de kenmerken van het cybersysteem, de netwerkconfiguratie en het menselijk gedrag. Deze parameters worden systematisch gevarieerd om hun invloed op de digitale weerbaarheid te beoordelen. Tijdens de simulaties worden gegevens verzameld en geanalyseerd aan de hand van belangrijke prestatie-indicatoren, zoals de uptime van het systeem, de responstijd en het herstelvermogen, om de effectiviteit van het systeem bij het tegengaan van cyberdreigingen en verstoringen te evalueren (AlHidaifi et al. 2024).	G
Kwantitatieve indicatoren van digitale weerbaarheid	Kwantitatieve indicatoren van digitale weerbaarheid in CRQF omvatten complexiteitsscore, netwerkrobuustheid, benutting van middelen, effectiviteit van voorafgaande configuratie, buffercapaciteit en meetwaarden voor absorptie-, adaptieve en vitale capaciteiten. Daarnaast zijn Belief Networks (BN) gerichte cyclische grafieken die voorwaardelijke waarschijnlijkheidsrelaties tussen gegevensvariabelen weergeven, maar ze kunnen geen tijdsafhankelijke systemen modelleren. Dynamic Bayesian Networks (DBN), gebaseerd op verborgen Markov-modellen, lossen dit op door twee tijdsegmenten te gebruiken om de temporele systeemprestaties vast te leggen, waardoor ze geschikt zijn voor het modelleren en kwantificeren van digitale weerbaarheid, met knooppunten die digitale weerbaarheidprestaties vertegenwoordigen en koppelingen die voorwaardelijke overgangskansen illustreren.	G
Output	De output van het CRQF is een gekwantificeerde beoordeling van de digitale weerbaarheid van een organisatie, waarbij de sterke en zwakke punten van belangrijke factoren en capaciteiten worden benadrukt.	G
Onbekende bedreigingen	De stappen van risicobeoordeling en voortdurende verbetering maken het mogelijk om opkomende en zich ontwikkelende bedreigingen te identificeren en dragen bij aan de actualisering van het raamwerk.	G
Beperkingen	De nauwkeurigheid van de resultaten van de simulaties kan worden beïnvloed door factoren zoals modelvereenvoudigingen, aannames die tijdens de scenario-ontwikkeling zijn gedaan en de mate waarin de gesimuleerde omgeving de werkelijke cyberomstandigheden weerspiegelt.	A
Betrouwbaar-heid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R

Validiteit	Volgens de ontwikkelaars van het raamwerk is het simulatiemodel voor digitale weerbaarheid ontwikkeld op basis van gevestigde principes, gevalideerde algoritmen en input uit theoretische raamwerken en empirische gegevens (AlHidaifi et al. 2024). Er zijn echter geen evaluaties van de validiteit van het raamwerk gevonden in de literatuur.	R

10. Cyber Resilience Recovery Model (CRRM)

Beschrijving	Door beveiligingsverbeteringen onafhankelijk te simuleren, kan de effectiviteit van elke invoerparameter gecontroleerd worden geëvalueerd, waardoor beveiligingsmanagers op basis van kostenbeperkingen prioriteiten kunnen stellen bij de toewijzing van middelen. Bovendien kunnen organisaties de weerbaarheid van CRRM beoordelen door scenario's met worst-case- en best-case-scores opnieuw uit te voeren en de incidentpercentages te vergelijken. De methode richt zich op de simulatie van de verspreiding van malware. Daarom worden andere soorten cyberdreigingen, zoals phishing, ransomware, DDoS-aanvallen of bedreigingen van binnenuit, niet getest (Tran et al., 2016).	
Toegankelijk-heid	Het raamwerk mag niet vrij worden gebruikt, gewijzigd, commercieel geëxploiteerd of opnieuw verspreid zonder de uitdrukkelijke toestemming van de auteur.	A
Toepassings-gebied	Digitale weerbaarheid voor elke organisatie tegen de verspreiding van malware.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	A
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	De onderzochte elementen van digitale weerbaarheid omvatten het benutten van deskundige input om de besluitvorming te verbeteren, het prioriteren van meerdere criteria om cyberdreigingen aan te pakken en het waarborgen van betrouwbaarheid door middel van consistentieverhoudingen. Deze aanpak biedt een uitgebreide evaluatie van vier onafhankelijke gebieden (training in veiligheidsbewustzijn; verbetering van inbraak- en incident-detectie; verbetering van quarantaine; en verbetering van uitbanning en herstel), waardoor een holistisch beeld wordt gegeven van de digitale weerbaarheid van een organisatie (Tran et al., 2016). Het raamwerk omvat de elementen 'reageren' en 'herstellen' die in deze studie zijn vastgesteld, maar richt zich op technische en organisatorische maatregelen en laat procedurele maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	Het model verzamelt gegevens door meerdere criteria en alternatieven te prioriteren via een intuïtieve methode, waardoor het geschikt is voor het verzamelen en analyseren van input van cyberbeveiligingsexperts. In deze studie werden gegevens van 26 experts geaggregeerd met behulp van de geometrische gemiddelde methode, waarbij de nadruk lag op het handhaven van een bevredigende consistentieverhouding om de betrouwbaarheid te waarborgen. Dit proces evalueert vier onafhankelijke gebieden, die als input dienen voor het CRRM en een gestructureerde en consistente aanpak van gegevensintegratie bieden.	G
Kwantitatieve indicatoren van digitale weerbaarheid	Niet gespecificeerd.	R
Output	De output van dit proces is een betrouwbare en geprioriteerde evaluatie van meerdere criteria en alternatieven op vier onafhankelijke gebieden, gebaseerd op input van experts. Deze gestructureerde beoordeling vormt de basis voor het Cyber Resilience Response Model (CRRM), waardoor het effectief kan reageren op cyberdreigingen door gebruik te maken van consensus onder experts en een bevredigende consistentiegraad voor besluitvorming te handhaven.	A
Onbekende bedreigingen	CRRM is ontworpen om actieve incidenten af te handelen en de effectiviteit van verschillende verdedigingsconfiguraties te evalueren; daarom is de fase 'Activiteiten na het incident' niet in het model geïmplementeerd. Er wordt aangenomen dat er voorafgaand aan een aanval een risicobeoordeling wordt uitgevoerd.	G
Beperkingen	Niet vermeld.	A
Betrouwbaar-heid	Er zijn geen evaluaties gevonden van de betrouwbaarheid van het raamwerk.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

11. Cyber Resilience Self-Assessment Tool (CR-SAT)

Beschrijving	De CR-SAT dient als checklist voor organisaties om hun digitale weerbaarheid te evalueren en te verbeteren door beschrijvingen te selecteren die overeenkomen met hun huidige situatie en door verbeterpunten te identificeren (Carías et al., 2021).	
Toegankelijk-heid	Het auteursrecht op de tool en de bijbehorende documentatie blijft bij de auteurs of de uitgever, tenzij duidelijk wordt aangegeven dat er sprake is van een open licentie.	A
Toepassings-gebied	MKB.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	A
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	De onderzochte elementen van digitale weerbaarheid omvatten beleidsimplementatie en -volwassenheid, door experts gestuurde evaluatie, aanpassingsvermogen en voortgangsbewaking, en vergelijkende analyse, die allemaal bijdragen aan het verbeteren van het vermogen van een organisatie om weerstand te bieden aan en om zich aan te passen aan veranderende cyberdreigingen. Het raamwerk omvat de elementen 'herkennen' en 'beschermen' die in deze studie zijn vastgesteld, maar richt zich op procedurele en organisatorische maatregelen en laat technische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens worden verzameld via een vragenlijst die is afgeleid van een progressiemodel dat bestaat uit 33 beleidsmaatregelen. Elke beleidsmaatregel wordt gepresenteerd als een stelling en gebruikers selecteren hun implementatieniveau op basis van een schaal die de voortgang van de beleidsmaatregel in de loop van de tijd weergeeft. De schaal begint met een optie voor niet-geïmplementeerd, gevolgd door opties die verschillende voortgangsstadia aangeven. Dit progressiemodel is ontwikkeld aan de hand van een raamwerk dat is gebaseerd op de expertise van 11 professionals met 3 verschillende profielen: cybersecuritymanagers, -providers en -onderzoekers. Hun inzichten zijn verzameld tijdens semigestructureerde interviews van ongeveer anderhalf uur, waarin zij de initiële volwassenheidsgraad (beoordeeld op een schaal van 1 tot 5) en de progressie in de tijd voor elk beleid hebben gedefinieerd. Deze input van experts was cruciaal voor het opstellen van de vragenlijst, die vervolgens is gebruikt om een onlineprototype te ontwikkelen.	R
Kwantitatieve indicatoren van digitale weerbaarheid	Deze zelfbeoordeling wordt idealiter gekoppeld aan een volwassenheidsmodel en dit volwassenheidsmodel moet bij voorkeur een progressiemodel of hybridemodel zijn. De reden hiervoor is dat progressiemodellen eenvoudige progressies of schaalvergrotingen van kenmerken, indicatoren, attributen of patronen weergeven, en hybridemodellen een combinatie zijn van capaciteitsvolwassenheidsmodellen en progressiemodellen. Deze eenvoudige weergaven van de progressie of schaalvergroting van beleid inzake digitale weerbaarheid kunnen midden- en kleinbedrijven helpen om zich gemakkelijk te positioneren binnen een volwassenheidsniveau en op basis van hun huidige situatie gemakkelijk verbeteringsmaatregelen te definiëren (Carías et al., 2021).	A
Output	Na voltooiing van de zelfbeoordeling kunnen gebruikers een resultatenrapport bekijken dat wordt weergegeven door middel van verschillende radargrafieken die helpen om de niveaus van beleidsimplementatie en de geboekte voortgang met elkaar te vergelijken.	G
Onbekende bedreigingen	Niet vermeld.	A
Beperkingen	De beperkingen van deze aanpak zijn onder meer de moeilijkheid die bedrijven kunnen ondervinden bij het verkrijgen van toegang tot de resultaten, aangezien deze gefragmenteerd zijn en geen samenhangende, vertrouwde interface hebben die bedrijven doorgaans gebruiken.	R
Betrouwbaar-heid	De resultaten en de tool zelf zijn niet getest in praktijksituaties, wat van invloed kan zijn op de betrouwbaarheid ervan in de praktijk.	R
Validiteit	De resultaten en de tool zelf zijn niet geëvalueerd in praktijktoepassingen, wat twijfels kan oproepen over hun validiteit in praktische contexten.	R

12. Cyber Resiliency Engineering Framework (CREF)

Beschrijving	Het raamwerk schetst doelen, doelstellingen en praktijken die gericht zijn op het verbeteren van de weerbaarheid tegen ongunstige cybergebeurtenissen. De doelen – anticiperen, weerstaan, herstellen en evolueren – zijn gericht op het aanpassen van missies of cybercapaciteiten om de gevolgen van daadwerkelijke of verwachte aanvallen van tegenstanders te beperken (Munusamy & Khodadadi, 2023).	
Toegankelijk-heid	De CREF-documentatie van MITRE (inclusief fundamentele whitepapers en technische hulpmiddelen) kan gratis worden gedownload en gebruikt door het publiek via de officiële website van MITRE. Het is niet toegestaan om de documentatie te wijzigen, aan te passen of er afgeleide werken van te maken en deze te herdistribueren zonder uitdrukkelijke toestemming van MITRE.	G
Toepassings-gebied	IT-infrastructuur van elke organisatie.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	CREF onderzoekt digitale weerbaarheid aan de hand van vier primaire doelstellingen: anticiperen, weerstaan, herstellen en evolueren, waarbij gebruik wordt gemaakt van specifieke technieken, doelstellingen en ontwerpprincipes om de overlevingskansen van cybersecuritysystemen te vergroten. Het raamwerk biedt een gestructureerde aanpak voor het begrijpen en implementeren van digitale weerbaarheidsstrategieën in alle organisatorische systemen. Het raamwerk omvat alle elementen die in deze studie zijn vastgesteld, maar richt zich op procedurele maatregelen en laat technische en organisatorische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	Organisaties verzamelen inputgegevens door middel van risicobeoordelingen, dreigingsinformatie, kwetsbaarheidsscans en incidentlogboeken ter ondersteuning van de vier doelstellingen van het CREF-model: anticiperen, weerstaan, herstellen en evolueren.	G
Kwantitatieve indicatoren van digitale weerbaarheid	CREF biedt organisaties een structuur om hun eigen meetcriteria te ontwikkelen en te implementeren op basis van hun unieke behoeften en context. Deze meetcriteria kunnen maatregelen omvatten voor systeemprestaties onder ongunstige omstandigheden, hersteltijd na aanvallen, kwetsbaarheidsbeoordelingen, implementatie van weerbaarheidstechnieken en systeemdiversiteit. Het raamwerk maakt de integratie van verschillende gegevensbronnen en methoden mogelijk om relevante kwantitatieve indicatoren te creëren die aansluiten bij de weerbaarheidsdoelstellingen van de organisatie.	G
Output	Het CREF levert een gestructureerd raamwerk voor digitale weerbaarheid, met doelstellingen, technieken en ontwerpprincipes om organisaties te helpen cyberdreigingen te anticiperen, te weerstaan, ervan te herstellen en zich eraan aan te passen. De belangrijkste output is een uitgebreide aanpak voor het begrijpen en implementeren van cyberweerbaarheidsstrategieën op verschillende organisatieniveaus.	A
Onbekende bedreigingen	Het raamwerk omvat vier hoofddoelen: anticiperen op potentiële bedreigingen of tegenstanders, aanvallen of tegenstanders weerstaan, bedrijfsfuncties herstellen na een aanval, en organisatiefuncties aanpassen om de impact van een aanval te minimaliseren (Munusamy & Khodadadi 2023).	G
Beperkingen	Het CREF-model zou baat hebben bij een sterkere nadruk op leiderschapselementen. Er zou meer aandacht moeten worden besteed aan het creëren van een duidelijk doelbewustzijn (Munusamy & Khodadadi, 2023).	A
Betrouwbaar-heid	Het CREF wordt door MITRE, de eigenaar ervan, gepresenteerd als zeer betrouwbaar vanwege de uitgebreide methodologie, voortdurende updates, afstemming op gevestigde normen, praktische implementatiebegeleiding en flexibiliteit, hoewel de effectiviteit ervan afhankelijk is van een juiste implementatie binnen de organisatie (MITRE, 2023). In de literatuur is echter geen evaluatie van de betrouwbaarheid van het raamwerk gevonden.	R

Validiteit	MITRE werkt voortdurend aan de verbetering van CREF en heeft in 2023 de CREF Navigator-tool uitgebracht voor het aanpassen van cyberweerbaarheidsstrategieën. CREF sluit aan bij NIST's SP 800-160 v2 en biedt een uitgebreid raamwerk voor het anticiperen op, weerstaan van, herstellen van en aanpassen aan ongunstige cyberomstandigheden (Venkataramanan & Culler, 2024). Er is echter geen evaluatie van de validiteit van het raamwerk gevonden in de literatuur.	R

13. Cybersecurity Maturity Model Certification (CMMC)

Beschrijving	CMMC is een raamwerk dat is ontworpen om gevoelige informatie te beschermen door ervoor te zorgen dat defensiecontractanten robuuste cybersecuritypraktijken implementeren. Het bestaat uit drie volwassenheidsniveaus (Foundational, Advanced, Expert) en omvat certificering door een externe beoordelaar om naleving van cybersecuritynormen te waarborgen.	
Toegankelijk-heid	Eigendom van en beheerd door het Amerikaanse Ministerie van Defensie. Het certificeringsprogramma en de bijbehorende intellectuele eigendom staan onder toezicht van het Ministerie van Defensie en aanverwante instanties zoals de Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB). Het CMMC-model en de bijbehorende documentatie zijn openbaar beschikbaar. Het raamwerk kan niet vrij worden gewijzigd, waardoor het niet is toegestaan om afgeleide werken te wijzigen of te creëren en deze als officiële CMMC-materialen te presenteren. CMMC-certificering vereist beoordeling door geaccrediteerde externe beoordelaars (C3PAO's). Alleen gecertificeerde beoordelingen kunnen de naleving van DoD-contracten valideren (DoD, 2024).	A
Toepassings-gebied	CMMC is van toepassing op organisaties binnen de defensie-industrie, waaronder hoofdaannemers, onderaannemers en leveranciers die omgaan met federale contractinformatie en gecontroleerde niet-geclassificeerde informatie. Dit raamwerk is ontworpen om ervoor te zorgen dat deze organisaties robuuste cybersecuritypraktijken implementeren om gevoelige gegevens te beschermen, wat gevolgen heeft voor meer dan 300.000 bedrijven in de toeleveringsketen.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Het onderzoekt verschillende elementen van digitale weerbaarheid door zich te richten op 14 cybersecuritydomeinen die cruciaal zijn voor het beschermen van gevoelige informatie en het handhaven van de operationele continuïteit. Deze domeinen omvatten toegangscontrole, incidentrespons, risicobeoordeling en systeem- en informatie-integriteit. Door praktijken in deze domeinen te implementeren, verbeteren organisaties hun vermogen om cyberdreigingen te weerstaan en zich daarvan te herstellen, wat bijdraagt aan digitale weerbaarheid. Daarnaast benadrukt CMMC de weerbaarheid van de toeleveringsketen en zorgt ervoor dat organisaties de risico's in verband met hun toeleveringsketen beoordelen en beheren, wat essentieel is voor het behoud van de algehele digitale weerbaarheid. Het raamwerk omvat alle elementen en maatregelen die in deze studie zijn vastgesteld.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens voor CMMC omvatten een systeembeveiligingsplan, bewijs van naleving van beveiligingsvereisten, organisatorische informatie en details die de reikwijdte van de beoordeling definiëren.	G
Kwantitatieve indicatoren van digitale weerbaarheid	Het CMMC gebruikt kwalitatieve indicatoren om de naleving van zijn beveiligingsvereisten te beoordelen op drie volwassenheidsniveaus.	R
Output	De output van het CMMC is een certificering die het niveau van cybersecurityvolwassenheid van een organisatie aangeeft, variërend van niveau 1 (basis) tot niveau 3 (expert), wat vereist is voor het omgaan met federale contractinformatie en gecontroleerde niet-geclassificeerde informatie.	A
Onbekende bedreigingen	Het CMMC zelf detecteert niet direct onbekende bedreigingen, maar benadrukt de implementatie van robuuste cybersecuritypraktijken die kunnen helpen bij het identificeren en beperken van bedreigingen.	R
Beperkingen	Het CMMC heeft beperkingen, waaronder complexiteit en kosten, een zware documentatie- en nalevingslast, voortdurende behoefte aan middelen en uitdagingen bij het navigeren door gedetailleerde overheidsrichtlijnen.	A
Betrouwbaar-heid	Er is geen evaluatie van de betrouwbaarheid van het raamwerk gevonden.	R

Validiteit	Er is geen evaluatie van de validiteit van het raamwerk gevonden.	R

14. International Organization for Standardization's (ISO) 27000-series

Beschrijving	De ISO 27000-serie omvat normen voor informatiebeveiliging die organisaties helpen bij het beheren en beveiligen van hun informatieactiva, waarbij ISO/IEC 27001 zich richt op acht belangrijke functies, zoals contextbegrip en prestatie-evaluatie. De normen van het raamwerk bevorderen praktijken zoals bewustwording van beveiliging, gegevensback-up en continuïteitsplanning, waardoor de digitale weerbaarheid wordt vergroot.	
Toegankelijk-heid	Niet vrij verkrijgbaar: organisaties en individuen moeten officiële exemplaren rechtstreeks bij ISO, nationale instellingen of geautoriseerde wederverkopers aanschaffen om toegang te krijgen tot de volledige tekst en documentatie. Officiële documentatie (de volledige normen) moet worden aangeschaft.	A
Toepassings-gebied	Digitale weerbaarheid voor elke organisatie.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Dit omvat verbeterd risicobeheer, verbeterde beveiligingscontroles, naleving van wettelijke en regelgevende vereisten en effectieve incidentrespons en -beheer. Bovendien bevordert het raamwerk voortdurende verbetering, waardoor organisaties zich kunnen aanpassen aan veranderende bedreigingen en zakelijke behoeften. Daardoor blijft het vertrouwen van belanghebbenden behouden en wordt de algehele beveiligingspositie verbeterd. Het raamwerk omvat alle elementen die in deze studie zijn vastgesteld, al zijn technische maatregelen veelal procedureel geformuleerd.	
Inputgegevens (wat wordt verzameld en hoe)	Het ISO 27000-raamwerk helpt organisaties bij het verzamelen van gegevens om de informatiebeveiliging te verbeteren, met de nadruk op risicobeoordeling, beveiligingsmaatregelen, naleving, incidentbeheer en prestatiestatistieken. Gegevens worden verzameld via methoden zoals enquêtes, audits en geautomatiseerde tools, waardoor organisaties weloverwogen beslissingen kunnen nemen en hun beveiligingsmaatregelen kunnen verbeteren in overeenstemming met de normen. Er wordt echter geen gestandaardiseerde manier voor het verzamelen van inputgegevens geboden. Dit biedt flexibiliteit in de organisatorische context, maar leidt ook tot inconsistenties en moeilijkheden bij het vergelijken van organisaties (Dupont, 2019).	G
Kwantitatieve indicatoren	Er worden kwantitatieve maatstaven gebruikt. De potentiële indicatoren die worden gebruikt zijn echter niet vrij toegankelijk.	G
Output	Dit omvat verbeterd risicobeheer, verbeterde beveiligingsmaatregelen, naleving van wettelijke en regelgevende vereisten en effectieve respons op en beheer van incidenten. Bovendien bevordert het raamwerk voortdurende verbetering, waardoor organisaties zich kunnen aanpassen aan veranderende bedreigingen en zakelijke behoeften, waardoor het vertrouwen van belanghebbenden behouden blijft en de algehele beveiligingspositie wordt verbeterd.	A
Onbekende bedreigingen	Een meer gerichte norm (ISO/IEC 27035) biedt een reeks richtlijnen voor het plannen, voorbereiden en uitvoeren van activiteiten voor cyberincidentrespons. Door aan deze norm te voldoen, krijgen organisaties de capaciteit om onverwachte en onbekende bedreigingen het hoofd te bieden. De vijf fasen van de norm weerspiegelen het dynamische karakter van digitale weerbaarheid: plannen en voorbereiden, detecteren en rapporteren, beoordelen en beslissen, reageren en er lessen uit trekken.	G
Beperkingen	Dupont (2019) merkt op dat ISO27001 geen rangorde van de maatregelen vaststelt om aan te geven welke maatregelen het belangrijkst zijn in tegenstelling tot secundaire maatregelen, of maatregelen die alleen door de meest volwassen gebruikers in overweging moeten worden genomen.	G
Betrouwbaar-heid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

15. Linkov's Resilience Matrix Framework

Beschrijving	Het raamwerk maakt gebruik van een levenscyclusmodel met vier fasen – plannen/voorbereiden, absorberen, herstellen en aanpassen – in combinatie met vier domeinen uit de doctrine van netwerkcentrische operaties: fysiek, informatie, cognitief en sociaal. Het snijpunt van deze fasen en domeinen levert weerbaarheidsmetrieken op, die in een vervolgstudie verder zijn verfijnd door kwantitatieve en kwalitatieve maatregelen uit bestaande literatuur te integreren.	
Toegankelijk-heid	Aangezien het conceptuele en methodologische raamwerk onderworpen is aan het auteursrecht van het tijdschrift of de uitgever, kan het vrij worden bestudeerd, geciteerd en geïmplementeerd in onderzoek, industriële rapporten en interne documenten.	A
Toepassings-gebied	Theoretische raamwerken.	R
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	A
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Het raamwerk maakt het mogelijk om de capaciteit van een organisatie om te plannen, op te vangen, te herstellen en zich aan te passen binnen de fysieke, informatie-, cognitieve en sociale domeinen te evalueren (Annarelli et al., 2020). Het raamwerk omvat de elementen 'herkennen', 'beschermen', 'reageren' en 'herstellen' die in deze studie zijn vastgesteld, terwijl het zich richt op technische, procedurele en organisatorische maatregelen.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens voor het raamwerk kunnen bestaan uit strategische plannen, incidentrapporten, herstelanalyses en aanpassingsverslagen op fysiek, informatie-, cognitief en sociaal gebied, verzameld door middel van inspecties, audits, enquêtes en literatuuronderzoek.	A
Kwantitatieve indicatoren van digitale weerbaarheid	Niet vermeld.	A
Output	De output van het raamwerk is een reeks verfijnde weerbaarheidmetrieken die de organisatie beoordelen op haar vermogen om te plannen, te absorberen, te herstellen en zich aan te passen op fysiek, informatie-, cognitief en sociaal gebied, waardoor een uitgebreide evaluatie van haar weerbaarheidscapaciteit tot stand komt (Annarelli et al., 2020).	A
Onbekende bedreigingen	Niet (aannemelijk) vastgelegd.	R
Beperkingen	Niet vermeld.	A
Betrouwbaar-heid	Er zijn geen evaluaties gevonden van de betrouwbaarheid van het raamwerk.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

16. National Institute of Standards and Technology (NIST) Framework

Beschrijving	Het NIST-raamwerk bestaat uit vijf belangrijke functies – identificeren, beschermen, detecteren, reageren en herstellen – die zijn onderverdeeld in 23 categorieën en 108 subcategorieën, in overeenstemming met andere normen zoals ISO/IEC 27001 (raamwerk nr. 14 in dit rapport) en COBIT 5. Het biedt vier "implementatieniveaus" (gedeeltelijk, risicogebaseerd, herhaalbaar en adaptief) om tegemoet te komen aan verschillende organisatorische capaciteiten, waarbij elk niveau een vooruitgang in digitale weerbaarheid en aanpassingsvermogen weerspiegelt.	
Toegankelijkheid	Het raamwerk en alle officiële documentatie zijn volledig gratis toegankelijk en te gebruiken. NIST publiceert het CSF en aanverwante materialen openlijk op hun website, zonder kosten voor het downloaden of gebruiken ervan.	G
Toepassingsgebied	Digitale weerbaarheid voor elke organisatie.	G
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	G
	Het NIST Cybersecurity Framework beslaat digitale weerbaarheid door cybersecurityrisico's te identificeren en te beheren, beschermende maatregelen te implementeren en incidenten snel op te sporen om de levering van kritieke infrastructuurdiensten te waarborgen. Het omvat ook het element 'reageren' om de impact van cybersecurityincidenten te beperken en het onderhouden van herstelplannen om aangetaste capaciteiten of diensten te herstellen, waardoor het vermogen om verstoringen te weerstaan en hiervan te herstellen, wordt verbeterd. Het raamwerk omvat alle elementen en maatregelen die in deze studie zijn vastgesteld.	
Inputgegevens (wat wordt verzameld en hoe)	Het raamwerk verzamelt gegevens over drie hoofdcomponenten: de Kern, die betrekking heeft op technische beveiligingsmaatregelen; de Implementatieniveaus, die risicobeheerpraktijken beoordelen; en de Profielen, die de toepassing binnen specifieke sectoren of organisaties weerspiegelen, waarbij de Kern verder bestaat uit functies, categorieën, subcategorieën en informatieve referenties.	G
Kwantitatieve indicatoren van digitale weerbaarheid	Niet vermeld.	R
Output	Het raamwerk biedt een reeks resultaten om prioriteit te geven aan cybersecurityrisico's en deze aan te pakken, maar specificeert geen acties om deze resultaten te bereiken en biedt ook geen certificering.[6]	A
Onbekende bedreigingen	Stappen van de NIST-risicobeoordeling: ID.RA-03: interne en externe bedreigingen voor de organisatie worden geïdentificeerd en geregistreerd; ID.RA-04: Potentiële gevolgen en waarschijnlijkheid van bedreigingen die misbruik maken van kwetsbaarheden worden geïdentificeerd en geregistreerd.	G
Beperkingen	Deze aanpak wordt bekritiseerd omdat ze mogelijk leidt tot zelfgenoegzaamheid bij de risicobeoordeling, meer aandacht besteedt aan cyberaanvallen dan aan weerbaarheid, en steunt op vrijwillige richtlijnen, wat investeringen in cybersecurity kan ontmoedigen als de kosten of de benodigde middelen hoog zijn (Dupont, 2019).	G
Betrouwbaarheid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

[6] Zie: https://www.nist.gov/cyberframework/faqs

17. National Infrastructure Advisory Council (NIAC) Resilience Model

Beschrijving	Het model heeft tot doel de weerbaarheid van kritieke infrastructuur te vergroten door middel van concepten als robuustheid, vindingrijkheid, snel herstel en aanpassingsvermogen. Het biedt hoogwaardige weerbaarheidsdoelstellingen die zijn afgestemd op specifieke sectoren, waardoor organisaties deze concepten binnen hun bedrijfscontext kunnen interpreteren en implementeren, hoewel de brede aanpak kan leiden tot uiteenlopende interpretaties.	
Toegankelijkheid	Het kernmodel en de officiële documentatie zijn vrij beschikbaar. De eigenaar is de federale overheid van de Verenigde Staten, met name de NIAC, die onder het Department of Homeland Security (DHS) valt.	G
Toepassingsgebied	IT-infrastructuur van elke organisatie.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	A
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	Het NIAC-weerbaarheidsmodel onderzoekt digitale weerbaarheidselementen zoals robuustheid (bestand zijn tegen verstoringen), vindingrijkheid (beheren van middelen tijdens crises), snel herstel (snel herstellen van activiteiten) en aanpassingsvermogen (aanpassen van strategieën aan veranderende bedreigingen). Deze elementen helpen organisaties bij het implementeren van op maat gemaakte weerbaarheidsstrategieën. Het raamwerk omvat de elementen 'reageren' en 'herstellen' die in deze studie zijn vastgesteld, maar richt zich op procedurele en organisatorische maatregelen en laat technische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	De invoergegevens voor het NIAC-weerbaarheidsmodel omvatten branche-specifieke informatie, organisatorische beoordelingen, gegevens over incidenten en verstoringen, input van belanghebbenden, inventarisaties van middelen en omgevingsscans. Deze worden verzameld via interne audits, brancheverslagen, enquêtes onder belanghebbenden en marktonderzoek om de weerbaarheidsdoelstellingen af te stemmen op de bedrijfscontext van de organisatie.	G
Kwantitatieve indicatoren van digitale weerbaarheid	Het NIAC-weerbaarheidsmodel definieert niet expliciet kwantitatieve indicatoren voor digitale weerbaarheid, omdat het zich meer richt op weerbaarheidsdoelstellingen op hoog niveau die zijn afgestemd op industriesectoren.	A
Output	De output van het NIAC-weerbaarheidsmodel is een reeks weerbaarheidsdoelstellingen op hoog niveau die zijn afgestemd op specifieke industriesectoren, waardoor organisaties weerbaarheidsconcepten – zoals robuustheid, vindingrijkheid, snel herstel en aanpassingsvermogen – kunnen interpreteren en toepassen binnen hun unieke bedrijfscontext. Deze output biedt organisaties een raamwerk voor het implementeren van noodzakelijke weerbaarheidsmaatregelen en -strategieën, terwijl er flexibiliteit is voor interpretatie en aanpassing op basis van hun specifieke behoeften en omstandigheden (NIAC, 2020).	A
Onbekende bedreigingen	Niet vermeld.	A
Beperkingen	Het NIAC-weerbaarheidsmodel tracht weerbaarheidsdoelen te identificeren die zijn afgestemd op specifieke industriesectoren.	A
Betrouwbaarheid	Er zijn geen evaluaties gevonden van de betrouwbaarheid van het raamwerk.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk.	R

18. TNO raamwerk

Beschrijving	Het raamwerk bestaat uit 47 meetcriteria die zijn samengevoegd in 10 kerncategorieën, gestructureerd rond het *cyber kill chain*-model van Lockheed Martin, om te beoordelen in hoeverre een organisatie voorbereid is op gerichte cyberaanvallen of Advanced Persistent Threats (APT's). Elke categorie vertegenwoordigt een cruciale capaciteit voor het voorkomen of beheersen van dergelijke aanvallen, zoals het vermogen om social engineering te voorkomen of malware te weerstaan, en weerspiegelt belangrijke aspecten van de weerbaarheid van een organisatie bij het omgaan met geavanceerde cyberdreigingen.	
Toegankelijkheid	Het raamwerk is niet gratis voor onbeperkt gebruik/wijziging. Het intellectuele eigendom berust bij TNO of haar projectpartners, en er zijn geen aanwijzingen dat het raamwerk onder opensource- of Creative Commons-licenties wordt gepubliceerd.	A
Toepassingsgebied	Financiële diensten.	A
Welke elementen van digitale weerbaarheid worden onderzocht	Herkennen | Beschermen | Detecteren | Reageren | Herstellen	G
	Technische maatregelen | Procedurele maatregelen | Organisatorische maatregelen	A
	Het raamwerk onderzoekt belangrijke aspecten van digitale weerbaarheid door de paraatheid van een organisatie voor gerichte cyberaanvallen, met name Advanced Persistent Threats (APT's), te evalueren. Het onderzoekt het vermogen om social engineering-tactieken, zoals phishing – vaak worden ze gebruikt in de verkenningsfase van aanvallen – af te wenden en beoordeelt het vermogen om malware te weerstaan door kwaadaardige software op te sporen, in te dammen en te verhelpen. Indicatoren zijn moeilijk te evalueren zonder ze te vergelijken met die welke in de *service level agreements* van de organisatie zijn gespecificeerd. Bovendien lijkt de huidige aanpak een risicogebaseerd perspectief te missen en houdt deze geen rekening met de omvang of sector van de organisatie. Het raamwerk omvat alle elementen die in deze studie zijn vastgesteld, maar richt zich specifiek op technische en procedurele maatregelen en laat organisatorische maatregelen buiten beschouwing.	
Inputgegevens (wat wordt verzameld en hoe)	Inputgegevens worden verzameld via processen of technische voorzieningen die waarschijnlijk de gegevens bieden die nodig zijn om de meetwaarden in de praktijk te kwantificeren.	G
Kwantitatieve indicatoren van digitale weerbaarheid	De meetcriteria van het raamwerk zijn als volgt in tien categorieën onderverdeeld: 1. Social engineering voorkomen (bijv. percentage werknemers dat social engineering herkent en meldt wanneer het wordt onderworpen aan een telefonische beoordeling) 2. Gebruikmaken van dreigingsinformatie (percentage dreigingsmeldingen die aanleiding gaven tot concrete maatregelen, zoals het aanpassen van firewallregels of het monitoren van IoC, in operationele beveiligingsprocessen) 3. Kwetsbaarheden aanpakken (bijv. percentage IT-middelen dat wordt gedekt door geautomatiseerde kwetsbaarheidsscans) 4. Cyberincidenten afhandelen (bijv. de gemiddelde tijd – uren, dagen – die verstreken is tussen het begin en de detectie van een cyberincident) 5. Weerstaan van malware (bijv. aantal unieke malwarevarianten dat vóór activering is gedetecteerd) 6. Weerstaan van inbraken (bijv. jaarlijks aantal onafhankelijke systeemintrusie-incidenten) 7. Weerstand bieden tegen DDoS (bijv. gemiddelde tijd (minuten, uren) die nodig is om een DDoS-aanval te erkennen, d.w.z. de gemiddelde tijd die verstrijkt tussen de eerste waarschuwing en de formele diagnose van een aanhoudende DDoS-aanval) 8. Bescherming van inloggegevens (bijv. jaarlijks aantal pogingen tot inbraak waarbij aantoonbaar sprake was van ongeoorloofd gebruik van geldige inloggegevens of tokens) 9. Bescherming van belangrijke activa (bijv. jaarlijks percentage pogingen tot gegevensdiefstal die zijn voorkomen door automatische of menselijke interventie) 10. Schade minimaliseren (bijv. geld dat verloren is gegaan als gevolg van cyberincidenten als percentage van het overgemaakte geld)	G

Output	De output van het raamwerk is een gedetailleerde beoordeling van de digitale weerbaarheid van een financiële organisatie tegen gerichte cyberaanvallen, zoals Advanced Persistent Threats (APT's). Het evalueert belangrijke capaciteiten, zoals het afweren van social engineering en het weerstaan van malware, en helpt organisaties bij het identificeren en aanpakken van kwetsbaarheden in hun cyberverdediging.	G
Onbekende bedreigingen	Niet vermeld.	A
Beperkingen	Specifiek voor grote financiële organisaties en voornamelijk gericht op operationele elementen, minder op organisatorische elementen.	A
Betrouwbaar-heid	Er zijn geen evaluaties van de betrouwbaarheid van het raamwerk gevonden.	R
Validiteit	Er zijn geen evaluaties gevonden over de validiteit van het raamwerk of de statistische deugdelijkheid van de indicatoren.	R

3.3. Analyse van bestaande benaderingen om digitale weerbaarheid te meten

De term 'digitale weerbaarheid' wordt minder vaak gebruikt dan 'cyberweerbaarheid' om de beveiligingsstatus van een organisatie te beschrijven, die op zijn beurt weer minder vaak wordt gebruikt dan 'cyber security'. Bovendien worden de begrippen `cyberweerbaarheid' en `digitale weerbaarheid' gekenmerkt door een reeks van definities, wat leidt tot uiteenlopende en soms tegenstrijdige interpretaties van hun reikwijdte wanneer ze worden toegepast op praktische organisatorische metingen.

Deze ambiguïteit in de definitie is terug te zien in de literatuur over de hierboven besproken benaderingen. Duidelijk is dat digitale weerbaarheid van organisaties een multidimensionaal construct is waarvoor geen algemeen aanvaarde definitie of gestandaardiseerd meetraamwerk bestaat. Bestaande benaderingen variëren aanzienlijk in hun thematische focus, detailniveau en wijze waarop de implementatie beoordeeld wordt, als een dergelijke beoordeling al wordt uitgevoerd. Deze variabiliteit onderstreept de inherente complexiteit van het digitale weerbaarheidslandschap en weerspiegelt de uiteenlopende eisen van organisaties die daarin actief zijn.

Door de kleurgecodeerde aspecten van de verschillende besproken benaderingen in één tabel samen te voegen, creëren we een visueel overzicht dat de sterke punten en beperkingen van de verschillende raamwerken illustreert. Tabel 7 laat zien op welke punten de benaderingen overeenkomen en verschillen, en hoe elke benadering verschillende facetten van digitale weerbaarheid aanpakt.

Tabel 7. Samenvatting van bestaande benaderingen voor het meten van digitale weerbaarheid

	Toegankelijk-heid	Kern-elementen	Input	Kwantitatieve indicatoren	Output	Onbekende dreigingen	Beperkingen	Betrouwbaar-heid	Validiteit
1. Ambidextrous cybersecurity-approach	G	G	G	A	A	G	G	R	R
2. Blanchet et al. (2017) conceptueel raamwerk	G	A	A	A	A	R	A	R	R
3. De criteria van Bradford Hill	G	A	A	A	A	R	A	R	R
4. CERT Resilience Management Model (CERT-RMM)	A	A	A	G	A	A	A	R	R
5. Common Vulnerability Scoring System (CVSS)	G	A	G	G	G	A	A	R	R
6. Cyber Essentials	G	A	G	R	A	R	A	R	R
7. Cyber Physical Systems Security Framework (CPSS)	G	A	G	A	G	A	A	R	R
8. Cyber Assessment Framework (CAF)	G	G	G	R	A	R	A	R	R
9. Cyber Resilience Quantification Framework (CRQF)	G	G	G	G	G	G	A	R	R
10. Cyber Resilience Recovery Model (CRRM)	A	A	G	R	A	G	A	R	R
11. Cyber Resilience Self-Assessment Tool (CR-SAT)	A	A	R	A	G	A	R	R	R
12. Cyber Resiliency Engineering Framework (CREF)	G	A	G	G	A	G	A	R	R
13. Cybersecurity Maturity Model Certificate	A	G	G	R	A	R	A	R	R
14. International Organization for Standardization's (ISO) 27000-series	A	G	G	G	A	G	G	R	R
15. Linkov's Resilience Matrix Framework	A	A	A	A	A	R	A	R	R
16. National Institute of Standards and Technology (NIST) Framework	G	G	G	R	A	G	G	R	R
17. National Infrastructure Advisory Council (NIAC) Resilience Model	G	A	G	A	A	A	A	R	R
18. TNO-raamwerk	A	A	G	G	G	A	A	R	R

Tabel 8. Samenvattende beoordeling van elementen van digitale weerbaarheid die onder de raamwerken vallen

	Fasen van digitale weerbaarheid					Soorten maatregelen		
	Herken	**Bescherm**	**Detecteer**	**Reageer**	**Herstel**	**Technisch**	**Procedureel**	**Organisatorisch**
1. Ambidextrous cybersecurity-approach	G	G	G	G	G	G	G	G
2. Blanchet et al. (2017) conceptueel raamwerk	G	G	G	G	G	R	G	G
3. De criteria van Bradford Hill	R	R	R	R	R	R	G	R
4. CERT Resilience Management Model (CERT-RMM)	G	G	G	G	G	G	R	G
5. Common Vulnerability Scoring System (CVSS)	R	R	G	G	R	R	G	R
6. Cyber Essentials	G	G	R	R	R	G	R	R
7. Cyber Physical Systems Security Framework (CPSS)	G	G	G	G	G	G	G	R
8. Cyber Assessment Framework (CAF)	G	G	G	G	G	G	G	G
9. Cyber Resilience Quantification Framework (CRQF)	G	G	G	G	G	G	G	G
10. Cyber Resilience Recovery Model (CRRM)	R	R	R	G	G	G	R	G
11. Cyber Resilience Self-Assessment Tool (CR-SAT)	G	G	R	R	R	R	G	G
12. Cyber Resiliency Engineering Framework (CREF)	G	G	G	G	G	R	G	R
13. Cybersecurity Maturity Model Certificate	G	G	G	G	G	G	G	G
14. International Organization for Standardization's (ISO) 27000-series	G	G	G	G	G	R	G	G
15. Linkov's Resilience Matrix Framework	G	G	R	G	G	G	G	G
16. National Institute of Standards and Technology (NIST) Framework	G	G	G	G	G	G	G	G
17. National Infrastructure Advisory Council (NIAC) Resilience Model	R	R	R	G	G	R	G	G
18. TNO-raamwerk	G	G	G	G	G	G	G	R

Concluderend kan worden gesteld dat bestaande meetinstrumenten en raamwerken weliswaar waardevolle inzichten en operationele richtsnoeren bieden, maar vaak grotendeels conceptueel blijven en niet alle cruciale aspecten van digitale weerbaarheid volledig lijken te behandelen. Bovenstaande tabellen onderstrepen de volgende belangrijke aspecten:

- **De benaderingen zijn voornamelijk gericht op het helpen van organisaties om inzicht te krijgen in hun eigen cybersecuritypositie**. Organisatiespecifieke resultaten kunnen niet onmiddellijk worden vergeleken met de resultaten van andere organisaties. Hoewel dit waarschijnlijk moeilijk te realiseren is, zouden dergelijke resultaten in theorie ten minste een totaalbeeld op maatschappelijk niveau kunnen opleveren. Om verschillende redenen, waaronder de gevoeligheid van gegevens, gebeurt dit echter zelden. Deze raamwerken bieden meerwaarde op organisatieniveau door gestructureerde richtlijnen te geven om bekende bedreigingen aan te pakken en de weerbaarheid te vergroten. Niet alle geanalyseerde raamwerken bieden echter gedetailleerde methodologieën. Veel raamwerken, zoals het NIST Cybersecurity Framework, vermijden het bewust om voor te schrijven hoe organisaties bepaalde maatregelen moeten implementeren om flexibiliteit te behouden, waardoor ze in een breed scala aan organisaties kunnen worden toegepast. Dit kan echter ook leiden tot verwarring over wat in de praktijk 'goed' is. Bovendien kan het ertoe leiden dat organisaties verschillende benaderingen implementeren ofschoon ze hetzelfde raamwerk volgen.
- **De meeste benaderingen zijn toepasbaar in verschillende sectoren** en benadrukken flexibiliteit in hun kaders of richtlijnen. In plaats van hun methodologieën af te stemmen op specifieke sectoren, richten deze benaderingen zich op het creëren van aanpasbare structuren die kunnen worden toegepast in organisaties van verschillende soorten, omvang en sectoren. Deze flexibiliteit legt de verantwoordelijkheid bij organisaties om interventies te identificeren en toe te passen die zijn afgestemd op hun unieke operationele behoeften en doelstellingen, waardoor een bredere toepasbaarheid wordt gewaarborgd zonder dat dit ten koste gaat van de relevantie.
- **De meeste benaderingen richten zich op kwalitatieve in plaats van kwantitatieve indicatoren**, waarbij de nadruk ligt op beschrijvende beoordelingen en subjectieve evaluaties in plaats van numerieke of datagestuurde meetcriteria. Deze kwalitatieve indicatoren bieden vaak contextuele inzichten in de cybersecuritypositie en weerbaarheidscapaciteiten van een organisatie en zijn wellicht beter geschikt om de nuances van complexe beveiligingsmaatregelen weer te geven. Het vertrouwen op kwalitatieve maatregelen kan echter het vermogen beperken om prestaties te benchmarken of weerbaarheidsniveaus tussen organisaties op een gestandaardiseerde manier te vergelijken. Slechts vier van de geïdentificeerde benaderingen richten zich specifiek op kwantitatieve indicatoren:
    - Het CERT Resilience Management Model (CERT-RMM, methode nr. 4 in paragraaf 3.2) is ontworpen om de operationele weerbaarheid van een organisatie te verbeteren door beveiliging, bedrijfscontinuïteit en IT-activiteiten te integreren. Door middel van gestructureerde processen en praktijken ondersteunt het organisaties bij het handhaven van kritieke functies tijdens verstoringen, waardoor hun algehele weerbaarheid wordt verbeterd.

  - Het Common Vulnerability Scoring System (CVSS, nr. 5) is een gestandaardiseerd raamwerk voor het evalueren van de ernst van beveiligingskwetsbaarheden in computersystemen. Het kent een numerieke score toe, waardoor organisaties hun responsinspanningen kunnen prioriteren door rekening te houden met factoren zoals de complexiteit van de aanval en de impact op de vertrouwelijkheid, integriteit en beschikbaarheid. CVSS is echter beperkt tot kwetsbaarheidsbeoordeling en omvat geen bredere aspecten van digitale weerbaarheid.
  - Het Cyber Risk Quantification Framework (CRQF, nr. 9) biedt een methodologie om cyberrisico's te vertalen naar financiële termen, waardoor organisaties de economische impact van cyberdreigingen kunnen beoordelen. Door risico's uit te drukken in geldwaarden, vergemakkelijkt het raamwerk het stellen van prioriteiten voor investeringen in cybersecurity en ondersteunt het weloverwogen besluitvormingsprocessen.
  - Het TNO-raamwerk (nr. 18) richt zich op het versterken van de weerbaarheid van een organisatie tegen bekende gerichte cyberaanvallen, zoals Advanced Persistent Threats (APT's). Het evalueert kritieke capaciteiten, waaronder weerbaarheid tegen social engineering en malware, en biedt een gestructureerde, op meetbare criteria gebaseerde aanpak voor het beoordelen en verbeteren van de digitale weerbaarheid van organisaties met betrekking tot geavanceerde bedreigingen.

- **Hoewel de meeste benaderingen niet expliciet ingaan op het beheer van onbekende bedreigingen, benadrukken verschillende van de onderzochte meetraamwerken een proactieve strategie om met dergelijke onzekerheden om te gaan.** Deze raamwerken geven prioriteit aan het opbouwen van weerbaarheid door organisaties in staat te stellen te anticiperen op, zich aan te passen aan en te reageren op opkomende en veranderende dreigingen, in plaats van maatregelen te nemen die specifiek gericht zijn op onbekende bedreigingen. Door deze strategieën toe te passen, kunnen organisaties een robuuste basis leggen die niet alleen de huidige risico's beperkt, maar ook hun vermogen versterkt om onbekende en toekomstige bedreigingen effectief te beheersen.
- **Deze studie heeft geen bewijs gevonden voor de validiteit en betrouwbaarheid van de geïdentificeerde benaderingen.** Hoewel er een breed scala aan benaderingen bestaat, zijn deze niet noodzakelijkerwijs gericht op digitale weerbaarheid en meten ze vaak diverse aspecten van organisatorische veiligheid. Ondanks hun potentieel om gestructureerde benaderingen te bieden voor het verbeteren van digitale weerbaarheid, is er een opvallend gebrek aan bewijs met betrekking tot hun validiteit en betrouwbaarheid. Er lijkt een gebrek aan onderzoek te zijn om na te gaan of de indicatoren en methodologieën die door deze raamwerken worden gebruikt, nauwkeurig meten wat ze beogen en of ze consistent zinvolle resultaten opleveren in verschillende organisatorische contexten. Dit roept vragen op over de werkelijke waarde die deze raamwerken bieden en de mate waarin ze bijdragen aan het verbeteren van de digitale weerbaarheid. Bovendien blijven de specifieke mechanismen waarmee deze raamwerken van invloed zijn op weerbaarheid onduidelijk, waardoor het moeilijk is om hun effectiviteit te bepalen. Zonder robuust bewijs ter ondersteuning van hun betrouwbaarheid en validiteit, lopen de kaders het risico te worden gezien als theoretische constructies in plaats van bruikbare instrumenten voor het versterken van digitale weerbaarheid.

4. Conclusie

In dit hoofdstuk analyseren we wat de vorige twee hoofdstukken ons leren over hoe digitale weerbaarheid meetbaar kan worden gemaakt, en onderzoeken we de betekenis van deze bevindingen voor de NCTV. Ook bespreken we de mogelijkheden voor de NCTV tot het ontwikkelen van een uniforme meetmethode voor organisatorische digitale weerbaarheid in Nederland, rekening houdend met alle geïdentificeerde uitdagingen.

4.1. Huidige benaderingen en beperkingen bij het meten van digitale weerbaarheid

De belangrijkste implicatie voor de NCTV is dat er op dit moment geen bestaand raamwerk beschikbaar is om de specifieke gegevens te genereren die nodig zijn voor het meten van digitale weerbaarheid. Bovendien ontbreken de empirische gegevens die nodig zijn om de validiteit van de huidige meetmethoden te toetsen. Dit betekent dat er, ondanks de vele raamwerken en methodologieën, nog steeds een lacune bestaat in zowel inzetbare meetinstrumenten als in het ondersteunende bewijs dat nodig is om de betrouwbaarheid en effectiviteit ervan voor de doeleinden van de NCTV te waarborgen.

De benaderingen die in deze studie zijn geïdentificeerd en geanalyseerd, benadrukken de inherente afwegingen en spanningen die gepaard gaan met het conceptualiseren en het meten van digitale weerbaarheid op organisatieniveau. De kenmerken, inhoud en structuur van deze benaderingen worden grotendeels bepaald door de ontwerpkeuzes die tijdens de ontwikkeling ervan zijn gemaakt, die uiteindelijk worden bepaald door het beoogde doel van het raamwerk.

Het uiteindelijke doel van een raamwerk voor het meten van digitale weerbaarheid is dus inherent verbonden met de onderliggende conceptualisering van de term ‘digitale weerbaarheid’. Hoewel de meeste benaderingen verschillende definities en karakteriseringen van digitale weerbaarheid bieden, bevatten veel benaderingen een vergelijkbare cyclische logica zoals die in de ISO- en NIST-raamwerken, met overkoepelende componenten zoals herkennen, beschermen, detecteren, reageren en herstellen. Deze worden vaak aangevuld met elementen zoals governance of leiderschap om een uitgebreider perspectief te bieden. Dit benadrukt het continue karakter van digitale weerbaarheid en benadrukt dat het geen eenmalige inspanning is, maar een continu proces dat aanhoudende middelen en investeringen op meerdere dimensies vereist. Bovendien benadrukt deze cyclische benadering een belangrijk verschil tussen traditionele cybersecurity, waarbij historisch gezien prioriteit werd gegeven aan bescherming, en het zich ontwikkelende begrip van digitale weerbaarheid, dat meer nadruk legt op het vermogen van een organisatie om cyberincidenten op te vangen, erop te reageren en ervan te herstellen.

Sommige benaderingen, zoals ISO en NIST, leggen de nadruk op volledigheid en streven ernaar om zoveel mogelijk aspecten van de digitale weerbaarheid van organisaties te omvatten. Ze schrijven echter geen specifieke prestatie-indicatoren (KPI's) of metingen voor elk kenmerk voor. Deze flexibiliteit stelt diverse organisaties in staat om het raamwerk toe te passen en zich aan te passen aan erkende goede praktijken, zonder te worden beperkt door rigide indicatoren die mogelijk niet passen bij hun operationele context. Benaderingen zoals het TNO-raamwerk bieden daarentegen gedetailleerde kwantitatieve indicatoren die zijn ontworpen om op organisatieniveau te worden gemeten en die inzicht bieden in de relatieve prestaties binnen een bepaalde context. Deze raamwerken richten zich doorgaans op specifieke aspecten van digitale weerbaarheid of sectorale behoeften, in plaats van te proberen de algehele digitale weerbaarheid te meten.

Sommige van de geïdentificeerde meetmethoden zijn ook gericht op het waarborgen van een minimaal vereist niveau van cybersecurity of digitale weerbaarheid. Deze methoden focussen doorgaans op een beperktere reeks normen of indicatoren die toegankelijk zijn voor elk type organisatie, ongeacht de omvang of het budget. Een goed voorbeeld van deze benadering is het Britse Cyber Essentials-programma (NCSC, 2024a), dat is ontworpen om ervoor te zorgen dat organisaties een basisniveau van technische controles hebben geïmplementeerd om een goede cybersecurity en fundamentele digitale weerbaarheid te waarborgen. Soortgelijke initiatieven in Nederland, zoals CYRA[7], zouden kunnen worden uitgebreid. Het zwakke punt van deze benaderingen is echter dat ze vaak slechts een momentopname geven van de beveiliging van een organisatie en dat ze doorgaans gebaseerd zijn op zelfevaluaties, die onderhevig kunnen zijn aan vooringenomenheid of misverstanden. Ze bieden ook slechts beperkt bewijs voor de causale effecten van beleidsmaatregelen. Met andere woorden: het is maar de vraag of een specifiek initiatief direct heeft bijgedragen aan vergroting van de digitale weerbaarheid. Een afname van bijvoorbeeld het aantal geregistreerde incidenten hoeft niet noodzakelijkerwijs te duiden op een verbetering van de weerbaarheid, aangezien een afname van het aantal incidenten het gevolg kan zijn van verschillende factoren, waaronder veranderingen in het gedrag van aanvallers of verschuivingen in de keuze van doelwitten, en niet noodzakelijkerwijs het directe gevolg van een bepaald beleid.

Zoals opgemerkt zijn er ook bestaande initiatieven in zowel Nederland als elders, zoals Internet.nl[8], die tot doel hebben basismaatregelen voor internetbeveiliging te waarborgen. Hoewel deze inspanningen kunnen bijdragen aan het vergroten van de digitale weerbaarheid, zijn ze beperkt tot specifieke gebieden, zoals internetdomeinen en e-mailbeheer, die slechts een klein onderdeel vormen van de algehele digitale weerbaarheid. Er worden ook inspanningen geleverd om proxyindicatoren te gebruiken om de staat van de digitale weerbaarheid te meten, of beter gezegd, de omgekeerde parameter daarvan, namelijk kwetsbaarheid. In Nederland kijkt het NCSC bijvoorbeeld naar indicatoren zoals het aantal gemelde cyberincidenten, ransomware-aanvallen, DDoS-aanvallen en ICT-beveiligingsinbreuken die de drempelwaarden overschrijden om de toestand van het Nederlandse cybersecuritylandschap in de loop van de tijd te volgen. Dit meet niet direct de digitale weerbaarheid van organisaties, maar geeft wel een indicatie van hoe kwetsbaar Nederlandse organisaties nog steeds zijn in een steeds veranderend dreigingslandschap. Een

[7] Dit staat voor 'CYber RAting'. Voor meer informatie, zie: https://cyberrating.nl/

[8] Internet.nl is een platform waarmee een gebruiker kan controleren of domeinen voldoen aan de nieuwste beveiligingspraktijken met betrekking tot internetdomein- en e-mailbeheer, beheerd door de Nederlandse internetgemeenschap en de Nederlandse overheid.

belangrijke beperking van het bijhouden van geregistreerde of gemelde incidenten is echter dat dergelijke gegevens vaak geen inzicht geven in de effecten of de omvang van het functieverlies als gevolg van deze incidenten, wat een essentieel aspect van weerbaarheid is. Dit kan veranderen met de gegevensrapportagevereisten van de NIS2-richtlijn, aangezien deze ook vereist dat zogenaamde essentiële en belangrijke entiteiten gegevens over effectbeoordelingen opnemen (Richtlijn (EU) 2022/2555). De overheid zal hiermee toegang krijgen tot nieuwe informatie over de feitelijke impact van cyberincidenten op het functioneren van organisaties.

Op vergelijkbare wijze worden de gestelde doelen en doelstellingen van een meetaanpak weerspiegeld in de manier waarop de indicatoren van het raamwerk zijn ontworpen en geïmplementeerd. Sommige benaderingen zijn gebaseerd op een grotendeels zelfgestuurd proces, waarbij van organisaties wordt verwacht dat zij op zelfstandige wijze goede praktijken op bepaalde gebieden toepassen. Andere benaderingen maken gebruik van gestructureerde zelfbeoordelingen, waarbij organisaties gedetailleerde vragenlijsten moeten invullen om aan te tonen of en hoe zij voldoen aan goede praktijken of minimumnormen. Andere benaderingen schrijven daarentegen meer uitgebreide meetprocessen voor, waarbij mogelijk ook externe auditors nodig zijn om de naleving onafhankelijk te beoordelen en te verifiëren. Net als bij het ontwerp van de meetmethode zelf, zijn er geen sterke aanwijzingen dat een bepaalde beoordelingsmethode het geschiktst is om digitale weerbaarheid te meten. In plaats daarvan brengt elke benadering voor- en nadelen met zich mee en heeft iedere benadering verschillende sterke en zwakke punten, zoals samengevat in de onderstaande tabel.

Tabel 9. Samenvatting van voor- en nadelen van beoordelingsparameters

Beoordelingsparameter	Voordelen	Nadelen
Binair (ja/nee)	Eenvoudig en gemakkelijk te implementeren Gemakkelijk te interpreteren en te vergelijken tussen organisaties Handig voor nalevingscontroles op hoog niveau	Ontbreekt aan nuance en geeft geen beeld van de mate van weerbaarheid of gedetailleerde inzichten Kan complexe aspecten van digitale weerbaarheid te veel vereenvoudigen Als weerbaarheid beperkt wordt gedefinieerd, zoals het voldoen aan binaire criteria, kan dat leiden tot vals vertrouwen
Ordinale schaal	Biedt een fijnere onderverdeling dan binaire beoordelingen door vooraf gedefinieerde opties aan te bieden Gemakkelijker te standaardiseren binnen organisaties in vergelijking met open tekstantwoorden Maakt categorisering van weerbaarheidsniveaus mogelijk	Beperkt door de vooraf gedefinieerde keuzes, die mogelijk niet volledig aansluiten bij de situatie van de organisatie Kan subjectiviteit introduceren bij het selecteren van de geschiktste optie Moeilijk te gebruiken voor benchmarking als de opties niet uniform worden begrepen

Kwalitatieve open tekst	Stelt organisaties in staat om gedetailleerde, contextspecifieke inzichten te geven in hun weerbaarheid Geeft de complexiteit van weerbaarheid weer op een manier zoals gestructureerde opties niet kunnen Stimuleert diepere reflectie op weerbaarheidspraktijken	Moeilijk te standaardiseren en te vergelijken tussen organisaties Tijdrovend om reacties te analyseren en te interpreteren Risico op inconsistenties in taalgebruik en interpretatie
Numeriek	Biedt gedetailleerdere, meetbare gegevens die kunnen worden gebruikt voor benchmarking en het bijhouden van voortgang Vergemakkelijkt vergelijkingen tussen organisaties en sectoren Ondersteunt evidencebased besluitvorming en toewijzing van middelen	Vereist robuuste indicatoren en (de ontwikkeling van) methodologieën om de validiteit en betrouwbaarheid te waarborgen Kan een vals gevoel van nauwkeurigheid geven door zich te richten op numerieke meetwaarden zonder rekening te houden met kwalitatieve nuances Kan veel middelen vergen om gegevens te verzamelen en te analyseren

Uitgebreidere methoden voor het meten van digitale weerbaarheid kunnen audits omvatten die gebruikmaken van verschillende beoordelingsparameters. Auditbeoordelingen bieden externe evaluaties van digitale weerbaarheid en leveren verificatie door derden waardoor de geloofwaardigheid en verantwoordingsplicht worden ondersteund. Deze beoordelingen kunnen hiaten en kwetsbaarheden aan het licht brengen die mogelijk niet worden gevonden door interne beoordelingen. Ze worden gebruikt om naleving van regelgevende of industrienormen aan te tonen. Auditbeoordelingen kunnen aanzienlijke kosten met zich meebrengen en vereisen aanzienlijke middelen van organisaties. Ze kunnen ook leiden tot terughoudendheid om gevoelige informatie openbaar te maken en de kwaliteit van de audit kan variëren naargelang de expertise van de auditor. Bovendien kunnen auditprocessen prioriteit geven aan het voldoen aan vastgestelde criteria, in plaats van verbeteringen in de algehele digitale weerbaarheid aan te moedigen.

Het onderzoek toont ook aan dat de geïdentificeerde benaderingen zelden alleen worden gebruikt om de mate van digitale weerbaarheid te beoordelen. In plaats daarvan worden deze raamwerken vaak gebruikt voor verschillende doeleinden, waaronder risicobeheer of het waarborgen van basisbeveiligingsmaatregelen of naleving, wat indirect kan bijdragen tot een beter begrip van weerbaarheid, ook al is dat niet hun primaire doel. Er lijken maar weinig methoden te zijn die door de overheid zijn ingezet met het doel de digitale weerbaarheid te meten. Belangrijk is dat we geen sterk bewijs hebben gevonden dat de ene methode inherent beter presteert dan de andere wat betreft validiteit of betrouwbaarheid, of dat de NCTV een bepaald meetkader voor digitale weerbaarheid zou moeten hanteren. In plaats daarvan weerspiegelen deze methoden verschillende doelstellingen en zijn ze afgestemd op verschillende organisatorische of sectorale vereisten. Hoewel er geen definitief bewijs is voor de effectiviteit van de geïdentificeerde methoden, blijft het implementeren van een of andere vorm van meting de voorkeur verdienen boven het ontbreken daarvan, zelfs wanneer de directe effectiviteit niet kan worden aangetoond.

4.2. Illustratieve voorbeelden van bestaande praktijk

Hoewel er geen kant-en-klare aanpak bestaat om digitale weerbaarheid op organisatieniveau te meten, zijn er in de bestaande benaderingen die in deze studie zijn onderzocht goede praktijken te vinden die kunnen helpen bij het ontwikkelen van een toekomstige meetmethode, afhankelijk van het uiteindelijke doel ervan. In dit hoofdstuk worden drie illustratieve voorbeelden gegeven van hoe dit in de praktijk zou kunnen werken, voortbouwend op drie veelvoorkomende usecases die in hoofdstuk 3 zijn geïdentificeerd:

1. Benaderingen voor het opzetten en meten van basismaatregelen voor digitale veiligheid en weerbaarheid binnen organisaties.
2. Benaderingen om de gereedheid van organisaties op belangrijke gebieden van digitale weerbaarheid, zoals herkenning, bescherming, detectie, respons en herstel, kwalitatief te meten.
3. Benaderingen voor het verzamelen en analyseren van uitgebreide en sectorspecifieke gegevens over hoe organisaties presteren in een praktijkcontext.

4.2.1. Benaderingen voor het ontwikkelen en meten van basismaatregelen voor digitale veiligheid en weerbaarheid van organisaties

Als het doel is om digitale weerbaarheid op organisatieniveau op te bouwen en de implementatie van basismaatregelen voor digitale weerbaarheid te meten, kan het Cyber Essentials-programma van de Britse overheid een nuttig uitgangspunt bieden:

- Het is een door de overheid gesponsorde minimumnorm voor cybersecurity.
- Het omvat technische basismaatregelen die van toepassing zijn op de meeste organisaties en die ook kunnen worden uitgebreid met bredere maatregelen voor digitale weerbaarheid.
- Het is een gestructureerde zelfbeoordeling die voornamelijk gebruikmaakt van een binaire beoordelingsmethode (ja/nee) om het risico van vooringenomenheid, misverstanden of uiteenlopende interpretaties van risiconiveaus door de deelnemende organisaties weg te nemen.
- Het biedt de mogelijkheid om een technische audit toe te voegen om ervoor te zorgen dat de zelfbeoordeling in de praktijk wordt weerspiegeld.
- Organisaties worden gestimuleerd om het programma te volgen, omdat het vaak een vereiste is om deel te nemen aan overheidsopdrachten en het ook automatisch een cyberaansprakelijkheidsverzekering biedt.[9]

De Cyber Essentials-zelfbeoordeling heeft betrekking op basiskenmerken van de organisatie en vijf gebieden van technische controles, zoals samengevat in de onderstaande tabel. Deze aanpak meet niet noodzakelijkerwijs de digitale weerbaarheid van alle organisaties, maar biedt wel nuttige gegevens over de basisnaleving als een vervangende maatstaf voor digitale weerbaarheid. Het biedt geen directe meting van hoe organisaties in de praktijk zouden presteren in een context van digitale weerbaarheid en hun mate van weerbaarheid in een reëel cyberincident. Uit een effectbeoordeling van het Cyber Essentials-programma bleek echter dat de meeste organisaties van mening waren dat het programma hun vermogen had verbeterd

[9] Voor organisaties met een jaaromzet van minder dan £20 miljoen.

om veelvoorkomende, eenvoudige cyberaanvallen op hun organisatie op te sporen, te monitoren, erop te reageren, ervan te herstellen en de financiële gevolgen ervan te minimaliseren.[10]

Tabel 10. Samenvatting van de Cyber Essentials-zelfbeoordeling

Firewalls	Evalueren van het gebruik en beheer van firewalls door de organisatie om haar netwerk te beschermen tegen externe bedreigingen. Dit omvat details over wachtwoordbeheer, configuratie en beoordelingsprocessen. Indicatieve dekking: • Firewalls worden geïmplementeerd op de grenzen tussen de netwerken van de organisatie en het internet. • De standaardwachtwoorden op firewallapparatuur zijn gewijzigd. • Firewallconfiguraties worden regelmatig gecontroleerd en niet-geverifieerde inkomende verbindingen worden toegestaan of beperkt.
Veilige configuratie	Beoordelen of apparaten en diensten veilig zijn geconfigureerd om kwetsbaarheden te minimaliseren, zoals het verwijderen van onnodige software en het wijzigen van standaardwachtwoorden. Indicatieve dekking: • Software en diensten die niet worden gebruikt, zijn verwijderd of uitgeschakeld. • Standaardwachtwoorden voor alle gebruikers- en beheerdersaccounts zijn gewijzigd om te voldoen aan de Cyber Essentials-vereisten. • Functies waarmee gedownloade bestanden automatisch kunnen worden uitgevoerd zonder toestemming van de gebruiker, zijn uitgeschakeld.
Beheer van beveiligingsupdates	Beoordelen of de organisatie ervoor zorgt dat alle apparaten en software up-to-date worden gehouden met regelmatige beveiligingsupdates en kwetsbaarheidsoplossingen. Indicatieve dekking: • Besturingssystemen op alle apparaten worden ondersteund door leveranciers die regelmatig beveiligingsupdates leveren. • Risicovolle updates voor applicaties, besturingssystemen en firmware worden binnen 14 dagen na release toegepast. • Niet-ondersteunde software is verwijderd uit alle apparaten en diensten die onder het beleid vallen.
Toegangscontrole voor gebruikers	Evalueren hoe gebruikersaccounts en toegangsrechten worden beheerd om ervoor te zorgen dat werknemers alleen de toegang hebben die nodig is voor hun functie. Het heeft ook betrekking op controles op beheerdersaccount en wachtwoordgebaseerde authenticatie. Indicatieve dekking: • Gebruikersaccounts worden aangemaakt na een goedkeuringsproces. • Accounts van voormalige medewerkers worden onmiddellijk verwijderd of uitgeschakeld. • Beheerdersaccounts worden formeel bijgehouden en toegangsrechten worden regelmatig gecontroleerd. • Multifactorauthenticatie (MFA) is ingeschakeld voor alle clouddiensten en beheerdersaccounts. • Medewerkers worden aangemoedigd om sterke en unieke wachtwoorden te gebruiken via vastgestelde organisatorische praktijken.
Bescherming tegen malware	Beoordelen van de maatregelen van de organisatie ter bescherming tegen malware, waaronder antimalwaresoftware en mechanismen voor applicatiecontrole. Indicatieve dekking: • Apparaten worden tegen malware beschermd door antimalwaresoftware of een lijst met toegestane applicaties. • Antimalwaresoftware is zo geconfigureerd dat deze regelmatig wordt bijgewerkt en voorkomt dat malware wordt uitgevoerd zodra deze wordt gedetecteerd. • Op apparaten geïnstalleerde applicaties zijn beperkt tot applicaties die door de organisatie zijn goedgekeurd, waarbij niet-ondertekende applicaties worden geblokkeerd.

Bron: RAND Europe-analyse van https://www.ncsc.gov.uk/cyberessentials/overview.

[10] Brits ministerie van Wetenschap, Innovatie en Technologie (2024).

Ook andere benaderingen besproken in Hoofdstuk 3 of de vijf basisprincipes van digitale weerbaarheid van het NCSC zouden gebruikt kunnen worden als startpunt om de implementatie van basismaatregelen voor digitale weerbaarheid te meten, maar het Cyber Essentials-programma is hier uitgelicht omdat er belangrijke lessen uit de implementatie te leren zijn. Benaderingen om de organisatorische paraatheid op belangrijke gebieden van digitale weerbaarheid kwalitatief te meten

Als het doel van de benadering voor het meten van digitale weerbaarheid daarentegen is om gegevens te verzamelen en de gereedheid van de organisatie om cyberincidenten te herkennen, te beschermen, te detecteren, erop te reageren en ervan te herstellen, gedetailleerder te meten, dan is een uitgebreider beoordelingskader op basis van de NIST- of ISO-raamwerken wellicht geschikter.

Deze aanpak zou een uitgebreid meetkader kunnen bieden dat verder gaat dan technische maatregelen en ook belangrijke organisatorische en proceselementen omvat, waaronder governance, leiderschap en opleiding. Bij dit soort beoordelingsmethoden wordt doorgaans gebruikgemaakt van vaste antwoordformats, bijvoorbeeld een Likert-schaal van 1 tot 5, aangevuld met kwalitatieve open tekstopties om context of aanvullende details te geven over de digitale weerbaarheidspraktijk van een organisatie. Soms worden deze ook ondersteund door een 'betrouwbaarheidsbeoordeling' van het bewijs dat het antwoord op specifieke vragen ondersteunt. Dit kan bijvoorbeeld de vorm aannemen van objectieve gegevens waarvan de kwaliteit is gewaarborgd (bijvoorbeeld geaudite organisatiegegevens), objectieve gegevens waarvan de kwaliteit niet is gewaarborgd (bijvoorbeeld organisatiegegevens), onafhankelijke meningen (bijvoorbeeld de mening van een auditor) of interne meningen (bijvoorbeeld de mening van het cybersecurityteam), waarbij de eerste meer vertrouwen wekken in het bewijs en de laatste minder. Dit soort beoordelingsmethoden zou de NCTV waarschijnlijk een volledi ger beeld geven van de digitale weerbaarheid van organisaties, terwijl de vereiste inspanningen en expertise enigszins in evenwicht worden gebracht. Het zou ook het bijkomende voordeel kunnen bieden dat potentiële aspecten worden geïdentificeerd waar organisaties mogelijk verdere ondersteuning, opleiding of financiering nodig hebben, wat de NCTV zou kunnen helpen bij het bredere beleidsvormingsproces. De onderstaande tabel geeft een indicatief overzicht van wat dit soort meetmethode zou kunnen omvatten op basis van de bestaande raamwerken die in paragraaf 3.2 en eerder RAND-onderzoek zijn geïdentificeerd.

Tabel 11. Samenvatting van een indicatieve meetmethode op basis van ISO27001-principes

Leiderschap, rapportage en verantwoordelijkheid	Onderzoek naar de leiderschapsstructuur en rapportagemechanismen voor cybersecurity binnen de organisatie, met inbegrip van toezicht op bestuursniveau, verantwoordingsplicht en toewijzing van middelen. Indicatieve dekking: • De raad van bestuur die verantwoordelijk is voor cybersecuritykwesties wordt geïdentificeerd, evenals de frequentie van rapportage aan de raad van bestuur. • De voorzitter van de raad van bestuur die verantwoordelijk is voor cybersecurity wordt geïdentificeerd. • De aanwezigheid van een specifiek cybersecuritybudget en de toereikendheid van de aan cybersecurity toegewezen middelen worden beoordeeld.

Governance, structuren en beleid	Beoordeling van de governance-structuren van de organisatie, waaronder risicoregisters, noodherstelplannen en beleid voor het detecteren, beheren en reageren op cyberincidenten. Indicatieve dekking: • De organisatie houdt een cybersecurity-risicoregister en een IT-rampenherstelplan bij, met details over de testfrequentie en praktijkscenario's. • De organisatie heeft een door de raad van bestuur goedgekeurde 'lijst met kritieke toepassingen' voor IT-weerbaarheid en herstelplanning. • Er zijn binnen de hele organisatie beleidsregels en processen voor het opsporen, beheren en reageren op cyberincidenten.
Partnerschappen, informatie, advies en begeleiding	Betreft de betrokkenheid van de organisatie bij externe entiteiten, zoals het National Cyber Security Centre, en het gebruik van cybersecuritydiensten voor informatie en begeleiding. Indicatieve dekking: • De organisatie is op de hoogte van regionale cybersecuritygroepen en werkt met hen samen, onder meer door vergaderingen bij te wonen en proactief informatie te verzamelen. • De organisatie werkt samen met nationale cybersecurityinstanties en maakt gebruik van diensten zoals platforms voor het delen van informatie of tools voor het monitoren van kwetsbaarheden. • De methoden die de organisatie gebruikt om met deze entiteiten samen te werken, zoals mailinglijsten of direct contact, worden beschreven.
Technologie, normen en naleving	In dit deel wordt beoordeeld in hoeverre de organisatie cybersecuritymaatregelen heeft genomen en welke technische voorzieningen er zijn getroffen voor cybersecurity. Indicatieve dekking in de ISO-fasen: **Herkennen** • De belangrijkste operationele diensten zijn geïdentificeerd. • Technologieën, diensten en afhankelijkheden die operationele diensten ondersteunen, zijn gedocumenteerd. • Gevoelige cybersecuritymiddelen, zoals apparaten, gegevens en netwerken, zijn gecatalogiseerd. **Beschermen** • Er zijn identificatieprocessen ingesteld om gebruikers te verifiëren en te autoriseren. • Bevoorrechte toegang tot kritieke systemen wordt beheerd met behulp van afzonderlijke accounts. • Gevoelige gegevens worden opgeslagen met behulp van geschikte versleutelingsmechanismen. **Detecteren** • Er zijn gestructureerde systemen voor kwetsbaarheids- en patchbeheer geïmplementeerd. • Er worden netwerkmonitoringtools gebruikt om inbreuken op de cybersecurity te detecteren. • *Threat intelligence feeds* zijn geïntegreerd in beveiligingsbeheerprocessen. **Reageren** • Cybersecurityincidenten worden systematisch geregistreerd. • Er zijn geteste back-ups beschikbaar voor herstel tijdens incidenten. • Het beleid voor incidentrespons heeft betrekking op essentiële diensten en een reeks scenario's. **Herstellen** • Na incidenten worden lessen geïdentificeerd en vastgelegd.

	• Er zijn processen om de geleerde lessen te integreren in risicoregisters en beleidsregels. • De organisatie houdt het aantal en de aard van cyberaanvallen bij die het afgelopen jaar hebben plaatsgevonden.
Training en bewustwording	Onderzoek naar de trainingsprogramma's en inspanningen van de organisatie om het bewustzijn van cybersecurity onder medewerkers te vergroten. Indicatieve dekking: • Alle medewerkers krijgen een basistraining in cybersecurity, hetzij verplicht, hetzij vrijwillig. • Er wordt specifieke training gegeven aan medewerkers die persoonlijke apparaten gebruiken om toegang te krijgen tot de IT-systemen van de organisatie. De organisatie vergroot het bewustzijn van cybersecurity door middel van methoden zoals nieuwsbrieven, phishingtests en onlinetrainingen.

Bron: Analyse van bestaande raamwerken voor digitale weerbaarheid door RAND Europe.

4.2.2. Benaderingen voor het verzamelen en analyseren van gegevens over hoe organisaties presteren in een praktijkcontext

Ten slotte, als het het algemene doel van de benadering voor het meten van digitale weerbaarheid is om uitgebreide en sectorspecifieke gegevens te verzamelen en te analyseren over hoe organisaties presteren in een reële digitale weerbaarheidscontext, dan is een benadering vergelijkbaar met het TNO-raamwerk waarschijnlijk nodig. Het TNO-raamwerk beoogt een uitgebreide beoordeling van de cybersecuritypositie van een organisatie door indicatoren te verzamelen op belangrijke gebieden zoals preventie, detectie, respons en herstel. Het evalueert het bewustzijn van medewerkers, dreigingsanalyse, kwetsbaarheidsbeheer en incidentrespons, en volgt statistieken zoals detectietijden, effectiviteit van mitigatie en operationeel herstel. Het beoordeelt ook malware- en inbraakbeheer, toegangscontroles en gegevensbescherming om gevoelige activa te beveiligen, terwijl bredere gevolgen zoals financiële verliezen, verlies van klanten en reputatieschade in kaart worden gebracht. Het nadeel van deze aanpak is dat deze waarschijnlijk sectorspecifiek moet worden uitgewerkt om de juiste soort gegevens te verzamelen op basis van het type organisatie en de sector, waarvoor aanzienlijke middelen van de NCTV nodig zouden zijn voor de ontwikkeling, implementatie en analyse. Daarnaast worden aanzienlijke middelen en expertise van de responsorganisaties verwacht om de gegevens te verzamelen. De onderstaande tabel geeft een selectie van de indicatoren weer en biedt een overzicht van wat deze aanpak zou kunnen inhouden op basis van het in paragraaf 3.2 geïdentificeerde TNO-raamwerk.

Tabel 12. Selectie van indicatoren uit het TNO-raamwerk

Analyse van medewerkers	Onderzoek naar het vermogen van de organisatie om phishingaanvallen te voorkomen, te herkennen en te melden. • Medewerkers kunnen social engineeringpraktijken herkennen die via illegale telefoontjes worden uitgevoerd en kunnen in dergelijke omstandigheden gewenst gedrag vertonen. • Een laag percentage van de werknemers wordt slachtoffer van phishing, terwijl een hoog percentage van hen gewenst gedrag vertoont wanneer ze worden blootgesteld aan phishing.

Bedreigingsanalyse	Onderzoek naar het vermogen van de organisatie om dreigingsinformatie te gebruiken. • De organisatie kan dreigingsinformatie gebruiken en relevante van irrelevante inhoud onderscheiden. • De organisatie kan dreigingsinformatie vertalen naar daadwerkelijke verbeteringen op het gebied van beveiliging. • De organisatie kan snel reageren op meldingen van bedreigingen.
Kwetsbaarheidsbeheer	Onderzoek naar de reikwijdte van kwetsbaarheidsscans en penetratietests van de organisatie. • Beoordeling van bestaande veelvoorkomende kwetsbaarheden in de IT-infrastructuur van de organisatie. • Identificatie van kwetsbaarheden in softwareconfiguraties, met een beperkt tijdsbestek. • Het vermogen van de organisatie om veelvoorkomende kwetsbaarheden in de IT-infrastructuur van de organisatie te verhelpen. • Meting van de blootstelling aan gekwalificeerde pogingen tot inbraak.
Incidentrespons	Onderzoek naar het vermogen van de organisatie om cyberincidenten snel te detecteren en mitigerende maatregelen te nemen. • Beoordeling van de ernst en het escalatieniveau van het incident. • Vertaling van de uitkomsten van forensisch onderzoek naar verbeteringen op het gebied van beveiliging. • Bewustmaking van cyberincidenten en beheerprocessen. • Beoordeling van processen voor incidentafhandeling en de effectiviteit van crisismanagement.

Bron: Analyse van RAND Europe van Cyber Security Shared Research Program (2017).

4.3. Omzetting van bevindingen naar een praktische meting van digitale weerbaarheid in verschillende sectoren in Nederland

Een belangrijke uitdaging die alle drie hierboven besproken gebruiksscenario's gemeen hebben, is dat ze niet volledig recht doen aan de organisatorische context waarin digitale weerbaarheid bestaat. De mate van digitale weerbaarheid wordt bijvoorbeeld mede bepaald door de risicobereidheid en investeringsdrempels van een organisatie. Zo kunnen aanzienlijke operationele verstoringen als gevolg van een groot cyberincident niet alleen een weerspiegeling zijn van de ernst van de aanval, maar ook van eerdere beslissingen van de organisatie over de aanvaardbaarheid van kosten in verband met verbeterde bescherming. Meetcriteria die incidenten, downtime of andere weerbaarheidsresultaten kwantificeren, moeten daarom ook rekening houden met de risicobereidheid en investeringsdrempels van de organisatie.

Een andere conceptuele uitdaging is dat de definitie van 'volledig weerbaar', zoals het behouden van volledige functionaliteit in de loop van de tijd, niet statisch is. Wat vandaag als volledig functioneel wordt beschouwd, kan morgen veranderen naarmate de eisen en verwachtingen evolueren. Weerbaarheid hangt zowel af van organisatorische systemen en infrastructuur als van de externe dreigingsomgeving. Als de dreigingen groter worden, kan de weerbaarheid afnemen, zelfs als de interne systemen ongewijzigd blijven. Het is daarom moeilijk om weerbaarheid op een zinvolle manier te meten in relatieve termen tussen organisaties of in de loop van de tijd, zonder rekening te houden met veranderingen in zowel interne capaciteiten als externe dreigingen. Bij beoordelingen moet idealiter worden erkend dat weerbaarheid een

dynamische toestand is die wordt bepaald door zowel organisatorische als externe factoren, maar in de praktijk blijft dit een uitdaging.

De hierboven geschetste implicaties benadrukken de uitdagingen bij het ontwikkelen van een praktische aanpak voor het meten van digitale weerbaarheid op organisatieniveau in Nederland. Uit dit onderzoek blijkt dat er geen enkele aanpak is die direct door de NCTV kan worden overgenomen. Bovendien zijn er beperkte mogelijkheden voor geautomatiseerde of kwantitatieve meetmethoden. Bijgevolg zal elke meetmethode op maat moeten worden gemaakt, waarbij gebruik wordt gemaakt van beproefde best practices. De bevindingen benadrukken ook dat het niet altijd praktisch of haalbaar is om een uitgebreide beoordeling van de digitale weerbaarheid van organisaties te realiseren. Tevens wijzen de bevindingen van het onderzoek op een aantal mogelijke belemmeringen en ontwerpkeuzes waarmee de NCTV rekening moet houden bij het ontwikkelen van een meetmethode voor digitale weerbaarheid:

- **Bij gebrek aan één enkele meetmethode zal de NCTV moeten bepalen welk aspect van digitale weerbaarheid moet worden gemeten.** Bij gebrek aan een uitgebreide manier om digitale weerbaarheid te meten, is het nog steeds beter om enige gegevens te verzamelen dan helemaal geen. In deze context zou het mogelijk zijn om zich te concentreren op een specifiek aspect van digitale weerbaarheid en dit als uitgangspunt voor de meting te gebruiken. Het beoordelen van het herstelvermogen van een organisatie na een cyberincident zou bijvoorbeeld een duidelijke en vergelijkbare maatstaf kunnen opleveren voor verschillende organisaties. Door te beginnen met één duidelijk omschreven gebied, wordt het mogelijk om te beginnen met het verzamelen van gegevens en een basis te leggen voor bredere metingen in de toekomst. Het identificeren en aanbevelen van praktische indicatoren voor deze eerste focus zou de geleidelijke ontwikkeling van een uitgebreider begrip van digitale weerbaarheid in de loop van de tijd ondersteunen.
- **De NCTV heeft geen duidelijk wettelijk mandaat om gegevens te verzamelen over de digitale weerbaarheid van organisaties.** Momenteel heeft de NCTV geen wettelijk mandaat om organisaties te verplichten gegevens over digitale weerbaarheid te verstrekken, wat betekent dat een mogelijke meting een vrijwillige regeling zou moeten zijn, tenzij het wettelijke mandaat wordt gewijzigd. De invoering van rapportageverplichtingen door de implementatie van de NIS2-richtlijn zal hier mogelijk verandering in brengen voor zogenoemde essentiële en belangrijke entiteiten. In Bijlage B geven we enkele praktische ideeën over hoe dit rapportagemechanisme kan worden gebruikt om te beginnen met het verzamelen van nieuwe gegevens die betrekking hebben op de digitale weerbaarheid van deze belangrijke organisaties in Nederland. Het moet echter opgemerkt worden dat het NCSC is aangewezen als centraal meldpunt, wat betekent dat de NCTV nauw met hen zal moeten samenwerken om de mogelijkheden voor analyse en gegevensuitwisseling te onderzoeken.
- **De effectiviteit van elk raamwerk hangt ook af van het type en de kwaliteit van de informatie die organisaties bereid zijn te delen.** Organisaties kunnen terughoudend zijn om potentieel gevoelige gegevens met betrekking tot specifieke cybersecuritymaatregelen te delen en geven in plaats daarvan de voorkeur aan kwalitatieve antwoorden op abstract niveau. Deze dynamiek zorgt voor spanningen tussen de relevante gegevens die nodig zijn om de weerbaarheid te meten en in hoeverre organisaties bereid of in staat zijn om gegevens te delen. Er is met name een gebrek aan toegankelijke

operationele gegevens. Interne rapporten, zoals die worden opgesteld voor periodieke ISO27001-certificeringsbeoordelingen, worden zelden buiten organisaties gedeeld. Deze rapporten zijn doorgaans zeer contextspecifiek en zijn meestal niet zo opgesteld dat ze gemakkelijk tussen organisaties kunnen worden vergeleken. Hoewel bredere toegang tot interne gegevens de reikwijdte van de analyse zou kunnen vergroten, zou het bereiken van een dergelijke transparantie aanzienlijke kosten met zich meebrengen en veel tijd vergen. Bovendien zou het, zelfs met uitgebreide gegevensuitwisseling, moeilijk zijn om conclusies te trekken over de algehele digitale weerbaarheid, aangezien de beschikbare informatie waarschijnlijk alleen betrekking zou hebben op specifieke deelprocessen en niet op de organisatie als geheel.

- **Vermijden van doublures met bestaande vereisten.** Nederland kent al verschillende initiatieven op het gebied van digitale weerbaarheid (zie Bijlage A.4), waardoor er een risico ontstaat voor doublures bij de ontwikkeling van een nieuw, op maat gemaakt meetkader voor digitale weerbaarheid. Eventuele toekomstige aanvullende eisen van de NCTV zouden als overbodig of onnodig kunnen worden beschouwd, tenzij de toegevoegde waarde ervan voor deelnemende organisaties duidelijk wordt aangetoond.
- **Het belang van het stimuleren van deelname door Nederlandse organisaties door de toegevoegde waarde duidelijk maken**. Om dit aan te pakken, moet de NCTV ervoor zorgen dat haar raamwerk voor digitale weerbaarheid een aanvulling vormt op bestaande initiatieven en tastbare voordelen biedt, zoals bruikbare inzichten of gerichte ondersteuning, om acceptatie en betrokkenheid te stimuleren. Er zijn ook alternatieve stimuleringsstructuren die de NCTV zou kunnen overwegen, zoals het koppelen van rapportagevereisten aan openbare aanbestedingsprocedures (d.w.z. de verplichting om aan de vereisten te voldoen om te kunnen meedingen naar overheidscontracten), financiële subsidies of beurzen voor organisaties die aan de vereisten voldoen om hun cybersecurity te verbeteren, of boetes voor niet-naleving. In het kader van een vrijwillige regeling bestaat het risico dat organisaties ervoor kiezen om geen informatie te delen, tenzij het raamwerk aansluit bij bestaande praktijken, zoals ISO27001-naleving of soortgelijke normen.
- **Elke methode voor het beoordelen van digitale weerbaarheid moet een evenwicht vinden tussen het type en de hoeveelheid informatie die van organisaties wordt gevraagd en hun beperkte middelen**. Organisaties vertonen verschillende niveaus van digitale weerbaarheid, afhankelijk van hun sectorale context en de beschikbare middelen voor investeringen in cybersecurity. Grotere organisaties beschikken vaak over robuuste infrastructuren en gespecialiseerde teams om uitdagingen op het gebied van de digitale weerbaarheid aan te pakken, terwijl kleine en middelgrote ondernemingen vaak te maken hebben met beperkte middelen, waardoor hun mogelijkheden om uitgebreide maatregelen te nemen beperkt zijn. Elk raamwerk voor het meten van digitale weerbaarheid moet rekening houden met deze verschillen en moet flexibiliteit bieden om organisaties met verschillende maturiteitsniveaus tegemoet te komen. Dit vormt echter een uitdaging om de breedte en diepte die nodig zijn voor een effectieve meting in evenwicht te brengen. Er zijn ook afwegingen te maken tussen generaliseerbaarheid en sectorspecifieke overwegingen, aangezien generieke benaderingen voor het meten van digitale weerbaarheid

weliswaar op meer organisaties van toepassing zijn, maar mogelijk geen rekening houden met gedetailleerde sectorspecifieke kenmerken. Het ontwikkelen van gedetailleerde sectorspecifieke metingen kan echter ook aanzienlijke investeringen en expertise vereisen.

- **De relatie tussen minimale cybersecuritynormen en verbeterde digitale weerbaarheid is onzeker**. Bestaande raamwerken, zoals Cyber Essentials in het Verenigd Koninkrijk, beoordelen in de eerste plaats of bepaalde praktijken worden toegepast, in plaats van de daadwerkelijke effectiviteit ervan bij het voorkomen van incidenten te evalueren. Deze normen zijn vaak gebaseerd op theorie en anekdotisch bewijs, in plaats van op robuust bewijs van de impact. Zodra minimale praktijken zijn geïmplementeerd, kunnen ze binnen organisaties aan prioriteit inboeten en bestaat het risico dat naleving wordt verward met toereikendheid. Belangrijk is dat naleving van basisvereisten niet noodzakelijkerwijs betekent dat de algehele digitale weerbaarheid verbetert.
- **De betrouwbaarheid en validiteit van bestaande methoden voor het beoordelen van digitale weerbaarheid zijn niet getest en dus onbekend.** De specificiteit en validiteit van de meetmethode spelen een belangrijke rol in de reproduceerbaarheid ervan en in het verminderen van het risico op verkeerde interpretaties, vooral als de meting in de loop van de tijd wordt herhaald. Op dit moment kan niet worden gezegd of de bestaande methoden betrouwbaar of geldig zijn. Door duidelijke richtlijnen te geven over wat 'sterke' digitale weerbaarheid inhoudt, in combinatie met duidelijk omschreven prestatie-indicatoren (KPI's), kan het raamwerk gebruiksvriendelijker en consistent toepasbaar worden. Zoals besproken in Tabel 9, is een van de belangrijkste uitdagingen bij kwalitatieve benaderingen dat ze aanzienlijke subjectiviteit in antwoorden kunnen introduceren, waardoor het moeilijk kan zijn om resultaten tussen organisaties of in de loop van de tijd te vergelijken. Aan de andere kant kunnen binaire vragen of strikt gedefinieerde opties nuttige context of details missen over de redenen waarom organisaties hun digitale weerbaarheid op die manier hebben benaderd.

Concluderend kunnen we stellen dat er geen kant-en-klare benaderingen zijn die de NCTV kan toepassen om realtime-informatie te verkrijgen over de digitale weerbaarheid op organisatieniveau in Nederland. Er zijn momenteel beperkte mogelijkheden voor geautomatiseerde of kwantitatieve meetmethoden. Het monitoren van veranderingen in het niveau van digitale weerbaarheid als gevolg van beleidsmaatregelen is nog ver weg en, gezien de verschillende uitdagingen die in dit rapport aan de orde komen, mogelijk in de praktijk niet haalbaar. Niettemin concluderen we ook dat er verschillende manieren zijn om gegevens te verzamelen die momenteel niet beschikbaar zijn voor de NCTV, maar die nieuwe inzichten kunnen opleveren in bepaalde aspecten van digitale weerbaarheid. Het ontwerp en de implementatie van deze methode zullen onder meer afhangen van de doelstellingen, de beschikbare middelen, de samenwerking met organisaties en het wettelijke mandaat van de NCTV om deze gegevens te verzamelen. Idealiter zou deze methode een aanvulling vormen op bestaande initiatieven. In Annex B bij dit rapport bespreken we een pragmatische en uitvoerbare eerste stap waarop de NCTV inzicht op nationaal niveau kan verbeteren, namelijk door gebruik te maken van de rapportageverplichtingen die voortvloeien uit de NIS2-richtlijn en door enkele aanvullende vragen toe te voegen aan het rapportageformulier. Hoewel NIS2 niet is bedoeld om een uitgebreide beoordeling van digitale weerbaarheid te geven, kan het een nuttig uitgangspunt zijn

voor het opbouwen van een kennisbasis die als input kan dienen voor toekomstig beleid en operationele beslissingen in Nederland.

Bronnen

AlHidaifi, Saleh Mohamed, Muhammad Rizwan Asghar, Imran Shafique Ansari. 2024. Towards a Cyber Resilience Quantification Framework (CRQF) for IT infrastructure. *Computer Networks*, Volume 247. Geraadpleegd 25 juni 2025: https://www.sciencedirect.com/science/article/pii/S1389128624002780?via%3Dihub

Annarelli, Alessandro, Fabio Nonino & Giulia Palombi. 2020. 'Understanding the management of cyber resilient systems.' *Computers and Industrial Engineering (149). Geraadpleegd 21 juli:* https://doi.org/10.1016/j.cie.2020.106829

Bagheri, Saba, Gail Ridley & Belinda Williams. 2023. 'Organisational Cyber Resilience: Management Perspectives.' *Australasian Journal of Information Systems* 27. https://doi.org/10.3127/ajis.v27i0.4183

Baskerville, Richard, Paolo Spagnoletti & Jongwoo Kim. 2014. 'Incident-centered information security: managing a strategic balance between prevention and response.' *Information & Management* 51 (1): 138–151. https://doi.org/10.1016/j.im.2013.11.004

Beljaarts, Dirk. 24 november 2024. *Beleidsreactie CSR Advies 'Verkleinen van de cyberweerbaarheidskloof'.* Geraadpleegd 2 januari 2025: https://www.cybersecurityraad.nl/binaries/cybersecurityraad/documenten/brieven/2024/12/19/beleidsreactie-csr-advies-verkleinen-van-de-cyberweerbaarheidskloof/Beleidsreactie+CSR+Advies+Verkleinen+Cyberweerbaarheidskloof.pdf

Bodeau, Deborah & Richard Graubart. 2016. 'Cyber Resilience Metrics: Key Observations.' *The MITRE Corporation.* Geraadpleegd 31 December 2024: https://icscsi.org/library/Documents/Best_Practices/MITRE%20-%20Cyber%20Resilient%20Metrics%20Key%20Observations.pdf

Brennenraedts, Reg, Melvin Hanswijk, Roos Jansen, Jessica Kats, Wazir Sahebali, Leonie Hermanussen. 2021. *Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda*. Dialogic/WODC Geraadpleegd 16 december 2024: https://repository.wodc.nl/bitstream/handle/20.500.12832/3065/3146-evalutie-opbouw-en-meebaarheid-van-de-nl-cybersecurity-agenda-volledige%20tekst.pdf?sequence=1&isAllowed=y

Cabinet Office. 2025. 'UK Government Resilience Action Plan.' Policy paper. Geraadpleegd 9 september 2025: https://www.gov.uk/government/publications/uk-government-resilience-action-plan/uk-government-resilience-action-plan-html

Caralli, R. A., J. H. Allen, P. D. Curtis, D. W. White and L. R. Young, 'Improving Operational Resilience Processes: The CERT Resilience Management Model.' *2010 IEEE Second International Conference on Social Computing*, Minneapolis, MN, USA, 2010, pp. 1165-1170. Geraadpleegd 28 juli 2025: doi: 10.1109/SocialCom.2010.173

Carayannis, Elias G., Evangelos Grigoroudis, Scheherazade S. Rehman, and Navodhya Samarakoon. 2021. 'Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience.' *IEEE Transactions of Engineering Management.* Geraadpleegd 28 juli 2025: https://ieeexplore.ieee.org/abstract/document/8703422

Carías, Juan F., Saioa Arrizabalaga, Leire Labaka & Josune Hernantes. 2021. 'Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs.' *IEEE Access*, vol. 9. Geraadpleegd 28 juli 2025: https://ieeexplore.ieee.org/document/9445083

CBS. 2023. *Cybersecuritymonitor 2022*. Geraadpleegd 13 december 2024: https://www.cbs.nl/-/media/_pdf/2023/31/cybersecuritymonitor_2022.pdf

CBS. 2024a. *Cybersecuritymonitor 2023*. Geraadpleegd 13 december 2024: https://www.cbs.nl/-/media/_pdf/2024/26/cybersecuritymonitor_2023.pdf

CBS. 2024b. *Vervolging en berechting misdrijven; persoonskenmerken*. CBS Statline. Geraadpleegd 10 augustus 2025: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85812NED/table?dl=AC5C7

CBS. 2024c. *Datalekmeldingen bij Autoriteit Persoonsgegevens, 1e helft 2024*. Geraadpleegd 10 augustus 2025: https://www.cbs.nl/nl-nl/maatwerk/2024/50/datalekmeldingen-bij-autoriteit-persoonsgegevens-1e-helft-2024

CBS. 2025a. *Cybersecuritymonitor 2024*. Geraadpleegd 17 juli 2025: https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

CBS. 2025b. *ICT-gebruik bedrijven. Wat behelst het onderzoek?*. Geraadpleegd 10 augustus 2025: https://www.cbs.nl/nl-nl/onze-diensten/methoden/onderzoeksomschrijvingen/korte-onderzoeksomschrijvingen/ict-gebruik-bedrijven

CBS. 2025c. *Toepassing van internetstandaarden voor websites van bedrijven, 2024*. Geraadpleegd 10 augustus 2025: https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/toepassing-van-internetstandaarden-voor-websites-van-bedrijven-2024/4-resultaten-e-mailscans

CBS. 2025d. *Online Veiligheid en Criminaliteit 2024.* Geraadpleegd 10 augustus 2025: https://www.cbs.nl/nl-nl/publicatie/2025/16/online-veiligheid-en-criminaliteit-2024

CCV. 2025 *Tool Cyberweerbaarheid*. Geraadpleegd 8 september 2025: https://hetccv.nl/tool-cyberweerbaarheid/

Conradie, Melle & Sara Kellij. 2024. *Cybersecurity onderzoek Alert Online 2024*. Ipsos I&O voor het Ministerie van Economische Zaken. Geraadpleegd 23 juli 2025: https://www.rijksoverheid.nl/documenten/rapporten/2024/09/30/cybersecurity-onderzoek-alert-online-2024

CSR. 2024. *'Verkleinen van de cyberweerbaarheidskloof': Advies over de cyberweerbaarheid van het Nederlandse midden- en kleinbedrijf*. Cyber Security Raad. https://www.cybersecurityraad.nl/documenten/adviezen/2024/06/04/csr-advies-verkleinen-van-de-cyberweerbaarheidskloof

Cyber Security Shared Research Program. 2017. *Library of Cyber Resilience Metrics.* TNO Innovation for life. Geraadpleegd 29 januari 2025: https://publications.tno.nl/publication/34626166/Xuq2bL/participants-2017-library.pdf

Department of Defense. 2024. 'Cybersecurity Maturity Model Certification (CMMC) Program.' *Office of the Secretary*. Geraadpleegd 28 juli 2025: https://www.govinfo.gov/content/pkg/FR-2024-10-15/pdf/2024-22905.pdf

DiMase, D., Z.A. Collier, K. Heffner, I. Linkov. 2015. 'Systems engineering framework for cyber physical security and resilience'. *Environ Syst Decis* 35. Geraadpleegd 25 juli 2025: https://doi.org/10.1007/s10669-015-9540-y

Driesse, Menno, Guido de Moor, Tessel Blom, Kimberly Deppe, Reg Brennenraedts. 2024. *Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie*. Dialogic/WODC Geraadpleegd 16 december 2024: https://repository.wodc.nl/bitstream/handle/20.500.12832/3341/3368-evaluatiekader-en-nulmeting-nederlandse-cybersecuritystrategie-volledige-tekst.pdf?sequence=1&isAllowed=y

Dupont, Benoît. 2019. 'The cyber-resilience of financial institutions: significance and applicability.' *Journal of Cybersecurity* 5 (1). https://doi.org/10.1093/cybsec/tyz013

Europese Commissie. 2019. *A cybersecure digital transformation in a complex threat environment – Brochure*. Geraadpleegd 17 juli 2025: https://digital-strategy.ec.europa.eu/nl/node/332

Garcia-Perez, Alexeis, Juan Gabriel Cegarra-Navarro, Mark Paul Sallos, Eva Martinez-Caro & Anitha Chinnaswamy. 2023. 'Resilience in healthcare systems: Cyber security and digital transformation.' *Technovation* 121. https://doi.org/10.1016/j.technovation.2022.102583

Goodman, Paul S. & Emily Haisley. 2007. 'Social comparison processes in an organizational context: New directions.' *Organizational Behavior and Human Decision Processes* 102 (1): 109–125. https://doi.org/10.1016/j.obhdp.2006.10.005

Grøtan, T. O., S. Antonsen & T. K. Haavik. 2022. 'Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda,' in F. Matos, P. M. Selig, and E. Henriqson, eds., *Resilience in a Digital Age: Global Challenges in Organisations and Society*, Springer, Cham. https://doi.org/10.1007/978-3-030-85954-1_12

Hoeffnagel, Wouter. 25 april 2025. 'Cyberaanvallen stijgen met 53% in Nederland in Q1 2025'. *Dutch IT Channel*. Geraadpleegd 16 juli 2025: https://www.dutchitchannel.nl/news/618197/cyberaanvallen-stijgen-met-53-in-nederland-in-q1-2025.

Hulsebosch, Bob, Henny de Vos & Koen de Jong. 2020. *Verkenning brede evaluatie NCSA: Inventarisatie van mogelijkheden voor de evaluatie van de volledigheid, realisatie en impact van de Nederlandse Cybersecurity Agenda op de digitale weerbaarheid van Nederland*. Innovalor/WODC. http://hdl.handle.net/20.500.12832/2483

INCIBE. 2019. *Indicadores para Mejora de la Ciberresiliencia (IMC).* Instituto Nacional de Ciberseguridad, Madrid, Spain.

ISO/IEC 27001. 2022. 'Information security, cybersecurity and privacy protection – Information security management systems – Requirements.' As of 22 July 2025: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Jacobs, N., S. Hossain-McKenzie & E. Vugrin. 2018. 'Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example.' 2018 Resilience Week (RWS), Denver, CO, USA, 2018, pp. 38-46. https://doi.org/10.1109/RWEEK.2018.8473549

Jansen, Jurjen. 2023. *Digitale weerbaarheid van mens en organisatie: de kracht van verbinding*. Lectorale rede Politieacademie/Thorbecke Academie, NHL Stenden. https://www.researchgate.net/publication/371292484_Digitale_weerbaarheid_van_mens_en_organisatie_De_kracht_van_verbinding

Kott, Alexander & Igor Linkov. 2021. 'To improve cyber resilience, measure it.' *IEEE Computer* 54 (2). https://doi.org/10.48550/arXiv.2102.09455

Krauwers, Julia. 2025. 'Cyberweerbaarheid Ondernemers Blijft Achter Bij Realiteit.' *ABN AMRO*. Geraadpleegd 10 juni 2025: https://www.abnamro.nl/nl/zakelijk/insights/sectoren-en-trends/alle-sectoren/cyberweerbaarheid-ondernemers-blijft-achter-bij-realiteit.html

Ligo, A. K., A. Kott &I. Linkov. 2021. 'How to Measure Cyber-Resilience of a System With Autonomous Agents: Approaches and Challenges.' *IEEE Engineering Management Review* 49 (2): 89-97. https://doi.org/10.1109/EMR.2021.3074288

Linkov & Trump. 2019. *The Science and Practice of Resilience. Springer Nature Switzerland AG*. Geraadpleegd op 21 juli 2025: https://link.springer.com/book/10.1007/978-3-030-04565-4

Kott, Alexander, Igor Linkov. 2021. 'To improve cyber resilience, measure it.' *IEEE Computer* 54 (2). Geraadpleegd op 01 augustus 2025: https://arxiv.org/abs/2102.09455

Mehedintu, A., & G. Soava. 2022. 'A Structural Framework for Assessing the Digital Resilience of Enterprises in the Context of the Technological Revolution 4.0.' *Electronics* 11 (15): 2439. Geraadpleegd op 21 juli 2025: https://doi.org/10.3390/electronics11152439

Munusamy, Thavaselvi & Touraj Khodadadi. 2023. 'Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security.' *Journal of Informatics and Web Engineering*. Geraadpleegd op 21 juli 2025: https://www.researchgate.net/publication/373895791_Building_Cyber_Resilience_Key_Factors_for_Enhancing_Organizational_Cyber_Security

Murphy, Colin. 2024. *Understanding Cybercrime*. European Parliamentary Research Service policy brief PE 760.356. Geraadpleegd 17 juli 2025: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

NATO. 2024a. 'NATO Allies take stock of progress on digital initiatives.' *nato.int,* 18 november 2024. Geraadpleegd 13 december 2024: https://www.nato.int/cps/en/natohq/news_230435.htm#:~:text=To%20advance%20NATO%27s%20digital%20transformation,future%20of%20the%20NATO%20Alliance.

NATO. 2024b. 'Resilience, civil preparedness and Article 3.' 13 November 2024. Geraadpleegd 9 september 2025: https://www.nato.int/cps/en/natohq/topics_132722.htm

NCSC. 2024a. *Cyber Assessment Framework V3.2.* Geraadpleegd 25 juli 2025: https://www.ncsc.gov.uk/static-assets/documents/cyber-assessment-framework-v3.2.pdf

NCSC. 2024b. Infosheet NIS2 verplichtingen: Meldplicht. Geraadpleegd 25 augustus 2025: https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/oktober/08/infosheet-meldplicht

NCSC. 2025. *Vijf basisprincipes van digitale weerbaarheid.* Geraadpleegd 25 juli 2025: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/september/27/basisprincipes/5+basisprincipes+van+digitale+weerbaarheid_092024_NL.pdf

NCTV. 2018. Nederlandse Cybersecurity Agenda. Geraadpleegd 13 december 2024: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda/CSAgenda_def_web_tcm31-322330.pdf

NCTV. 2022a. *Nederlandse Cybersecuritystrategie 2022-2028*. Geraadpleegd 2 januari 2025: https://www.nctv.nl/documenten/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028

NCTV. 2022b. *Actieplan Nederlandse Cybersecuritystrategie 2022-2028*. Geraadpleegd 25 juli 2025: https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028.

NCTV. 2023a. *Veiligheidsstrategie voor het Koninkrijk der Nederlanden*. Geraadpleegd 13 december 2024: https://www.nctv.nl/onderwerpen/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden

NCTV. 2023b. *Cybersecuritybeeld Nederland 2023*. Geraadpleegd 13 december 2024: https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023

NCTV. 2024a. *Cybersecuritybeeld Nederland 2024*. Geraadpleegd 13 december 2024: https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024

NCTV. 2024b. *Voortgangsrapportage 2024 Nederlandse Cybersecuritystrategie*. Geraadpleegd 19 december 2024 via: https://www.nctv.nl/binaries/nctv/documenten/publicaties/2024/10/28/voortgangsrapportage-nederlandse-cybersecuritystrategie-2024/241024_NLCS+Voortgangsrapportage+2024+DEF.pdf.

NCTV. 2024c. *Toekomstvisie Cyberweerbaarheidsnetwerk*. Geraadpleegd 7 mei 2025 via: https://www.nctv.nl/documenten/publicaties/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk

NCTV. 2024d. *Programmaplan Cyclotron*. Geraadpleegd 1 oktober 2025 via: https://www.nctv.nl/documenten/2024/01/26/programmaplan-cyclotron

Nederveen, Fook, Stijn Hoorens, Erik J. Frinking, and Henri van Soest. 2024. Weerbaarheid becijferd: Een methode om weerbaarheid tegen dreigingen voor de nationale veiligheid inzichtelijk te maken. RAND Corporation, RR-A2357-1. https://www.rand.org/pubs/research_reports/RRA2357-1.html

Neri, Martina, Federico Niccolini & Francesco Virili. 2025. 'Organizational cyber resilience: toward an integrative conceptual framework.' Management Review Quarterly. https://doi.org/10.1007/s11301-025-00496-7

NIAC. 2020. *NIAC Framework for Establishing Resilience Goals: Final Report and Recommendations*. Geraadpleegd 29 juli 2025: https://www.cisa.gov/resources-tools/resources/niac-framework-establishing-resilience-goals-final-report-and

NPC (Nationaal Platform Criminaliteitsbeheersing). 2022. *Actieprogramma Veilig Ondernemen 2023 tm 2026*. Geraadpleegd 20 januari 2025: https://open.overheid.nl/documenten/ronl-be1e5c0e98a7a23006eec873deb360ae971759b2/pdf

Panda, A., & Bower, A. 2020. 'Cyber security and the disaster resilience framework'. *International Journal of Disaster Resilience in the Built Environment* 11(4): 507-518. https://doi.org/10.1108/IJDRBE-07-2019-0046

Pescaroli, G., R.T. Wicks, G. Giacomello, D.E. Alexander. 2018. 'Increasing resilience to cascading events: The M.OR.D.OR. scenario'. *Safety Science* 110 (2018): 131-140. https://doi.org/10.1016/j.ssci.2017.12.012

Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG Voor de EER relevante tekst. http://data.europa.eu/eli/dir/2014/53/oj

Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn). http://data.europa.eu/eli/dir/2022/2555/2022-12-27

Rijksoverheid. 2021. *I-strategie Rijk 2021-2025*. Geraadpleegd 20 januari 2025: https://open.overheid.nl/repository/ronl-58d54cb8-dad1-4df9-a09e-1116167df02b/1/pdf/rapport-nieuwe-i-strategie-rijk-2021-2015.pdf

Shandilya, Shishir Kumar, Agni Datta, Yash Kartik, and Atulya Nagar. 2024. 'What Is Digital Resilience?' In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*, 3–42. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-53290-0_1

Snyder, Don, Lauren A. Mayer, Guy Weichenberg, Danielle C. Tarraf, Bernard Fox, Myron Hura, Suzanne Genc & Jonathan W. Welburn. 2022. *Measuring Cybersecurity and Cyber Resiliency*. Santa Monica, Calif.: RAND Corporation. RR-2703-AF. Geraadpleegd 30 mei 2024: https://www.rand.org/pubs/research_reports/RR2703.html.

Munusamy, Thavaselvi & Touraj Khodadadi. 2023. 'Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security.' *Journal of Informatics and Web Engineering* 2 (2): 59-71. https://doi.org/10.33093/jiwe.2023.2.2.5

Van Trigt, Marjolein. 2024. 'Kamer wil overal zelfde pentest-opdrachten'. *Binnenlands Bestuur*. Geraadpleegd 23 april 2025: https://www.binnenlandsbestuur.nl/digitaal/overheidsbrede-standaardisering-moet-lege-huls-voorkomen

Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening). http://data.europa.eu/eli/reg/2019/881/oj

Verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (digitalemarktenverordening). http://data.europa.eu/eli/reg/2022/1925/oj

Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening). http://data.europa.eu/eli/reg/2022/2065/oj

Verordening (EU, Euratom) 2023/2841 van het Europees Parlement en de Raad van 13 december 2023 tot vaststelling van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie. http://data.europa.eu/eli/reg/2023/2841/oj

Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid). http://data.europa.eu/eli/reg/2024/2847/oj

Vugrin, Eric & Jennifer Turgeon. 2015. 'Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments.' *International Journal of Secure Software Engineering* 4 (1): 75-96. http://dx.doi.org/10.4018/jsse.2013010105

The White House 2023. 'G7 Leaders' Statement on Economic Resilience and Economic Security.' *whitehouse.gov,* 20 mei 2023. Geraadpleegd 13 december 2024: https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security/

Tran, Hiep, Enrique Campos-Nanez, Pavel Fomin, James Wasek. 2016. 'Cyber resilience recovery model to combat zero-day malware attacks.' Computers & security. Geraadpleegd 25 juli 2025: https://www.sciencedirect.com/science/article/pii/S0167404816300505?via%3Dihub

World Economic Forum. 2023. *Global Risks Report 2023*. Geraadpleegd 17 juli 2025: https://www.weforum.org/publications/global-risks-report-2023/

Annex A. Digitale weerbaarheid in het Nederlandse cybersecuritybeleid

In deze bijlage bespreken we verschillende initiatieven en wetgevende stukken die relevant zijn voor digitale weerbaarheid van Nederlandse organisaties. De Cybersecuritystrategie is het overkoepelende beleidsstuk op dit terrein van de Nederlandse beleidscontext. Figuur 3 onder Paragraaf 2.3 geeft een grafische weergave van hoe de verschillende stukken en initiatieven zich tot de NLCS verhouden.

A.1. Nederlandse Cybersecuritystrategie 2022-2028 (NLCS)

De strategie van de Nederlandse overheid is niet alleen gericht op het creëren van een gemeenschappelijk begrip van digitale risico's, maar ook op het opbouwen van digitale weerbaarheid. Dergelijke doelen worden weerspiegeld in de NLCS, waarin wordt beschreven hoe de samenleving bestand kan worden gemaakt tegen bedreigingen van economische belangen en nationale veiligheid, verankerd in vier pijlers (NCTV 2022a). De eerste hiervan, en relevantste voor dit onderzoek, is Pijler I: 'Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties'. In deze pijler worden drie verschillende doelen beschreven die hier kort uitgelicht worden:

- **Doel 1: Organisaties hebben zicht op cyberincidenten, -dreigingen en risico's en hoe hiermee om te gaan.** Informatie over de dreiging en risico's wordt beschikbaar gemaakt en gedeeld door overheid, bedrijven en maatschappelijke organisaties om een actueel situationeel beeld te creëren over dreigingsinformatie en slachtofferinformatie. 'Organisaties mogen van de overheid verwachten dat deze actuele kennis en informatie over cyberdreigingen, -incidenten, -trends, en -kwetsbaarheden beschikbaar stelt zodat zij tot handeling kunnen overgaan' (NCTV 2022a, 24). Het Landelijk Dekkend Stelsel van cybersecurity-samenwerkingsverbanden wordt verder doorontwikkeld tot het nationaal Cyber Security Incident Response Team (CSIRT), en het NCSC, DTC en CSIRT zullen worden samengevoegd tot een organisatie. Dit wordt momenteel uitgewerkt tot het Cyberweerbaarheidsnetwerk (CWN) waar we onder 'cyberweerbaarheidsinitiatieven' verder op zullen ingaan. Door informatie bijeen te brengen hoopt de overheid beter in staat te kunnen zijn om deze te delen met organisaties. Voor organisaties die niet vallen onder een wettelijk kader zoals de aankomende Cyberbeveiligingswet (Cbw) zijn er echter geen verplichtingen verbonden aan dit doel.
- **Doel 2: Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties binnen de keten mee.** De overheid stimuleert organisaties om een basisniveau van maatregelen te implementeren en zet zich in op Europees niveau om dit te

stimuleren. Ook zorgt ze dat haar eigen systemen digitaal veilig zijn en voldoende beschermd tegen cyberincidenten. Daarnaast moet het inzichtelijk maken van en verantwoorden over cybersecurity door organisaties meer gemeengoed worden. Organisaties moeten personen aanwijzen die binnen de organisatie de verantwoordelijkheid dragen om inzicht te bieden in de mate van cyberweerbaarheid en het onderhouden of verbeteren hiervan. Belanghebbenden zoals afnemers, aandeelhouders en verzekeraars zouden daardoor gemakkelijker inzicht moeten krijgen in het cybersecurityniveau van organisaties. Er wordt echter niet benoemd hoe deze gegevens verzameld of verdeeld worden, noch of er wettelijke verplichtingen komen voor organisaties om hun cyberweerbaarheid te evalueren dan wel de resultaten hiervan te delen. De inzet is voornamelijk gericht op het laten groeien van de bewustwording omtrent digitale weerbaarheid bij organisaties door informatie en tools ter beschikking te stellen aan organisaties maar ook door oefeningen, trainingen en opleidingen. Voor bepaalde sectoren zoals het onderwijs, de zorg, infrastructuur en waterstaat zijn specifiekere maatregelen en vereisten ontwikkeld om digitale weerbaarheid te verhogen, zoals normenkaders met periodieke monitors en benchmarks (NCTV 2022b, 15).

- **Doel 3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en -crises.** Organisaties dienen incident-, continuïteit- en herstelplannen te ontwikkelen, passend bij het (risico)profiel van de organisatie, en deze regelmatig te oefenen. Organisaties evalueren cyberincidenten, leren hiervan en delen deze lessen onderling. De overheid biedt samenhangende cybersecuritydienstverlening met een herkenbaar aanspreekpunt voor organisaties. Verder werken de overheid, bedrijven en wetenschap intensief samen om cybersecurityexpertise effectief in te zetten. Door betere publiek-private samenwerking zal er sneller en effectiever gehandeld kunnen worden wanneer een cyberincident plaatsvindt.

Samenvattend wordt ingezet op het publiek-private karakter van digitale weerbaarheid, effectieve verspreiding van informatie en inzet van de beschikbare expertise en capaciteit, naleving van de aangescherpte regels, en de voorbereiding op incidenten. De maatregelen in de strategie zijn daarmee voornamelijk procedureel en organisatorisch van aard. De overheid draagt organisaties op actiever om te gaan met digitale weerbaarheid door systemen en gegevens beter te beschermen of ze worden daartoe dringend verzocht, afhankelijk van hun omvang. De directste maatregelen zijn gericht op het verbeteren van digitale weerbaarheid binnen overheidsorganisaties en binnen cruciale sectoren.

De Voortgangsrapportage Nederlandse Cybersecuritystrategie 2024 (NCTV 2024b) biedt een uitgebreid overzicht van de maatregelen die zijn genomen om de digitale weerbaarheid van organisaties te vergroten. Initiatieven worden daarbij verdeeld over relevante sectoren en doelgroepen, met een focus op concrete acties zoals het versterken van publiek-private samenwerking en het verbeteren van crisisresponsmechanismen. Hoewel deze rapportage inzicht geeft in de voortgang van de strategie, wordt er weinig inzicht geboden in de daadwerkelijke impact en effectiviteit van het beleid. Dit komt vooral door het ontbreken van gestandaardiseerde meetmethoden en concrete cijfers die de resultaten van de genomen maatregelen kwantificeren (zowel op organisatieniveau als andere niveaus). De nulmeting van de NLCS heeft geconcludeerd dat het meten van de effecten van cybersecuritybeleid complex is vanwege de dynamische aard van digitale dreigingen en de variërende niveaus van digitale weerbaarheid tussen organisaties (Driesse et al. 2022). Eenzelfde conclusie werd eerder ook al getrokken in de evaluatie van de

voorloper van de NLCS, de Nationale Cyber Security Agenda (NCSA) van 2018 (NCTV 2018; Hulsebosch et al. 2020).

A.2. Beleidsinformerende documenten

Naast de overkoepelende strategie en de voortgangsrapportage is er ook een aantal documenten die een belangrijke rol spelen in het opstellen en aanpassen van de strategie en het beleid rondom digitale weerbaarheid. Deze documenten geven eveneens inzicht in hoe de term 'digitale weerbaarheid' wordt toegepast en wat eronder verstaan wordt.

Cybersecuritybeeld Nederland (CSBN)

Het CSBN biedt een jaarlijks inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot digitale risico's. Het is bedoeld om de ontwikkelingen omtrent het actieplan dat is uitgewerkt in de NLCS 2022-2028 weer te geven, en de mogelijke strategische veranderingen die hebben plaatsgevonden te vatten. De focus van het CSBN ligt op de nationale veiligheid en op het informeren van verdere uitwerking van de NLCS. De analyse van de CSBN berust dan ook op een identificatie en duiding van de belangrijkste trends rondom cybersecurity in Nederland door de NCTV. De onderliggende data of informatie waarop dit gebaseerd is, worden niet gedeeld in het rapport.

Cybersecuritymonitor

In de Cybersecuritymonitor van het Centraal Bureau van de Statistiek (CBS) wordt een aantal aspecten van de digitale weerbaarheid van bedrijven op een rij gezet (CBS 2023; CBS 2024a; CBS 2025a). Zo wordt er gekeken naar het scala aan mogelijkheden die bedrijven nemen om de veiligheid van computers, smartphones, laptops, servers en netwerken te verhogen; naar het optreden van cybersecurityincidenten die de veiligheid van deze digitale systemen ondermijnen; naar de strafbare feiten die zich voordoen bij personen – zoals incidenten in de sfeer van oplichting en fraude, computervredebreuk, en incidenten in de interpersoonlijke sfeer die niet altijd strafbaar zijn – en er wordt gekeken naar de sancties die opgelegd zijn door het Openbaar Ministerie (OM) en door de rechter aan verdachten van computervredebreuk (CBS 2025a). De data met betrekking tot bedrijven worden onderverdeeld in verschillende categorieën. Zo wordt er gekeken naar de financiële omvang van bedrijven, het aantal werknemers, en de verdeling in 14 verschillende bedrijfstakken. De Cybermonitor somt zo de aanwezigheid van verschillende ICT-veiligheidsmaatregelen in deze categorieën op en omvat een analyse van de toename van deze verschillende maatregelen ten opzichte van eerdere perioden, evenals de mate van cybercrime in de samenleving. De Cybersecuritymonitor is hoofdzakelijk gebaseerd op CBS-cijfers van het desbetreffende jaar uit verschillende bronnen. In de Cybersecuritymonitor 2024 (CBS 2025a) worden bijvoorbeeld cijfers gebruikt uit het onderzoek ICT-gebruik bij bedrijven (CBS, 2025b), het rapport Toepassing van internetstandaarden voor websites van bedrijven, 2024 (CBS, 2025c), de monitor Online Veiligheid en Criminaliteit 2024 (CBS, 2025d), het onderzoek Strafrechtspraak (CBS, 2024b), en het onderzoek over datalekmeldingen bij de Autoriteit Persoonsgegevens, eerste helft 2024 (CBS, 2024c).

A.3. Juridische kaders

De juridische kaders die het Nederlandse digitale weerbaarheidsbeleid omlijsten, worden veelal direct of indirect bepaald door Europese verordeningen en richtlijnen. De belangrijkste hiervan in de context van digitale weerbaarheid van organisaties is de *Network and Information Security* (NIS2)-richtlijn, die in Nederlandse wetgeving getransponeerd zal worden als de Cyberbeveiligingswet (Cbw). Hieronder bespreken we deze en enkele andere van de voornaamste wetten die eveneens mogelijk aanknopingspunten kunnen bieden voor een methode voor het meten van digital weerbaarheid.

Network and Information Security (NIS2) Directive

De NIS2-richtlijn (Richtlijn (EU) 2022/2555) heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de EU te bereiken en bepaalt welke entiteiten aan welke verplichte securityeisen moeten voldoen. Dit geldt zowel voor overheden, vitale organisaties en andere organisaties die actief zijn in sectoren van maatschappelijk en/of economisch belang. De richtlijn stelt minimumeisen aan cyberbeveiliging die overal in de EU gelden, maar waar nationale overheden nog strengere regels bovenop kunnen stellen. De Cyberbeveiligingswet (Cbw) is het wetsvoorstel om de NIS2 naar nationale wetgeving om te zetten. Deze wet zal de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangen. De ontwerpregeling van de Cbw ligt op het moment van schrijven (september 2025) ter advies bij de Raad van State.

De vereisten voor digitale weerbaarheid in de NIS2-richtlijn bestaan voornamelijk uit procedurele en organisatorische maatregelen. Zo moeten organisaties zich verplicht registreren bij het MCSC, zijn zij verplicht om een risicoanalyse uit te voeren, passende beveiligingsmaatregel te treffen en moeten zij zorgdragen voor de beveiliging van de leveranciersketen. Daarnaast worden entiteiten verplicht om incidenten te melden aan het NCSC.

Cybersecurity Act (CSA)

De Cybersecurity Act (Verordening (EU) 2019/881) voert een Europees certificeringssysteem in voor IT-producten, -diensten en -processen. Dit systeem is bedoeld om het beveiligingsniveau tegen cyberdreigingen te verhogen en om te voorkomen dat fabrikanten en dienstverleners in elke lidstaat apart een certificaat moeten verkrijgen. De Europese regeling vervangt daarmee bestaande nationale certificeringen, wat bijdraagt aan een meer geharmoniseerde en efficiëntere interne markt. In het licht van digitale weerbaarheid gaat hier dus om procedurele maatregelen die genomen worden om systemen beter te beschermen tegen dreigingen.

Met de CSA is de rol van het European Union Agency for Cybersecurity (ENISA) uitgebreid en ontwikkelt het in opdracht van de Europese Commissie (EC) certificeringsregelingen. De CSA definieert drie beveiligingsniveaus waarop gecertificeerd kan worden; basis, substantieel en hoog. Er zijn ook Nationale Cybersecurity Certificeringsautoriteiten (NCCA), een rol die in Nederland wordt vervuld door de Rijksinspectie Digitale Infrastructuur (RDI). De taken van de NCCA bestaan uit: activiteiten voor de certificering op het CSA niveau ‘hoog’; toezicht op de naleving van de certificeringsvoorwaarden door certificaathouders op de CSA-niveaus ‘basis’, ‘substantieel’ en ‘hoog’; en toezicht op de naleving van de certificeringsvoorwaarden door de certificerende instellingen die de certificering uitvoeren en Europese

certificaten uitreiken, zogenaamde Conformiteit beoordelende instanties (CBI), en instellingen die onder de certificeringsregelingen technische tests uitvoeren.

Radio Equipment Directive (RED)

De Radio Equipment Directive (Richtlijn 2014/53/EU) vormt een belangrijk instrument voor de harmonisatie van regelgeving met betrekking tot radioapparatuur binnen de Europese Unie. Door het vastleggen van essentiële vereisten op het gebied van veiligheid, elektromagnetische compatibiliteit en efficiënt gebruik van het radiospectrum, waarborgt de RED dat uiteenlopende typen radioapparatuur, variërend van mobiele telefoons tot satellietzenders, op een veilige wijze aangeboden kunnen worden in de EU.

In reactie op de toenemende digitale dreigingen is de richtlijn uitgebreid met specifieke bepalingen op het gebied van cybersecurity. Sinds 2022 zijn fabrikanten verplicht om voor radioapparatuur verbonden met het internet te voldoen aan aanvullende cybersecurityeisen, zoals vastgelegd in artikel 3 lid 3 (RED 3.3) en de bijbehorende subartikelen. Deze bepalingen verplichten fabrikanten tot het implementeren van maatregelen ter bescherming van communicatienetwerken, het waarborgen van de privacy en de bescherming van persoonsgegevens, alsook het voorkomen van fraude, in het bijzonder bij apparaten die staat zijn om persoonsgegevens, verkeersgegevens of locatiegegevens te verwerken, om financiële transacties faciliteren, en bij radioapparatuur die ontworpen of bedoeld is voor kinderzorg, speelgoed en draagbare producten (wearable) die in staat zijn deze gegevens te verwerken, ongeacht of het product in staat is met het internet te communiceren. De richtlijn leidt tot een verplichting om technische maatregelen te nemen om een betere bescherming te bieden tegen dreigingen en deze effectief te detecteren.

Cyber Resilience Act (CRA)

De verordening cyberweerbaarheid (Verordening (EU) 2024/2847) is gericht op het verbeteren van de cyberbeveiliging van digitale producten en diensten. Het doel is om digitale weerbaarheid te versterken door ervoor te zorgen dat producten en diensten die binnen de EU worden verkocht, voldoen aan hoge normen van cyberbeveiliging. Wanneer digitale producten, zowel software als hardware, niet voldoen aan de normen kunnen deze van de Europese markt geweerd of verwijderd worden. Maatregelen die voortvloeien uit deze verordening zijn technisch van aard en dragen hiermee bij aan de fase ‘beschermen’ in de weerbaarheidscyclus.

Cyber Solidarity Act (CSOA)

De verordening cybersolidariteit (Verordening (EU) 2025/38) is gericht op het versterken van de samenwerking en solidariteit tussen EU-lidstaten op het gebied van cyberbeveiliging. De verordening is bedoeld om de collectieve digitale weerbaarheid van de EU te vergroten door middel van gedeelde middelen, informatie-uitwisseling en gezamenlijke responsstrategieën. De algehele digitale weerbaarheid van de EU en haar lidstaten wordt hierdoor verbeterd aangezien cybercriminelen en statelijke actoren minder ‘achterdeurtjes’ hebben om binnen te dringen op Europese datanetwerken. Deze maatregelen ondersteunen in de weerbaarheidscyclus de fase ‘beschermen’.

Digital Services Act (DSA)

De DSA (Verordening (EU) 2022/2065) heeft als doel om een veiliger en transparantere onlineomgeving te creëren en heeft betrekking op een breed scala aan digitale diensten, van socialemediaplatforms en onlinemarktplaatsen tot zoekmachines en clouddiensten. De wetgeving draagt bij aan digitale weerbaarheid door platforms te verplichten veiligheidsmaatregelen te treffen die gebruikers beschermen tegen schadelijke inhoud en cyberdreigingen. Ook moeten platforms periodieke risicobeoordelingen uitvoeren en maatregelen implementeren waar nodig. De maatregelen zijn hiermee procedureel, maar ook technisch van aard. In Nederland zijn de beoogd toezichthouders hierbij de Autoriteit Consument & Markt (ACM) en de Autoriteit Persoonsgegevens (AP).

Digital Markets Act (DMA)

De DMA (Verordening (EU) 2022/1925) regelt extra markt- en fusietoezicht op én concurrentieregels voor de wereldwijd grootste onlineplatforms. Hiermee draagt het bij aan een diversificatie van de onlinemarkt en een breder scala aan producten en diensten. Dit zorgt ervoor dat de digitale wereld minder afhankelijk is van enkele aanbieders, en dus beter beschermd is tegen grootschalige systeemstoringen. Hoewel de verordening voor de meeste Nederlandse organisaties geen directe maatregelen oplegt, versterkt zij wel de fase 'beschermen' in de weerbaarheidscyclus, doordat ze afhankelijkheden verkleint. In Nederland is ACM de nationale toezichthouder op de DMA.

Conclusies over juridische kaders

De Cyberbeveiligingswet (Cbw) zal expliciet minimumeisen stellen voor cyberbeveiliging, hetzij voor een beperkt aantal organisaties die een belangrijke publieke functie hebben. Zo moeten op basis van risicoanalyses passende beveiligingsmaatregelen worden getroffen door deze organisaties en moeten incidenten verplicht gemeld worden bij de toezichthouder. Organisaties hebben wat betreft digitale weerbaarheid een zorgplicht voor zichzelf op intern vlak, zowel op gebied van de technische maatregelen en voor de training van personeel, en op extern vlak voor de beveiliging van hun toeleverancierskeken. De implementatie van de Cbw zal zo leiden tot een breed scala aan maatregelen voor organisaties die onder deze wetgeving vallen en alle fasen van de weerbaarheidscyclus beslaan.

Veel andere wetgevende kaders, zoals de CSA, RED en CRA, zijn gericht op het beschermen van digitale weerbaarheid door certificeringsprocedures te vereisen voor producten die op de Europese markt aangeboden worden. In deze gevallen kan er gesproken worden over technische, maar vooral procedurele maatregelen die voortkomen uit de wetgeving. Ook de DSA en DMA dragen deels bij aan de digitale weerbaarheid van Europese burgers en organisaties door procedurele maatregelen te treffen om platformgebruikers te beschermen en om afhankelijkheden tegen te gaan. Al deze maatregelen zijn gefocust op de fase 'beschermen' in de weerbaarheidscyclus met interventies die vooral aan de voorkant moeten voorkómen dat digitale weerbaarheid van systemen of organisaties in het gedrang komen. De juridische insteek is daarmee om er met procedurele maatregelen voor te zorgen dat de digitale weerbaarheid bij organisaties gewaarborgd of verbeterd wordt.

A.4. Initiatieven ter versterking van de digitale weerbaarheid van Nederlandse organisaties en specifieke sectoren

Vaak zijn organisaties gedeeltelijk afhankelijk van andere actoren voor hun digitale weerbaarheid. Er zijn dan ook veel initiatieven opgezet om digitale weerbaarheid te vergroten in verschillende ketens, branches of regio's. Onderstaande voorbeelden zijn verschillend van aard, maar worden alle tenminste gedeeltelijk ingezet om de digitale weerbaarheid van Nederlandse organisaties te vergroten. Net als de eerder besproken beleidsstukken en wetgeving, worden enkele van deze initiatieven uitgelicht om te analyseren wat er onder digitale weerbaarheid verstaan wordt, welke maatregelen gestimuleerd worden, en wat dit leert over het meten van digitale weerbaarheid.

Cyberweerbaarheidsiniatieven

Nederland telt een breed scala aan initiatieven die als doel hebben de digitale weerbaarheid van organisaties te verbeteren. De Wegwijzer voor cybersecurityinitiatieven van het Digital Trust Center van het Ministerie van Economische Zaken omvat bijvoorbeeld al 55 verschillende initiatieven.[11] Sommige van deze initiatieven specificeren zich sterk op een organisatie, zoals het 'Cybersecurity Synergie Schiphol Ecosysteem', op een regio zoals 'Cyber Netwerk Drechtsteden', op een sector zoals 'Cybersecurity Centrum Maakindustrie', of breder op organisaties in Nederland zoals 'Cyberveilig Nederland'. Deze initiatieven hebben ten doel om een hoog niveau van cyberweerbaarheid in hun keten, branche of regio te bereiken, en werken samen om kennis en kunde te kunnen uitwisselen en zo, door breed op cyberweerbaarheid in te zetten, tot een sterkere gezamenlijke positie te komen.

Een voorbeeld is het Actieprogramma Veilig Ondernemen 2023 t/m 2026, gepubliceerd door het Nationaal Platform Criminaliteitsbeheersing (NPC 2022), waarin de actiepunten omtrent de preventie van cybercrime voor het bedrijfsleven uiteen worden gezet. Hierbij wordt er gefocust op de verantwoordelijkheid die ondernemers zelf dragen voor de digitale weerbaarheid van hun bedrijven en de faciliterende rol die de overheid en private partijen, zoals brancheverenigingen, hierbij hebben.

Een ander voorbeeld is het Programma Cyclotron, een publiek-private samenwerking tussen overheid, bedrijven en maatschappelijke organisaties, gericht op het snel en effectief delen van informatie over digitale incidenten en dreigingen. Via een gedeeld platform wisselen hoogvolwassen partijen ruwe data en inzichten uit, waardoor collectieve analyses mogelijk zijn en beveiligingsteams sneller kunnen reageren op cyberaanvallen (NCTV 2024d).

Deze grote verscheidenheid aan initiatieven weerspiegelt de strategieën ter bevordering van de cyberweerbaarheid van de gehele samenleving, van individuele burgers tot grote organisaties, die door de overheid worden geïmplementeerd, zoals de Nederlandse Cybersecuritystrategie 2022-2028 en de I-strategie Rijk 2021-2025 (NCTV 2022a; Rijksoverheid 2021).

Een belangrijke nieuwe uitdaging hierbij is het verkleinen van de kloof in digitale weerbaarheid die bestaat tussen het midden- en kleinbedrijf (mkb) en grotere organisaties in Nederland. Recent heeft de Cyber Security Raad (CSR) een advies uitgebracht over deze 'cyberweerbaarheidskloof' waarin ze stelt dat er een

[11] Zie: https://www.digitaltrustcenter.nl/wegwijzer-cybersecurity-initiatieven

gerichte, structurele en uniforme aanpak gerealiseerd moet worden om de cyberweerbaarheid van het mkb te verbeteren door passende hulpmiddelen te bieden en bedrijven te stimuleren actie te ondernemen (CSR 2024). De kabinetsreactie op dit advies geeft aan dat er gewerkt wordt aan de implementatie van veel onderdelen die in het advies benoemd worden. Zo is de integratie van het NCSC, het DTC en het Computer Security Incident Respons Team voor digitale diensten (CSIRT-DSP) ingezet om te zorgen dat ondernemers bij een loket terecht kunnen voor hulp, wordt er geïnvesteerd in de uitbouw van cyberweerbaarheidsnetwerken, worden hulpmiddelen geharmoniseerd, komen er brede maatschappelijke publiekscampagnes, en zal de NIS2-rictlijn worden geïmplementeerd (Beljaarts 2024).

Vijf basisprincipes van digitale weerbaarheid

Het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) hebben vijf basisprincipes van digitale weerbaarheid ontwikkeld om organisaties een handvat te geven om de basis van cybersecurity te organiseren, samen met bredere acties die ondernomen kunnen worden om digitaal weerbaar te worden. Deze vijf basisprincipes voor digitale weerbaarheid (NCSC 2024a) bestaan uit:

1. **Breng risico's in kaart:** Organisaties moeten een passend niveau van digitale weerbaarheid bereiken dat aansluit op hun specifieke situatie, door beveiligingsmaatregelen te nemen die hun informatie en informatiesystemen op een gepaste manier beschermen. Door in kaart te brengen welke risico's er zijn en hoe hierop gereageerd moet worden, kunnen de belangen van de organisaties en hun partners beter beschermd worden en kan de weerbaarheid groeien.
2. **Bevorder veilig gedrag:** Acties om medewerkers bewuster te maken van risico's en hen te trainen hoe om te gaan met incidenten kan veilig gedrag en weerbaarheid vergroten. Dit kan met technische middelen zoals spamfilters om phisingmails en schadelijke software te herkennen en weren, maar ook door in te zetten op trainingen en kennisverspreiding onder werknemers. Ook moet er gewerkt worden aan een cultuur waar veilig melding gemaakt kan worden van eventuele incidenten.
3. **Bescherm systemen, applicaties en apparaten:** Systemen, applicaties en apparaten moeten goed beschermd worden tegen aanvallen. Door tijdig updates en patches te installeren kunnen kwetsbaarheden zo snel mogelijk gedicht worden. Ook kunnen monitoring- en detectieoplossingen helpen om tijdig te kunnen reageren op een aanval en de schade te beperken.
4. **Beheer toegang:** Om de kans op ongelukken en misbruik zo klein mogelijk te houden, is het belangrijk om medewerkers en partners van buiten de organisatie alleen toegang te geven tot informatie, systemen en locaties die zij direct nodig hebben voor de uitvoering van hun taken (least privilige). Daarnaast moet toegang goed gemanaged worden. Zo moeten accounts van vertrekkende medewerkers toegang tot data en systemen ontzegd worden en ongebruikte accounts verwijderd worden.
5. **Bereid voor op incidenten:** Als een incident zich voordoet, is het belangrijk voor organisaties om zo snel mogelijk weer aan de slag te kunnen gaan. Er moet dus aandacht besteed worden aan bedrijfscontinuïteit, uitwijk- en herstelplannen, incidentenresponsplannen en back-upstrategieën. Om optimaal voorbereid te zijn, moeten deze plannen geoefend worden en moeten back-ups regelmatig getest worden.

De basisprincipes zijn zo opgesteld dat ze van toepassing kunnen zijn op iedere organisatie. Voor verdere informatie en uitwerking van de basisprincipes wordt er wel gedifferentieerd tussen organisaties. Zelfstandigen en mkb'ers worden doorverwezen naar de pagina van het Digital Trust Center terwijl grotere ondernemingen en organisaties die onder de NIS2 vallen, bij het NCSC terecht kunnen. Ook wordt er bij elk basisprincipe verwezen naar relevante richtlijnen en artikelen in wetgeving zoals NIS2 of bestaande informatiebeveiligingsnormen zoals ISO/IEC 27001 en BIO (Baseline Informatiebeveiliging Overheid). De basisprincipes omvatten alle typen maatregelen die eerder besproken zijn. Technische, procedurele en organisatorische maatregelen vloeien allemaal voort uit de basisprincipes. Binnen de weerbaarheidscyclus komen ook alle fasen van weerbaarheid aan bod, al ligt de nadruk op het beschermen. Herkennen komt aan bod in principe 1, beschermen in principes 2, 3 en 4; en principes 3 en 5 omvatten detecteren, reageren en herstellen.

Cyberweerbaarheidsnetwerk

Het Cyberweerbaarheidsnetwerk (CWN) is de toekomstige doorontwikkeling van het Landelijk Dekkend Stelsel (LDS) om samen met het bedrijfsleven het bereik van het LDS te verhogen (NCTV, 2024c). Naast de hoofdfunctie van het LDS, zijnde informatiedeling, krijgt het CWN ook de functies incidentafhandeling; doelwit- en slachtoffernotificatie; opleiden, trainen en oefenen; en kennisdeling. Hiermee gaat het CWN een veel grotere rol vervullen in het verbeteren van de cyberweerbaarheid van Nederland dan het LDS tot nu toe deed. De scope van het uitgebreide stelsel past dan ook beter binnen het concept weerbaarheid dan het LDS tot nu toe deed.

Ook moet het toekomstige CWN voor een hogere mate van duidelijkheid zorgen, duidelijkheid over de reikwijdte van het stelsel, de voorwaarden voor deelname, de regie en coördinatie van het stelsel. Door bestaande publiek-private samenwerkingsinitiatieven samen te voegen onder het CWN ontstaat er consolidatie in het cybersecuritylandschap van Nederland wat verder voor duidelijkheid en verbeterde samenwerking en coördinatie zal zorgen (NCTV, 2024c). Het CWN heeft de ambitie om alle organisaties in het Koninkrijk der Nederlanden te bereiken en hun weerbaarheid te verhogen door samen te werken met netwerkpartners die toegang hebben tot deze organisaties.

I-strategie Rijk 2021-2025

De overheid heeft in 2021 de I-strategie Rijk 2021-2025 opgesteld om adviezen en actiepunten te verzamelen en bundelen rond de grootste uitdagingen van de overheid op het gebied van informatiebeveiliging. Het versterken van de digitale weerbaarheid is dan ook een van de belangrijkste onderdelen hiervan. Om dit te verbeteren zijn er drie speerpunten geïdentificeerd in de strategie (Rijksoverheid 2021, 20-32). Ten eerste is er de governance omtrent digitale weerbaarheid. Zo moeten verantwoordelijke ambtenaren bijvoorbeeld in staat gesteld worden om goed te sturen op digitale weerbaarheid met gezamenlijke standaardfaciliteiten en kennisdeling, en moet crisismanagement geoefend en op orde zijn. Ten tweede moet er gewerkt worden aan feitelijke veiligheid, met preventieve maatregelen en voorzieningen in de administratieve omgeving, een actuele en robuuste architectuur als basis voor *lifecycle*management, ontwikkeling van werkplekvoorzieningen op staatsgeheimniveau en actualisering van rijksbrede cloudstrategie en -kaders. Het laatste speerpunt omvat weerbare medewerkers; zo moet er een

rijksbrede aanpak voor een digitale weerbaarheidscultuur ontstaan met een groot trainingsaanbod en gebruiksvriendelijke instrumenten.

Annex B. Mogelijk voortbouwend op NIS2-rapportagevereisten

Deze studie heeft de uitdagingen belicht bij het definiëren van en toegang krijgen tot realtime informatie over de digitale weerbaarheid van organisaties die op nationaal niveau kan worden geaggregeerd. Onze analyse van een breed scala aan raamwerken illustreert dat digitale weerbaarheid geen algemeen aanvaarde definitie of gestandaardiseerd meetkader kent. Er is ook geen duidelijk bewijs voor de validiteit en betrouwbaarheid van bestaande raamwerken voor het meten van digitale weerbaarheid, en het is daarom ook onduidelijk of een bepaalde manier om digitale weerbaarheid te meten meer valide of betrouwbaarder is dan een andere. Verschillende benaderingen zijn ontworpen voor verschillende doeleinden en zijn aangepast aan de behoeften van bepaalde organisaties of sectoren, maar hebben ook aanzienlijke uitdagingen gemeen:

- De meeste meetmethoden houden niet volledig rekening met de organisatorische context, zoals hoeveel risico een organisatie bereid is te accepteren of hoeveel zij investeert om digitale weerbaarheid te bereiken.
- Weerbaarheid is geen statisch gegeven. Wat organisaties nodig hebben en verwachten, kan in de loop van de tijd veranderen, en weerbaarheid is afhankelijk van zowel interne systemen als de externe bedreigingsomgeving. Als de externe bedreigingen toenemen, kan de weerbaarheid van een organisatie afnemen, zelfs als haar interne systemen hetzelfde blijven. Dit maakt het moeilijk om weerbaarheid nauwkeurig te meten en te vergelijken tussen verschillende organisaties of tijdsperioden.

In deze context zou een praktische volgende stap voor de NCTV kunnen zijn om te proberen enkele aspecten van digitale weerbaarheid te meten, in plaats van alle aspecten, wat vervolgens als basis zou kunnen dienen om verder op voort te bouwen. Als onderdeel van de samenwerking met de NCTV en de begeleidingscommissie voor dit onderzoek is de mogelijkheid geopperd om het rapportagemechanisme in het kader van de NIS2-richtlijn te gebruiken als een potentiële en praktische manier om te beginnen met het verzamelen van gegevens om de digitale weerbaarheid in Nederland te meten.[12]

Dit maakte geen deel uit van het overzicht van bestaande benaderingen in hoofdstuk 3, maar biedt niettemin een mogelijkheid om informatie te verzamelen die mogelijk kan worden gebruikt als proxyindicatoren voor digitale weerbaarheid, met name in kritieke infrastructuurorganisaties. Kader 1 somt een aantal passende

[12] De omzetting van de NIS2-richtlijn in de Nederlandse wet, de Cbw, zal naar verwachting in het tweede kwartaal van 2026 in werking treden, zie https://www.digitaleoverheid.nl/nieuws/informatiebrochure-cyberbeveiligingswet-gepubliceerd/

technische, operationele en organisatorische maatregelen op die essentiële en belangrijke entiteiten op grond van de NIS2-richtlijn moeten nemen.

Kader 1. Maatregelen die moeten worden genomen door entiteiten die onder de NIS2-richtlijn vallen

- Beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- Incidentafhandeling;
- Bedrijfscontinuïteit, zoals back-upbeheer en noodherstel, en crisisbeheer;
- Beveiliging van de toeleveringsketen, met inbegrip van beveiligingsaspecten met betrekking tot de relaties tussen elke entiteit en haar directe leveranciers of dienstverleners;
- Beveiliging bij de aanschaf, ontwikkeling en het onderhoud van netwerk- en informatiesystemen, met inbegrip van het omgaan met en bekendmaken van kwetsbaarheden;
- Beleid en procedures om de effectiviteit van maatregelen voor cyberbeveiligingsrisicobeheer te beoordelen;
- Basisprincipes van cyberhygiëne en cybersecuritytraining;
- Beleid en procedures met betrekking tot het gebruik van cryptografie en, indien van toepassing, encryptie;
- Beveiliging van human resources, beleid inzake toegangscontrole en activabeheer;
- Het gebruik van multifactorauthenticatie of continue authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit, indien van toepassing.

Bron: Richtlijn (EU) 2022/2555, art. 5.

De richtlijn bevat ook een aantal rapportageverplichtingen voor deze organisaties, onder meer met betrekking tot significante cyberdreigingen die de continuïteit of veiligheid van essentiële en belangrijke diensten kunnen beïnvloeden – zelfs als deze dreigingen nog niet tot een incident hebben geleid – en met betrekking tot incidenten. Incidentrapportage omvat eerste meldingen van een significant incident aan de relevante nationale autoriteit of het Computer Security Incident Response Team (CSIRT) zonder onnodige vertraging en, indien mogelijk, binnen 24 uur nadat het incident bekend is geworden; een tussentijds rapport met een update over het incident dat binnen 72 uur moet worden verstrekt, met inbegrip van een eerste beoordeling van de ernst, de gevolgen en de indicatoren van het incident; en een gedetailleerd eindrapport binnen een maand na het oplossen van het incident, met een overzicht van de oorzaken, de gevolgen en de stappen die zijn genomen om herhaling te voorkomen.

De rapporten onder deze meldplicht zullen ertoe leiden dat nieuwe gegevens, die voorheen niet direct beschikbaar waren voor de overheid, verzameld zullen worden. Dit biedt de gelegenheid om na te gaan welke informatie kan worden opgevraagd en kan worden gebruikt om te beginnen met het verzamelen van gegevens die verband houden met indicatoren van digitale weerbaarheid. In het kader van dit onderzoek biedt het gebruik van de NIS2-richtlijn potentiële voordelen en kansen voor het verzamelen van gegevens met betrekking tot digitale weerbaarheid verschillende, maar ook belangrijke beperkingen.

Tabel 13. Potentiële voordelen, beperkingen en kansen van het gebruik van de NIS2-richtlijn om digitale weerbaarheid te meten

Voordelen	• NIS2 biedt de Nederlandse overheid een duidelijk wettelijk mandaat om in geval van cyberbeveiligingsincidenten informatie te verzamelen bij aangewezen organisaties. • Het vormt geen doublure van bestaande cyberbeveiligingsinitiatieven, aangezien het geen afzonderlijk mechanisme invoert dat uitsluitend gericht is op het beoordelen van de digitale weerbaarheid van organisaties. • NIS2 kan worden afgestemd op de huidige rapportagevereisten en kan worden aangepast om informatie te verzamelen over de impact of de omvang van het functieverlies als gevolg van cyberbeveiligingsincidenten, wat een cruciaal element van weerbaarheid is.
Beperkingen	• De primaire focus van NIS2 ligt op het melden van incidenten en niet op het expliciet meten van digitale weerbaarheid. • De verplichte rapportagevereisten onder NIS2 zijn alleen van toepassing op een beperkte subgroep van essentiële en belangrijke entiteiten, en niet op alle organisaties in Nederland. • De rapportageverplichtingen van NIS2 worden geactiveerd door het optreden van relevante incidenten en verplichten niet tot regelmatige rapportage over bredere digitale weerbaarheidskwesties. • De gegevens die via incidentmeldingen worden verzameld, bieden geen contextuele informatie over de cyberbeveiligingspositie van organisaties, investeringen of het heersende dreigingslandschap.
Kansen	• Als de rapportagestructuur succesvol is, kunnen de reikwijdte en inhoud ervan in de toekomst worden uitgebreid om aanvullende aspecten van digitale weerbaarheid te omvatten. • De rapportagestructuur zou ook kunnen worden uitgebreid naar een groter aantal organisaties, mogelijk op vrijwillige basis. • Er kunnen mogelijkheden zijn om NIS2-rapportagegegevens te combineren met andere bronnen, zoals het Cybersecuritybeeld van het NCSC. Door bijvoorbeeld incidenten en de gevolgen daarvan die onder NIS2 zijn geregistreerd, te vergelijken met het bredere dreigingslandschap, kan worden bepaald of organisaties meer of minder worden getroffen door specifieke soorten incidenten.

Bron: Analyse van RAND Europe.

Het doel is niet om in dit stadium de doeltreffendheid van NIS2 te beoordelen, maar om diens meldplicht te gebruiken als uitgangspunt voor een systematische gegevensverzameling die in de loop van de tijd kan worden gevolgd. Zodra de transpositie is voltooid en de Cbw in werking treedt, zal het NCSC een centraal meldpunt voor NIS2-entiteiten opzetten (NCSC 2024b). De exacte vragenlijst die zal worden gebruikt, is nog niet beschikbaar, maar voorlopig verwijst het NCSC naar een formulier waarop incidenten vrijwillig kunnen worden gemeld.[13]Tabel 14 laat zien welke informatie momenteel via dit formulier wordt gevraagd en welke (soorten) aanvullende vragen de NCTV zou kunnen suggereren om zodoende samen met het NCSC gedetailleerdere informatie te verzamelen met betrekking tot specifieke indicatoren en NCTV-activiteiten. Zo kan meer inzicht worden verkregen in de digitale weerbaarheid van deze organisaties.

[13] Zie: https://www.ncsc.nl/contact/contactformulieren/incident-melden

Aangezien NIS2 zich voornamelijk bezighoudt met incidentmeldingen, zijn er ten minste twee aanvullende soorten informatie nodig om de beperkingen van incidentgegevens bij het beoordelen en meten van digitale weerbaarheid aan te pakken:

- Contextuele informatie over de organisatie en haar cyberbeveiligingshouding;
- Informatie over de relatie tussen het incident en de reële gevolgen ervan voor het functioneren van de organisatie.

Idealiter zou deze informatie in een gestandaardiseerd format moeten worden vastgelegd in plaats van als open tekst, om gegevensaggregatie, vergelijking en longitudinale analyse te vergemakkelijken.

Tabel 14. Informatie die moet worden verstrekt in het NIS2-incidentrapport

Categorie	**Actuele gevraagde informatie**	**Mogelijke aspecten van digitale weerbaarheid die kunnen worden toegevoegd**
Organisatorische gegevens	1. Naam van de organisatie, adres, KvK-nummer, sector, type entiteit 2. Gegevens contactpersoon	Contextuele informatie: • Omvang van de organisatie • Huidige cybersecuritystatus • Huidig investeringsniveau in cybersecurity De laatste twee gegevenspunten zouden waarschijnlijk zelfbeoordelingen moeten zijn. Het investeringsniveau zou mogelijk kunnen worden vastgelegd op een ordinale schaal in verhouding tot het type/de grootte van de organisatie (bijvoorbeeld laag/gemiddeld/hoog op basis van de gemiddelde organisatie-uitgaven).
Algemene informatie	3. Type incident [gesloten vraag, d.w.z. geen open antwoord] 4. Type melding [gesloten vraag] 5. Oorzaak (waarschijnlijkheid dat het incident is veroorzaakt door een onwettige of kwaadwillige handeling) [J/N] 6. Status van het incident [gesloten vraag] 7. Grensoverschrijdende gevolgen [J/N]	Geen verdere vereisten inzake digitale weerbaarheid in dit deel

Categorie	Actuele gevraagde informatie	Mogelijke aspecten van digitale weerbaarheid die kunnen worden toegevoegd
Incident-specifieke informatie	8. Datum en tijdstip van ontdekking van het incident 9. Type incident [gesloten vraag] 10. Beschrijving van het incident [open tekst] 11. Zichtbare en verwachte gevolgen van het incident [open tekst] 12. Oorzaken en maatregelen die zijn genomen om het incident in de toekomst te voorkomen [open tekst] 13. Of klanten zijn of zullen worden geïnformeerd [gesloten vraag] 14. Verwachte hersteltijd [in te vullen in dagen en uren] 15. Genomen/geplande maatregelen en behoefte aan hulp [open tekst] 16. Aangifte gedaan bij de politie [J/N] 17. Overige toevoegingen [open tekst]	Er is wellicht een mogelijkheid om dit duidelijker te structureren in overeenstemming met de digitale weerbaarheidsfasen zoals besproken in hoofdstuk 2 (herkennen, beschermen, detecteren, reageren, herstellen), om beter in kaart te brengen waar en waarom er mogelijke tekortkomingen waren. Momenteel wordt gesuggereerd dat de eerste vier fasen worden behandeld in vraag 10, maar respondenten geven hun antwoord mogelijk niet in die vorm. Ook zou er explicieter kunnen worden vermeld welke technische, procedurele of organisatorische maatregelen hebben gefaald of zullen worden verbeterd (met name in vraag 10/12). De belangrijkste verandering zou zijn om de 'zichtbare en verwachte gevolgen van het incident' systematisch bij te houden en te analyseren aan de hand van een gedetailleerdere ordinale schaal of gestructureerd antwoord, waardoor een vollediger inzicht in de gevolgen voor de weerbaarheid mogelijk zou worden.

Bron: Analyse van RAND Europe van het vrijwillige NIS2-incidentmeldingsformulier van het NCSC.

Samenvattend kan worden gesteld dat het gebruik van de NIS2-richtlijn een basis biedt voor het verzamelen van nieuwe gegevens over digitale weerbaarheid op een pragmatische en uitvoerbare manier. Hoewel NIS2 niet is ontworpen om een uitgebreide beoordeling van digitale weerbaarheid te bieden, vormt de meldingsplicht voor incidenten een waardevol uitgangspunt voor systematische gegevensverzameling voor een beperkt aantal maar belangrijke organisaties.

Door incidentgegevens aan te vullen met contextuele informatie over de cybersecuritypositie van organisaties en de reële gevolgen van incidenten, en door deze informatie in een gestandaardiseerd format vast te leggen, kan de NCTV de basis leggen voor een robuustere en longitudinale analyse van digitale weerbaarheid. Hoewel er nog aanzienlijke beperkingen zijn, met name wat betreft de reikwijdte van de betrokken organisaties en de breedte van de vastgelegde weerbaarheidsindicatoren, vormt de implementatie van de NIS2-rapportagevereisten een belangrijke stap in de richting van het opbouwen van een empirische basis die als input kan dienen voor toekomstig beleid en operationele beslissingen in Nederland.