SAMENVATTING

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

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. Het onderzoek is uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC), op aanvraag van de NCTV.

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?

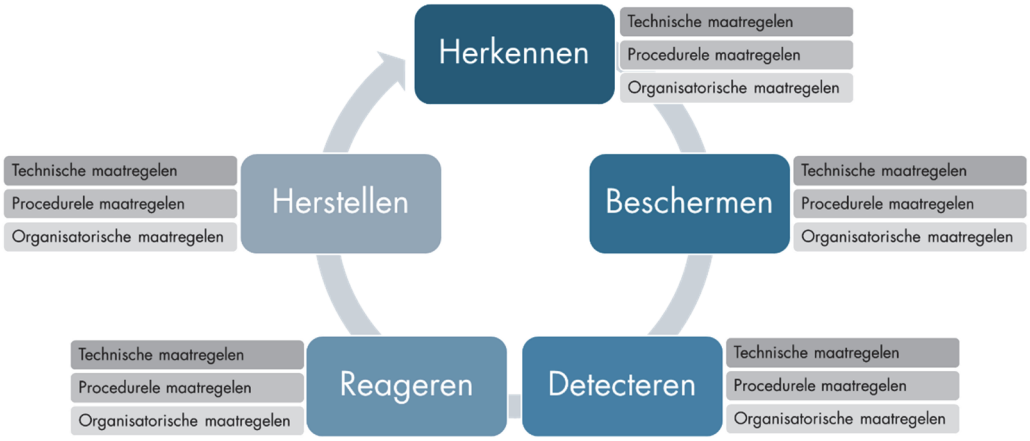
De NCTV definieert digitale weerbaarheid in Nederlandse Cybersecuritystrategie 2022-2028 als:

> 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.