Het antwoord op een cyberramp is niet: méér digitaal

Door **Erik Bouwer**
Beeld **Blinkerd**

“Nederland niet klaar voor digitale ramp” kopte de Telegraaf afgelopen september. Aanleiding: het WRR-rapport ‘Voorbereiden op digitale ontwrichting’. Wat blijft er over van een digitale samenleving als ‘digitaal’ ophoudt te functioneren? Inzet van nog meer technologie klinkt even onlogisch als zinloos. De oplossing zit grotendeels in ‘terug naar start’.

New Orleans is niet de titel van een nieuwe rampenfilm, maar een recent voorbeeld van digitale ontwrichting. Ransomware op de computersystemen van overheidsinstellingen dwong de stad om alle systemen uit te schakelen en los te koppelen. Ambtenaren zijn weer gebruik gaan maken van telefoon, pen en papier.

Voor incidenten in de fysieke wereld, zo betoogt de WRR in haar rapport, hebben we allerlei wetten, regels en crisisorganisaties opgetuigd. Voor ontwrichtende incidenten in de digitale wereld is nog geen aanpak en geen oplossing beschikbaar. Sinds het begin van het internettijdperk zijn de uitdagingen rondom ‘digitaal’ totaal veranderd. Werkten we in 1990 nog met één personal computer als ‘werktuig’, nu zijn we als burger, consument en medewerker verbonden met honderden IT-systemen. De opstellers van het WRR-rapport spreken dan ook niet meer over mediawijsheid of informatievaardigheden, maar over het vergroten van het bewustzijn van de risico’s van de digitale samenleving.

De vraag is of daarmee het echte probleem wordt geadresseerd. Er bestaan al programma’s gericht op het vergroten van het bewustzijn rondom risico’s. Zo heeft het NCSC (Nationaal Cyber Security Center) het Cyberkompas gelanceerd dat organisaties inzicht in hun digitale weerbaarheid moet geven. Daarbij draait het onder andere om het in kaart brengen van digitalisering, wet en regelgeving, de rol van de mens, monopolisering van het digitale domein, toename van complexiteit en afname van vrijheid van leveranciers-keuze. Tegenover aandacht voor preventie staat echter weinig aandacht voor de voorbereiding op digitale rampen.

Dat New Orleans ook Den Haag had kunnen zijn, bewijst het onderzoek van hoogleraar internetveiligheid Aiko Pras (Universiteit Twente), afgelopen zomer in dagblad Tubantia. “We vonden zo’n 1.000 apparaten die bijvoorbeeld gebruikt worden om sluizen of bruggen aan te sturen. Zo’n 60 vertonen dermate grote beveiligingslekken dat het voor hackers kinderspel is om ze uit te schakelen of te saboteren.” Maar niet alleen de vitale fysieke infrastructuur, vrijwel alle bedrijven en instellingen zijn voor hun huidige functioneren volledig afhankelijk van digitale infrastructuur. Als de stroom uitvalt, kun je thuis nog een kaars aansteken en schakelt een datacenter over op nood-

In Den Haag ontbreken de kennis en de alertheid om er iets aan te doen

stroom. Maar inmiddels gaat digitale weerbaarheid niet meer over lapmiddelen als kaarsen en noodstroomvoorzieningen. Het WRR-rapport refereert aan totale ontwrichting van de (digitale) samenleving. Wat doe je als grote gemeente, als systeembank of als uitkeringsverstrekker als het belangrijkste internetknooppunt van Nederland volledig down gaat?

Analoog scenario

"In New Orleans is men overgestapt op analoge werkwijzen omdat alle systemen uitgezet moesten worden. Je kunt dus niet 'half doordraaien' of even wat andere technologie inzetten", stelt Marleen Stikker, directeur Waag Society. "Ik vrees dat weinig organisaties zo'n analoog scenario hebben klaarliggen, met het idee dat het niet echt nodig is. Het is een interessante case als een stad als New Orleans alle systemen moet uitschakelen, waarbij men erop gericht is die systemen zo snel mogelijk weer in te schakelen, om daarna extra veel te investeren in cybersecurity." De respons wordt gezocht in 'méér digitaal', en niet in hoe technologie ontworpen wordt, concludeert Stikker. Zij zou liever terug naar de tekentafel gaan: "We maken nog steeds heel kwetsbare technologie, en die kwetsbaarheid wordt niet alleen uitgebuit door kwaadwillenden, maar ook door de ICT-industrie zelf die zichzelf tegen exorbitante kosten weer laat inhuren om het probleem op te lossen."

Ook UT-onderzoeker Pras sprak zijn vrees uit dat "een digitale aanval van buitenaf nodig zal zijn om de overheid wakker te schudden. En in Den Haag ontbreken de kennis en de alertheid om er iets aan te doen." Dat is heel andere taal dan de taal die vijftien tot twintig jaar geleden werd gebruikt, toen internetfans van het eerste uur nog geloofden dat het wereldwijde web mensen onderling zou verbinden, samenwerking zou vergemakkelijken, en informatie vrij zou laten stromen.

Ook nu nog wordt technologie vooral door een roze bril bekeken, aldus Melanie Peters, directeur van het Rathenau Instituut. "Wat niet helpt, is dat begrippen als digitalisering en disruptie primair als iets positiefs worden beschouwd. Ook ons eigen kabinet heeft in 2017 nog geschreven dat disruptie zou kunnen helpen om een aantal markten die niet goed functioneren, te herordenen. Voor techbedrijven zijn veel uitzonderingen op bestaande wetgeving gecreëerd. Een taxibedrijf moet aan eisen voldoen, zoals certificaten en diploma's, die niet voor Uber gelden. Uber's bedrijfsmodel is echter niet gericht op creëren van werkgelegenheid, maar verzamelt data van gebruikers en hun bewegingen; handig als je autonome auto's wilt laten rijden die verder geen werkgelegenheid opleveren en op termijn het openbaar vervoer bedreigen. Ook als het gaat om de overheid hebben we het beeld de wereld in geholpen dat deze niet bij de tijd is en hoognodig gedigitaliseerd moet worden. Maar misschien zit het probleem wel ergens anders."

Onlogisch vertrouwen

Ook technologie wordt primair gezien als een middel om tot oplossingen te komen. Het antwoord op kwetsbaarheid van digitale technologie – verstoringen door uitval, datalekken, hacks en ransomware – is meestal 'méér technologie' in de vorm van beveiligingsmaatregelen, back-ups, redundantie en noodvoorzieningen. Het grenzeloze vertrouwen in technologie is niet alleen onlogisch, het is – vanuit de overheid bezien – ook niet terecht. Peters: "Het BIT (Bureau ICT Toetsing) heeft herhaaldelijk geconstateerd dat Kamerleden niet tot nauwelijks in staat zijn digitale plannen kritisch te bekijken."

Ook het Centrum voor Informatiebeveiliging en Privacybescherming (CIP, een publiek-private organisatie, opgezet door de Belastingdienst, DUO, SVB en UWV, waaraan ook het bedrijfsleven deelneemt) kwam afgelopen najaar met slecht nieuws. Uit onderzoek van CIP blijkt dat de Chief Information Security Officer (CISO) bij de overheid relatief onervaren is en vaak geen of nauwelijks budget heeft. 40 procent heeft 0 tot 2 jaar ervaring en nog eens 40 procent heeft 2 tot 5 jaar ervaring. 69 procent heeft een parttime functie, 77 procent heeft geen medewerkers, 62 procent heeft geen of slechts een klein budget *(zie ook het artikel op pagina i28)*.

"Digitale weerbaarheid begint met de vraag: waarom zetten we technologie in? Welke waarden zijn dan het uitgangspunt? Hoe zet je de samenleving mee aan het stuur bij het ontwerp van technologie, zonder dat mensen niet alleen het subject zijn", somt Stikker op. "Dit eigenaarschap wordt vaak bij mensen weggehouden, omdat ze het niet zouden snappen – dat argument geldt dan óók voor beleidsmakers. Demystificeren is essentieel, net als bij staatsinrichting: in een democratie is basiskennis over macht en technologie essentieel en is toezicht op macht en technologie voorwaardelijk."

Stikker vindt dat er nog grote stappen gezet kunnen worden op het vlak van 'digitale geletterdheid'. "We zullen technologie een andere, interdisciplinaire, plek in het curriculum moeten geven: een midden tussen maatschappijleer, filosofie, creatieve vakken en informatica. Technologie is niet neutraal. Het doet ertoe waar je het voor ontwerpt, inzet en wat voor een samenleving je daarbij voor ogen hebt. Behandel het niet langer alleen als een apart bètavak, maar zorg ervoor dat iedereen de mogelijkheid heeft om betrokken te zijn bij wat technologie doet met onze wereld. Dat begint bij de basisschool."

Defensiemodel

"Het begrip weerbaarheid is een legerterm. Je kunt tot op zekere hoogte dingen voorkomen, maar je moet je ook voorbereiden op de situatie die ontstaat als het misgaat", aldus Peters. "Als in de digitale samenleving het aspect 'digitaal' wegvalt of tot stilstand komt, moet je niet verwachten dat nog meer technologie een ontstane crisis gaat oplossen. De overlast van de drone op de luchthaven van Gatwick duurde langer dan nodig, omdat niemand wist wie er in actie moest komen. Je kunt altijd terug naar degene die verantwoordelijk is geweest voor het nemen van het besluit om dat ding te laten vliegen. Ook dat is een defensiemodel: nagaan wie het bevel heeft gegeven. De nieuwe dronewetgeving die uit Brussel komt, maakt een uitzondering voor drones lichter dan 500 gram. Maar wat gebeurt er als je een zwerm van heel kleine drones hebt? Primair afgaan op technische eigenschappen is vaak een doodlopende weg, het nadenken over en vastleggen van verantwoordelijkheden is effectiever."

Niet steeds maar meer technologie, maar het herschikken van verantwoordelijkheden en ontwerpprincipes. Ook Peters benadrukt dat terug naar de tekentafel een deel van de oplossing is. "Wat voor samenleving willen we zelf? Hoe hebben we het georganiseerd? Dat gaat met name over verantwoordelijkheden. Als je weet dat iets niet goed gaat en je grijpt niet in, dan ben je schuldig. Het gaat over leiderschap en eigenaarschap en kritisch denkvermogen. Daarom is ook een minister van digitale zaken geen oplossing. Dat vergroot de kans dat je anderen vrijpleit om eigenaarschap te nemen. Je moet in alle domeinen aandacht voor digitaal hebben. Daarnaast kunnen burgers niet alles zelf regelen of in de gaten houden. Er spelen collectieve belangen. Verschillende soorten toezichthouders zullen daarom steeds meer moeten samenwerken."

Stikker ziet verschillende oplossingen voor het vraagstuk van digitale weerbaarheid, die deels ook terugkomen in haar boek 'Het internet is stuk'. "Als je mensen alleen 'geletterd' maakt, dus digitaal lezen en schrijven, versterk je de passieve kant van mensen en train je ze om een goede consument te zijn", zegt Stikker. "Dan heb je het over de Read & Write permissies. Maar de stroom van ellende verandert daar niet mee. We moeten ook de X van eXecute in stelling brengen. Een stevig digitaal publiek domein met executiekracht."

Digitale wasstraat

Stikker pleit daarom voor multidisciplinaire ontwerpprocessen en zou ook voorstander zijn van een maatschappelijke windtunnel die wordt ingezet voordat nieuwe technologie wordt uitgerold: "Is dit iets wat we willen? Voor wie wordt hier geoptimaliseerd? En daarnaast ben ik voorstander van een digitale wasstraat: heel veel mensen moeten opgefrist worden in hun kennis. Wat zit er in de black box die technologie vaak is? De Tijdelijke Commissie Digitale Toekomst die de kennis van Tweede Kamerleden moet vergroten is een goed initiatief. Ik zou heel graag de volledige Tweede Kamer in drie tot vier dagen door onze digitale wasstraat heen halen en ze een permanente onderzoekscapaciteit toewensen. Maar ook techneuten moeten leren begrijpen dat data en algoritmes niet objectief zijn en zich bewust worden van hun vooronderstellingen. Er is veel achterstallig onderhoud, het ontbreekt nog aan een gezamenlijke taal. We moeten werken aan nieuwe, doorleefde kennis: dat is een voorwaarde voor digitale weerbaarheid."