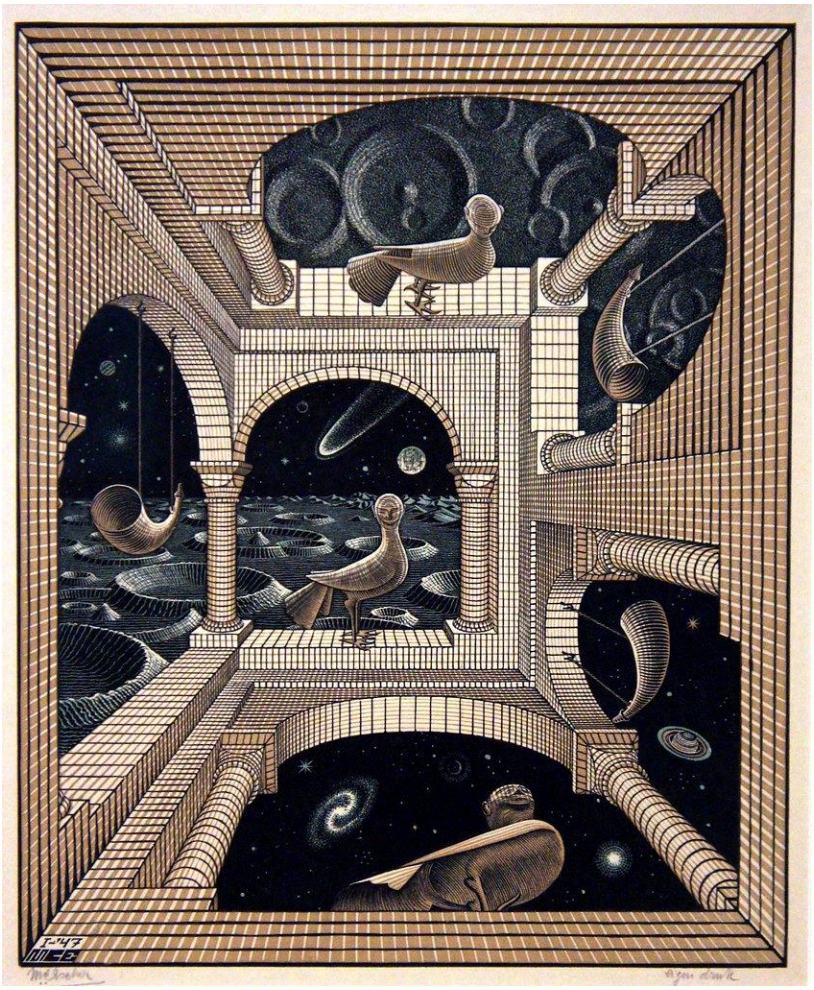
Politiefunctie en rechtsstaat in de gedigitaliseerde samenleving

Positionering in een meervoudige context



Advies aan de korpschef van politie

1 december 2019

Politiefunctie en rechtsstaat in de gedigitaliseerde samenleving.
Positionering in een meervoudige context

Advies aan de korpschef van politie

Opdrachtgevers:	E.S.M. Akerboom
	H.P. van Essen
Opdrachtnemer:	B.J.A.M. Welten
In samenwerking met:	A.J. van Dijk
	A.M. de Bruin
	F.C. Hoogewoning
	G.F.S.J. Kuijlaars
	L.O. Luinenburg
	D. Roest
	R.R.H. van Zeijst

Voorwoord

We zijn terecht gekomen in een nieuw tijdperk: het tijdperk van de digitalisering. Als samenleving worden we geconfronteerd met een nieuwe werkelijkheid, waarin alles complexer wordt en sneller lijkt te gaan, die de menselijke maat overstijgt en die raakt aan de grenzen van het menselijk bevattingsvermogen. Welkom in de wereld van *cybersecurity, cybercrime, cyber-enabled crime, Big Data, datamining*, kunstmatige intelligentie, *cybernetica*, stromen en netwerken. Die nieuwe wereld stelt de samenleving voor nieuwe vraagstukken en uitdagingen.

De nieuwe wereld, waarvan het zogeheten cyberdomein inmiddels deel uitmaakt, is diffuus en dat leidt ertoe dat veel maatschappelijke actoren er zich vol overgave in storten: private partijen en overheidsinstanties als ministeries, provincies, gemeenten, de inlichtingen- en veiligheidsdiensten, de krijgsmacht en *last but not least* de politie. Nieuwe organisaties, coördinatiepunten, informatieknooppunten, netwerken en wat dies meer zij, schieten als paddenstoelen uit de grond.

Kun je in die wereld differentiatie aanbrengen en is het dan denkbaar vast te stellen wie wat doet? Is er sprake van een bijzondere positie van de politie of is er geen principiële rol voor de politie weggelegd en is zij slechts één van de partijen die een rol en verantwoordelijkheid heeft in de nieuwe wereld, en met name in het cyberdomein? En als dat laatste zo is, hoe verhoudt de politie zich tot andere in dit domein acterende partijen? Daarbij is een relevante dimensie hoe de politie – als representant van de 'publieke zaak' in een in toenemende mate internationale context – zich verhoudt tot private partijen.

Niet voor niets heeft de korpsleiding van de politie de vraagt gesteld, hoe het zit met:

> **Het acteren van partijen in het cyberdomein in het licht van de waarden van de rechtsstaat en het leveren van maximale toegevoegde waarde aan veiligheid?**

Het lijkt op voorhand helder dat er een omvangrijke rol is weggelegd voor private partijen, maar ook voor onder andere de krijgsmacht en de inlichtingendiensten. Dat vraagt om een conceptueel kader op basis waarvan de nieuwe context kan worden geordend en dat de politie houvast biedt om te bepalen welke positie zij daarin kiest en op grond van welke overwegingen. Dat laatste betreft ten minste twee – aan de politiefunctie eigen – invalshoeken. Ten eerste, bescherming van de waarden van de rechtsstaat, die in het cyberdomein geen vanzelfsprekendheid zijn, en ten tweede, het leveren van maximale toegevoegde waarde aan veiligheid, onder andere door de bestrijding van cybercrime en cyber-enabled crime.

Als werkgroep reiken wij in dit advies een handvat aan dat we de 'rechtsstaatwaaier' hebben genoemd. Het is te zien als een hulpmiddel om te komen tot ordening en het duiden van samenhang in een complexe context die zich nog niet in al haar facetten laat doorgronden. Hoe kun je de wereld om je heen interpreteren en welke consequenties verbind je daaraan wat betreft je positionering ten opzichte van anderen? Het is een volgende stap in de bewustwording van de politieorganisatie, nodig om te kunnen vaststellen of – en met betrekking tot welke dimensies – deze voldoende bekwaam is om grip te krijgen op de uitdagingen van de nieuwe sociale werkelijkheid.

De rechtsstaatwaaier bieden we in eerste instantie aan aan de vraagsteller, de korpsleiding van de politie. Maar, we beseffen ons terdege dat de vraag nadrukkelijk gaat over het acteren van partij*en* en niet alleen over de politie zelf. Dat betekent dat we de rechtsstaatwaaier nadrukkelijk ook zien als een strategisch hulpmiddel voor de politieleiding om het gesprek aan te gaan met partners, publiek en privaat, over hoe zij zich tot elkaar verhouden en hoe zij gezamenlijk kijken naar de toekomst. In aanvulling daarop hebben we de conceptuele exercitie die uitmondt in de rechtstaatswaaier nadrukkelijk verbonden met de huidige en toekomstige praktijken. Positionering heeft in onze opvatting altijd betrekking op

theorie EN praktijk. Dat betekent dat we onze analyse laten uitmonden in een aantal aanbevelingen vanuit de werkgroep aan de politie.

Na het vinden en mogen committeren van teamleden (die ik zeer dankbaar ben) zijn we als werkgroep gestart met het verzamelen van literatuur, het schetsen van een eerste inzicht in de stand van zaken met betrekking tot dit onderwerp en het voeren van gesprekken met ingewijden uit de wereld van cyber en veiligheid. We startten met een veelheid aan vragen waaronder:

- Wie is er behalve de politie (al) met het onderwerp bezig, bestaan er strategische opvattingen?
- Hoe ziet het (overheids)beleid eruit?
- Wat zijn de meest relevante (internationale) ontwikkelingen?
- Hoe zijn bedrijven er mee aan de slag?

Het denken werd door de complexiteit een soort jojoën tussen inzoomen en uitzoomen, divergeren en convergeren, concretiseren en abstraheren.

Dat heen en weer bewegen komt ook tot uitdrukking in de tekst van dit advies, en ik realiseer me terdege dat we een groot beroep doen op de capaciteiten van de lezer. Maar, het is de moeite waard. Want, zoveel is ons wel duidelijk geworden: digitalisering – van *Big Data* en *Artificial Intelligence* tot gedragsbeïnvloeding in economie en democratie – vormen onze samenleving; in positieve en negatieve zin. En, de snelheid waarmee veranderingen zich voltrekken, is fenomenaal. Als het gebruik van nieuwe (digitale) technologieën botst met de kernwaarden van onze samenleving – en we ons daar onvoldoende rekenschap van geven en verzuimen daar tegen stelling te nemen – dan zullen ze vroeg of laat grote schade aanrichten. Als dat al niet gebeurt.

Dit advies biedt een kader voor positionering van de politie ten opzichte van andere partijen – en de burger – en geeft een bescheiden aanzet tot wat dat dan betekent voor de organisatie. Dit alles in het licht van een maatschappelijke ontwikkeling die zijn weerga niet kent en waarbij de waarden van de rechtsstaat niet op voorhand veilig zijn.

Bernard Welten

Warmond, 1 december 2019

Inhoudsopgave

Samenvatting

Digitalisering verandert de economie, democratie en samenleving op ingrijpende wijze. Er is sprake van een nieuwe werkelijkheid. Deze is diffuus en laat zich moeilijk duiden. Duidelijk is wel dat een veelheid aan instanties, publiek en privaat, zich intussen bezighoudt met de positieve en negatieve aspecten van die nieuwe werkelijkheid. Ook de politie staat voor de opgave hoe om te gaan met de veranderingen op het gebied van informatie- en communicatietechnologie en de maatschappelijke gevolgen daarvan. Korpschef Erik Akerboom heeft de vraag gesteld hoe het zit met het acteren van partijen in het cyberdomein in het licht van de waarden van de rechtsstaat en het leveren van maximale toegevoegde waarde aan veiligheid.

De vraag van de korpschef is in dit advies opgevat als een vraag naar duiding van de nieuwe werkelijkheid. Het antwoord dat dit rapport biedt is een strategisch hulpmiddel, een instrument dat aangeeft hoe de nieuwe werkelijkheid kan worden begrepen en welke consequenties daaraan kunnen worden verbonden voor de positionering van de politie ten opzichte van al die andere spelers die zich bezighouden met zaken als *cybersecurity, cybercrime, cyber-enabled crime* etc. Dat hulpmiddel is de 'rechtsstaatwaaier' die in hoofdstuk 4 wordt gepresenteerd. In de hoofdstukken die vooraf gaan, krijgt de lezer de achtergrondinformatie die aan de waaier ten grondslag ligt.

In het inleidende hoofdstuk van dit rapport wordt beschreven dat de nieuwe werkelijkheid niet los staat van de oude werkelijkheid. Er is geen apart, eigenstandig cyberdomein. Het cyberdomein is onlosmakelijk verbonden met het fysieke domein. Bestaande, klassieke denkbeelden over de samenleving (zoals plaats, grens, formele identiteit en rechtsorde) zijn echter sterk geworteld in het fysieke domein en het is onzeker of, en zo ja, in hoeverre dergelijke denkbeelden standhouden. Voor de politiefunctie is dat bijzonder van belang. De politiefunctie is immers afgeleid van de staat, die in essentie wordt gedefinieerd door het monopolie op het legitiem gebruik van geweld 'binnen een bepaald gebied', dús grondgebonden. Het zogeheten geweldsmonopolie is daarnaast verbonden met het denken in termen van het (denkbeeldig) sociaal contract. Het sociaal contract regelt de bescherming van burgers dóór, maar ook tégen de overheid, en heeft vorm en inhoud gekregen in het vruchtbare koppel democratie en rechtsstaat. Het is in die context dat de politie zich heeft verbonden aan de waarden van de rechtsstaat met haar missiestatement 'Waakzaam en dienstbaar staat de politie voor de waarden van de rechtsstaat'.

In hoofdstuk 1 wordt een schets gegeven van maatschappelijke ontwikkelingen die kunnen worden geschaard onder de noemer van digitalisering van de samenleving. Het gaat om technologische ontwikkelingen en hoe deze zijn vervlochten met brede maatschappelijke ontwikkelingen, in positieve en in negatieve zin. Aan de orde komen zaken als online en verbonden, disruptieve techniek, digitaal vertrouwen, Big Data en Artificial Intelligence; en ook hoe eerdere paradigmaverschuivingen samenhingen met revoluties in de ontwikkeling van de technologie en hoe dat samenlevingen dwingt tot aanpassing.

Hoofdstuk 2 volgt met een beschrijving van hoe de publieke veiligheidspartijen reageren op de nieuwe veiligheidsvraagstukken. Het laat zien dat er – zoals ook op andere terreinen – sprake is van een institutionele reflex: diffusie en een gevoel van urgentie maken dat heel veel partijen zich vol overgave storten op een nieuw fenomeen, in dit geval *cyber*. Achtereenvolgens wordt beschreven hoe de Nederlandse overheid reageert op de digitalisering van de samenleving, wat de uitkomst is van de institutionele reflex en hoe op regionaal en lokaal niveau invulling wordt gegeven aan de uitdagingen van digitalisering. Tot slot wordt betoogd dat succesvolle aanpassing aan de nieuwe werkelijkheid betekent dat er veranderingen plaatsvinden, terwijl de kernfunctie van de betreffende organisaties overeind blijft. Voor de politiefunctie is die essentie dat deze altijd betrekking heeft op mensen met onvervreemdbare rechten en dat daarmee is uitgesloten dat 'de mens' wordt opgeofferd voor veiligheid.

In hoofdstuk 3 wordt aangegeven wat onder de politiefunctie wordt verstaan en hoe deze zich verhoudt tot de andere, klassieke veiligheidsfuncties: de defensiefunctie, de inlichtingenfunctie en de private veiligheidsfunctie. In feite wordt daarmee de situatie beschreven van waaruit wordt vertrokken bij de waaier van hoofdstuk 4. Twee begrippen staan in dit hoofdstuk centraal: de eerder genoemde waarden van de rechtsstaat en het begrip toegevoegde waarde. In *Politie in ontwikkeling* uit 2005 heeft de politie, geconfronteerd met maatschappelijke fenomenen als grotere mobiliteit (van geld, goederen, informatie en mensen), ontgrenzing en anonimisering, weerstand geboden aan de reflex om vanwege toenemende complexiteit terug te vallen op kerntaken. In plaats daarvan werd het pad ingeslagen om toegevoegde waarde aan veiligheid ("doen wat het meeste oplevert") als leidraad voor positionering van de politie te nemen. Basis daarvoor is de unieke combinatie van kenmerken van de politie, kortweg: het geweldsmonopolie, vergaande bevoegdheden om te interveniëren en desnoods inbreuk te maken op grondrechten, de continue aanwezigheid in de frontlinie en daarop toegespitste professionaliteit, een daarmee samenhangende informatiepositie, en maatschappelijke verankering. Met die keuze uit 2005 werd wat de politie doet, afhankelijk van de context en daarmee onderwerp van gesprek met bevoegd gezag, partners, burgers en bedrijven. Randvoorwaarde daarbij is vanzelfsprekend dat de politie weet hoe die context eruit ziet. Dat laatste lijkt als gevolg van de toegenomen digitalisering van de samenleving in toenemende mate ingewikkeld: de nieuwe werkelijkheid is complex, diffuus, verandert razendsnel en lijkt de menselijke maat te overstijgen.

Om de nieuwe context te kunnen duiden, wordt in hoofdstuk 4 de rechtsstaatwaaier geïntroduceerd. In feite een nieuw wereldbeeld of maatschappijmodel, dat kan dienen als gids in de nieuwe werkelijkheid. Kenmerkend is dat het gaat om een meervoudige context: verschillende combinaties van karakteristieken zijn tegelijk waar: oud èn nieuw, fysiek èn digitaal, bekend èn onbekend, geregeld èn ongeregeld. De ingeklapte waaier staat voor de meervoudigheid; de uitgeklapte waaier laat zien dat er sprake is van vier onderling verbonden velden, die niet van elkaar zijn te scheiden, maar wel kunnen worden onderscheiden. Dit zijn (van links naar rechts) de *stationaire rechtsstaat*, de *reizende rechtsstaat*, de *geprivatiseerde rechtsstaat* en de *afwezige rechtsstaat*. In elk van de vier velden zijn de verhoudingen tussen de voornaamste instituties anders en verschillen de randvoorwaarden voor het uitvoeren van de politiefunctie. Onderkennen van de essentiële verschillen tussen de velden is de eerste stap naar het bepalen van hoe de politie en haar partners zich in de verschillende contexten zouden kunnen positioneren. Wat de waaier vooral laat zien is dat hoe verder naar rechts, hoe minder traditioneel de situatie is, beschouwd vanuit de politiefunctie, en hoe minder rechtsstatelijke waarborgen er zijn voor de burger. Naarmate we verder naar rechts gaan is er in afnemende mate sprake van een overheidsgezag dat uitkomsten kan afdwingen. Bewegen van links naar rechts door de velden van de waaier geeft gelijktijdig veranderingen te zien in de volgende dimensies:

- Hiërarchisch → Anarchisch
- Monopolistisch → Volledig Vrije Mededinging
- Publiek → Privaat
- Lokaliseerbaar → Plaatsloos
- Uniforme waarden → Pluriforme Gemeenschappen

Bij de stationaire rechtsstaat gaat het om de rechtsstaat in de klassieke betekenis. Hier geldt dat de democratische rechtsstaat een (rechts)gemeenschap veronderstelt. Er is een centrale rol ingeruimd voor de traditionele instituties en in het bijzonder voor de rechtsorde. De basis is een boven de partijen staande arbiter die uitkomsten kan afdwingen. In de stationaire rechtsstaat zijn de fundamenten van de politiefunctie duidelijk. Deze is afgeleid van het geweldsmonopolie van de staat.

In de reizende rechtsstaat is de staat nog altijd de centrale actor, nationaal en internationaal – maar hij heeft zich hier dus te verhouden tot andere staten, ook voor haar eigen interne processen en procedures. Omdat subjecten en fenomenen die staten willen reguleren steeds minder grondgebonden zijn, neemt het belang van internationale samenwerking en internationale normen en verdragen sterk toe. Staten kunnen andere soevereine staten niet 'dwingen' maar wel proberen te overtuigen, met meer of minder politieke druk of vormen van wisselgeld. Voor zover mogelijk wordt daarbij gebruik gemaakt van

het internationale recht. Waar er geen aanvaard wettelijk kader in enge zin is (zoals een rechtsstaat), vormen van de rechtsstaat afgeleide algemene beginselen – zoals het Europees Verdrag voor de Rechten van de Mens (EVRM) – veelal het uitgangspunt voor normering.

In de geprivatiseerde rechtsstaat is een veelheid aan actoren actief op het veiligheidsterrein en het gaat hierbij in toenemende mate om private partijen met een eigen verdienmodel. De dominante sociale processen vinden in toenemende mate plaats in een digitaal stromenland (netwerken) waarbij allerlei vooral ook private partijen een rol spelen. De afdwingbaarheid van gedrag bij partijen in netwerken is gering. Het ontbreekt aan een bovenliggende partij die anderen kan dwingen zich aan afspraken te houden, maar samenwerking is in principe mogelijk. In dit veld is de staat nog niet verworden tot louter 'één van de spelers' en heeft deze nog steeds een bijzondere positie maar is deze wel in toenemende mate 'in concurrentie' met andere, 'private instituties' zoals de op wereldschaal opererende grote technologiebedrijven. Dit type bedrijven kan niet eenvoudig door staten gereguleerd worden. Het zijn echter spelers die eigen 'wetten en regels' maken voor wat is toegestaan op hun platforms en er ontstaan als het ware nieuwe 'sociale contracten' waar nieuwe 'burgers' – nu consumenten – akkoord gaan met soms zeer vergaande voorwaarden ten aanzien van 'persoonsinformatie' in ruil voor diensten.

De afwezige rechtsstaat beschrijft de situatie zonder rechtsstaat en zonder 'aangewezen' hoeder van de waarden van de rechtsstaat. In dit veld staat de klassieke taakverdeling markt – staat – samenleving ter discussie. Zeer veel wordt door partijen zelf opgelost waarbij de klassieke staat niet op de voorgrond treedt. Maar als er iets gebeurt waartegen iemand zou moeten optreden, en wel nu, is niet altijd duidelijk wie aan zet is en op basis waarvan. De ervaren noodzaak opnieuw te begrenzen, noopt tot nadenken over nieuwe strategieën en nieuwe coalities. Noodgedwongen wordt in hoge mate gehandeld naar bevind van zaken.

In hoofdstuk 5 volgt een nadere beschrijving van de vier velden van de waaier en wordt geanalyseerd wat de betekenis is als het gaat om de positionering van de politie. Dat was immers de essentie van de vraag van de korpschef. Voor de politie zijn daarbij het staan voor de waarden van de rechtsstaat en het willen bieden van toegevoegde waarde met betrekking tot veiligheid steeds de richtinggevende principes. In het veld van de stationaire rechtsstaat zijn de verhoudingen relatief helder, maar desondanks niet altijd geheel vrij van kwesties. Er is een normenkader (de Nederlandse rechtsstaat) waarbinnen de politiefunctie gestalte krijgt, de voornaamste spelers zijn vooral publieke partijen, en er zijn instanties die zo nodig met drang en dwang kunnen ingrijpen in ongewenste situaties. Toch zorgt digitalisering ook in deze context voor uitdagingen. Waar de klassieke aanknopingspunten voor de opsporing van strafbare feiten, te weten locatie, omstandigheden, object, dader en slachtoffer (LOODS) vroeger in elkaars nabijheid lagen, kunnen deze nu verdeeld zijn over verschillende jurisdicties: een dader in land A verricht met behulp van infrastructuur (servers, netwerken) in land B en C handelingen die strafbaar zijn in B en C, maar niet in A, en maakt daarbij slachtoffers in land C, D en E. Dit eenvoudige voorbeeld laat zien dat een traditionele manieren van werken en organiseren onder druk staan. Bewegend van links naar rechts door de velden van de waaier neemt die druk toe. In het vierde veld, dat niet voor niets 'de afwezige rechtsstaat' heet, is er geen duidelijk aanwijsbare publieke partij die kan optreden tegen ongewenste situaties en is het zeer de vraag of private partijen met veelal commerciële belangen zich verantwoordelijk voelen om ongewenste situaties tegen te gaan of te (doen) beëindigen. Dat vraagt dan ook om een andere opstelling van de politie dan handhaving van de rechtsorde met de klassieke middelen. In deze context past het bijvoorbeeld meer om betrokken te partijen aan te spreken op hun eigen verantwoordelijkheid vanuit het perspectief dat de politie gericht is op bescherming van (potentiële) slachtoffers, vooral waar het de kwetsbaren in de samenleving betreft.

Op basis van de beschreven positionering van de politie in de meervoudige context worden in hoofdstuk 6 aanbevelingen gedaan hoe meer concreet vorm gegeven kan worden aan de rechtstatelijke politiefunctie in de gedigitaliseerde samenleving.

Inleiding: digitale transformatie

> *"Digitalisering verandert onze economie, onze democratie en onze samenleving op ingrijpende wijze. Het besef is het afgelopen anderhalf jaar ontstaan dat we met digitalisering voor een transitieopgave van formaat staan, met zowel positieve als negatieve aspecten. Ook het kabinet spreekt van een digitale transitie. Het Rathenau Instituut is blij dat er nu een nationale digitaliseringsstrategie ligt. Dat neemt niet weg dat er nog grote uitdagingen liggen voor de Nederlandse overheid, en bedrijfsleven, maatschappelijke organisaties en parlement" (Rathenau Instituut, 2018).*

De 'transitieopgave van formaat' en de 'grote uitdagingen' waarnaar in het citaat hierboven wordt verwezen, gelden uiteraard ook de politieorganisatie, als belangrijkste uitvoerder van de politiefunctie. Ook, of misschien wel juist, de politie – als uitvoeringsorganisatie midden in de samenleving – staat voor de opgave hoe om te gaan met de veranderingen op het gebied van informatie- en communicatietechnologie en de maatschappelijke gevolgen daarvan. Dit betreft zowel de positieve aspecten van digitalisering – zoals toegenomen mogelijkheden voor burgers waar het gaat om het organiseren van veiligheid – als de negatieve aspecten, zoals nieuwe (verschijnings-)vormen van criminaliteit.

Er is de nodige aandacht van de politie voor het bestrijden van de relatief nieuwe fenomenen als *cybercrime* – criminaliteit verbonden met digitale systemen – en *cybersecurity*: het beschermen van digitale systemen en de (digitale) infrastructuur tegen misbruik en/of ontwrichting. Ook tal van andere partijen zijn op dit zogeheten *cyberdomein* actief. Tegelijkertijd zijn inspanningen van de politie erop gericht om wat betreft de eigen organisatie (mensen, middelen, werkprocessen) gebruik te maken van de kansen die digitalisering biedt; of ten minste in de pas te blijven lopen met de snelle veranderingen in de samenleving. In de woorden van korpschef Akerboom:

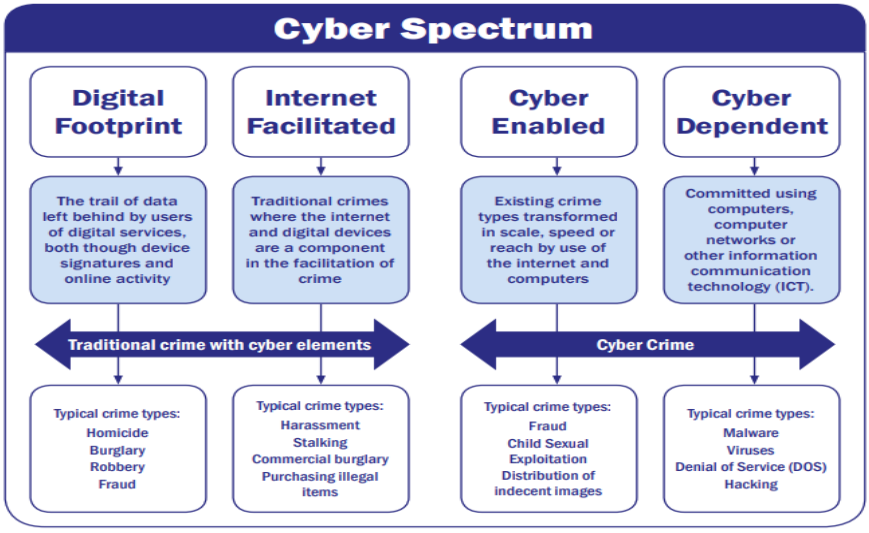
> *"De politie gaat naar een organisatie die permanent meebeweegt met huidige en toekomstige ontwikkelingen die over elkaar heen buitelen. Het korps, en dus ook onze mensen, dienen telkens opnieuw antwoord te geven op deze veiligheidsontwikkelingen. Onveiligheid verschuift naar onze cyberwereld. Polarisatie neemt toe. De internationale conflicten raken ons. Bovendien verandert de verhouding tussen mens en technologie ook in een digitale wereld. Als je de fysieke weg op gaat, zijn er allemaal regels. Maar op de digitale snelweg heerst de anarchie. Hoe stel je je daar als overheid tegenover op? De infrastructuur is voor 90% in handen van het bedrijfsleven; wat moet dan de rol van de overheid zijn? En die van de politie? Omdat de omgeving flexibeler wordt, minder voorspelbaar, moet je als collega ook in een minder voorspelbare omgeving uit de voeten kunnen" (2016).*

Het begrip 'transitieopgave' of 'digitale transformatie' (Derksen, 2019) geeft al aan dat er meer aan de hand is dan meebewegen met maatschappelijke veranderingen. De snelheid, complexiteit, grenzenloosheid en wijdverbreide impact van het digitaliseringsproces wijzen erop dat dit proces te zien is als de grondslag voor een 'paradigmaverschuiving, vergelijkbaar met die van de industriële revolutie of de uitvinding van de boekdrukkunst' (Onderwijsraad, 2017: 10). Dat maakt dat het redeneren vanuit bestaande theorieën en 'grondgebonden' concepten ontleend aan de oude, louter fysieke wereld mogelijk tekortschiet: de ordeningsprincipes uit de oude wereld zijn wellicht niet meer adequaat. Traditionele concepten kunnen helpen maar zijn tegelijkertijd nooit vanzelfsprekend: wat betekent 'surveilleren op het internet', het 'geweldsmonopolie in cyberspace', de 'digitale wijkagent' of het inrichten van een speciale 'online politiemacht' (The Telegraph 2019) – en wat is de wenselijkheid daarvan?

Soms lijkt men al te gemakkelijk bestaande concepten te hanteren in een nieuwe context. Daarbij is de impliciete veronderstelling dat cyberspace (het virtuele domein) als apart domein kan worden beschouwd, terwijl kenmerkend voor de gedigitaliseerde samenleving is dat cyberspace en de fysieke wereld sterk met elkaar zijn verweven. Er is geen 'virtuele wereld' naast een 'echte' wereld: "De virtuele

wereld bestaat niet"[1]. We hebben te maken met een nieuwe, nogal andere sociale werkelijkheid waarin we moeten onderzoeken of bestaande theorieën – ontwikkeld in een wereld gekarakteriseerd door een andere 'stand der techniek' – standhouden in een gedigitaliseerde samenleving (Van Erp et al. 2013, 327). Dat betreft meer dan alleen criminaliteit en criminaliteitsbestrijding, maar we leggen op dit aspect van politiewerk voorlopig de nadruk om de impact van digitalisering inzichtelijk te maken.

In het zich ontwikkelende denken over de relatie tussen cyber en criminaliteit wordt de verwevenheid fysiek-digitaal wel degelijk onderkend. Onderstaand schema geeft een beeld van verschillende vormen van onveiligheid en – meer specifiek – verschillende vormen van criminaliteit waarbij het aan de linkerkant gaat om traditionele misdaad met digitale componenten en aan de rechterkant om misdaad die mogelijk wordt gemaakt door het bestaan van digitale systemen of daarvan afhankelijk is.



Figuur 1. Het cyberspectrum (Lincolnshire Police 2018, p.2)

De vraag of bestaande, klassieke denkbeelden (zoals plaats, grens, formele identiteit en rechtsorde) standhouden in een gedigitaliseerde samenleving is bijzonder relevant met betrekking tot de politiefunctie. De politiefunctie is immers afgeleid van de staat, die in essentie wordt gedefinieerd door het monopolie op het legitiem gebruik van geweld *'binnen een bepaald gebied'* (Weber 1917/2012). Dat maakt dat de politiefunctie en het geweldsmonopolie sterk verbonden zijn met territoir (grondgebied). Het geweldsmonopolie is daarnaast verbonden met het denken in termen van het (denkbeeldig) sociaal contract: mensen leven niet langer in een 'natuurstaat' zonder beperkingen, maar zij hebben sommige individuele vrijheidsrechten (waaronder het recht op eigenrichting) overgedragen aan een soeverein. In termen van Thomas Hobbes (1651/2010) gaat het hier over de bijna almachtige *Leviathan* die zorgdraagt voor de veiligheid van de burgers die zich hebben onderworpen aan zijn gezag. Gaandeweg heeft zich een model ontwikkeld waarbij deze hoogste macht wordt gecontroleerd – door een volksvertegenwoordiging – en wordt gereguleerd door de wet. Het sociaal contract regelt daarmee bescherming van burgers door, maar ook tegen de overheid en heeft vorm en inhoud gekregen in het vruchtbare koppel democratie en rechtsstaat. Het is in die context dat de politie zich heeft verbonden aan de waarden van die rechtsstaat met haar missiestatement 'Waakzaam en dienstbaar staat de politie voor de waarden van de rechtsstaat' (PIO 2005).

De vraag is welke betekenis hieraan verbonden wordt in de gedigitaliseerde samenleving. Want, het geweldsmonopolie heeft vooral een sterk ordenende werking in de 'grondgebonden' functies van de

[1] Heikelien, 20 maart 2011.

politie ('binnen een bepaald gebied') en er is reden om de ordenende werking van het monopolie op legitiem gebruik van geweld te koesteren[2]. Maar, het geweldsmonopolie geeft op het eerste gezicht minder richting voor ontwikkelingen die zich in toenemende mate onttrekken aan het idee van het territoir als integratiekader met de bijbehorende klassieke eenheid van plaats, tijd en handeling. Dat geldt zeker voor digitalisering en de daarmee verbonden verandering van de sociale ruimte. Daarbij komt dat de verhouding tussen de klassieke grondgebonden staat en wereldwijde private (technologie) bedrijven nog niet is uitgekristalliseerd. Dat geldt ook voor de sociale en institutionele gevolgen van tal van specifieke technologische ontwikkelingen die onder de noemer 'digitalisering' vallen – *Big Data, Artificial Intelligence, Internet of Things*, enzovoort.

Een andere sociale werkelijkheid, waarin de fysieke wereld en cyberspace innig met elkaar zijn verweven, en een politiefunctie die afgeleid is van de staat, welke laatste in essentie wordt gedefinieerd door het monopolie op het legitiem gebruik van geweld, maken dat *juist* de politie zich in een aantal opzichten 'opnieuw moet uitvinden'. Vragen die daarbij een rol spelen zijn:

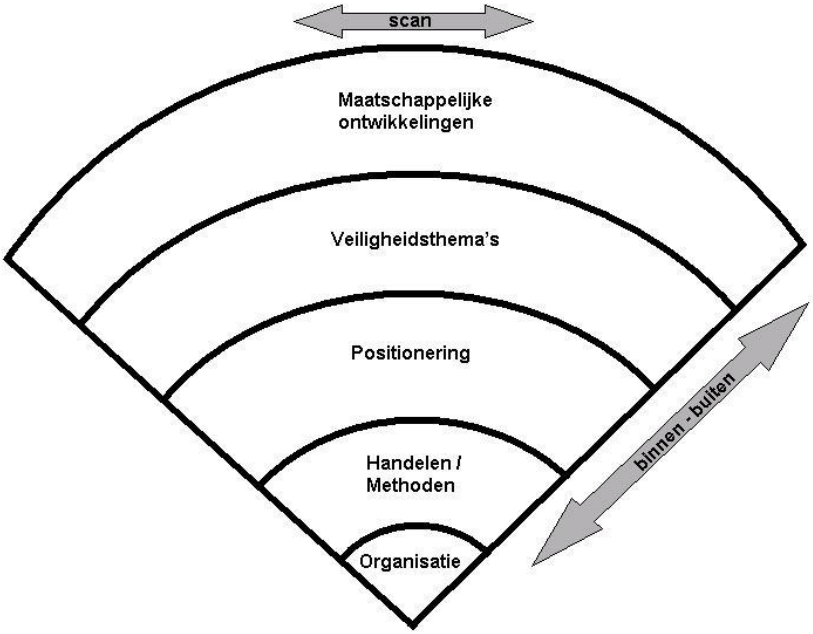
1. Hoe kijkt de politie aan tegen de gedigitaliseerde samenleving?
2. Welke functie ziet de politie voor zichzelf in de gedigitaliseerde samenleving?
3. Op grond van welke overwegingen komt zij tot deze opvatting?
4. Hoe ziet de politie haar positie ten opzichte van andere spelers op het veld?

Dit zijn 'grote vragen' die het risico in zich dragen dat bij de beantwoording daarvan de 'hele wereld wordt' meegenomen: alles hangt met alles samen, en de wijze waarop verandert voortdurend. Om focus aan te brengen zonder tunnelvisie maken we gebruik van het RADAR-model (Van Dijk, Hoogewoning en Welten 2011; Van Dijk en Hoogewoning 2014). Het RADAR-model is ontwikkeld als een hulpmiddel om te bepalen wat de betekenis is van grote maatschappelijke ontwikkelingen voor veiligheid en welke consequenties de politie daaraan zou moeten verbinden. Vijf vragen stonden daarbij centraal:

1. Welke, voor de politie relevante, ontwikkelingen doen zich voor in de samenleving?
2. Tot welke vraagstukken op het gebied van veiligheid leiden deze ontwikkelingen?
3. Wie zijn er aan zet om deze problemen, samen met de politie, aan te pakken?
4. Welke methoden/strategieën/instrumenten worden daarbij ingezet, door de politie en door anderen?
5. Wat betekent dit voor de organisatie van de politie?

De vijf vragen liggen ten grondslag aan de structuur van de RADAR, die is opgebouwd uit de lagen *maatschappelijke ontwikkelingen*, *veiligheidsthema's*, *positionering*, *handelen / methoden* en *organisatie*. Deze vormen onderdeel van een model dat erop is gericht dat de verschillende lagen in samenhang met elkaar worden bezien: wat er in de ene laag gebeurt, heeft consequenties voor de andere lagen. In die optiek is het ontwikkelen van strategische visies ('vergezichten') alleen zinvol als duidelijk wordt dat hieraan consequenties worden verbonden voor de politie op het gebied van positionering, handelen en organisatie. De RADAR is weergegeven in figuur 2.

[2] Advies geweldsmonopolie (november 2018, p.19): '[…] de aan strikte voorwaarden gebonden institutionalisering van fysiek geweld lijkt een minimumvereiste – een onbetwistbaar fundament – waarop iedere volgende denkbare ontwikkeling is gebouwd (Punch 2010 & 2012; Jackson 2013)'.



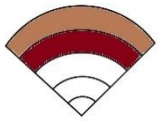
Figuur 2: Het raamwerk van de RADAR (Van Dijk et al. 2011, 2014)

We gebruiken dit raamwerk om de denklijn tussen – en waar dienstig binnen – de hoofdstukken te ordenen. De opbouw is als volgt.

Hoofdstuk 1 gaat in op enkele aspecten van de gedigitaliseerde samenleving: wat zien we gebeuren op het gebied van technologische ontwikkeling en op welke wijze is dat vervlochten met brede maatschappelijke ontwikkelingen (laag 1 van de RADAR). Tegelijkertijd geven we een eerste beeld van de aard van de veiligheidsthema's (laag 2). In hoofdstuk 2 kijken we naar op welke wijze de publieke veiligheidspartijen reageren op de nieuwe veiligheidsvraagstukken (laag 3). Hoofdstuk 3 zoomt in op de politiefunctie, die berust op twee pijlers die bepalend zijn voor de positionering (laag 3): de waarden van de rechtsstaat en het leveren van toegevoegde waarde aan sociale veiligheid. De beschrijvingen en analyses uit de voorgaande hoofdstukken monden in hoofdstuk 4 uit in een nieuw 'wereldbeeld' vanuit het perspectief van de politiefunctie (laag 1 en 2): de rechtsstaatwaaier. Dat is niet eenvoudig; sterker nog, het gaat om een meervoudige context. Het nieuwe wereldbeeld beslaat vier vlakken: vier contexten die niet van elkaar zijn te scheiden, maar wel kunnen worden onderscheiden op een aantal wezenlijke dimensies. In hoofdstuk 5 gebruiken we de rechtsstaatwaaier om de nieuwe positionering van de politie (laag 3) te beschrijven en waar mogelijk iets te zeggen over wat die betekent voor het handelen van de politie en belangrijke aspecten van haar organisatie (laag 4 en 5) [3]. In hoofdstuk 6 worden de aanbevelingen gepresenteerd.

[3] Hier lezen we van 'buiten naar binnen'; andersom kan ook. De essentie is dat de verschillende lagen in onderlinge samenhang worden bezien.

1. Digitale revolutie en de rechtsstaat

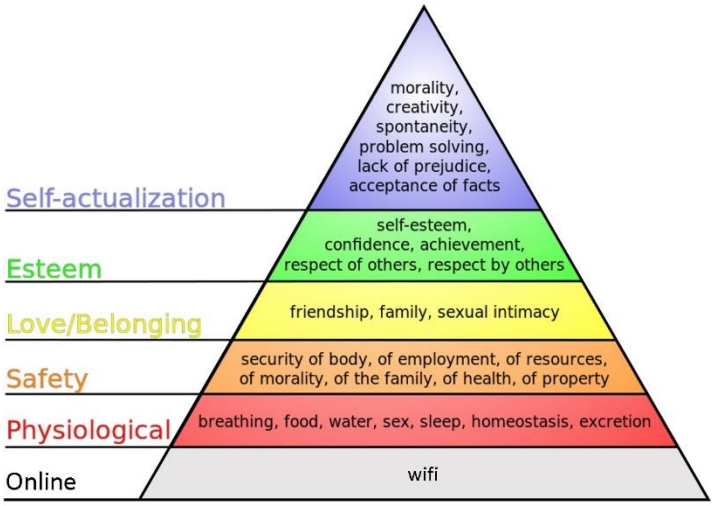


In dit hoofdstuk beschrijven we een aantal technologische ontwikkelingen die worden gezien als onderdeel van de digitalisering van de samenleving. Tegelijkertijd geven we een doorkijkje naar de betekenis van die ontwikkelingen voor de politie of ten minste de vragen en dilemma's die deze oproepen. Dit is geen uitputtend overzicht van wat er speelt op het gebied van digitalisering noch van de zon- en schaduwkanten die daarmee verbonden zijn. Het is evenmin een doorwrochte analyse van verschillende technologieën. Onze ambitie met dit hoofdstuk is bescheiden: bij wijze van introductie geven we een ruwe schets van waaraan men kan denken bij digitalisering van de samenleving.

1.1 Online en verbonden

Zo'n dertig jaar geleden kon voor het eerst buitenshuis worden getelefoneerd met een mobiele telefoon[4], terwijl men tegenwoordig met de doorontwikkelde variant, de smartphone, een scala van activiteiten kan uitvoeren: bekijken van het laatste nieuws, de weersverwachting, de stand op beurs, bankzaken verrichten en communiceren via een veelheid aan sociale media. Burgers hebben een steeds omvangrijker 'digitaal aura' om zich heen: allerlei sensoren meten en leggen veelsoortige privacygevoelige data vast, bijvoorbeeld met smartwatches en smartphones. Ook worden in de publieke ruimte door overheden, burgers en commerciële partijen steeds meer data vastgelegd.

Voor ieder vraagstuk is er tegenwoordig wel een app. En, bijna van de ene op de andere dag vinden velen het gemak van digitalisering de gewoonste zaak van de wereld. Met een knipoog kunnen we stellen dat het lijkt alsof er een nieuwe onderkant is toegevoegd aan de Piramide van Maslow. Voedsel, kleding en onderdak zijn weliswaar vitaal, maar er is een dimensie bijgekomen: we moeten online zijn. Wifi als de hedendaagse, eerste levensbehoefte.



Figuur 3. De Piramide van Maslow herzien
(Naar: J. Finkelstein - https://en.wikipedia.org/wiki/File:Maslow%27s_hierarchy_of_needs.svg, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=79015890)

[4] De autotelefoon kwam in 1986, de draadloze telefoon 'Kermit' in 1992, de eerste GSM in 1994.

Die individuele menselijke afhankelijkheid van '*being connected*' staat niet op zichzelf. Het geldt evenzo voor de samenleving als geheel en de afhankelijkheid van de fysieke, en vooral digitale infrastructuur. Als het noodnummer 112 enige tijd niet bereikbaar is (zoals op 24 juni 2019), wordt duidelijk hoe afhankelijk, en daarmee kwetsbaar, de samenleving is geworden. Ook het politieapparaat is anno 2020 gebouwd op apps en andere digitale toepassingen, die het handelingsvermogen versterken maar ook een nieuwe zwakte introduceren: de afhankelijkheid van de gebruikte technologie. Dit geldt evenzeer voor de luchtverkeersleiding, het betalingsverkeer, ProRail of een van de grote Medische Centra. Als deze offline raken is de chaos niet te overzien.

In de publieke ruimte worden door (gemeentelijke) overheden, commerciële partijen en burgers steeds meer data vastgelegd. Burgers stellen blijkbaar veel vertrouwen in commerciële bedrijven, of vinden althans mogelijke inbreuken op hun privacy ondergeschikt aan het gemak dat wordt geboden. Gevolg is bijvoorbeeld dat burgers op basis van geanalyseerde gegevens aangeboden krijgen wat bij hun geconstrueerde profiel past, vaak zonder dat de burger dit zelf in de gaten heeft: de zogeheten *filter bubble*. Als de verzamelde gegevens gecombineerd worden, kan iemands leven steeds vollediger in kaart worden gebracht en komt de door George Orwell geschetste situatie van "*Big Brother is watching you"* steeds dichterbij.

Data zijn het in economische zin het nieuwe goud, en als de bezitters/eigenaars van die data zich niet gebonden voelen aan publieke waarden, raakt de overheid (en dus ook de politie) uit positie om nog te kunnen staan voor de waarden van de rechtsstaat. Een enkele klik om te bevestigen dat men akkoord is met de inhoud van een honderd pagina's tellende "gebruiksvoorwaarden"-overeenkomst (wat tegenwoordig het geval is voor veel informatieplatforms) is helaas ontoereikend.

De grote vraag is wat burgers van de overheid en de politie verwachten en hoe zich dit verhoudt tot hun privacy. Het idee van een politie die al het gedrag in kaart brengt en misschien wel preventief handelt, is geen scenario waar iedere burger enthousiast van wordt. Wanneer deze data echter worden gebruikt om terroristische aanslagen te voorkomen, vergeven burgers de overheid vaak deze schendingen van hun privacy.

1.2 Kansen en bedreigingen

Nederland beschikt over een uitstekende uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren en zet daar ook vol op in. Maar de keerzijde is dat tegelijkertijd kwetsbaarheden en dreigingen in het digitale domein toenemen (NCSA 2018:7). In het boek *Future Crimes* uit 2016 schetst Marc Goodman een naargeestig beeld van wat de samenleving te wachten staat of inmiddels ook overkomt (Hijink 2015, Welten 2016). Cybercrime is een businessmodel geworden voor criminelen, als gevolg waarvan het bedrijfsleven jaarlijks voor miljarden euro's schade lijdt (Van Wieren 2019).

In 2018 ligt het cijfer van 'traditionele' zichtbare criminaliteit uitgedrukt in het aantal geregistreerde misdrijven ruim 20 procent lager dan in 2014. Dat lijkt een positieve ontwikkeling, maar 'harde' politiecijfers zeggen niet alles. De laatste jaren is een duidelijke verschuiving naar 'onzichtbare' criminaliteit, zoals ondermijning en gedigitaliseerde criminaliteit. Dat is criminaliteit waar mensen vaak geen aangifte van doen, maar die wel degelijk een maatschappelijk probleem vormt[5].

Slachtofferenquêtes geven een ander beeld dan de aangiftecijfers. Van alle Nederlandse internetgebruikers van 12 jaar en ouder zegt 8,5 procent in 2018 slachtoffer te zijn geweest van een vorm van digitale criminaliteit. Dat komt neer op ruim 1,2 miljoen mensen (Koenis 2019). In een tv-uitzending van Nieuwsuur (juni 2016) spreekt ook de voorzitter van het College van procureurs-generaal, Gerrit van

[5] https://www.politie.nl/nieuws/2019/januari/17/misdaadcijfers-2018-verder-gedaald.html

der Burg, zich uit over de verwachte groei van cybercrime en stelt dat in 2021 de helft van alle criminaliteit te maken heeft met computers. Daarbij gaat het om uiteenlopende vormen: computervirussen, *malware, ransomware, phishing*, cyberaanvallen met *botnets, cryptojacking*, pinpasfraude, helpdeskfraude, identiteitsfraude, bedreiging, DDoS-aanvallen, *hacking*, internetoplichting, kindermisbruikmateriaal, terrorisme etc.[6]. Daarnaast maken criminelen in toenemende mate zelf gebruik van de mogelijkheden die de digitale wereld biedt om zich in anonimiteit aan elkaar te verbinden en zich te beschermen tegen bijvoorbeeld de politie (Van de Sandt 2019).

Daders zijn niet alleen individuen of groepen. In het in 2019 verschenen boek van Huib Modderkolk (*Het is oorlog maar niemand die het ziet*) wordt nog eens pijnlijk duidelijk dat ook statelijke actoren zich richten op digitale economische en politieke spionage of zelfs digitale sabotage. De inlichtingendiensten hebben daarvoor in hun rapportages al herhaaldelijk aandacht gevraagd. Het aantal landen dat digitale aanvalscapaciteiten ontwikkelt neemt toe, terwijl de ingezette aanvallen steeds complexer worden. Criminele werkwijzen blijven zich in een hoog tempo ontwikkelen. Naast individuele (burger)slachtoffers is er dus ook sprake van een directe dreiging voor economische belangen en de nationale veiligheid (NCSA 2018:7).

1.3 Disruptieve techniek

Een belangrijke basis van digitalisering is de exponentiële ontwikkeling van steeds snellere rekenkracht, steeds grotere opslagruimte en steeds complexere chips. De zogeheten Wet van Moore – computerkracht verdubbelt elke twee jaar – is in 1965 bedacht door een medewerker van chipbedrijf Intel en blijkt tot de dag van vandaag te gelden. Op dit moment is een grote wedloop gaande om quantumcomputers te ontwikkelen. Deze hebben de potentie om bepaalde typen berekeningen veel sneller uit te kunnen voeren dan traditionele computers en zelfs sneller dan de supercomputers die vandaag de dag in gebruik zijn. Een voor de hand liggende toepassing is decryptie, wat voor de politie enerzijds kansen biedt om verouderde encryptie te ontsleutelen maar anderzijds opsporing kan bemoeilijken omdat de beveiliging van politiegegevens makkelijker te doorbreken is.

Parallel hieraan zien we de ontwikkeling van het *Internet of Things* (IoT) en sensoren. De tijd dat alleen levende wezens met elkaar communiceerden is voorbij. Steeds meer objecten bevatten kleine computers die met elkaar verbonden zijn via het internet en bevatten sensoren om de wereld om zich heen te meten. De politie maakt ook steeds meer gebruik van slimme sensoren, zo worden politieagenten uitgerust met *bodycams* en worden in de publieke ruimte sensoren geplaatst. Deze worden bijvoorbeeld gebruikt voor *crowd control* en het (preventief) handelen bij een incident. Een keerzijde van deze ontwikkeling is dat niet altijd duidelijk is wat er met de vergaarde gegevens gebeurt, of en hoe lang ze bewaard worden en of deze voldoende beveiligd zijn tegen ongewenst gebruik of tegen bewuste pogingen van anderen om deze gegevens illegaal te verwerven of te manipuleren (inbreken in systemen).

Wat deze technologieën disruptief maakt, is vaak de combinatie met redeneren vanuit overvloed, in plaats van redeneren vanuit schaarste. Elke burger is in potentie een hotelhouder doordat apps het mogelijk maken om de eigen woning te verhuren aan toeristen van over de hele wereld. Voor een klassiek taxibedrijf zijn de auto's en de chauffeurs schaarse productiemiddelen. Met de apps, sensoren en AI van vervoers-apps zijn alle automobilisten potentieel een taxi. Een klassiek beveiligingsbedrijf investeert in bewakers en camera's. Maar met de smartphones van burgers is iedereen op straat een potentiële sensor en medebewaker. Voor een adviesbureau is de kennis en ervaring van de adviseurs een schaars goed. Maar sommige bedrijven maken door het bieden van (digitale) ontmoetingsplaatsen van iedere ZZP-er een potentiële adviseur in hun netwerk. Door zo te redeneren vanuit overvloed in plaats vanuit schaarste ontstaan "platformbedrijven" die enorm snel kunnen opschalen in omvang en impact. Dergelijke platformenbedrijven zijn, mede door de snel toenemende digitalisering van de samenleving, het dominante businessmodel geworden.

[6] https://veiliginternetten.nl/themes/situatie/welke-vormen-van-cybercrime-zijn-er/

Tegelijk kleven hieraan allerlei risico's en bezwaren. Hoe verhoudt het woningtoerisme zich tot het gemeentelijke bestemmingsplan? Zijn de taxichauffeurs wel bekwaam? Wie let er nog op de arbeidstijdenwet? Hoe zit het met de privacy van burgers? De kwaliteit van het geleverde advies? En waar de platformen disruptief zijn in de bovenwereld, zijn ze dat te meer in het criminele circuit: iedere burger kan drugs verhandelen, een DDoS-aanval plegen, kindermisbruikmateriaal wereldwijd distribueren. Als ook criminelen redeneren vanuit overvloed, heeft dit enorme opschalingseffecten. En een vergunningstelsel of andere traditionele manier van reguleren werkt niet in het criminele circuit.

1.4 Digitaal vertrouwen

Technologische ontwikkeling heeft gevolgen voor basale sociale begrippen, waaronder vertrouwen. Zelfs het klassieke adagium 'Eerst zien, dan geloven' staat onder druk door de mogelijkheid zogenoemde '*deep fakes'* te genereren. Dit zijn afbeeldingen of video's van mensen die door de computer zijn gegenereerd, maar niet echt bestaan of onherkenbaar zijn gemanipuleerd. Omdat deze nauwelijks van echt te onderscheiden zijn, is het voor burgers moeilijk te duiden of er sprake is van nepnieuws. Een *fake* bericht op internet kan hierdoor grote onrust of schade veroorzaken en burgers kunnen zelfs aangesproken worden op basis van levensechte beelden waarin hun gelijkenis te zien is, zonder dat zij betrokken waren bij het maken daarvan. Daarbij wordt het voor de politie en uiteindelijk de rechter heel lastig om digitaal bewijs op waarde te schatten.

Elkaar vertrouwen in de anonimiteit van het internet is zowel voor burgers als overheden lastig. Hoe weet je dat je contact hebt met de legitieme website die je dacht te bezoeken? Het 'groene slotje' in de adresbalk zegt niet alles. En hoe weet de website dat er niet iemand anders achter de knoppen zit, of dat inloggegevens niet zijn gestolen? De opkomst van biometrische sensoren maakt het mogelijk om naast authenticatie met codes ook authenticatie te koppelen aan biometrische gegevens. Bijvoorbeeld met vingerafdrukscanners, gezichtsherkenning of stemherkenning. De technologie is echter nog lang niet waterdicht en mensen zullen altijd op zoek gaan naar het omzeilen van dergelijke systemen als ze hun identiteit willen verbergen. Maar ook privacy-bewuste burgers zijn bevreesd voor systemen waar klassieke persoonsgegevens worden gekoppeld aan biometrische data. De impact van identiteitsdiefstal of het lekken van gegevens is dan immers gigantisch groot.

Een andere technologische ontwikkeling die wordt ingezet om elkaar en elkaars transacties te vertrouwen is de blockchain-technologie. Blockchain maakt het door een gedistribueerd netwerk mogelijk om gezamenlijk elkaars transacties goed te keuren, in plaats van dat dit door een centrale autoriteit gebeurt. De bekendste toepassing van de blockchain-technologie is in cryptovaluta. De blockchain kan in theorie op veel meer gebieden en in kleinere netwerken worden toegepast, wat frauderen met transacties moeilijk maakt. Tegelijkertijd kan het ook worden gebruikt om een schaduweconomie te creëren waarbij de overheid buitenspel staat.

Voor overheidsorganisaties heeft dit een grote impact. Burgers zullen tot op zekere hoogte bescherming nodig hebben van een overheid die begrenst. Maar voor de overheid zal het steeds lastiger worden hier de juiste balans in te vinden: tussen economische vooruitgang en beperking van invloed van technologiebedrijven, tussen privacybescherming en veiligheid, tussen toezicht houden en zelf profiteren van technologie.

De Rijksdienst voor het Wegverkeer (RDW) bijvoorbeeld, van oorsprong gericht op het fysieke rijgedrag van voertuigen, is een rap tempo een hightech organisatie aan het worden. Een '*type approval*' voor een Tesla gaat inmiddels over miljoenen regels code en complexe zelflerende algoritmen. De idee dat zulke programmatuur afdoende te evalueren is, is achterhaald. De situatie valt te vergelijken met het maken van een MRI-scan van de hersenen: hieruit kan vrijwel niets worden afgeleid van de intenties of het gedrag van de persoon in kwestie. Hoe kun je het gedrag van een auto nog voorspellen? Zeker als

die auto's ook nog gaan interacteren met elkaar, en met stoplichten? En hoe veilig is die auto tegen cyberaanvallen, of zelfs maar voor digitale storingen? Is dat ook de taak van de RDW? Dezelfde dilemma's zijn zichtbaar bijvoorbeeld op de financiële markten of in de medische sector.

Overigens is ook bij de 'tegenpartij' van de politie, de criminele wereld, vertrouwen een heet hangijzer, zeker in de digitale wereld. Waar enerzijds maximale afscherming de boventoon voert, zal men anderzijds toch tot een onderling vertrouwen moeten komen om 'zaken' met elkaar te kunnen doen. Hierdoor ontstaat een systeem van crimineel reputatiemanagement, gestut op digitale dienstverleners die als tussenpersoon fungeren en zorg dragen voor bijvoorbeeld een onderpand. Interventies door de politie kunnen dit vertrouwen ondermijnen. Digitaal vertrouwen is voor de politie dus niet alleen een uitdaging maar tevens een nieuw aangrijpingspunt bij het uitvoeren van de functie. Dit 'dubbele perspectief' geldt voor alle technologische ontwikkelingen en hun consequenties.

1.5 Big Data en Artificial Intelligence

De partij, commercieel of overheid, die beschikt over grote hoeveelheden data en deze kan inzetten voor zijn doelen, heeft goud in handen. Dit is in het bijzonder voor een rechtstatelijke overheid niet zo eenvoudig als het lijkt. Er wordt niet voor niets gesproken over 'Big Data'. Het gaat over zeer grote hoeveelheden gestructureerde en ongestructureerde gegevens met een zeer grote kans dat verschillende dataregimes en wettelijke kaders door elkaar lopen. Om waarde te kunnen halen uit 'big data' moet deze worden geanalyseerd. Voor het analyseren van data en het zoeken naar patronen of juist anomalieën met behulp van geavanceerde algoritmen (*datamining*) wordt in toenemende mate gebruik gemaakt van zelflerende systemen, waarbij de rol van de mens naar de achtergrond wordt gedrongen of geheel verdwijnt. De daar gebruikte technologie van Kunstmatige Intelligentie of *Artificial Intelligence* (AI) is niet één technologie, maar is beter te begrijpen als een 'cybernetisch systeem' dat waarneemt, analyseert (denkt) en handelt, en daarvan kan 'leren' (Rathenau 2019). Artificial Intelligence kent vele toepassingen, van chatbots tot navigatiesystemen en van spraakherkenning tot gezichtsherkenning. In het politiedomein kent AI verschillende toepassingen, bijvoorbeeld om te komen tot betere afhandeling van meldingen of het selecteren van kansrijke *cold cases* (SAAI 2019: 16).Een spanningsveld dat zich aandient met de inzet van AI is hoe de uitkomsten zich verhouden tot de uitkomsten die het resultaat zijn van menselijke waarneming – analyse – handelen – leren, met inbegrip van de juridische kaders en het besef van risico's en randvoorwaarden. Wie 'gidst' het cybernetische systeem en hoe wordt de uitkomst getoetst?

Door de complexiteit van AI wordt het voor overheden en burgers steeds moeilijker te begrijpen wat er onder de motorkap gebeurt en welk algoritme tot een bepaalde uitkomst heeft geleid. Zeker voor de overheid is transparantie en herleidbaarheid van groot belang. Het kan immers niet zo zijn dat de computer onschuldige burgers gaat beschuldigen en op grond hiervan de politie dwangmiddelen in gaat zetten, terwijl onduidelijk is waarom. Algoritmes zijn immers zo goed als de data waarmee ze zijn getraind. Zit in deze data een bias, dan kan het bijvoorbeeld zomaar zijn dat de overheid een racistisch algoritme toepast, zonder dat ze het zelf doorheeft. Daarbij zijn mensen ook bezorgd dat hun vrijheid ernstig ingeperkt raakt doordat data uit het verleden tot in lengte van dagen bepalen hoe ze vandaag worden gezien. Menselijke verificatie en tegenspraak lijken dus juist in deze situaties aangewezen.

In bredere zin zal de politie steeds pregnanter geconfronteerd worden met de ethische vraagstukken die de gegevenscomplexiteit oplevert. Neem de toepassing van AI binnen de politie. Bijvoorbeeld wanneer AI wordt ingezet om criminaliteit te voorspellen (het zogenaamde *predictive policing*) en/of resources efficiënter en effectiever in te zetten. Vooral wanneer er op basis van data uit het verleden risicoinschattingen worden gedaan over toekomstig gedrag van individuen, lijkt terughoudendheid geboden. Burgers hebben immers (nog) geen wet overtreden. Maar wat als de politie op basis van de toepassing van statistische modellen met bovengemiddelde zekerheid slachtofferschap kan zien aankomen? Kan zij zich dan ook permitteren om terughoudend te zijn?

Ongewenste selectie en uitsluiting doet zich tevens voor bij toepassing van AI bij commerciële partijen. Als een bepaald algoritme bij een verzekeringsmaatschappij een inschatting maakt van iemands mogelijke schades, kan het zomaar zo zijn dat bepaalde klanten geen verzekering kunnen afsluiten, omdat ze voldoen aan een bepaald profiel. Toepassing van AI – in het bijzonder voor cybersecurity, politie en defensie – vraagt dus om meer aandacht voor ethische aspecten en proportionaliteit (SAAI 2019: 15).

De combinatie van AI, IoT en sensoren heeft impact op de maatschappij en daarmee ook op de politie. De zelfrijdende auto is nabij en dit betekent dat er geen mens meer aan te pas komt als een auto schade rijdt. Maar wie is dan aansprakelijk? Met auto's is dit nog redelijk herleidbaar, maar wat geldt er voor zelfstandig vliegende drones of gehackte devices? Of als er een softwarefout in een device zit wat leidt tot grote schades of bedreigingen voor de openbare orde?

Big Data kunnen, of misschien zijn ze dat al, een bedreiging vormen voor de democratie. In maart 2018 raakte Facebook verzeild in een groot schandaal omdat bleek dat gegevens van meer dan 50 miljoen Facebook gebruikers waren gebruikt om politieke advertenties op hen los te laten die gebruik maakten van de 'gemeten' persoonlijkheid van de gebruikers. Het doel was om grote politieke stemmingen te beïnvloeden (Kaiser 2019; Wylie 2019). Heeft Trump zijn presidentschap hieraan te danken?[7].

Technologie, en zeker digitale technologie, brengt zowel kansen als bedreigingen met zich mee. Opbrengsten en risico's van technologische toepassingen dienen telkens tegen elkaar te worden afgewogen (Akerboom 2017). Daarbij speelt mee wat de inzet van de technologie is. Zo is er techniek die erop gericht lijkt de mens te vervangen, maar die ook kan worden ingezet om de mens te ondersteunen. Er is techniek die de veiligheid van burgers beoogt te vergroten door het afschermen van internetverkeer, maar die kan ook worden ingezet om burgers onder de duim te houden, waarmee de weg wordt ingeslagen naar een controlestaat met alom aanwezig toezicht en maatschappelijke onveiligheid. En, het maakt nogal wat uit of in technologische toepassingen het systeem centraal staat, of juist de mens. In de democratische rechtsstaat behoort de mens 'van vlees en bloed' centraal te staan. Tegelijkertijd is in een snel veranderende omgeving de inzet van technologie ook onmisbaar geworden om je snel te kunnen aanpassen en essentiële functies overeind te houden.

1.6 Technologie en revolutie

Technologische ontwikkelingen vragen om aanpassing en maatregelen om bij de tijd blijven. In de afgelopen eeuwen is meermalen een nieuwe technologie geïntroduceerd en iedere keer leidde dit tevens tot belangrijke sociale veranderingen.

Technologische ontwikkelingen hebben belangrijke gevolgen voor de ordening van sociale relaties en daarmee voor het soort van vraagstukken waar samenlevingen zich voor zien gesteld. Met andere woorden: ze leiden tot een andere sociale werkelijkheid. Sommige technologische ontwikkelingen hebben een zodanig grote impact dat ze het label 'revolutie' krijgen. Hoe staat het met het digitaliseringsproces? Is er inderdaad sprake van een paradigmaverschuiving, vergelijkbaar met die van de industriële revolutie of de uitvinding van de boekdrukkunst, zoals in het inleidende hoofdstuk is gesuggereerd?

De huidige technologische ontwikkelingen kunnen ook worden gezien als een volgende fase in de industriële revolutie. De verschillende fasen worden gekarakteriseerd door verschillende dominante technologieën, als volgt.

- Eerste Industriële Revolutie: gietijzer en stoommachine (18/19e eeuw).

[7] De Netflix-serie *The Great Hack* beschouwt de affaire als een kantelpunt: "Ontdek hoe het databedrijf Cambridge Analytica in de nasleep van de Amerikaanse presidentsverkiezingen van 2016 een symbool werd voor de duistere kant van social media", aldus het mediabedrijf. Zie voor een meer journalistieke benadering tevens https://www.theguardian.com/news/series/cambridge-analytica-files.

- Tweede Industriële Revolutie: staal, elektriciteit, turbine en verbrandingsmotor (19/20e eeuw)
- Derde Industriële Revolutie: computer, communicatie en globalisering (20/21e eeuw)

Volgens het *World Economic Forum* staan we op de drempel van de Vierde Industriële Revolutie waarbij het vervagen van de grenzen tussen fysieke, digitale en biologische domein centraal staat. De consequenties hiervan zijn zeer ingrijpend en de snelheid van de verandering is exponentieel (Schwab, 2015):

> *"The speed of current breakthroughs has no historical precedent. When compared with previous industrial revolutions, the Fourth is evolving at an exponential rather than a linear pace. Moreover, it is disrupting almost every industry in every country. And the breadth and depth of these changes herald the transformation of entire systems of production, management, and governance. The possibilities of billions of people connected by mobile devices, with unprecedented processing power, storage capacity, and access to knowledge, are unlimited. And these possibilities will be multiplied by emerging technology breakthroughs in fields such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing."*

Er is weinig fantasie nodig om te begrijpen wat dit alles betekent voor overheden – in het bijzonder voor regulering – en voor veiligheid. Aanpassen aan de voortdurend veranderende condities, is Schwabs devies:

> *Ultimately, the ability of government systems and public authorities to adapt will determine their survival. If they prove capable of embracing a world of disruptive change, subjecting their structures to the levels of transparency and efficiency that will enable them to maintain their competitive edge, they will endure. If they cannot evolve, they will face increasing trouble.*

De gedachten verwoord door het *World Economic Forum* klinken door in de zeer compacte samenvatting van de drijvende krachten en de gevolgen voor de politie in de recente verkenning van de politie Amsterdam (Hageman et al. 2019: 7), als volgt. De maatschappelijke ontwikkelingen en de daarmee verbonden veiligheidsthema's brengen twee belangrijke 'motoren' van voortdurende verandering naar voren die betekenis (blijven) hebben op het politiewerk. Het gaat daarbij om een decennialange ontwikkeling met onderlinge wisselwerking:

- De versterking van de infrastructuur met als uitkomst 'connecting people';
- De toenemende sociale instabiliteit met als uitkomst 'disconnected people'.

De eerste 'motor' werkt vanuit de markt en is gericht op profijt. Veelal financieel en materieel gericht. Het gaat om een wereld met kenmerken als flexibel, anoniem, grenzeloos, adaptief en netwerken. Het gaat vooral om meer hiervan. De tweede 'motor' werkt vanuit de samenleving en heeft zich gericht op identiteit. Het gaat om een wereld met als kenmerken gemeenschap, verbondenheid, 'kennen en gekend worden' en er (onderdeel van) zijn. Hier gaat het vooral om minder van dit alles. Beide geven in toenemende mate maatschappelijke spanningen en hebben uitwerking op veiligheidsvraagstukken.

Bovenstaande beschrijving schetst als het ware een nieuwe 'natuurstaat' zonder sociaal contract. Een natuurstaat waarin menselijke relaties vorm en inhoud krijgen onder invloed van informatie- en communicatietechnologie: *connecting people* en *disconnected people*. Het is de 'menselijke conditie' zoals die ook naar voren komt in het boek Atopia van Helmut Wilke (2001). Wilke beschrijft een mondiale samenleving, zonder grenzen en zonder nationale identiteiten zoals we die laatste nu kennen. Een hernieuwde aandacht voor verschillende 'identiteiten' is dan een begrijpelijke reactie. Enerzijds is er sprake van grote druk op en soms fragmentatie van klassieke functies en instituties, en anderzijds vormen zich nieuwe regimes van 'samenleven'. Er is ook in de publieke sector een sterk bewustzijn dat aanpassen op dit moment van groot belang is, met sleutelbegrippen als flexibiliteit, veerkracht en wendbaarheid. En, dat het daarbij gaat om het leggen van nieuwe verbindingen. Dicht bij huis: het strategisch kompas

van de Politie spreekt over een “politie verbonden met wijk, web en wereld”. Hoe dat er precies uit moet zien is nog niet helder, maar wel dát er nieuwe verbindingen moeten worden gelegd.

Duidelijk is dat het niet gaat over een eenvoudige aanpassing, maar echt over een fundamentele verandering. Het vraagstuk is complex en zeer dynamisch. Hoe reageert Nederland hierop? Hoe reageert de politie hierop? Dat is het onderwerp van het volgende hoofdstuk.

2 De politiek-bestuurlijke reactie

In dit hoofdstuk geven we een grove schets van hoe de digitale transformatie vanuit Nederlands perspectief vorm en inhoud begint te krijgen. Onderdeel daarvan zijn de instituties die gecreëerd worden om de nieuwe uitdagingen het hoofd te bieden. Ook voor dit hoofdstuk geldt: de beschrijving is ongetwijfeld niet uitputtend, maar geeft een beeld van wat er aan de hand is: er is een veelheid aan organisaties die zich bezighoudt met vraagstukken rond digitalisering en veiligheid.

2.1 Reactie van de overheid op de digitale uitdaging

De Nederlandse overheid onderkent de impact die digitalisering heeft en nog verder zal hebben, het meest duidelijk wat betreft cybercrime en de bedreiging van cybersecurity. In december 2016 heeft de Tweede Kamer de gewijzigde motie van het lid-Recourt aangenomen (TK 34 550 VI nr. 53). In deze motie wordt het kabinet opgeroepen in samenspraak met de private sector te komen tot een integraal plan van aanpak voor cybercrime, waarbij aandacht is voor preventie tot en met vervolging (TK 28684 nr. 522). De maatschappelijke opgave voor de overheid is het terugdringen van cybercrime, het verminderen van de gevolgen ervan en het aanpakken van de daders. De aanpak van cybercrime richtte zich tot dan toe op het opsporen, vervolgen en verstoren van strafbare feiten, alsook op preventie en het versterken van wet- en regelgeving. Die aanpak wordt voortgezet en geïntensiveerd. Strafrechtelijke handhaving is een kerntaak van de overheid, ook in het digitale domein. “Het versterken van strafrechtelijke aanpak blijft nodig ter bescherming van (potentiële) slachtoffers en om te zorgen dat misdaad niet loont”, aldus de minister (TK 28684 nr. 522).

Rapporten als die van het eerdere aangehaalde Rathenau Instituut hebben er mede toe geleid dat de Nederlandse overheid in 2018 is gekomen tot drie actuele digitale agenda’s:

- de Nederlandse Digitaliseringsstrategie (EZK, BZK en JenV, 2018)
- de Agenda Digitale Overheid (BZK, 2018) en
- de Cybersecurity Agenda (JenV, 2018).

Naast deze digitale agenda’s verschijnen met enige regelmaat meer specifieke publicaties, bijvoorbeeld de WODC-publicatie uit 2018 over de digitalisering van georganiseerde misdaad, of het verslag van de WRR bijeenkomst uit hetzelfde jaar over de impact van Artificiële Intelligentie (AI) op publieke waarden[8]. In oktober 2019 zijn het *Strategische Actieplan voor Artificiële Intelligentie* (SAAI 2019) van het Ministerie van Economische Zaken en Klimaat en het WRR-rapport *Voorbereiden op Digitale Ontwrichting* (WRR 2019) aan dit rijtje toegevoegd.

De Nederlandse Digitaliseringsagenda zet in op het benutten van de kansen die digitalisering biedt, maar vraagt ook aandacht voor het versterken van de weerbaarheid van bedrijven en burgers met als trefwoorden: privacy, digitale veiligheid, grondrechten en ethiek. Illustratief is de langdurige discussie over de invoering van de Wet op de inlichtingen- en veiligheidsdiensten (WIV, alias de “Sleepwet”). Nieuwe thema’s zijn bijvoorbeeld de verspreiding van desinformatie, de bescherming van democratie en de betekenis van algoritmen voor grondrechten (Derksen 2019).

Op 20 april 2018 is de Nederlandse Cybersecurity Agenda (NCSA) aan de Tweede Kamer gestuurd, en inmiddels is er een voortgangsrapportage van 19 oktober 2019. In de begeleidende brief van april 2018 stelt de minister dat het beschermen van waarden en grondrechten in het digitale domein eveneens een belangrijk onderdeel van cybersecurity is. Burgers moeten er op kunnen rekenen dat hun grondrechten

[8] https://www.wrr.nl/publicaties/publicaties/2018/11/9/verslag-van-de-hollands-spoor-bijeenkomst-over-artificiele-intelligentie

zowel offline als online gewaarborgd zijn, en dat hun privacy ook in het digitale domein gegarandeerd is[9].

In de Nederlandse Cybersecurity Agenda (NCSA) worden kaders gesteld voor de volgende noodzakelijke stap in cybersecurity. De gezamenlijke koers wordt aangegeven, en diverse publieke, private, nationale en internationale maatregelen worden in samenhang beschouwd. De NCSA (2018) bestaat uit zeven ambities die bijdragen aan het doel dat Nederland in staat moet zijn om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen (NCSA 2018:7). Daartoe:

- Heeft Nederland zijn digitale slagkracht op orde;
- Draagt Nederland bij aan internationale vrede en veiligheid in het digitale domein;
- Loopt Nederland voorop in het bevorderen van digitaal veilige hard- en software;
- Beschikt Nederland over weerbare digitale processen en een robuuste infrastructuur;
- Werpt Nederland door middel van cybersecurity succesvol barrières op tegen cybercrime;
- Is Nederland toonaangevend op het gebied van cybersecurity kennisontwikkeling; en
- Beschikt Nederland over een integrale, publiek-private aanpak van cybersecurity.

Om de slagkracht van publieke en private partijen te versterken wordt een landelijk dekkend stelsel van samenwerkingsverbanden op het gebied van cybersecurity ingericht waarbinnen informatie over cybersecurity breder, efficiënter en effectiever wordt gedeeld tussen publieke en private partijen.

2.2 Institutionele reflex

Het bouwen van een veelheid aan organisaties is een herkenbare reactie op nieuwe ontwikkelingen. Dat geldt zeker ook ten aanzien van digitalisering van de samenleving. Dit betreft bijvoorbeeld de zogeheten incident-response-organisatie. Om snel te kunnen handelen bij ICT-inbreuken die de nationale veiligheid bedreigen, worden de incident-response-capaciteiten van onder andere de inlichtingen- en veiligheidsdiensten, Defensie Computer Emergency Response Team (DefCERT), Nationaal Cyber Security Centrum (NCSC) en Rijkswaterstaat versterkt, aldus de plannen. Ook wordt de versterking van meer private sectorale computercrisisteams aangemoedigd, zoals Z-CERT (voor de zorgsector) en I-CERT (voor de verzekeringssector). De capaciteiten van de inlichtingen- en veiligheidsdiensten, DefCERT en het NCSC worden structureel versterkt om inzicht te krijgen in dreigingen en digitale aanvallen, deze te signaleren, te verstoren en de weerbaarheid te verhogen. Het kabinet maakt daar geld voor vrij. Datzelfde geldt voor het meer technische Nationaal Detectie Netwerk (NDN). Het landelijk situationeel beeld wordt versterkt met de inrichting van een samenwerkingsplatform[10]. Het NCSC en het Digital Trust Centre (DTC) zullen andere samenwerkingsverbanden op het gebied van cybersecurity voor overheden, het bedrijfsleven en maatschappelijke organisaties stimuleren, en – waar nodig – hieraan ondersteuning bieden. Ook wordt aandacht gegeven aan het opstellen van een set van basisbeveiligingsmaatregelen voor bedrijfsleven en maatschappelijke organisaties. En natuurlijk wordt bezien in hoeverre wetgeving gericht op het beschermen van nationale veiligheid voldoende handvatten biedt om deze veiligheid ook in het digitale domein te bevorderen.

De lijst van instanties belast met de enige vorm van cybersecurity is indrukwekkend. Want, naast de eerder genoemde instellingen kennen we intussen het Defensie Cyber Commando (DCC), de Joint Sigint Cyber Unit (JSCU), het NRN (Nationaal Respons Netwerk), de Cyber Innovation Hub (CIH) en

[9] https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/20/tk-aanbieding-nederlandse-cybersecurity-agenda-ncsa

[10] De mogelijkheden met welke partijen en in welke vorm dit samenwerkingsplatform kan worden vormgegeven, worden nader onderzocht.

de Cyber Security Raad (CSR). Verder ook: Nationaal Bureau voor Verbindingsbeveliging (NBV) onderdeel van de AIVD, Platform Interceptie Decryptie en Signaalanalyse, Platform 13 en Afstemmingsoverleg Cyber, waarin ook de politie is vertegenwoordigd.

Binnen de politie bestaan aan operationele zijde onder meer het Expertisecentrum Digitale Opsporing (ECDO), cybercrimeteams, Teams Digitale Opsporing (TDO), de Electronic Crimes Taskforce (ECTF), het Team High Tech Crime (HTC) en het Digital Intrusion Team (DIGIT), naast cyber-gerichte werkwijzen in de intelligence (DLIO) en het Team Criminele Inlichtingen (TCI). Daarnaast verdedigt de politie zich ook zelf tegen cyberdreigingen, onder coördinatie en toezicht van de CISO.

Deze opsommingen laten mogelijk nog een aantal instanties onbenoemd. Want ook in de private sector wordt veel geïnvesteerd en vormgegeven. Datzelfde geldt voor internationale ontwikkelingen, in en buiten Europa. Dat laat onverlet dat we kunnen concluderen dat een belangrijke reactie op de bedreigingen van digitalisering is dat we – zowel publiek als privaat – veel geld investeren en veel organisaties en instituties bouwen. Ook de traditionele statelijke veiligheidspartijen – krijgsmacht, politie, inlichtingen- en veiligheidsdiensten – zetten stuk voor stuk flink in op digitalisering, in het bijzonder het waarborgen van cybersecurity en de bestrijding van cybercrime. Op grond waarvan zij dat precies doen en waarom zij de dingen doen, die ze nu doen, is in elk geval naar buiten toe niet altijd duidelijk. En, hoe zij zich opstellen ten opzichte van elkaar al evenmin. Daarbij komt nog dat tal van niet-publieke organisaties eveneens in dit domein opereren.

Het bouwen van een veelheid aan organisaties en instituties lijkt sterk op een reflex. Eenzelfde beweging zagen we immers na de aanslagen van 11 september 2001 in de VS: enkele jaren nadien bleek dat er ten minste 21 instanties zich bezighielden met de bestrijding van terrorisme, terwijl er geen sprake was van heldere doelstellingen of een transparante verdeling van taken, bevoegdheden en verantwoordelijkheden (Politie Amsterdam-Amstelland 2006). Er blijkt nu dus (opnieuw) sprake van een tamelijk onstuimige groei in reactie op een nieuwe werkelijkheid. De regie van alle ontwikkelingen is belegd bij de Nationaal Coördinator Terrorisme en Veiligheid (NCTV). De dynamiek om 'vorm te geven' is indrukwekkend en de ambitie blijkt groot. Vraagt dit om een Cyber Delta Plan met een bijpassende cybercommissaris en budget, zoals door sommigen (Prins 2017; Bank, Cobelens & Welten 2017[11]) is gesuggereerd?

Het lijkt op de kolonisatie van een Terra Incognita, waar talloze instanties zich een plek verwerven in een nieuw domein. Het doet tevens denken aan wat er gebeurde rond de Californische Goldrush in Amerika halverwege de 19e eeuw. De eerste kolonisten troffen een gebied waar wetteloosheid heerste, zodat zij noodgedwongen zelf hun claimrecht moesten organiseren.

2.3 Lokale en regionale vraagstukken

Er is – samengevat – een groot aantal landelijke overheidsorganisaties, die een taak hebben in het cyberdomein, gecombineerd met een toenemend aantal private of semipublieke organisaties. Daarbij ligt de focus op de strafrechtelijke kant (cybercrime), de bescherming van vitale infrastructuur en publiek-private samenwerkingen om economische belangen te beschermen. Op lokaal (gemeenten) en regionaal niveau (bijvoorbeeld de veiligheidsregio) gaat de aandacht tevens uit naar handhaving in (of in combinatie met) het cyberdomein, alsmede conflict- en crisisbeheersing. Een studie van Bantema c.s. uit 2018 liet al zien dat "de toepassing van openbare-orde bevoegdheden in de digitale wereld lastig is en dat het openbaar bestuur verdeeld is over de vraag hoe het huidige en toekomstige bestuurlijke landschap eruit zou moeten zien". Ook in 2018 publiceerden het Veiligheidsberaad, de Regioburgemeesters en de VNG een gezamenlijk memo 'Bestuurlijke aspecten digitaal domein'. Daarin worden de diverse rollen van de burgemeester verkend (college B&W; openbare orde; gezag over de politie; crisis-

[11] https://www.volkskrant.nl/columns-opinie/nederland-moet-deltaplan-voor-nationale-veiligheid-krijgen~ba6c171d/

en rampenbestrijding). Geconcludeerd kan worden dat het lokaal bestuur nog zoekende is met betrekking tot zijn rol, de informatiepositie nog fysiek- en locatie gebonden is en dat de verantwoordelijkheden en bevoegdheden nog lang niet altijd aansluiten bij de gedigitaliseerde samenleving.

In de zoektocht naar antwoorden wordt er veel ondernomen. Steden als Rotterdam, Den Haag en Amsterdam hebben programma's opgetuigd die de cyberweerbaarheid van de stad moeten vergroten. Een ransomware-aanval op de gemeente Lochem in maart 2015 heeft ervoor gezorgd dat er ook meer urgentie wordt gevoeld bij bestuurders voor de eigen digitale veiligheid[12]. De VNG heeft in het voorjaar van 2019 een training gemaakt om burgemeesters bewuster te maken van hun rol bij cyberincidenten. En, het Veiligheidsberaad is in juli 2019 gekomen met een 'Bestuurlijk Routeboek digitale ontwrichting'.

Naast de rol van instituten en bestuurders is ook te zien dat ook op lokaal niveau steeds meer (publiek/private) coalities worden gevormd om de grotere vraagstukken van digitalisering en cyber op te pakken. Dit zijn coalities waar de politie veelal in participeert, maar die daarmee de vraag nog belangrijker maken hoe de politie zich wil positioneren in het digitale domein.

2.4 Aanpassing

Als zich een nieuw fenomeen, of – zoals betoogd – een nieuwe werkelijkheid aandient, staan veiligheidspartijen voor de opgave zich daartoe te verhouden op basis van hun functie. We constateren dat dit met betrekking tot het digitaliseringsproces nog onvoldoende is uitgekristalliseerd. Niet voor niets is dus vanuit de politieorganisatie de vraag opgeworpen hoe de politie zich in de nieuwe werkelijkheid moet opstellen om maximale toegevoegde waarde te kunnen leveren aan sociale veiligheid. En, welke invulling in de nieuwe werkelijkheid kan worden gegeven aan haar missie "Waakzaam en dienstbaar staat de politie voor de waarden van de rechtsstaat".

De politie dient zich aan te passen aan belangrijke ontwikkelingen in de samenleving, niet in de laatste plaats de technologische ontwikkeling. De Nederlandse politie heeft daarin een zekere traditie. Zo werd in 2005 met Politie in ontwikkeling (PIO) een visie op de politiefunctie ontwikkeld, omdat de tijd rijp werd gevonden om opnieuw[13] de bakens te verzetten (2005: 4-7). Aan de toen ontwikkelde visie op de politiefunctie liggen veel van de ontwikkelingen ten grondslag die eerder in dit hoofdstuk zijn aangestipt. Ook toen ging het om de veranderende aard van criminaliteit onder invloed van globalisering, waarbij anonimiteit, mobiliteit en ontgrenzing werden beschouwd als criminogene factoren. Ook toen ging het om fragmentatie van de politiefunctie. Sindsdien is de impact van verschillende ontwikkelingen samenhangend met ICT sterk toegenomen met als gevolg dat vandaag-de-dag de noodzaak om 'de bakens te verzetten' bepaald niet is afgenomen.

De politie moet zich in een aantal opzichten opnieuw 'uitvinden' en zich meer fundamenteel aanpassen aan de zich voortdurend vernieuwende context. In feite is met PIO – en de daarin bepleite keuze van de politie om toegevoegde waarde te leveren aan sociale veiligheid ten opzichte van andere partijen ("doen wat het meeste oplevert in termen van veiligheid") – 'aanpassing' zelfs in het hart van de politiefunctie terecht gekomen (Van Dijk & Hoogewoning 2014: 3). Dat is bijna per definitie geen eenvoudige opgave.

Het is op dit punt wel van belang vast te stellen wat 'aanpassing' precies betekent. Dat is overigens voor bedrijven ogenschijnlijk eenvoudiger dan voor de politie. Als Philips als kernfunctie winst wil blijven maken door medische apparatuur te gaan verkopen in plaats van uit de markt gerakende gloeilampen, is dat een lucratief besluit. Maar bij de politie gaat het niet om winst maken, door wat dan ook, maar om een fundamenteel andere kernfunctie: Waakzaam en dienstbaar aan de waarden van de rechtsstaat.

[12] https://www.security.nl/posting/422141/Gemeente+Lochem+getroffen+door+ransomware.
[13] Opnieuw, na *Politie in Verandering* (1977), waarin eveneens werd verwezen naar Thorbeckes pleidooi uit 1872 voor tijdige aanpassing aan veranderende omstandigheden.

Een politie die – bij wijze van absurd voorbeeld – zich aanpast door het gebruik van bijzondere bevoegdheden dienstbaar te maken aan de hoogste bieder, is wellicht een succesvol bedrijf maar van behoud van de politiefunctie is geen sprake. Wezenlijk is dat we niet vergeten dat die waarden in essentie gaan over mensen met onvervreemdbare rechten en dat daarmee dus is uitgesloten dat 'de mens' wordt opgeofferd voor veiligheid – operatie geslaagd, patiënt overleden. Het volgende hoofdstuk gaat in op de functie van de politie.

3 De functie van de politie

Om vast te stellen wat 'aanpassing aan nieuwe omstandigheden met behoud van vitale functies' betekent voor de politie kijken we in dit hoofdstuk naar de politiefunctie. Wat was die functie ook alweer? Welke aanpassingen hebben we eerder gezien? Dit alles als een opmaat naar volgende hoofdstukken waarbij we zullen ingaan op welke aanpassingen dan nu worden gevraagd; en wat dat dan betekent voor de positionering van de politie ten opzichte van andere veiligheidspartijen?

3.1 Klassieke onderscheidende kenmerken

De politie staat voor de opgave zich aan te passen aan technologische ontwikkelingen en de impact die deze hebben op de samenleving. En, hoe zich te verhouden tot andere veiligheidsfuncties. Dit komt uitgebreid aan de orde in de navolgende hoofdstukken. Dit proces is verre van uitgekristalliseerd. In deze paragraaf beperken we ons tot de traditionele karakteristieken van de verschillende veiligheidsfuncties in relatie tot de politiefunctie. De traditionele *politiefunctie* betreft de daadwerkelijke handhaving van de rechtsorde op het grondgebied van de staat. We onderscheiden daarnaast de *defensiefunctie*, de *inlichtingenfunctie* en de *private veiligheidsfunctie*.

De *defensiefunctie* betreft de verdediging – de integriteit en het voortbestaan – van de staat tegen dreiging van buiten de staat; en indien noodzakelijk het verlenen van bijstand binnen de staat onder civiele aansturing. De verhouding met de politiefunctie is ook historisch altijd onderwerp van (politiek) debat. Zo was in aanvang in Nederland (1848) de politiefunctie een zuiver lokale aangelegenheid en waren zaken van nationaal belang het domein van de krijgsmacht (Welten 2018). Er is op zeer veel terreinen sprake van structurele samenwerking tussen politie en defensie en het traditionele onderscheid tussen binnen- en buitenland verschaft in afnemende mate helderheid. Er zijn andere perspectieven denkbaar op het onderscheid tussen krijgsmacht en politie, zoals de aard van het geweld – waarbij de krijgsmacht dan hoog in het geweldspectrum opereert – of het verschil tussen een nadruk op legitimiteit (politie) versus effectiviteit (krijgsmacht). De politiefunctie en defensiefunctie raken elkaar ook waar het gaat om het bevorderen van de internationale rechtsorde. Er lijkt wel overeenstemming over het feit dat politie en defensie niet langer kunnen worden gezien als feitelijk gescheiden werelden (Welten 2000, 2006).

De *inlichtingenfunctie* betreft de inzet van bijzondere bevoegdheden voor het verkrijgen van informatie in binnen- en buitenland nodig voor het beschermen van de integriteit en het voortbestaan van de staat en de rechtsorde[14]. Waar de politie zich richt op binnenlandse wetshandhaving, beschermen de inlichtingen- en veiligheidsdiensten (AIVD, MIVD) de belangen van de staat tegen (mogelijke) dreigingen, zowel van buiten als van binnen. Op basis van de zogenoemde A-taak (artikel 8 lid 2 a van de WIV) doet de AIVD: […] "onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat". Hier geldt evenzeer als bij de defensiefunctie dat de verhouding tot de politiefunctie voortdurend onderwerp van discussie is. Het klassieke onderscheid is vooral dat de politiefunctie primair gericht is op de rechtshandhaving – opsporing en openbare orde – en dat de politie daar ook uitvoering aan geeft, terwijl de inlichtingendiensten traditioneel geen uitvoerende organisaties zijn. Dat klassieke onderscheid staat in de praktijk in toenemende mate onder druk en noopt tot voortdurende afweging over de reikwijdte van de taak. Met betrekking tot de inlichtingsdiensten speelt de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) een belangrijke rol en de in het kader van de WIV ingestelde Toetsingscommissie Inzet Bevoegdheden (TIB).

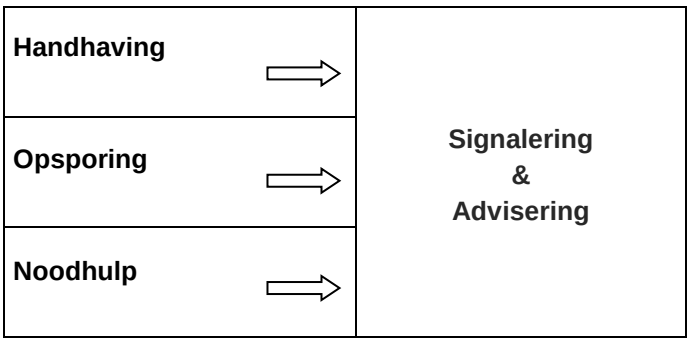
[14] We gaan hier niet in op het onderscheid tussen criminele- en algemene inlichtingen, of tussen de inlichtingenfunctie en de veiligheidsfunctie, of tussen algemene inlichtingen en militaire inlichtingen.

De *private veiligheidsfunctie* verwijst naar het uitgangspunt dat van private partijen en burgers verwacht mag worden dat zij binnen de context van de rechtsstaat in beginsel zorgdragen voor de eigen veiligheid – vaak ook vastgelegd in regels – en dat de staat in beeld komt daar waar veiligheid een zogeheten collectief goed is en dus niet op basis van zelfwerkzaamheid en vrijwillige ruil tot stand komt, er anderszins sprake is marktfalen of externe effecten, de inzet van bijzondere bevoegdheden noodzakelijk is of de waarden van de democratische rechtsstaat in het geding zijn. Het onderscheid tussen privaat en publiek is niet altijd duidelijk. Een goed voorbeeld is huiselijk geweld, waarbij de politie worstelt ten aanzien van dat fenomeen met haar rol en positie, met bijbehorende concepten als 'achter de voordeur komen' en 'aan de voorkant van het probleem komen'. En, bij het vermoeden van geweld in afhankelijkheidsrelaties in de (semi-)private sfeer kan niet gewacht worden totdat er iemand aangifte doet, terwijl bij politieoptreden zonder aangifte niet altijd helder is wat de grondslag is voor optreden.

Bovenstaande beschrijving maakt duidelijk dat ook voordat er sprake was van digitalisering en een nieuwe sociale werkelijkheid, er voortdurend discussie was over de onderscheidende kenmerken van verschillende veiligheidsfuncties. Digitalisering versterkt echter wel de urgentie van de vraag hoe de verschillende functies – en gerelateerde partijen – zich tot elkaar verhouden. Dat komt doordat digitalisering een aantal van de klassieke onderscheidende kenmerken verder ter discussie stelt, zoals het onderscheid tussen binnen- en buitenland, tussen oorlog en vrede – is er sprake van een cyberoorlog? – en tussen de publieke en private sfeer. Wat dat laatste betreft: het Engelse *College of Policing* constateerde al eens: "People want to feel safe, not only in the streets but also in their homes and online" (geciteerd in Van Dijk 2016). En, het Britse National Cyber Security Center heeft in 2016 als missie gekozen "Making the UK the safest place to live and do business online". Ga daar maar aanstaan, en wie gaat dan wat doen? In de volgende paragrafen concentreren we ons op de politiefunctie. De verhouding tot andere spelers is daarvan – in dit advies – een afgeleide.

3.2 Politiefunctie

De politie is er voor de daadwerkelijke handhaving van de rechtsorde. Dat vertaalt zich in strafrechtelijke handhaving van de rechtsorde, handhaving van de openbare orde en het verlenen van hulp aan hen die dit behoeven (Politiewet 2012, art. 3). Deze drieledige taakopdracht aan de politie, is eerder vertaald in de zogeheten politieprocessen, weergegeven in onderstaand schema die in onderlinge samenhang worden uitgevoerd.



Figuur 4. Taakopdracht van de politie (Projectgroep Opsporing-2, 2003)

Dit betreft handhaving van de openbare orde, de opsporing van strafbare feiten en het verlenen van hulp bij noodsituaties, en signaleren & adviseren. In tegenstelling tot de eerste drie functies is signaleren & adviseren niet rechtstreeks terug te voeren op de Politiewet. Signaleren & adviseren vloeit echter uit de eerste drie functies voort. Het gaat er daarbij om dat de politie vanuit haar operationele ervaringen, de daarmee samenhangende informatiepositie en haar professionaliteit, problemen op het gebied van veiligheid signaleert en waar mogelijk omvormt tot adviezen aan andere spelers op het veiligheidsveld,

zonder in hun verantwoordelijkheden te treden. Daarmee is dus begin deze eeuw een vierde taak van de politiefunctie 'in de nieuwe tijd' geëxpliciteerd: Signaleren & adviseren.

De onderlinge verhouding tussen de verschillende onderdelen van de politiefunctie is een onderwerp van vrijwel voortdurend debat. Zo geeft Wilson (1968) aan dat de essentie van politiewerk niet zozeer het handhaven van de wet is, maar vooral neerkomt op '*handling the situation'* – handelen naar bevind van zaken. Die opvatting bouwt voort op het onderscheid tussen '*law officers'* en '*peace officers'* dat Banton in 1964 heeft gemaakt. De eersten zijn vooral gericht op het doen van aanhoudingen ten behoeve van het aan justitie overleveren van overtreders en misdadigers. De laatsten bedienen zich van een breed handelingsrepertoire met als doel de vrede te bewaren en te voorkomen dat het recht van de sterkste de norm wordt. Daarvoor is geen heldere wettelijke grondslag en aan wie over het optreden verantwoordelijkheid moet worden afgelegd, is evenmin helder. Hun bestaansreden is ooit adequaat verwoord door Bittner (1970) als het stoppen van "*something-that-ought-not-to-be-happening-and-about-which-someone-had-better-do-something-now*" (Van Dijk 2016).

Bittners karakterisering geeft ook aan dat de politie een uitvoeringsorganisatie in de frontlinie is. De essentie van een frontlinie is dat de interactie met burgers niet-routinematig is en dat er in veel gevallen sprake is van een (potentieel) conflict en de noodzaak gedrag (bij) te sturen. Dit is waar de politiefunctie gestalte krijgt. De frontlinie beperkt zich niet langer tot de publieke ruimte. Mensen willen zich ook thuis en online veilig voelen. De essentie van het werk in de frontlinie is dat de situatie als het ware wordt geconstrueerd in interactie: wat is hier precies aan de hand en wat is de beste wijze van handelen? En, in toenemende mate gaat het hier ook om de samenwerking met andere partijen die al bij het definiëren van de situatie een rol spelen (Van Dijk en Hoogewoning 2018). Een bijkomend aspect is dat het beroep op de politieorganisatie toeneemt, naarmate andere organisaties in de frontlinie, zoals op het terrein van de (geestelijke) gezondheidszorg, zich terugtrekken, bijvoorbeeld vanwege personeelstekort en/of bezuinigingen. Het aandeel van gevraagde politie-interventies die niets te maken hebben met rechtshandhaving, neemt hierdoor sterk toe (Charman 2018).

Tot welke invulling men komt, is sterk afhankelijk van de achterliggende filosofie op de politiefunctie, of anders geformuleerd, het paradigma dat men aanhangt. Meestal worden twee paradigma's tegenover elkaar geplaatst, dat van consent (instemming) en control (beheersing). In het control-paradigma is de politie een instrument van de staat op afstand van de bevolking. In deze opvatting ligt de nadruk op misdaadbestrijding en handhaven van de openbare orde als belangrijkste elementen van het politiewerk. Het consent-paradigma verwijst naar maatschappelijk geïntegreerde politie. Dit paradigma gaat uit van een breed mandaat, een brede taakopvatting voor de politie en van een politieorganisatie die haar legitimiteit ontleent aan instemming van het publiek. Zij werkt in en ten dienste van de gemeenschap, is maatschappelijk betrokken en gericht op – met inbegrip van misdaadbestrijding en ordehandhaving – bevordering van de veiligheid en het welzijn van burgers. Het instemmingsparadigma wordt vooral geassocieerd met de politie in het Verenigd Koninkrijk. Het voert terug op de bekende slogan "*the police are the public and the public are the police*" toegeschreven aan Robert Peel. Dit is het model dat in Nederland vanaf eind jaren zeventig gestalte heeft gekregen en dat ook nog steeds wordt beleden, bijvoorbeeld in de visie van de Nederlandse politie: "het optreden van de politie betreft beschermen – begrenzen – bekrachtigen".

Het onderscheid tussen control en consent is simplistisch en suggereert een onterechte tweedeling. Het is goed mogelijk om beide benaderingen te integreren, zolang het instemmingsparadigma de overhand heeft, dat wil zeggen dat wordt onderkend dat politiewerk een breed palet van taken betreft, die in onderlinge samenhang moeten worden uitgevoerd in en ten behoeve van de gemeenschap. Dat palet kan nader worden onderverdeeld in drie dimensies. De eerste dimensie is die van het managen van misdaad en veiligheid in de ruimste zin van het woord, bijvoorbeeld opsporing en voorbereiding van vervolging, misdaadpreventie, contra-terrorisme, etc. De tweede dimensie is die van taken die samenhangen met sociaal welzijn en verbinding met gemeenschappen. Dit betreft onder meer samenwerking met partnerorganisaties, beschermen van kwetsbare groepen, *community policing* en buurtgericht werken evenals

het reageren op hulpverzoeken en het verlenen van diensten aan het publiek. Deze dimensie is ooit raak getypeerd als: *"the police as a secret social service*" (Punch 1979). De derde dimensie is die van het handhaven van de orde in ruimst denkbare zin, waaronder optreden bij verstoringen van de openbare orde, het managen van grote (sport)evenementen, noodsituaties, rampen, risicovolle politieke bezoeken en bijeenkomsten, etc. De dimensies zijn elk in zichzelf belangrijk én zouden onderling verbonden moeten zijn. Aldus ontstaat er een nieuw paradigma: het omvattend paradigma of *comprehensive paradigm* (Van Dijk et al. 2015).

3.3 Traditie van aanpassing

De politie dient zich dus te bezinnen op de vraag welke invulling wordt gegeven aan de politiefunctie gegeven de nieuwe sociale werkelijkheid. Zoals gezegd, de Nederlandse politie heeft een zekere traditie van aanpassing, waarvan Politie in Verandering (PIV, 1977) en Politie in ontwikkeling (PIO, 2005) uitdrukkingen zijn. PIV zag het licht in de periode waarin sprake was van een overgang van een eenduidige en stabiele wereld naar een situatie waarin de overheid een actieve bijdrage moet leveren aan veranderingen. PIO start met de schets van een wereldbeeld waarin snelle veranderingen en complexiteit een gegeven zijn geworden. Ook dan wordt al verwezen naar de impact van technologische ontwikkelingen – in het bijzonder informatie- en communicatietechnologie – op criminaliteit. Ontgrenzing, mobiliteit en anonimiteit worden in PIO gezien als belangrijke criminogene factoren. Bovendien wordt gesignaleerd dat de verschijningsvorm van veel typen misdaad is veranderd. Lokale, interlokale en internationale veiligheid zijn steeds meer verweven geraakt. Bovendien ontstaan er nieuwe vormen van criminaliteit die niet of nauwelijks meer aan territoir gebonden zijn. Voorbeelden van wat we inmiddels cybercrime zijn gaan noemen, bevestigen dit beeld: een dader in land A verricht met behulp van infrastructuur (servers, netwerken) in land B en C handelingen die strafbaar zijn in B en C, maar niet in A, en maakt daarbij slachtoffers in land C, D en E. En dan gaat dit voorbeeld er nog van uit dat überhaupt is vast te stellen wie de dader is en waar op de wereld deze zich bevindt. In PIO wordt al geconstateerd dat deze ontwikkelingen beproefde concepten onder druk zet. In PIO wordt een relatie gelegd met het onder druk staan van de grondslagen van de staat.

> *"Het veiligheidsconcept van de overheid is echter nog altijd gebaseerd op de fictie van het samenvallen van territorialiteit (gebondenheid aan het grondgebied van de staat), soevereiniteit (op basis van de wetten van de staat) en de democratische gemeenschap, die controle uitoefent en waaraan verantwoording wordt afgelegd."*

We zien in PIO dus al de noodzaak tot aanpassing aan de nieuwe omstandigheden; aan een politie die zich opnieuw weet uit te vinden. De keuze die dan wordt gemaakt is niet die van een terugkeer naar zogenaamde kerntaken en een afbakening vooraf van taken en verantwoordelijkheden tussen verschillende partijen die vorm en inhoud geven aan de veiligheidsfunctie. Wat dan wel?

3.4 Voor de rechtsstaat

In PIO wordt de missie voor de gezamenlijke Nederlandse politie geformuleerd, met als mission statement: "Waakzaam en dienstbaar staat de politie voor de waarden van de rechtsstaat". De missie geeft aan waartoe de politie er is en waarvoor zij zich sterk maakt; zij geeft aan welke positie de politie kiest in de samenleving en zegt iets over haar identiteit als organisatie. PIO schetst vier richtinggevende principes voor de politieorganisatie van na 2005: een brede samenhangende taakuitvoering, optimale samenwerkingsgerichtheid, het bereiken van overtuigende resultaten en ondergeschiktheid MET gezag. Deze principes kunnen worden gezien als het antwoord van de politie op de toestand van de politiefunctie zoals die aan het begin van deze eeuw werd geduid. In aansluiting op de vier richtinggevende principes introduceert PIO vier operationele concepten: 1) lokale & nodale oriëntatie, als antwoord op de vervlechting van plaatsen en stromen, 2) *policing of communities*, wat uitdrukt dat er niet langer

sprake is van een eenduidige woongemeenschap, maar van verschillende gemeenschappen naast elkaar en door elkaar, ook online 3) programmasturing, een poging om in de situatie waarin de overheid geen monopolist meer is toch op een niet-vrijblijvende manier samenwerking vorm en inhoud te geven en ten slotte 4) informatiesturing, wat aangeeft dat de inzet van de politie vooral gebaseerd zou moeten zijn op *intelligence*.

3.5 Toegevoegde waarde

In PIO wordt nadrukkelijk gesteld dat de Nederlandse politie het tot haar verantwoordelijkheid rekent een bijdrage te leveren aan het verminderen van onveiligheid. De politie wil datgene doen, wat het meeste oplevert in termen van veiligheid. Met andere woorden: zij wil toegevoegde waarde leveren ten opzichte van andere partijen op het veiligheidsdomein. Ingewikkeld aan deze opstelling is dat hiermee het feitelijk optreden van de politie afhankelijk wordt van de situatie: wat de politie doet, is afhankelijk van de context en onderdeel van die context is van andere partijen (kunnen) doen of nalaten te doen.

Deze toegevoegde waarde van de politie ten opzichte van andere partijen stoelt op een combinatie van unieke kenmerken, te weten:

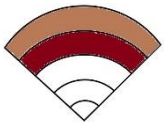
- de mogelijkheid tot gelegitimeerde uitoefening van geweld;
- de beschikking over opsporingsbevoegdheden;
- de continue aanwezigheid in de frontlinie van de samenleving en de hierop toegespitste professionaliteit;
- de daarmee samenhangende informatiepositie en;
- de maatschappelijke verankering.

Toegevoegde waarde is bepalend voor het rangschikken van activiteiten en voor het antwoord op de vraag of een activiteit op een bepaald moment en op een bepaalde plaats tot de taken van de politie moet worden gerekend. Ook wordt er in PIO voor gekozen om de specifieke invulling van de taakopdracht van de politie voortdurend te herzien, in wisselwerking met bestuur en samenleving. Alleen zo kan, aldus PIO, de impasse van voortdurende oplaaiende discussies over ‘kerntaken’ worden doorbroken (2005: 13). Tegelijkertijd wordt in PIO afstand genomen van de vrijblijvendheid en de situatie waarin iedereen verantwoordelijk is voor veiligheid en daardoor uiteindelijk niemand. Het debat met bevoegd gezag en samenleving moet vooral gaan over hoe de politie vanuit haar unieke rol de grootste bijdrage levert aan veiligheid, rekening houdend met het feit dat ook andere partijen daaraan een bijdrage behoren te leveren. In PIO wordt daaraan toegevoegd dat de politie zich zal verantwoorden aan het bevoegd gezag en aan de samenleving – dit laatste onder de noemer van horizontale verantwoording – over haar concrete bijdrage, over de toegevoegde waarde die zij levert met betrekking tot veiligheid.

3.6 Tot slot

We begonnen dit hoofdstuk met het de beschrijving van de klassieke veiligheidsfuncties en waar de bijbehorende organisaties zich in beginsel op richten. De politie richt zich in het bijzonder op de (binnenlandse) handhaving van de rechtsorde (opsporing, handhaving openbare orde, bewaren van de vrede), waarbij de aandacht vooral uitgaat naar de veiligheid van inwoners en ondernemingen. De krijgsmacht is vooral gericht op de bescherming van het land en de infrastructuur (de nationale veiligheid) en de inlichtingen- en veiligheidsdienst is traditioneel gericht het inwinnen van binnen- en buitenlandse informatie ten behoeve van het staatsbelang. Voor de politiefunctie hebben we nader uitgewerkt waar het optreden van is afgeleid – de waarden van de rechtsstaat – en waar het zich op richt: toegevoegde waarde in termen van sociale veiligheid voor burgers en ondernemingen ‘in relatie tot andere die een bijdrage kunnen leveren aan veiligheid’. Die toegevoegde waarde stoelt op een unieke combinatie van kenmerken, waaronder de maatschappelijke verankering. Dit alles krijgt altijd gestalte een specifieke context, en de vraag is wat de betekenis is van verandering in de context – *in casu* de vergaand gedigitaliseerde samenleving. Dat is het onderwerp van het volgende hoofdstuk.

4 De meervoudige context: de rechtsstaatwaaier



In hoofdstuk 3 hebben we beschreven dat de politiefunctie rust op twee pijlers: de waarden van de rechtsstaat en het leveren van toegevoegde waarde aan sociale veiligheid (‘doen wat het meeste oplevert’). Vooral dat tweede aspect maakt dat hoe de politiefunctie invulling krijgt, afhankelijk is van de context. Daarbij kan het gaan om een lokale context en om de concrete vraag hoe politieoptreden er op moment-X in stad-Y uitziet: bijvoorbeeld vooral opsporingsactiviteiten, of juist de nadruk op handhaving, en moet er meer aandacht komen voor wijk A of wordt de capaciteit evenredig verdeeld over alle wijken. etc. De uitkomst staat dan niet van tevoren vast, maar is het resultaat van een samenspel van actoren en stakeholders op verschillende niveaus (uitvoeringsorganisaties, bevoegd gezag, de politiek, de burgerij, media) en hun beelden en interpretaties van wat er speelt en hoe dat zou kunnen worden aangepakt.

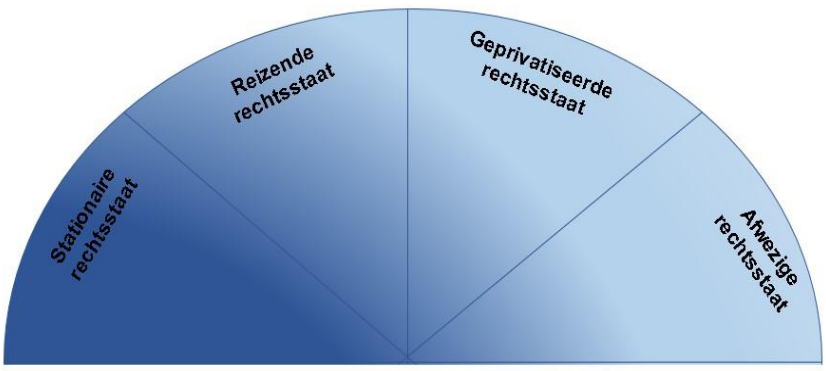
Het kan ook gaan om een veel ruimere context, namelijk die van de samenleving, en de meer abstracte vraag hoe de politiefunctie daarin gestalte krijgt. De vraag is dan: hoe duiden we deze, grote maatschappelijke context? Welke beelden hebben we daarbij en wat is de betekenis daarvan voor de invulling die wordt gegeven aan de politiefunctie? Anders geformuleerd: wat is ons nieuwe ‘wereldbeeld’ of ‘maatschappijmodel’ (De Jager 1975) gegeven het digitaliseringsproces? Dat is het onderwerp van dit hoofdstuk, waarmee we in feite de buitenste twee lagen van de RADAR van inhoud voorzien. De beschrijvingen en analyses uit de voorgaande hoofdstukken monden dus uit in een nieuw ‘wereldbeeld’ vanuit het perspectief van de politiefunctie. Dat is niet eenvoudig, want het gaat om een meervoudige context, die we proberen inzichtelijk te maken.

4.1 Een nieuw wereldbeeld

Het nieuwe wereldbeeld beslaat vier vlakken: vier contexten die niet van elkaar zijn te scheiden, maar wel kunnen worden onderscheiden op een aantal wezenlijke dimensies. Om te beginnen krijgt het rechtsstaatsbegrip in elk van deze velden een andere inkleuring, wat tot uitdrukking komt in de titel van elk van de velden. We onderscheiden achtereenvolgens:

- de stationaire rechtsstaat
- de reizende rechtsstaat
- de geprivatiseerde rechtsstaat
- de afwezige rechtsstaat.

Samen vormen deze de ‘rechtsstaatwaaier’. Deze is grafisch weergegeven in figuur 5.



Figuur 5. De rechtsstaatwaaier ©.

Wat de waaier vooral laat zien is dat hoe verder naar rechts, hoe minder traditioneel de situatie is, beschouwd vanuit de politiefunctie, en hoe minder rechtsstatelijke waarborgen er zijn voor de burger. Naarmate we verder naar rechts gaan is er in afnemende mate sprake van een overheidsgezag dat uitkomsten kan afdwingen. Bewegen van links naar rechts door de velden van de waaier geeft gelijktijdig veranderingen te zien in de volgende dimensies:

- Hiërarchisch → Anarchisch
- Monopolistisch → Volledig Vrije Mededinging
- Publiek → Privaat
- Lokaliseerbaar → Plaatsloos
- Uniforme waarden → Pluriforme Gemeenschappen

De rechtsstaatwaaier, waarvan we de vier velden verderop in dit hoofdstuk in detail zullen beschrijven, geeft een indruk van hoe onder invloed van digitalisering de 'oude wereld' overgaat naar een 'nieuwe wereld'. Die nieuwe wereld, zoals we die in het door ons geconstrueerde wereldbeeld proberen te begrijpen, wortelt in het oude, maar omvat tegelijkertijd nieuwe elementen. Die hebben consequenties voor de politiefunctie en dus vragen ze om herijking en vernieuwing van gebruikelijke noties.

Eerder gebruikten we het begrip 'meervoudige context': het nieuwe wereldbeeld bestaat uit vier velden die door en naast elkaar bestaan. Als de waaier is ingeklapt dan onttrekken de onderscheidende kenmerken zich aan onze waarneming. Door de waaier uit te klappen, treden de onderscheidende kenmerken aan het licht en kunnen deze worden geanalyseerd met betrekking tot hun betekenis voor de politiefunctie.

4.2 De rechtsstaatwaaier uitgeklapt

Na de eerste ruwe schets van de rechtsstaatwaaier is het nu tijd deze verder in te kleuren. Daartoe geven we per veld een nadere omschrijving van de institutionele verhoudingen en de randvoorwaarden voor het uitoefenen van de politiefunctie. Ook geven we voorbeelden die kenmerkend zijn voor wat er in de betreffende velden speelt.

I. De stationaire rechtsstaat

Het veld van de *stationaire rechtsstaat* beschrijft de rechtsstaat in de klassieke betekenis. Hier geldt dat de democratische rechtsstaat een (rechts)gemeenschap veronderstelt. Er is een centrale rol ingeruimd voor de traditionele instituties en in het bijzonder voor de rechtsorde. De basis is een boven de partijen staande arbiter die – indien noodzakelijk – uitkomsten kan afdwingen. Het daadwerkelijk afdwingen dient zich tot een minimum te beperken, want de staat geeft uitdrukking aan het welbegrepen eigenbelang van de gemeenschap. Er is idealiter sprake van gezag – aanvaarde macht – op basis van een denkbeeldig sociaal contract tussen overheid en burgerij. Dat laat onverlet dat er een partij is die zo nodig kan afdwingen dat anderen zich aan hun afspraken houden[15].

In de *stationaire rechtsstaat* zijn de fundamenten van de politiefunctie duidelijk. Deze is afgeleid van het geweldsmonopolie van de staat. Dat betekent natuurlijk niet dat er niets aan de hand is. Er is een veelheid aan maatschappelijke ontwikkelingen die nadrukkelijk ook consequenties hebben voor de vormgeving van de politiefunctie. Maar, het fundament is helder: de democratische rechtsstaat is vol in bedrijf.

[15] In spel-theoretische termen spreken we dan van een coöperatief spel. Dit staat tegenover spelen waar een dusdanige actor ontbreekt, de zogenoemde non-coöperatieve spelen. Dat laatste betekent nadrukkelijk niet dat er geen sprake is van samenwerking (Taylor 1976).

Institutionele verhoudingen

- Er is een staat, gedefinieerd door de aanspraak op het monopolie van de legitieme toepassing van fysiek geweld binnen een welbepaald gebied. Binnen dat gebied bevindt zich een eveneens welbepaalde gemeenschap van burgers.
- De relaties tussen staten worden bepaald door macht en onderhandelingen, soms vastgelegd in verdragen (bijvoorbeeld het Cybercrimeverdrag van Boedapest) op basis van welbegrepen eigenbelang.
- De relaties tussen burgers – en tussen de staat en de burgers – worden gereguleerd door binnen dat gebied algemeen geldende wetten en regels.
- De staat kan indien noodzakelijk naleving van wetten en regels afdwingen.
- De wetten en regels zijn democratisch tot stand gekomen en voldoen aan rechtsstatelijke waarborgen.
- Er is een als legitiem ervaren balans tussen de bescherming door en bescherming tegen de staat.
- Er is formeel duidelijkheid over het gezag.
- De staat draagt zorg voor de bescherming van de gemeenschap en de daadwerkelijke handhaving van de rechtsorde.
- Andere staten en structuren hebben (vrijwel) geen rechtstreekse invloed op wat er 'aan de binnenkant' gebeurt.

Dit hele bouwwerk berust op de aanwezigheid van een hoogste autoriteit – met de bijhorende claim op het monopolie van gebruik van geweld – met een duidelijk begrensd territoir en burgers die binnen dat grondgebied wonen. Dat is ook het theater waarin de daadwerkelijke handhaving van de rechtsorde en de hulpverlening gestalte krijgt. Dat is niet alleen van fundamentele betekenis maar zeker ook voor de daadwerkelijke handhaving – openbare orde en strafrechtelijk – en voor het vormgeven van hulpverlening.

Randvoorwaarden voor de uitvoering van de politiefunctie

- Het is bekend welke burgers (identiteit) zich op het grondgebied bevinden en waar zij wonen (adres).
- Door controle aan de grens is ook duidelijk wie zich verder op dit grondgebied bevinden waarbij (indien noodzakelijk) te achterhalen is waar zij verblijven.
- De wet is helder en geldt voor iedereen, en iedereen wordt verondersteld de wet te kennen.
- Er is sprake van een delict met een dader en slachtoffer – en causaliteit kan in principe worden vastgesteld – op een welbepaald grondgebied (klassieke eenheid van plaats – tijd – handeling). De vijf klassieke beïnvloedingsvelden voor criminaliteitsbeheersing, locatie, object, omstandigheden, dader, slachtoffers (LOODS[16]) bevinden zich overwegend binnen de invloedssfeer van de rechtsstaat.
- Grondgebied is ook bepalend bij reguliere openbare orde, inclusief de heldere relatie met het gezag (burgemeester en gerelateerde regelgeving – van Algemene Plaatselijke Verordening tot Nationale Veiligheid).
- Territoir staat evenzeer centraal bij rampen en crises, met als centrale begrippen op- en afschalen, waarbij 'opschalen' overigens ook verwijst naar een toename van belang en het involveren van meer partijen, ook in de uitvoering.
- De verstoringen van de openbare orde zijn gelokaliseerd en zichtbaar, zichtbaarheid is in praktische zin onderdeel van de definiëring van openbare orde.
- De organisatie van de hulpverlening is eveneens territoriaal georganiseerd en vereist ook fysieke aanwezigheid.
- Er wordt op tal van terreinen met tal van partijen samengewerkt en waar dit de politiefunctie betreft is de politie leidend in de uitvoering.

[16] LOODS wordt gebruikt als instrument voor criminaliteitsbeheersing (Projectgroep Opsporing-2 2003, Snel & Van der Zee 2005) en risicoanalyse.

Digitalisering heeft ook in de context van de *stationaire rechtsstaat* de nodige impact op rechtsstaat en veiligheid. Dat begint bij de sociale impact van technologie: door bijvoorbeeld de smartphone is er veel veranderd in de sociale interactie en dat heeft ook zijn invloed op de handhaving van de rechtsorde. Soms is die invloed ook heel direct, bijvoorbeeld als diezelfde smartphone wordt gebruikt om politieoptreden te filmen en dat vervolgens op internet te plaatsen. Het filmen met de smartphone leidt tevens tot zeer praktische vragen, bijvoorbeeld hoe om te gaan met de opslag van deze beelden wanneer een burger deze beelden inbrengt – al dan niet in combinatie met het doen van aangifte. Dit geldt overigens ook voor de beelden die de politie zelf maakt, met de smartphone of met de *bodycam*. Sowieso maakt ook de politie steeds meer gebruik van digitale toepassingen als MEOS en een veelheid aan apps, maar ook 'ogen en oren' in de vorm van sensoren, met vooralsnog als meest bekende vorm cameratoezicht.

Verder geldt dat ook bij zogeheten klassieke misdrijven digitale sporen en technologieën een steeds grotere spelen bij de opsporing van daders, ook al wordt dat in de media soms anders gezien. Een bericht met als kop 'Google lost moord op'[17] blijkt in feite te gaan over een klassiek opsporingsonderzoek waarbij ook naar digitale sporen is gekeken. Maar ook de misdrijven zelf hebben steeds vaker een expliciet digitale component, en dat heeft soms ook een eigenstandige betekenis. Dus pesten wordt dan cyberpesten, maar dat heeft wel een paar nieuwe karakteristieken, zoals: beelden blijven altijd op internet en hebben een groot bereik, het verstoort het sociale leven 'online' en blijft dus niet beperkt tot het schoolplein, pesten komt dus ook bij je thuis en kan altijd doorgaan, slachtoffer en dader hoeven niet eens fysiek bij elkaar in de buurt te komen.

Het gaat ook hier niet alleen om criminaliteit maar ook om ongeoorloofde handelingen met het oog op de openbare orde, bijvoorbeeld opruiing via Facebook – zoals bij de zogenoemde 'blokkeerfriezen' – of ons eigen Nederlandse project-X: Haren (2012). Er zijn veel nieuwe technologische mogelijkheden waar het gaat om het verstoren van de openbare orde. Bij de kroningsrellen (1980) werd een radiozender ingezet, die kon je nog proberen 'uit de lucht te halen'. Het was minder eenvoudig (en nadrukkelijk meer omstreden) om sociale media 'uit de lucht te halen' bij de rellen in Londen (zomer 2011).

Waar het gaat om grootschalige incidenten – rampen en crisis – komt ook de impact van digitalisering steeds hoger op de agenda te staan, getuige bijvoorbeeld het WRR-rapport over digitale ontwrichting (2019). Dit geldt zeker voor wat we vitale infrastructuur noemen. De digitale dimensie krijgt daarbij in toenemende mate aandacht. Let wel, het gaat hierbij nog steeds in de eerste plaats over plaatsgebonden incidenten gerelateerd aan over het algemeen plaatsgebonden functies.

Hack_Right
In 2018 lanceerden (o.a.) politie en OM, na jaren voorbereiding, het traject Hack_Right: een eigentijdse variant op de HALT-straf, speciaal voor 'first offenders' van cybercrime. Door excuses aan te bieden en een training te volgen lopen ze geen strafblad op en blijven ze behouden als cybersecuritytalent voor de BV Nederland. De jongeren 'kiezen' voor Hack_Right omdat het alternatief een reguliere straf is.

Responsible Disclosure
Wanneer een 'white hat' (ethische) hacker in Nederland haar bevindingen tijdig en op de juiste wijze aan het gehackte bedrijf meldt en geen misbruik maakt, zal vervolging normaliter uitblijven. De politie is voorstander van zulke spontane kennisdeling die Nederland veiliger maakt. De kracht van het merk 'Politie' helpt om voorbeeldgedrag de juiste navolging te laten vinden.

[17] https://www.technischweekblad.nl/nieuws/tip-google-lost-moord-op/item13567

II. De reizende rechtsstaat

Het veld van de *reizende rechtsstaat* beschrijft de confrontatie van de rechtsstaat met de invloed van digitalisering op de territoriale grondslag van het recht en de handhaving daarvan, zoals ten dele al beschreven in het WRR-rapport *Staat zonder land* (1998). De staat is in dit veld nog altijd de centrale actor, nationaal en internationaal – maar hij heeft zich hier dus te verhouden tot andere staten, ook voor haar eigen interne processen en procedures. Hoewel de notie van de 'centrale staat' al geruime tijd ter discussie staat (Waltz 1979: 94) constateren we dat het de (machtige) staten zijn – al dan niet verenigd in geopolitieke machtsblokken – die voor een groot deel bepalen hoe onze wereld er uitziet. De staat is overduidelijk nog de centrale partij waar het gaat om rechtshandhaving. Zo kunnen staten nog steeds grote impact hebben op de grootste economische spelers (denk aan de grote technologiebedrijven) door regels te stellen en ook de naleving daarvan af te dwingen.

Omdat subjecten en fenomenen die staten willen reguleren, steeds minder grondgebonden zijn, neemt het belang van internationale samenwerking en internationale normen en verdragen sterk toe. Staten kunnen andere soevereine staten niet 'dwingen' maar wel proberen te overtuigen, met meer of minder politieke druk of vormen van wisselgeld. En, als er eenmaal expliciete afspraken zijn, hebben deze wel degelijk een ordenende werking. Bovendien, staten hebben wel autoriteit over niet-statelijke actoren. De afspraken tussen staten zijn in feite ook 'contracten' en gebaseerd op welbegrepen eigenbelang. Sommige belangen zijn universeel maar niet altijd gelijkgericht – zoals economische voordelen – maar andere staan voortdurend ter discussie zoals het belang van rechtsstatelijke waarden. De staat kan ook in het internationale systeem normstellend optreden. Voor zover mogelijk wordt daarbij gebruik gemaakt van het internationale recht. Nederland kiest hier zelfs een actieve rol, in lijn met artikel 90 van de Nederlandse Grondwet. Waar er geen aanvaard wettelijk kader in enge zin is (zoals een rechtsstaat), vormen van de rechtsstaat afgeleide algemene beginselen – zoals het Europees Verdrag voor de Rechten van de Mens (EVRM) – veelal het uitgangspunt voor normering.

Institutionele verhoudingen

- Staten (meervoud!) zijn de centrale spelers waar het gaat om de handhaving van de rechtsorde;
- Staten zijn soeverein en zijn dus de hoogste autoriteit waar het gaat om binnenlandse aangelegenheden;
- De relaties tussen staten worden bepaald door macht en onderhandelingen, soms gecodificeerd in verdragen op basis van welbegrepen eigenbelang;
- De relaties tussen burgers – en tussen de staat en zijn burgers – variëren over staten, een belangrijke scheidslijn betreft of er al dan niet gesproken kan worden van een democratische rechtsstaat;
- Er is in meer of mindere mate sprake van een internationaal juridisch regime, afhankelijk van het onderwerp. Ten aanzien van sommige onderwerpen geeft het gemeenschappelijk belang tot coördinatie de doorslag, bijvoorbeeld in de luchtvaart. Soms ook is er sprake van een gedeelde waardengemeenschap als onderdeel van de politieke gemeenschap, waarvan het Europees Verdrag voor de Rechten van de Mens (EVRM) een sprekend voorbeeld is;
- In veel gevallen is samenwerking en de voorwaarden waaronder een kwestie van gefundeerd vertrouwen, vaak omdat het gedeelde belang – of wederzijdse afhankelijkheid – duidelijk is en wordt ondersteund door het nemen van zogenoemde 'vertrouwenwekkende maatregelen';
- Landen en machtsblokken proberen hun waardenstelsels actief uit te dragen middels verdragen die hierdoor een effect kunnen krijgen op andere samenlevingen;
- De strafbaarheid van feiten is niet universeel en kan hierdoor tot onverwachte uitkomsten leiden;
- In principe geldt: 'wat gij niet wilt dat u geschiedt, doe dat ook een ander niet', maar dat principe legt het met regelmaat af tegen zwaarder wegende belangen van staten;
- Hoewel staten soeverein zijn en dus niet anders dan door macht gedwongen kunnen worden hun gedrag te wijzigen, rekent de Nederlandse staat het tot zijn opdracht de internationale rechtsorde te bevorderen;
- Er is altijd discussie mogelijk over gezag en rechtmatigheid bij optreden 'over de grens'.

Het gaat in dit veld primair om het 'oplossen' van problemen die ontstaan omdat bijvoorbeeld criminaliteit zich niet netjes houdt aan landsgrenzen met bijbehorende jurisdicties. De vijf klassieke beïnvloedingsvelden (LOODS) zijn verspreid over verschillende jurisdicties en dat stelt grenzen aan de beïnvloedingsmogelijkheden. Dader en slachtoffer zijn niet op dezelfde plek, onduidelijk is wat de link is tussen het misdrijf en de dader, of zelfs, wie de daders eigenlijk zijn, etc. Het idee is nog steeds dat er herkenbare slachtoffers zijn en daders die gestraft en gestopt moeten worden. De daden zijn 'in principe' wel strafbaar maar de handhaving is moeilijk. In de *reizende rechtsstaat* worden de voorwaarden voor optreden gevormd door verdere ontwikkeling van de nationale wetgeving in combinatie met internationale samenwerking, soms ook vastgelegd in verdragen tussen staten.

Randvoorwaarden voor de uitvoering van de politiefunctie

- Rechtshulpverzoeken en gezamenlijke opsporing (EMPACT, Joint Cybercrime Action Taskforce)
- Fysieke locatie van dader – slachtoffer – infrastructuur.
- Recherche-expertise (digitale drieslag): gedigitaliseerde criminaliteit, 'pure' cybercrime, digitale forensische expertise.
- Internationale samenwerking, o.a. INTERPOL-grondwet en Cybercrimeverdrag van Boedapest.

In de *reizende rechtsstaat* wordt het voorheen eenduidige grondgebied verlaten – wel met de waarden van de rechtsstaat onder de arm – en dat leidt tot belangrijke vragen met betrekking tot de rechtsstatelijke waarborgen en problemen rondom daadwerkelijke handhaving van de rechtsorde. Omgekeerd komen ook rechtsvragen vanuit andere jurisdicties, met soms een afwijkende rechtsopvatting, ons grondgebied binnen en vereisen deze regelmatig een politieel antwoord.

ICCOS
Het strategische belang van Nederland voor de 5 Eyes neemt toe op het moment dat het Verenigd Koninkrijk Europol verlaat. Nederland draagt al enkele jaren actief bij aan ICCOS, het samenwerkingsverband van de 5 Eyes gericht op het samen ontwikkelen van software. Door samen 'brillen' te maken waarmee ieder land naar de eigen datasets kan kijken wordt meer inzicht verkregen. Nederland promoot deze werkwijze ook internationaal via INTERPOL.

Cyberaanval (Not)Petya
Dinsdag zijn wereldwijd bedrijven en instellingen getroffen door een aanval met ransomware, ook wel gijzelsoftware genoemd. Containeroverslagbedrijf APM Terminals, dat onder meer in de haven van Rotterdam actief is, was een van de eerste bedrijven die melding maakten van een IT-storing. Volgens cyberveiligheidsbedrijf Fox-IT zijn meer Nederlandse bedrijven getroffen door de cyberaanval, genaamd 'Petya'. Volgens de Russische antivirusreus Kaspersky Lab gaat het echter niet om een nieuwe variant van dit oude virus. In Nederland zijn onder de slachtoffers pakketbezorger TNT en medicijnfabrikant MSD, die fabrieken heeft in andere landen. In het buitenland gaat het onder meer om banken en overheidsinstanties in Oekraïne en Rusland. APM en moederbedrijf Maersk melden alleen dat er IT-problemen zijn. Tegenover AP laat Maersk-woordvoerder Anders Rosendahl weten dat alle geledingen binnen het Deense bedrijf, zowel in Denemarken als daarbuiten, slachtoffer zijn van een "cyberaanval". https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693. De politie was niet welkom bij het slachtoffer en kon mede daardoor ook de veiligheid van andere getroffenen in de haven niet dienen.

III. De geprivatiseerde rechtsstaat

Het derde veld hebben we de *geprivatiseerde* rechtsstaat gedoopt. Zoals eerder uitgebreid beschreven, is er een veelheid aan actoren actief op het veiligheidsterrein en het gaat hierbij in toenemende mate om private partijen. In tegenstelling tot de klassiek grondgebonden staat vinden de dominante sociale processen in toenemende mate plaats in een digitaal stromenland (netwerken) waarbij allerlei vooral ook private partijen een rol spelen (Castells 1996). De afdwingbaarheid van gedrag bij partijen in net-

werken is gering. Het ontbreekt aan een bovenliggende partij die anderen kan dwingen zich aan afspraken te houden. Dat betekent niet dat er niet samengewerkt kan worden, het betekent alleen dat dat zonder afdwingbaarheid moet. Dat kan soms leiden tot vrijblijvendheid maar dat hoeft niet. In dit veld is de staat is nog niet geworden tot louter 'één van de spelers' en heeft deze nog steeds een bijzondere positie maar is wel in toenemende mate in concurrentie met andere, 'private instituties'.

Op wereldwijde schaal gaat het hier om de grote technologiebedrijven met als belangrijke symbolische merken de *big five*: Google, Apple, Microsoft, Amazon, Facebook. De vijf grootste merken ter wereld zijn ondertussen technologiebedrijven, waar in het vorig decennium Coca-Cola, Marlboro en McDonalds nog in de Top 5 voorkwamen[18]. Dit type bedrijven kan niet eenvoudig door staten gereguleerd worden, hoewel er ondertussen wel tegenkrachten ontstaan, bijvoorbeeld in de context van de Europese Unie. Het zijn ook spelers die eigen 'wetten en regels' maken voor wat is toegestaan op hun platforms en er ontstaan als het ware nieuwe 'sociale contracten' waar nieuwe 'burgers' – nu consumenten – akkoord gaan met soms zeer vergaande voorwaarden ten aanzien van 'persoonsinformatie' in ruil voor diensten. Een belangrijk veiligheidsvraagstuk in de geprivatiseerde rechtsstaat is 'informatieveiligheid' en daarnaast cybersecurity; en ook de 'pure' cybercrime veelal ook in de private sfeer: malware, virussen, DDoS. Ook de overheid – als één van de partijen – wordt hiermee geconfronteerd.

Institutionele verhoudingen

- Waar voorheen de staat het kader was waarbinnen marktrelaties gestalte kregen, is in dit veld het omgekeerde het geval. De markt vormt het kader waarbinnen het handelen van de staat gestalte krijgt.
- Dit is meer het geval naarmate de grondgebondenheid van de processen geringer is. Het gaat hierbij in het bijzonder om diensten en informatie – waaronder de financiële markten. Dominante economische en maatschappelijke processen spelen zich in toenemende mate af in een digitaal stromenland in plaats van op lokaliseerbare plaatsen.
- De staat gaat nog steeds in hoge mate over de grondgebonden processen, objecten en subjecten. Stromenland en plaatsen raken elkaar en daar spelen staten – of breder internationale regimes of samenwerkingsverbanden – nog steeds een rol.
- Staten hebben nadrukkelijk veel 'naar de markt gebracht' inclusief onderdelen van de maatschappelijke infrastructuur, dat maakt dat het handelingsvermogen in veel gevallen is afgenomen.
- Binnen het kader van de markt wordt 'het recht' bepaald door marktposities en privaatrechtelijke overeenkomsten. Het strafrecht – de 'harde kant' van de staat – komt meestal pas in beeld als marktpartijen daartoe aankloppen bij de overheid.
- Private partijen spelen een belangrijke rol op het veiligheidsdomein waarbij het gaat om effectiviteit, efficiency en reputatie.
- De staat heeft vooral een toezichthoudende rol.
- Het gaat niet zozeer om *government* maar vooral om *governance.*

De randvoorwaarden voor de uitvoering zijn in dit veld principieel anders van karakter dan in de twee eerder beschreven velden, waarin 'afdwingbaarheid' centraal staat. In dit veld gaat het om de volgende randvoorwaarden.

Randvoorwaarden voor de uitvoering van de politiefunctie

- Partijen – en soms ook de vraagstukken waarmee ze worden geconfronteerd – bevinden zich nog wel 'ergens' en in veel gevallen kan worden samengewerkt met relevante partijen op basis van territoir: nationaal, regionaal en lokaal.
- De beïnvloedingsvelden (LOODS) hebben nog steeds betekenis, maar de manier waarop beïnvloeding kan plaatsvinden, verandert van karakter. Er is een grotere rol voor private partijen.
- Het delen van informatie staat centraal en deelname van de politie in (in min of meer geformaliseerde) samenwerkingsverbanden genereert extra mogelijkheden.

[18] https://www.winmagpro.nl/content/de-5-grootste-merken-ter-wereld-zijn-tech-bedrijven

- Politie-informatie is met waarborgen omkleed met het oog op de rechten van betrokken burgers en later de eventuele rechtsgang. In die zin is de politie een verbindende schakel met het strafrecht. Daar gaat in sommige netwerken ook een disciplinerende werking van uit.
- De algemene politietaak wordt ruim opgevat en dat maakt dat de politie kan optreden in situaties die wellicht slecht zijn gedefinieerd maar waarbij optreden wel als noodzakelijk wordt gezien: 'we leggen het later wel uit!'. Belangrijk probleem in dit veld is dan wel dat de eventuele economische vervolgschade dan dreigt voor rekening van de staat te komen.
- Afhankelijk van de context is de politie van belangrijke symbolische betekenis – er wordt recht gedaan – en heeft zij een vertrouwenwekkende reputatie: betrokkenheid van de politie garandeert dat zaken 'volgens het boekje' worden uitgevoerd.

Centraal probleem is hier het risico van uitsluiting en het optreden van eigenrichting, naast wat ook wel *private justice* wordt genoemd: geld bepaalt wie in welke mate recht wordt gedaan. Dit kan heel subtiel gebeuren, simpelweg doordat sterke marktpartijen mensen – middelen – expertise hebben om de politie te beïnvloeden. Doelstelling van commerciële partijen is ultimo marktaandeel en winst. Er zijn natuurlijk ook niet-commerciële partijen actief, maar ook daarbij is de vraag wiens belang wordt gediend: is het een publiek belang of een eigenbelang? En hoe staat het dan met de waarden van de rechtsstaat, bijvoorbeeld in de buurtpreventie WhatsApp-groepen van burgers. De zelforganisatie en zelfwerkzaamheid staan in dit veld centraal. Het gaat vaak om veiligheidsvraagstukken waar private partijen in principe zelf voor hun veiligheid kunnen zorgen maar waarbij nog niet aan de randvoorwaarden om dat te doen is voldaan – bijvoorbeeld omdat het ontbreekt aan bewustwording of organisatie. In andere gevallen zijn partijen prima in staat hun veiligheid te organiseren maar komen de waarden van de rechtsstaat in het gedrang. Heel vaak weet de politie niet wat er in die netwerken gebeurt. Sommige van die partijen – zie de bespreking hierboven van de technologiereuzen – zijn zo groot dat het heel ingewikkeld is geworden nog in te grijpen bij schending van de waarden van de rechtsstaat. Interessant is dat een aantal van die partijen nu zelf vraagt om overheidsingrijpen om het zelfgecreëerde monster dat men niet meer onder controle heeft, te beteugelen[19].

Electronic Crimes Taskforce ('bankenteam')
Al jarenlang werken Nederlandse grootbanken en creditcardbedrijven samen om gezamenlijk opsporingsonderzoeken aan te dragen voor prioritering. Ze doen dit omdat ze onderling niet willen concurreren op veiligheid; zonder de ECTF zouden ze uit imago-angst geen aangifte doen. Dit verband werkt doordat politie en OM stelselmatig aangedragen zaken draaien.

NoMoreRansom
De Nederlandse politie is initiatiefnemer van het NoMoreRansom-platform. Op deze website is antivirussoftware te downloaden tegen allerlei verschillende soorten ransomware. Wie slachtoffer is geworden, kan hier aangifte doen en hopelijk de gegijzelde data 'bevrijden'. Het platform werkt als een magneet: er werken inmiddels tientallen bedrijven aan mee, maar ook politiediensten uit de hele wereld. NoMoreRansom is een antwoord op het vraagstuk van versplinterde oplossingen voor ransomware, een vraagstuk waar het bedrijfsleven moeilijk een eenduidig antwoord op kan formuleren. Door dit platform te initiëren, liet de Nederlandse politie zien: ransomware tolereren we als politie wereldwijd niet (begrenzen), met deze software en tips kunnen burgers zich ertegen wapenen (beschermen) en het gebruik ervan is gratis en gegarandeerd veilig, ten behoeve van een betrouwbaar internet (bekrachtigen).

[19] Met als bekend voorbeeld Marc Zuckerberg van Facebook, ervan uitgaande dat dit voorkomt uit oprechte bezorgdheid.

IV. De afwezige rechtsstaat

Het veld van de *afwezige rechtsstaat* betreft, zoals de naam al aangeeft, de situatie dat er geen rechtsstaat is en geen 'aangewezen' hoeder van de waarden van de rechtsstaat. Zeer veel wordt door de partijen zelf opgelost waarbij de klassieke politie geen rol van betekenis speelt. Heel vaak is dat niet erg, maar terug naar Bittner (1970): wat nu *als er iets gebeurt waartegen iemand zou moeten optreden en wel nu*? Het gaat om zaken waar iets 'nieuws' aan de hand is, of in ieder geval dat de karakteristieken dusdanig anders zijn dat we er niet mee uit de voeten kunnen op basis van – afgeleiden van – de traditionele aanpak. In veel gevallen willen we opnieuw begrenzen, voor een deel kunnen we wellicht dezelfde strategieën gebruiken (bewustwording, preventie, etc.) maar wellicht moeten we ook nadenken over nieuwe strategieën en vooral ook over grondslagen en criteria voor het optreden. In het vorige veld van de *geprivatiseerde rechtsstaat* komt een veelheid van motieven bij elkaar zodat op basis van vrijwilligheid een geleidelijke transformatie van de publieke sfeer – de beweging van *government* naar *governance* – vorm krijgt. In het veld van de *afwezige rechtsstaat* is dat vanuit het perspectief van de waarden van de rechtsstaat onvoldoende. Concreet gaat het hierbij bijvoorbeeld over seksuele exploitatie in het bijzonder van minderjarigen, en de bijbehorende wereldwijde verspreiding van beeldmateriaal. De grondslagen voor politieoptreden zijn vaak beperkt en van duidelijke generieke institutionele verhoudingen is geen sprake. Er wordt noodgedwongen in hoge mate gehandeld naar bevind van zaken (Wilson 1968).

In dit veld staat ook de klassieke taakverdeling markt – staat – samenleving ter discussie, en is speciale aandacht voor 'informatie' in veel gedaanten aangewezen. Dat varieert van verantwoordelijkheid voor nieuws – al dan niet *fake* – tot verantwoordelijkheid voor data. Zou de staat andere partijen moeten kunnen dwingen publieke verantwoordelijkheid te nemen? Dus, bij wijze van voorbeeld, als een organisatie de data heeft om een ongewenste situatie te beëindigen, zou zij dat ook moeten doen? We zouden dat Maatschappelijk Verantwoord Ondernemen kunnen noemen.

In de huidige situatie is dit niet eenvoudig. Enerzijds vanwege privacy, anderzijds omdat communicatiebedrijven geringe verantwoordelijkheid hebben voor de inhoud, zolang ze 'maar doen wat de politie zegt'. Dat betekent dat hier mogelijk een rol is weggelegd voor de staat om de bedrijven te helpen zichzelf de goede kant op te laten duwen. Het is een lastig spanningsveld, want er zijn zelfs '*bad hosters*', bedrijven die slim criminaliteit faciliteren, die zich verschuilen achter verschillende wettelijke verplichtingen, teneinde die criminaliteit te ondersteunen. Een ernstig voorbeeld zijn hostingbedrijven die er door het Meldpunt op gewezen worden dat er kindermisbruikmateriaal op hun servers staat, maar die dan zeggen: "(1) Dat is de verantwoordelijkheid van de gebruiker. (2) We kunnen niet zomaar in gegevens van de gebruiker kijken. (3) We kunnen niet zomaar gegevens van de gebruiker verwijderen zonder dat we zeker weten dat het illegaal materiaal betreft EN nu we weten dat het wellicht illegaal materiaal betreft, (4) kunnen we dit materiaal zelf niet bekijken om te verifiëren of het illegaal materiaal betreft, omdat we daarmee zelf illegaal materiaal aan het verwerken zouden zijn". Alleen een vordering door de politie beweegt deze bedrijven in sommige gevallen nog enigszins, omdat ze snappen dat als ze daar niet aan voldoen, er grond voor verder onderzoek/interventie zou kunnen zijn. Van een robuust geweldsmonopolie is dus geen sprake. In feite wordt hier de traditionele vormgeving van de rechtsstaat misbruikt om de waarden van de rechtsstaat te ondergraven!

De rechtsstaat is afwezig door verschillende oorzaken. Ten eerste, de staat 'kan er niet bij' en daarom is er geen controle. Dit gaat over *dark web* en *dark markets* en de alternatieve (internet) waarden en normen die in deze context bepalend zijn. Ten tweede, het is nieuw en daarom nog niet gereguleerd en/of we weten (nog) niet wat we er mee zouden willen. Ten derde, het is weliswaar strafbaar (volgens Nederlands recht) maar het ontbreekt aan een effectief handelingskader, in veel gevallen ook door aan digitalisering gerelateerde karakteristieken in termen van schaalbaarheid, impact, snelheid, enzovoort.

Institutionele verhoudingen

- Het ontbreekt aan een generiek kader en er wordt primair gehandeld naar bevind van zaken.

- De impact van *framing* / media is sterk bepalend in deze context. De klassieke instituties worstelen daar mee en worden in de publieke beeldvorming soms weggezet als onderdeel van het probleem in plaats van een deel van de oplossing. Dit is geen *formele* 'institutionele verhouding' maar wel een belangrijke dimensie van de nieuwe *informele* institutionele verhoudingen.
- Er zijn morele noties en een beroep op de staat 'er iets aan te doen'.
- Uit de aard der zaak is het soms niet mogelijk om te weten 'waar' een misdrijf plaatsvindt; bij de aanpak daarvan bestaat dan het risico dat de politie 'op de tenen van een andere staat' trapt.

Randvoorwaarden voor de uitvoering van de politiefunctie

- In dit veld zijn de klassieke beïnvloedingsvelden (LOODS) variabel en in veel gevallen ook moeilijk te definiëren. De relatie met de rechtsstaat en de klassieke handhaving van de rechtsorde ontbreekt. Er kan op voorhand niet worden gesteld wat centraal dient te staan en vanuit welk perspectief. De aandacht verschuift naar het slachtoffer en naar kwetsbaarheid.
- De inzet van oud gereedschap in een nieuwe context; met een 'hamer' kun je niet alleen een spijker inslaan maar ook een server onklaar maken – 'roeien met de riemen die je hebt'.
- Waarde-gedreven professioneel optreden dat voldoende vertrouwen geniet.
- In toenemende mate technologische of door techniek ondersteunde oplossing, van slimme camera's tot risicoanalyses.

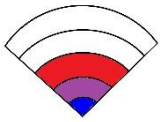
Hansa Market
In 2017 haalde de politie met de FBI twee illegale marktplaatsen neer, maar niet tegelijkertijd. Achterdochtige handelaren ontvluchtten de marktplaats die in handen was van de FBI, om te belanden op de marktplaats die door Nederland was overgenomen... Toen die óók onderuit werd gehaald, gooiden veel criminele handelaren de handdoek in de ring, bleek uit TNO-onderzoek.

4.3 De rechtsstaatwaaier als hulpmiddel

In de voorgaande paragrafen hebben we een uitgebreide karakterisering gegeven van de vier velden van de rechtsstaatwaaier, die samen een nieuw 'wereldbeeld' vormen. Die exercitie is geen doel in zichzelf, maar moet ten dienste staan aan het beantwoorden van de vraag of vragen die ten grondslag liggen aan de exercitie. In lijn met de RADAR moet de constructie van het nieuwe wereldbeeld voldoende houvast geven om in het volgende hoofdstuk iets te kunnen zeggen over de verhouding tussen de politiefunctie, de inlichtingenfunctie en de defensiefunctie en over de vraag welke posities de politieorganisatie – als de partij die traditioneel het leeuwendeel van de politiefunctie uitoefent – zou kunnen of moeten innemen. Hoe dat zou kunnen werken laten we in het volgende schema zien. Daarin hebben we één aspect uitgelicht – LOODS – om te laten zien dat dit in de vier onderscheiden contexten een andere invulling krijgt.

Stationaire rechtsstaat	*Reizende rechtsstaat*	*Geprivatiseerde rechtsstaat*	*Afwezige rechtsstaat*
Locatie, object, omstandigheden, dader, slachtoffer (LOODS)			
Er is sprake van een delict met een dader en slachtoffer – en causaliteit kan in principe worden vastgesteld – op een welbepaald grondgebied. Locatie, object, omstandigheden, dader, slachtoffers (de klassieke beïnvloedingsvelden) en hun onderlinge relaties bevinden zich overwegend binnen de invloedssfeer van de rechtsstaat. Er is helderheid over de rechtsorde en wat daadwerkelijke handhaving daarvan inhoudt. Het delict staat centraal.	Criminaliteit houdt zich niet aan landsgrenzen en bijbehorende jurisdicties. Locatie, object, omstandigheden, dader, slachtoffers zijn verspreid over jurisdicties en dat beperkt de beïnvloedingsmogelijkheden. Dader en slachtoffer zijn niet op dezelfde plek, onduidelijk is wat de link is tussen delict en dader, of zelfs, wie de daders zijn. Het idee is nog steeds dat er herkenbare slachtoffers zijn en dat daders gestraft en gestopt moeten worden. De daden zijn 'in principe' wel strafbaar maar de opvolging is moeilijk. Voorwaarden voor optreden zijn afhankelijk van verdere ontwikkeling van de nationale wetgeving in combinatie met internationale samenwerking soms vastgelegd in verdragen tussen staten. De aandacht verschuift van delict naar dader en locatie.	De vijf beïnvloedingsvelden hebben nog steeds betekenis, maar de manier waarop beïnvloeding kan plaatsvinden, verandert van karakter. Het delict als uitgangspunt van denken wordt hier losgelaten. Onduidelijk is wat de link is tussen delict en dader, of zelfs, wie de daders eigenlijk zijn. De focus verschuift naar private partijen van wie meestal niet kan worden 'geëist' overstijgende publieke belangen te dienen, maar private partijen kunnen wel worden gestimuleerd om dat te doen. De staat kan de context veranderen door wetgeving. De aandacht verschuift naar object en omstandigheden: waar is het handelen op gericht – bijvoorbeeld het verkrijgen van persoonsgegevens – en welke omstandigheden zijn bepalend – bijvoorbeeld de kwaliteit van de beveiliging	De vijf beïnvloedingsvelden zijn variabel en in veel gevallen ook moeilijk te definiëren. De relatie met de rechtsstaat en de klassieke handhaving van de rechtsorde ontbreekt. Er kan op voorhand niet worden gesteld wat centraal dient te staan en vanuit welk perspectief. De aandacht verschuift naar het slachtoffer en diens kwetsbaarheid
Delict	**Dader en locatie**	**Object en omstandigheden**	**Slachtoffer**

5 Positionering en de consequenties daarvan



In hoofdstuk 4 hebben we de vier velden van de rechtsstaatwaaier geschetst. Daarmee hebben we de twee buitenste lagen van de RADAR van inhoud voorzien. In dit hoofdstuk richten we ons vooral op het vullen van de volgende laag van de RADAR, die van positionering, waarbij we ook de verbinding leggen met aspecten van handelen en organisatie (laag 4 en 5). Daarbij komt de in de eerste plaats de in het voorwoord gestelde vraag weer naar voren: *Wat betekent de geschetste context voor het acteren van partijen in het licht van de waarden van de rechtsstaat en het leveren van maximale toegevoegde waarde aan veiligheid?* En, hoe moet de politie zich dan opstellen ten opzichte van andere relevante partijen? Het gaat dan uiteindelijk om de positie van de politie in samenwerkingsrelaties. De centrale vraag is daarbij steeds: *Wat draagt de politie bij aan (sociale) veiligheid ten opzichte van wat anderen (kunnen) doen en wat zou dat kunnen betekenen voor die anderen.* Bij 'partijen' gaat het dan vooral om de volgende functies: krijgsmacht, inlichtingenwezen, marktpartijen, en niet zozeer om afzonderlijke instituties.

In de volgende paragrafen plaatsen we de functie van de politie in de verschillende velden van de waaier en onderzoeken we wat in deze vier contexten de toegevoegde waarde van de politie kan zijn. Let wel, dit levert geen blauwdruk op, noch een afbakening van kerntaken, maar geeft richting aan de ontwikkeling die kan worden ingezet. Dat laatste steeds nadrukkelijk in relatie tot andere spelers op het veld.

5.1 De stationaire rechtsstaat

In dit veld is de rechtsstaat in vol bedrijf en gaat het vooral over hoe om te gaan met digitalisering en daar daaraan verbonden sociaal maatschappelijke consequenties. Het politieoptreden is in hoge mate klassiek en gericht op het maximaal bijdragen aan sociale veiligheid. De digitalisering vraagt dat de politie als het ware meebeweegt en haar achterstand inloopt. Het gaat hier in feite om relatief eenvoudige aanpassing om ervoor te zorgen dat de politie voldoende aangesloten blijft bij de samenleving, in die zin *business as usual*.

In de stationaire rechtsstaat is de verhouding tussen de veiligheidsfuncties zoals beschreven in hoofdstuk 3. Kortweg, als volgt.

- De politiefunctie betreft de daadwerkelijke handhaving van de rechtsorde op het grondgebied van de staat. De politie richt zich op (binnenlandse) slachtoffers/burgers en bedrijven, die aangifte hebben gedaan en gebruikt digitale technieken bij de oplossing van ambtshalve vervolgbare misdrijven.
- De defensiefunctie betreft de verdediging van de staat tegen dreiging van buiten de staat; en indien noodzakelijk het verlenen van bijstand binnen de staat onder civiele aansturing.
- De inlichtingenfunctie betreft de inzet van bijzondere bevoegdheden voor het verkrijgen van informatie in binnen- en buitenland nodig voor het beschermen van de integriteit en het voortbestaan van de staat en de rechtsorde.
- De private veiligheidsfunctie geeft aan dat van private partijen en burgers verwacht mag worden dat zij binnen de rechtsstaat zorgdragen voor de eigen veiligheid en dat de staat in beeld komt daar waar veiligheid een zogeheten collectief goed is.

De toegevoegde waarde van de politie komt in hoge mate voort uit de mogelijkheid tot de gelegitimeerde uitoefening van geweld en de opsporingsbevoegdheden. Het zijn de hoofdpijnvrije (delen van) dossiers waarin korte klappen gemaakt kunnen worden omdat de politie situaties zelf het hoofd kan bieden, vanuit haar 'ondergeschiktheid met gezag'. Dit behelst bijvoorbeeld kleinere digitale criminaliteit waarbij verdachten in Nederland worden geïdentificeerd, zoals scholieren die online hun school aanvallen. Het gaat dan om veelvoorkomende criminaliteit die vanuit een lokale oriëntatie kan worden aangepakt, bij voorkeur door programmasturing (PIO 2005) gericht op de bestrijding van een fenomeen. Het gaat hier

heel concreet om bevestiging van de norm op zaken die burgers rechtstreeks raken. Dit kan ook betekenen dat fors wordt ingegrepen om een einde te maken aan een ongewenste situatie, zoals de betreding – door de politie – van een server met het oogmerk om illegale informatie rechtstreeks ontoegankelijk te maken. Hierbij moet vanzelfsprekend vooraf aan rechtsstatelijke waarborgen worden voldaan.

Het optreden van de politie heeft hier een belangrijke symbolische betekenis, namelijk het afgeven van een helder signaal dat digitalisering niet betekent dat vrijplaatsen noodgedwongen moeten worden geaccepteerd. Met andere woorden, internet is geen toezichtvrije ruimte. De politie staat voor de waarden van de rechtsstaat door ongeaccepteerd gedrag daadwerkelijk te begrenzen en te stoppen. Dit kan worden gevat onder de noemer 'digitale handhaving'.

De partners die de politie in dit veld tegenkomt, zijn 'oude bekenden'. Het zijn partijen uit de strafrechtketen, waaronder de reclassering, domein-specifieke partijen, zoals NCSC/DTC[20], en meer lokaal georiënteerde organisaties. De politie is 'hofleverancier' van het Openbaar Ministerie en andere activiteiten zijn daar veelal van afgeleid. De politie sluit aan bij lokale initiatieven onder gezag van het bestuur, waarbij de toegevoegde waarde van de politie – gegeven het geweldsmonopolie en de opsporingsbevoegdheden – voortvloeit uit haar aanwezigheid in de frontlinie en een daarop toegespitste professionaliteit, alsmede de daarvan afgeleide informatiepositie en haar maatschappelijke verankering.

Omwille van het behoud van haar toegevoegde waarde, dient de politie ook in de gedigitaliseerde samenleving te zorgen voor een stevige maatschappelijke verankering. Dat is een noodzakelijke voorwaarde voor handhaving en dat betekent ten minste dat burgers en organisaties de politie kunnen bereiken als zij de politie nodig hebben of iets willen melden. Daarnaast dient de politie zelf te weten wat er speelt door – zoals gesteld – aanwezig te zijn in de frontlinie van de gedigitaliseerde samenleving en tevens te beschikken over een daarop toegespitste professionaliteit. Een belangrijk aspect van professionaliteit in de frontlinie is het correcte gedrag dat procedureel op orde is. Procedurele legitimiteit is in dit veld cruciaal.

Nederlanders vertrouwen op de politie als 'instituut' en dit vertrouwen is zeer waardevol in de gedigitaliseerde samenleving. Behoud van vertrouwen veronderstelt in het licht van het bovenstaande in ieder geval het volgende op het niveau van de organisatie.

- Een adequate digitale intake-functie als noodzakelijke – maar niet voldoende – voorwaarde voor maatschappelijke verankering;
- Voldoende – tijdig beschikbare – digitale deskundigheid en verankering daarvan in geografische structuren zodat burgers het vertrouwen in de politie ook op dit domein behouden;
- Het prioriteren van tegen haarzelf gepleegde cybercriminaliteit indien deze ook burgers kan raken;
- Een optimale bescherming van digitale politiegegevens, niet alleen tegen digitale inbreuken maar ook tegen vermenging met niet-politiegegevens;
- Het vervullen van een voorbeeldfunctie waar het gaat om rechtsstatelijke waarborgen.

Dit laatste is van belang in twee opzichten: de kwaliteit van structurele digitale toepassingen en het rechtsstatelijk optreden van de professionals. Ten aanzien van de toepassingen gaat het hierbij bijvoorbeeld om het waarborgen van privacy. Het gaat daarbij niet alleen om een deugdelijke visie maar vooral ook om de mate waarin daaraan uitvoering wordt gegeven. Dat laatste zou geen keuze moeten zijn, maar een randvoorwaarde voor de inzet van technologie, zoals de verplichting van de ontwerpprincipes van *Privacy & Security by Design* bij elke gehanteerde toepassing.

Met betrekking tot de professionals betekent digitale deskundigheid altijd ook een scherp oog voor de bijbehorende rechtsstatelijke waarborgen en de risico's daaromtrent. Digitaal vaardige dienders hebben nu niet altijd voldoende zicht op de beperkingen in internetgebruik voor de politietaak. Daarnaast is door de verbondenheid van internet de landsgrens zo overschreden met als het potentieel ernstige risico dat

[20] Zie Hoofdstuk 2, par. 2.

een politieambtenaar actief is in het buitenland zonder dit te beseffen. Tot slot zouden de klassieke begrippen subsidiariteit en proportionaliteit ook integraal onderdeel moeten uitmaken van de afwegingen bij de voornoemde digitale handhaving. De directheid van deze activiteiten maakt expliciete verantwoording van – 'controle op' – de proportionaliteit van de inzet nodig.

5.2 De reizende rechtsstaat

Veel complicaties in het digitale domein vinden hun oorsprong in de fragmentatie van een zaak over verschillende jurisdicties, zoals geïllustreerd met LOODS. Kenmerkend voor dit veld is vooral dat landsgrenzen worden overschreden en de gevolgen die dat heeft voor de feitelijke handhaafbaarheid van de rechtsorde en de daarmee verbonden rechtsstatelijke waarborgen.

De verhouding tussen de veiligheidsfuncties in de reizende rechtsstaat kan als volgt worden geschetst.

- De politiefunctie krijgt hier vooral vorm door internationale politiesamenwerking in het kader van opsporing en bij (terroristische) dreiging. Dit in meer of minder georganiseerd verband: politie-politie-informatie, formele rechtshulpverzoeken, Europol, INTERPOL. Daarbij speelt het uitwisselen van informatie een hoofdrol, wat gepaard gaat met een aantal dilemma's; tussen grondrechten en veiligheid (ook van mogelijke betrokkenen in andere jurisdicties in de toekomst) / tussen 'instemming' (*consent*) en 'beheersing' (*control*)[21], tussen rechtsgemeenschap en staat. Onderdeel van dit spanningsveld is ook de afbakening tussen de inlichtingenfunctie en de politiefunctie.
- De defensiefunctie heeft hier nadrukkelijk een relatie met de internationale rechtsorde en ook met het optreden in het buitenland met het oog op de binnenlandse veiligheid. De Nederlandse regering ziet een rol voor de Nederlandse staat weggelegd als het gaat om het bestendigen van de rechtsorde 'in het digitale domein: zij wil een "leidende rol spelen bij het toepassen en versterken van een internationaal normatief kader voor de regulering van cyberoperaties tussen staten" (TK 2018-2019, 33694, nr. 47). De krijgsmacht is zeer actief op wat het cyberdomein wordt genoemd waarbij het onderscheid tussen binnen- en buitenland vaak niet – en zeker niet op voorhand – helder is. Binnen de defensiefunctie geldt – net als bij de politiefunctie – dat informatie en inlichtingen een steeds belangrijker rol spelen. De defensiefunctie krijgt bijna zonder uitzondering gestalte binnen internationale samenwerkingsverbanden, meer of minder geïnstitutionaliseerd, overigens ook met alle risico's van dien.
- Het belang van de inlichtingenfunctie in dit domein is groot en groeiende, waarbij onder invloed van digitalisering inlichtingendiensten ook in toenemende mate uitvoerende partijen zijn geworden[22].
- De private veiligheidsfunctie heeft hier vooral betrekking op de (vermeende) relatie tussen enerzijds (wereldwijde) technologiebedrijven en serviceproviders en anderzijds staten, en de nationale kwetsbaarheden die daar mogelijk mee gemoeid zijn.

De toegevoegde waarde van de politie is nog steeds verbonden met de mogelijkheid tot de gelegitimeerde uitoefening van geweld en de opsporingsbevoegdheden. Maar, wanneer onderdelen van een delict op andermans grondgebied plaatsvinden, komen rechtshulpverzoeken, internationale verdragen en dito samenwerkingsverbanden in beeld om informatiesturing mogelijk te maken. In de reizende rechtsstaat is een traditioneel aandachtsgebied – internationaal – enorm in belang toegenomen. Dat betekent ook dat herbezinning op (deel)functies noodzakelijk is, mede gezien het gemak waarmee vanuit andere jurisdicties aan 'zijsturing' gedaan kan worden met behulp van rechtshulpverzoeken. Dat neemt niet weg dat de politiefunctie zich richt op dader en locatie, en in die zin grondgebonden blijft. Daarbij gaat het nog steeds primair over het vorm en inhoud geven aan bevoegdheden in de context van een rechtsstatelijk regime.

Hoewel grensoverschrijding en rechtshulpverzoeken al veel langer spelen, is internationale samenwerking toch iets dat zich vooral afspeelt in de marge van de politieorganisatie en (nog) niet in het centrum.

[21] Zie Hoofdstuk 3, par. 2.
[22] Zie: Huub Modderkolk (2019), Het is oorlog maar niemand die het ziet.

Meer hierin investeren en het versterken van rechtsstatelijke waarborgen bij internationale samenwerking is van groot belang. Een belangrijk probleem is dat buitenlandse politiediensten niet tot inzet kunnen worden verplicht, terwijl hun bevoegdheden wel noodzakelijk zijn. Omgekeerd geldt dit ook bij rechtshulpverzoeken vanuit het buitenland. Dat vraagt om actieve opstelling binnen de intelligence- en opsporingsgemeenschap.

Met betrekking tot het leveren van toegevoegde waarde in een internationale context is van belang dat in Nederland (met Amsterdam als hub) veel internetverkeer samenkomt. Dat maakt de Nederlandse politie een interessante partij voor internationale collega's. De ervaring leert dat Nederland het goed doet als medetrekker in gevarieerde multilaterale coalities: één voor allen, allen voor één. Natuurlijke partners in dit veld zijn andere landen via rechtshulpverzoeken, politie-politie-informatie, Europol, het Cybercrime-verdrag van Boedapest, INTERPOL en de G7.

Nederland heeft dus een strategische positie in het internationale internetverkeer en is goed toegerust wat betreft technologische voorzieningen, taalonderwijs en juridische grondslagen. Door een positiefkrachtige houding aan te nemen en te investeren in capaciteit voor internationale samenwerking, slaagt de Nederlandse politie er niet alleen in om zaken opgelost te krijgen, maar versterkt zij ook buitenlandse politiediensten met kennis en kunde én is de politie in staat mensenrechten te behartigen.

De focus op dader/locatie en op de bevoegdheden in de context van een rechtsstatelijk regime maken dat de politie niet primair gericht is op bescherming van de vitale infrastructuur. Andere partijen zijn daarvoor beter toegerust en kunnen in positie worden gebracht. Ook de afbakening van wat de politie doet ten opzichte van wat de inlichtingendiensten doen, dient te worden bewaakt. Deze verdeling veronderstelt dat er, wanneer er zich een mogelijk 'digitaal' veiligheidsprobleem voordoet, helderheid is over de aard van dit probleem en wie het probleem veroorzaakt. Dat vraagt per geval om een definitie van de situatie, een vorm van triage, op grond waarvan vervolgens kan worden bepaald wie er '*in the lead is'* om het gesignaleerde probleem het hoofd te bieden.

Het behouden van toegevoegde waarde voor burgers en bedrijven vormt in dit veld een uitdaging. Het probleem is dat *nationale* politie de neiging heeft zich vooral op *nationale* aangelegenheden te richten, in heel veel gevallen ten koste van lokale aandacht, terwijl de aandacht juist zou moeten uitgaan naar *internationaal* en *lokaal*[23]. In de gedigitaliseerde samenleving blijven uiteindelijk alleen de leefomgeving en de wereld over als relevante schalen en dit leidt tot de noodzaak tot een gelijktijdige schaalvergroting en schaalverkleining (Raad voor het openbaar bestuur 2003: 22). Het nationaal niveau is, in navolging van het provinciale, steeds meer een noodzakelijke hulpstructuur tussen het hogere en het lagere niveau, maar ook niet meer – of minder – dan dat. Een perspectiefwijziging is dus aangewezen: niet alle aandacht naar nationaal, maar juist naar internationaal en lokaal – met inachtneming van de op nationaal niveau geïnstitutionaliseerde rechtsstatelijke waarden.

In dit veld bestaat immers het risico de rechtsstaat 'onderweg te verliezen'. En, dat gebeurt sluipenderwijs, als volgt:

- Het gevaar bestaat dat Nederland zich in haar onderzoeken laat zijsturen door landen die de politie door middel van rechtshulpverzoeken wijzen op 'voor Nederland interessante' data.
- Bij informatiedeling moet rekening gehouden worden met het risico dat informatie gedeeld wordt met partijen die hieraan gevolgen verbinden die strijdig zijn met de mensenrechten. Hoe zwaar dit weegt en op welke wijze de afweging wordt gemaakt is een belangrijk issue.
- Zaken met een internationale component komen niet vaak voor een Nederlandse of Europese rechter, zeker niet als er geen dader is opgespoord (maar bijvoorbeeld wel aan verstoring is gedaan). De vraag is dan ook hoe de inzet van gebruikte opsporingsmiddelen wordt getoetst? Bovendien: geen rechtszaak betekent geen jurisprudentie. De vraag is hoe hier mee om te gaan.

[23] We kunnen stellen dat dit in feite de belangrijkste inhoudelijke reden was om over te gaan tot het formeren van één Nederlandse politie.

Aandacht voor de rechtsstaat kan worden weggezet als naïef – en ernaar verwijzen als plichtmatige teksten voor de bühne. Het is echter de kern van de toegevoegde waarde van de politie in dit domein, en het is bepalend voor de ontwikkeling van de politiefunctie op lange termijn. Dit betreft in het bijzonder behoud van zuiverheid in de relatie met de inlichtingendiensten.

5.3 De geprivatiseerde rechtsstaat

In de geprivatiseerde rechtsstaat is de toegang tot steeds meer essentiële gegevens in handen geraakt van andere partijen dan de politie. Dit heeft tot gevolg dat de politie in de uitvoering van de functie afhankelijk is geraakt van toegang tot data, die deze bedrijven en organisaties om verschillende redenen niet altijd willen of kunnen delen. Tegelijkertijd valt de waarachtigheid van de gegevens ook steeds minder goed vast te stellen. Ondanks een intussen lange traditie van samenwerken wordt hier een principieel andere opstelling van de politie gevraagd. Nieuw is dat samenwerking *noodzakelijk* is voor de uitvoering van de functie terwijl de politie medewerking niet (of moeilijk) kan afdwingen. Dit veld is onder invloed van digitalisering en internationalisering enorm aan belang toegenomen.

In de geprivatiseerde rechtsstaat is de verhouding tussen de veiligheidsfuncties, als volgt.

- De politiefunctie krijgt in toenemende mate gestalte in bijzondere opsporingsdiensten en toezichthouders. Daarnaast worden er – vooral ook omdat hoog-specialistische kennis en specifieke aanpakken nodig zijn – aparte organisatieonderdelen in het leven geroepen. De verhouding met de private veiligheidsfunctie is een belangrijk vraagstuk, zowel waar het gaat om het delen van informatie maar ook – heel praktisch – om het kunnen aantrekken en behouden van gekwalificeerde mensen.
- Voor zowel de defensiefunctie als de inlichtingenfunctie vervaagt het onderscheid tussen statelijke en niet-statelijke actoren, en mogelijk ook tussen belangen van nationale veiligheid en andere politieke en economische belangen. Juist hier is de impact van digitalisering voelbaar. Nederland loopt in een aantal opzichten behoorlijk ‘voorop’ omdat het ook relatief vroeg was met het omarmen van de mogelijkheden die digitalisering biedt aan een hoogontwikkeld handelsland met een relatief beperkt grondgebied en dito bevolkingsomvang.
- Waar het gaat om informatieveiligheid staan (grote) bedrijven centraal. In reactie op de gedigitaliseerde samenleving worden er echter ook tal van initiatieven ondernomen door andere publieke, semipublieke en non-gouvernementele organisaties – en door burgers zelf – om veiligheid vorm te geven.

Met betrekking tot de toegevoegde waarde van de politie is van belang dat de politie over een unieke (beschermde) verzameling van informatie beschikt, die wordt samengesteld met oog op toetsing door de rechter. De politie kan opsporingsinformatie en *intelligence* samenbrengen met oog op waarheidsvinding en kan dan bijzondere opsporingsmiddelen en geweld inzetten. Ze kan slachtoffers helpen met haar forensische en operationeel-juridische expertise en haar grote internationale netwerk. Vanzelfsprekende partners hierbij zijn NCSC (J&V), DTC (EZK), bedrijfsleven, en partijen gekoppeld aan de zogeheten vitale infrastructuur (de vitale sectoren), al dient het primaat daar bij defensie te liggen.

Het Nationaal Cyber Security Centrum faciliteert samenwerking tussen partijen in de vitale sectoren, zowel publiek als privaat, onder meer door per sector regelmatige bijeenkomsten tussen beveiligingsautoriteiten te houden (ISAC’s), waarbij de politie aanhaakt. Daarmee geeft de politie op operationeel niveau invulling aan wat in PIO (2005) *policing of communities* is gedoopt. Het betreft hier het onderhouden van contacten met verschillende gemeenschappen, waaronder ook overheidsorganisaties en het bedrijfsleven (via koepels als VNO-NCW en MKB-Nederland en via sector- en brancheorganisaties) ter versterking van de informatiepositie en om ‘in vredestijd’ contacten te leggen die als het erom spant, kunnen worden benut. Uit het oogpunt van effectiviteit is het wellicht nuttiger dat de politie dit ‘netwerken met vitaal’ overlaat aan defensie, zoals in sommige ISAC’s al wordt gedaan.

Succes en noodzaak van publiek-private samenwerking zijn zo groot bevonden dat de politie in 2019 voor elke politie-eenheid liaisons heeft aangesteld, om de lokale spelers te kennen en zelf door hen gekend te worden. Hun taak is om verbinding te leggen met inachtneming van het politiële gewelds- én gegevensmonopolie. Hierbij geldt dat nooit alles mogelijk is wat organisaties willen, maar door hun wensen en suggesties bijeen te brengen, kunnen wel successen worden geboekt. Enerzijds gaat het dan om directe opsporingsonderzoeken, anderzijds om rapportages in het kader van signaleren & adviseren, waarin de politie het door publieke en private partijen opgeroepen beeld kan ondersteunen.

Voor het behouden van toegevoegde waarde is van belang hoe de politie publiek-private samenwerking vorm en inhoud geeft, en waarom zij dat doet. Tot nu toe gaat veel aandacht uit naar 'beveiliging' en dat behoort niet tot de kern van de politiefunctie. De politie dient een heldere eigen koers te varen: wat vindt zij belangrijk en waar sluit zij bij aan, en waarom? Vooralsnog is dat in hoge mate ongericht. Opnieuw gaat het hier in de eerste plaats om de rechtsstaat, of in de woorden van de korpschef 'het toevoegen van rechtvaardigheid'. De politie dient toezicht te houden waar *private justice* in beeld dreigt te komen. Zij dient ook private partijen aan te spreken op hun eigen verantwoordelijkheid iets op te pakken op grond van informatie waarover die partijen beschikken. Daar kan de politie nadrukkelijk assertiever in worden.

Daarmee geeft de politie (nieuwe) invulling aan signaleren & adviseren, en het uitdragen van de boodschap idealiter samen met andere (publieke) partijen en het gezag. De politie doet hier dus een stap naar voren: proactief en gericht. Om met Tjeenk Willink (2019) te spreken, de politie moet geen manusje van alles worden en daadwerkelijk staan voor de waarden van de rechtsstaat. Zo kan de politie een belangrijke rol spelen bij het vormgeven van een meer integrale benadering van veiligheidsvraagstukken: partijen organiseren waar dat node wordt gemist en toezicht houden op hun rechtsstatelijke houding en handelen.

Op het niveau van de organisatie vraagt dat wel aandacht voor het volgende.

- Bij interacties met rechtspersonen is het van belang dat privacy, beveiliging en alle juridische waarborgen – bijvoorbeeld: welk regime geldt voor uitwisseling van gegevens: AVG of WPG? – glashelder zijn. Dit geldt tevens voor enige uitwisseling met de bedrijfsvoering van de politie zelf: het politiedienstencentrum (PDC) geldt in dit opzicht juridisch gezien als een externe burgerpartij, met wie geen inhoudelijke politie-informatie gedeeld mag worden.
- Het publiceren van informatie vanuit de politie zonder acute politiële noodzaak kan leiden tot concurrentievervalsing; sectorgewijs werken kan dit probleem verminderen.
- Een grotere rol voor private partijen kan ook leiden tot strategisch gedrag van partijen, door wie politie-inzet wordt uitgelokt om voordeel te behalen of concurrenten te schaden (zoals ook criminelen over andere criminelen lekken naar de politie voor eigen gewin). Dit onderstreept het belang van een heldere, eigenstandige lijn die de politie volgt en duidelijkheid over ieders rol.
- Onder geen beding mogen andere partijen middelen – bijzondere opsporingsbevoegdheden – inzetten zonder tussenkomst van politie en OM. Dat een verzekeringsmaatschappij rechtstreeks zaken aanlevert bij het OM, is een vorm van eigenrichting en daarmee ongewenst.

5.4 De afwezige rechtsstaat

In de *afwezige rechtsstaat* is er geen 'aangewezen' hoeder van de waarden van de rechtsstaat. Zeer veel wordt door de partijen zelf opgelost (of niet) waarbij de klassieke politie geen rol van betekenis speelt. De vraag is wat te doen als zich ongewenste situaties voordoen, die om ingrijpen vragen, maar waartoe de traditionele benaderingswijzen niet adequaat zijn en onhelder is welke partijen zouden moeten ingrijpen. De verhouding tussen de veiligheidsfuncties is in de afwezige rechtsstaat problematisch. Het klassieke onderscheid tussen de verschillende veiligheidsfuncties (inlichtingen, defensie, politie en privaat) lijkt zeggingskracht te hebben verloren. Dat blijkt wel uit het feit dat additionele functies worden

ingebracht in de richting van '*whole of government'*[24] *(publiek-publiek)* of zelfs *'whole of society'* (*publiek-privaat*) benaderingen.

Met betrekking tot de toegevoegde waarde van de politie en haar relatie tot partners is het volgende van belang. Er zijn 'ongure plekken' op het internet – vrijplaatsen, het *dark web* – waar criminelen denken dat ze de dienst uitmaken en ongestoord met elkaar misdrijven kunnen voorbereiden en plegen. Wáár die plekken precies zijn, onder welke jurisdictie ze vallen, is vaak moeilijk te zeggen, en dat geldt nog meer voor de vraag wie zich daar precies ophouden. Zodra de politie voldoende details kent over wat zich in het zogeheten *dark web* afspeelt, bijvoorbeeld via informatie-gestuurde opsporingsactiviteiten, ontstaat er meer grip op de situatie. Dan kan worden bepaald welke criminele hangplekken in aanmerking komen voor een digitaal-nodale aanpak, bijvoorbeeld op basis van de verdenking dat hierbij Nederlanders actief zijn, de gebruikte infrastructuur (servers) zich op Nederlands grondgebied bevindt en data in Nederland zijn opgeslagen.

In feite zijn we in dat geval terug in de velden waar de rechtsstaat in meer of mindere mate 'aanwezig' is. De politie komt dan weer in haar traditionele rol te staan ten opzichte van het Openbaar Ministerie en zij maakt gebruik van haar traditionele bevoegdheden. Doordat veel internethosting in Nederland plaatsvindt, heeft de politie over veel criminele vrijplaatsen jurisdictie. De politie heeft sinds 2019 bevoegdheden om harder te kunnen optreden op vrijplaatsen. Het bij een breed publiek bekend maken van dergelijke acties leidt tot normstelling in de maatschappij.

Een ander aangrijpingspunt voor het uitoefenen van de politiefunctie in dit veld is het feit dat criminelen bij hun internetactiviteiten gebruik maken van de mogelijkheden voor versleutelde communicatie (cryptografie). Dat biedt hun zowel voordeel in de zin van afscherming van hun onderlinge berichtenverkeer als nadeel: door de versleutelingen is het ook voor misbruikers van het internet vaak onzeker met wie ze eigenlijk te maken hebben, terwijl hun wijze van werken vooral stoelt op onderling vertrouwen. De politie slaagt er regelmatig in dit vertrouwen te ondermijnen door middel van activiteiten waarmee ze laat zien dat ook in de donkerste krochten van het internet rekening gehouden dient te worden met de waarden van de Nederlandse rechtsstaat. Hoe optreden tegen ongewenste situaties verbonden met internet eruit ziet, is nog veelal onvoorspelbaar, wat samenhangt met het feit dat er geopereerd wordt in onontgonnen gebied. De partners met wie wordt samengewerkt en de inhoud van de samenwerking verschilt van geval tot geval. Het gaat dus om gelegenheidscoalities met uiteenlopende partijen, zoals onderzoeksinstellingen, antivirusbedrijven en andere opsporingsdiensten.

Het slecht gedefinieerde en onvoorspelbare karakter van wat er gebeurt – en hoe er moet worden opgetreden en door wie – betekent in zekere zin dat we weer terug zijn bij de oorspronkelijke politiefunctie zoals ooit beschreven door Banton (1964) en aangehaald in hoofdstuk 3: de politie als *peace officer*. Maar, het bewaren van de vrede krijgt nu gestalte in een nieuw veld; in een nieuwe context met andere karakteristieken. Daarbij wordt een breed handelingsrepertoire ingezet om de vrede te bewaren en te voorkomen dat het recht van de sterkste de norm wordt. Zoals eerder beschreven, een heldere wettelijke grondslag ontbreekt, evenals duidelijkheid aan wie over het optreden verantwoordelijkheid moet worden afgelegd. Daarnaast wordt de politie in dergelijke situaties door de criminele actoren vaak beschouwd als 'een van de vele tegenstanders' (ook omdat vaak niet meteen duidelijk is dat de politie een actie onderneemt), hetgeen tegenzetten en andere nieuwe risico's oplevert. Helder is dat het ook in dit veld gaat om situaties die vragen om ingrijpen, bijvoorbeeld omdat er slachtoffers vallen en schade wordt aangericht: "*something-that-ought-not-to-be-happening-and-about-which-someone-had-better-do-something-now*".

[24] De zogeheten "Whole-of-Government Approach" (WGA) verwijst naar gezamenlijke activiteiten van verschillende ministeries, overheidsdiensten en publieke instanties om een gezamenlijk een oplossing te bedenken voor een bepaald probleem of issue.

Het behouden van toegevoegde waarde voor de politie in situaties met onvoorspelbare tegenstanders, veel variatie en flexibiliteit vraagt om een duidelijk ‘moreel kompas’ voor de organisatie in de vorm van de waarden van de rechtsstaat: vrijheid, gelijkwaardigheid en rechtvaardigheid. Concrete vragen als:

- Mag de politie ongewenste situaties tegenhouden door ze te verstoren (begrenzen) en een positieve sociale normering bevorderen (bekrachtigen)?
- Waar probeert de politie vertrouwen te ondermijnen en waar zou zij dit juist moeten versterken?
- Maken we nieuwe instituties vanuit een ‘nieuwe natuurstaat’, maar wellicht deze keer zonder centraal gezag?
- Hoe werkt dat en onder welke condities kan ‘het goede’ het winnen van ‘het kwade’?
- Met welke ‘goeden’ doen we dit en hoe houden we er zicht op dat die partijen de rechtsstaat volgen?

Als de ‘goeden’ elkaar weten te vinden en elkaar vertrouwen zijn ze vele malen productiever dan de ‘kwaden’. Online criminelen opereren en communiceren met elkaar op basis van reputatie. Mutatis mutandis zou ook de politie op die manier kunnen werken, met als doel de reputatie op te bouwen dat als de politie betrokken is, de zaak te vertrouwen is. In termen van de rechtsstaatwaaier brengen we dan de logica van veld 3 naar veld 4.

Aandachtspunten vanuit de rechtsstatelijke waarden zijn in ieder geval:

- Technisch ingrijpen brengt het risico’s mee dat aanpalende (niet-illegale) diensten worden meegetrokken.
- Hoe onduidelijker de locatie, des te belangrijker is het dat de vermeende misdrijven internationaal zwaar genoeg worden gevonden om deze actie op te ondernemen.
- Ook – of juist! – als de modi operandi van de politie geheim worden gehouden, is toetsing aan de waarden van de rechtsstaat aangewezen.

5.5 Tot slot

Het is evident dat de positionering van de politie op basis van de rechtsstaatwaaier consequenties heeft voor het handelingsrepertoire waarover zij, gegeven de nieuwe orde, geacht wordt te beschikken. Dit vereist niet alleen nadenken over de organisatorische consequenties, maar zeker ook het ontwikkelingen van competenties – kennis, vaardigheden en attitude – van zittende en instromende politiemedewerkers.

De urgentie van de aanpassing aan de gewijzigde omstandigheid vraagt dus om een snelle doorontwikkeling van zowel strategie, sturing als structuur. Weliswaar blijft de politie zichzelf nog steeds richten op ‘wat het meeste toevoegt’, maar dat heeft gevolgen voor selectiebeleid, inrichting van de organisatie en het opleiden en ontwikkelen van de medewerkers.

6 Beschouwing en aanbevelingen

Op basis van de beschreven positionering van de politie in de meervoudige context worden in dit hoofdstuk aanbevelingen gedaan op welke wijze vorm en inhoud gegeven kan worden aan de rechtsstatelijke politiefunctie in de gedigitaliseerde samenleving.

Beschouwing

Er is op dit moment onvoldoende helderheid over de verhouding tussen de publieke veiligheidsfuncties in de gedigitaliseerde samenleving. Het betreft hier in het bijzonder de inlichtingenfunctie, de defensiefunctie en de politiefunctie. Een veelheid aan instanties is actief op het domein van cybercrime en cybersecurity. Dit is deels een gevolg van wat we in hoofdstuk 2 de institutionele reflex hebben genoemd. In de rechtsstaatwaaier (hoofdstuk 4) hebben we geprobeerd de meervoudige context van de gedigitaliseerde samenleving uiteen te rafelen. In hoofdstuk 5 is vervolgens aangegeven hoe dit zich vertaalt in verschillende posities van de politie ten opzichte van andere partijen, rekening houdend met de karakteristieken van de politiefunctie zoals we die in hoofdstuk 3 hebben geduid.

In hoofdstuk 3 hebben we de missie van de politie aangehaald: Waakzaam en dienstbaar staat de politie voor de waarden van de rechtsstaat. Bij waarden van de rechtsstaat gaat het op het hoogste abstractieniveau om vrijheid, gelijkwaardigheid en rechtvaardigheid. Deze waarden zijn vertaald in institutionele vereisten en burgerrechten. Het belang hiervan is toegenomen: mede als gevolg van de digitalisering van de samenleving opereert de politie in toenemende mate in internationaal verband. Het is zaak dat de politie zich ervan rekenschap geeft dat bevordering van de internationale rechtsorde is opgenomen in de Nederlandse Grondwet (artikel 90) en dat de politie borgt dat in ieder onderzoek waarbij de Nederlandse politie betrokken is, de mensenrechten worden gegarandeerd.

Onder invloed van (digitale) technologische ontwikkelingen neemt de snelheid (en impact) van veranderingen toe. Aanpassing van wet- en regelgeving loopt altijd achter op dit proces. Mede daardoor zullen er telkens (nieuwe) rechtsstatelijke dilemma's ontstaan. De politie moet daar oog voor hebben, hierover communiceren met de politiek en bestuurlijk verantwoordelijken, en waar nodig zelf het maatschappelijke debat beginnen.

De institutionele reflex en de onduidelijkheid over de verdeling van rollen, taken en verantwoordelijkheden is er mede een oorzaak van dat er onvoldoende focus is in het vormgeven van de politiefunctie en bijbehorende interventies. De activiteiten van de politie, zowel in de opsporing als in de andere aspecten van het politiewerk, zouden zich mede daarom in beginsel moeten concentreren op gevallen waarin slachtoffers zich in Nederland bevinden en/of verdachten de Nederlandse nationaliteit hebben en/of de gebruikte faciliteiten zich op Nederlands grondgebied bevinden.

In de gedigitaliseerde samenleving is het belang van private partijen met betrekking tot de aanpak van criminaliteit en onveiligheid toegenomen. Het aangaan van (permanente) verbindingen met dergelijke partijen voor bijvoorbeeld het delen van informatie ligt daarom voor de hand. Dat laat onverlet dat die partijen in eerste aanleg zelf verantwoordelijk zijn voor hun eigen veiligheid, alsook voor de digitale veiligheid van de gebruikers van hun product of voorziening ('zelfregulering'). De overheid, en daarmee de politie, komt pas in beeld als bijzondere bevoegdheden noodzakelijk zijn of wanneer er sprake is van een publiek goed of belang, bijvoorbeeld als blijkt dat zelfregulering onvoldoende is. Die boodschap mag met nadruk naar buiten worden gebracht.

Private partijen – al dan niet in georganiseerd verband – beschikken over grote hoeveelheden data op grond waarvan zij activiteiten kunnen ontplooien die dicht aanzitten tegen de politiefunctie. Dat kan ertoe leiden dat commerciële belangen doorslaggevend zijn, bijvoorbeeld als het gaat om de vraag wie er wordt vervolgd en eventueel veroordeeld (*private justice*). Dat vraagt dat de politie er tegen waakt dat

commerciële belangen – veelal gekoppeld aan de beschikbaarheid van middelen – bepalend zijn voor welke zaken aandacht krijgen. Het is nodig dat de politie dit type activiteiten scherper in de gaten houdt en kan toetsen vanuit het perspectief van rechtsstatelijkheid. Het aanleveren van zaken door derden aan het Openbaar Ministerie zonder betrokkenheid van de politie is dus ongewenst.

Bij bedreiging van (onderdelen van) de vitale infrastructuur van Nederland is veelal onduidelijk waar de dreiging vandaan komt en wie er achter zitten. Het is daarom van belang dat inlichtingendienst(en), krijgsmacht en de politie gezamenlijk optrekken bij het identificeren, beoordelen en aanpakken van dergelijke bedreigingen. Overeind blijft daarbij dat het gaat om gescheiden functies, maar vaststellen wat er aan de hand is, is een gezamenlijk inspanning. Het ruimste regime – de inlichtingenfunctie – is daarbij leidend. Van belang is dat wordt geregeld hoe zo'n gezamenlijke instantie politiek-bestuurlijk wordt ingebed: wie beslist uiteindelijk over de vraag wie wat doet en hoe wordt daarover verantwoording afgelegd? Een voorziening die het mogelijk maakt dat informatie door betrokken partijen gezamenlijk kan worden beoordeeld, vergelijkbaar met de manier waarop dat nu al gebeurt met betrekking tot de bestrijding van terrorisme (CT-infobox), is hiermee onlosmakelijk verbonden.

De Nederlandse politie is een dienstverlenende organisatie waarbij burgers en bedrijven terecht kunnen om iets te melden, aangifte te doen of als 'de nood aan de man is' hulp in te roepen. Dit is een belangrijke basis voor een maatschappelijk verankerde politie die weet wat er gebeurt en ook wordt gekend. Het is zaak dat dat ook in een gedigitaliseerde samenleving – en daarmee ten aanzien van cybercrime – op orde is, zowel voor burgers als voor bedrijven.

Een en ander overwegende, komen we tot de volgende aanbevelingen als eerste stappen in het vormgeven van de rechtsstatelijke politiefunctie in de gedigitaliseerde samenleving.

Aanbevelingen

1. *Maak op basis van de rechtsstaatwaaier met verschillende partijen gezamenlijk afspraken waarin – rekening houdend met de karakteristieken van elke partij en hun toegevoegde waarde – de rollen, bevoegdheden en verantwoordelijkheden van een ieder zijn vastgelegd.*

2. *Neem het initiatief tot het formeren van een representatieve en gezaghebbende institutie waar private partijen, het openbaar ministerie en de politie voor de uitwisseling van kennis en informatie over de verschijningsvormen en de aanpak van geconstateerde vormen van cybercrime, en zorg dat de geaggregeerde inzichten worden ingebracht in het politiek-bestuurlijke proces gericht op overheidsinterventies op (on)veiligheidskwesties (signaleren en adviseren).*

3. *Zorg dat de eigen organisatie in de pas blijft lopen met ontwikkelingen in de gedigitaliseerde samenleving; dit betekent ten minste:*
    a. *borg als Nederlandse politie uniforme en laagdrempelige toegang voor burgers en bedrijven en organiseer vertrouwenwekkende opvolging op dit relatief nieuwe domein om te voorkomen dat de politie de aansluiting bij de ontwikkeling van de samenleving verliest;*
    b. *vergroot deskundigheid binnen het korps niet alleen door aantrekken van gespecialiseerde mensen van buiten de organisatie, maar ook door activiteiten gericht op het leren en ontwikkelen (formeel, informeel en non-formeel leren) van 'zittende' medewerkers;*
    c. *geef het voorgaande expliciet vorm en inhoud op strategisch niveau en communiceer hierover permanent met alle medewerkers in de organisatie.*

* * *

Literatuur

Akerboom, Erik (2016), Speech opening academisch jaar 2016-2017, Apeldoorn: Politieacademie, 5 september 2016.

Akerboom, Erik (2017), Nederlandse Politie: Technologie noodzakelijk voor aanpassing aan snel veranderende samenleving, https://www.rathenau.nl/nl/digitale-samenleving/nederlandse-politie-technologie-noodzakelijk-voor-aanpassing-aan-snel.

Bantema, W, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau en W.Ph. Stol (2018), *Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*, NHL Stenden Hogeschool / Rijksuniversiteit Groningen, Politie en Wetenschap, Politiewetenschap 103.

Banton, Michael (1964), *The Policeman in the Community*. New York: Basic Books.

Bittner, Egon (1970), *The Functions of the Police in Modern Society: a review of back-ground factors, current practices, and possible role models*. Chevy Chase, Md: National Institute of Mental Health, Center for Studies of Crime and Delinquency.

Castells, M., *The rise of the network society*, Cambridge M.A. / Oxford U.K.: Blackwell 1996

Charman, Sarah (2018), 'From Crime Fighting to Public Protection: The Shaping of Police Officers' Sense of Role', *Perspectives on Policing*: Paper 3, London (UK): Police Foundation.

Cocking, Dean & Jeroen van den Hoven (2018). *Evil Online*. Oxford (UK): Wiley / Blackwell.

Custers, B.H.M. (2018) 'Nieuwe online opsporingsbevoegdheden en het recht op privacy: een analyse van de Wet computercriminaliteit III.' in *Justitiële Verkenningen*, Issue 5 / Volume 44, p.100-117.

Derksen, Marco (2019) 'Digitale transformatie van de Nederlandse samenleving', 16 januari 2019 via https://koneksa-mondo.nl/2019/01/16/digitale-transformatie-van-de-nederlandse-samenleving/ (11 augustus 2019).

Dijk, Auke van (2016), 'Why localism matters in a globalising world. Consequences for people and organisational development', paper gepresenteerd op de Scottish International Policing Conference, Edinburgh, 10 november 2016.

Dijk, Auke van, Frank Hoogewoning & Bernard Welten (2011), *Dienstbaar aan de rechtsstaat: biografie van een agora*. Amsterdam: Boom.

Dijk, A.J. van & F.C. Hoogewoning (2014), 'Vergezichten naderbij: maatschappelijke ontwikkelingen en hun praktische betekenis voor de politie', *Cahiers Politiestudies*, Jaargang 2014-3, nr. 33 p. 83-96.

Dijk, A. van, Hoogewoning, F. and Punch, M. (2015) *What matters in policing? Change, values and leadership in turbulent times*. Bristol: Policy Press.

Erp, Judith van, Wouter Stol & Johan van Wilsem (2013), 'Criminaliteit en criminologie in een gedigitaliseerde wereld, *Tijdschrift voor Criminologie* 2013 (55) 4 – pp. 327-341.

Ferguson, Andrew G. (2017). *The rise of big data policing. Surveillance, race and the future of law enforcement*. New York: New York University Press.

Frissen, Paul (2016). *Het geheim van de laatste staat. Kritiek van de transparantie.* Amsterdam: Boom Uitgevers.

Future of Humanity Institute et al. (February 2018). *The Malicious Use of Artificial Intelligence. Forecasting, Prevention, and Mitigation*. https://maliciousaireport.com/

Goodman, Marc (2016), Future *Crimes. Inside The Digital Underground and the Battle For Our Connected World.* Transworld Publishers.

Hamer, J. & L. Kool (red.) (2018). *Beschaafde Bits – Zeventien experts over fatsoenlijk digitaliseren*. Den Haag: Rathenau Instituut.

Hobbes, Thomas (1651/2010), *Leviathan*. Amsterdam: Boom Uitgevers.

Hageman, Niels (mei 2019) *Formatie.22. De leidende principes voor het organiseren van het werk van de eenheid Amsterdam*.

Hijink, Marc (2015), 'Internetgebruikers zijn zo naïef', NRC Handelsblad 26 juni 2015.

Hirsch Ballin, Marianne (2018). 'De rol van grenzen bij opsporing: grenzeloze inzet van opsporingsbevoegdheden?' in *Ars Aequi*, juni 2018, p.462-467.

INTERPOL (2017), *Global Cybercrime Strategy*. Lyon: INTERPOL General Secretariat.

Jager, H. de (1975), *Mensbeelden en maatschappijmodellen. Kernproblematiek der sociale wetenschappen.* 2e oplage. Leiden: Stenfert Kroese.

Kaiser, Brittany (2019), *Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again.* Harper Publishing.

Kamluk, V. (2015). 'Simda's Hide and Seek: Grown-up Games', *SecureList*, 13 april 2015. Moskou: Kaspersky Lab.

Kansil, Timo (2017). 'De staat versterkt. Over het nieuwe veiligheidslandschap en de Nederlandse politie.' in *Cahiers Politiestudies*, Jaargang 2017-3, nr. 44 (*Vervloeiing interne en externe veiligheid*), p. 35-54.

Kansil, Timo (2019). 'Een grenzeloos perspectief.' In *Cahiers Politiestudies*, Jaargang 2019-1, nr. 50, p. 67-71.

Koenis, Chris (2019) in *NRC Handelsblad* 17 juli 2019.

Koops, E.J., van der Hof, S., & Bekkers, V.J.J.M. (2005). 'Risico's in de Netwerksamenleving: over vervlochten netwerken en kwetsbare overheden.' in A.M.B. Lips, V.J.J.M. Bekkers, & A. Zuurmond (editors), *ICT en openbaar bestuur*, p.671-706. Utrecht: Lemma BV.

Leukfeldt, R., Notté, R. & Malsch, M. (2019). *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Onderzoek in opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC).

Lincolnshire Police (2018), *Cyber Crime Strategy.* https://www.lincs.police.uk/media/252353/cyber-crime-strategy.pdf

Modderkolk, Huib (2019) *Het is oorlog maar niemand die het ziet*. Amsterdam: Podium.

NCSA (2018), *Nederlandse Cyber Security Agenda: Nederland Digitaal Veilig*, Rijksoverheid.

NCTV (2019) *Cybersecuritybeeld Nederland (CSBN)*. https://www.politie.nl/nieuws/2019/juni/13/00-cybersecuritybeeld-nederland-2019.html

Oerlemans, Jan-Jaap (2017). *Investigating cybercrime.* Leiden: *Meijers Research Institute*, Universiteit Leiden.

Onderwijsraad (2017), advies 'Doordacht Digitaal, Onderwijs in het digitale tijdperk'. Den Haag: Onderwijsraad.

PIO (2005) – zie Projectgroep Visie op de politiefunctie.

PIV (1977) – zie Projectgroep Organisatiestructuren.

Plas, Theo van der (2018) 'Bijna alle criminaliteit heeft digitaal deel, zegt 'cyber chef' Theo van der Plas van de politie'. https://www.nporadio1.nl/1-op-1/onderwerpen/475350-bijna-alle-criminaliteit-heeft-digitaal-deel-zegt-cyberchef-theo-van-der-plas-van-de-politie

Plas, Theo van der (2019) '1,2 miljoen slachtoffers van digitale criminaliteit'. https://www.politie.nl/nieuws/2019/juli/17/00-12-miljoen-slachtoffers-van-digitale-criminaliteit.html

Politie Amsterdam-Amstelland (2006) – interne rapportage opgesteld door Ed Hogervorst in opdracht van korpschef Bernard Welten.

Prins, Ronald (2017), 'Op het internet geldt nu het recht van de sterkste. Wat gaan we er aan doen?', *Gonsalveslezing* 2017. Den Haag: ProDemos.

Projectgroep Opsporing-2 (Raad van Hoofdcommissarissen) (2003), *Tegenhouden troef, een nadere verkenning van Tegenhouden als alternatieve strategie van misdaadbestrijding*. Den Haag: Nederlands Politie Instituut.

Projectgroep Organisatiestructuren, *Politie in Verandering: Een voorlopig theoretisch model*, Den Haag: Staatsuitgeverij 1977.

Projectgroep Visie op de politiefunctie (Raad van Hoofdcommissarissen) (2005). *Politie in ontwikkeling. Visie op de politiefunctie*. Den Haag: Nederlands Politie Instituut.

Punch, M. (1979), 'The secret social service' in S. Holdaway (ed.) *The British Police*. London: Edward Arnold.

Raad voor het openbaar bestuur (2003), *Legio voor de regio. Bestuurlijke antwoorden voor regionale vraagstukken*. Den Haag: Rob.

Rathenau Instituut (2018), *Digitaliseringsstrategie in de praktijk. Schriftelijke bijdrage rondetafelgesprek 13-09-2018.* Den Haag: Rathenau.

Rathenau Instituut (2019), *Zo beïnvloedt AI onze mensenrechten,* https://www.rathenau.nl/nl/digitale-samenleving/zo-beinvloedt-ai-onze-mensenrechten.

SAAI – Strategische Actieplan voor Artificiële Intelligentie (2019). Den Haag: Ministerie van Economische Zaken en Klimaat, oktober 2019.

Sandt, Erik van de (2019). *Deviant security: the technical computer security practices of cyber criminals*. Bristol: University of Bristol.

Scott, James C. (1998). *Seeing like a state. How certain schemes to improve the human condition have failed*. New Haven & London: Yale University Press.

Schwab, Klaus (2015) 'The Fourth Industrial Revolution: What It Means and How to Respond?' in Foreign Affairs, December 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

Sen, Amartya (2009). *The idea of justice*. London: Allen Lane / Penguin Books.

Smith, Adam (1759 / 2006). *The Theory of Moral Sentiments*. Dover: Dover Publications Inc.

Snel, Gerard en Simone van der Zee (2005), *Effectieve criminaliteitsbeheersing. Tweede, herziene druk.* Studiereeks Recherche nr. 13. Elsevier Overheid.

Steed, Danny (2019). *The Politics and Technology of Cyberspace.* London/New York: Routledge.

Taylor, Michael (1976), *Anarchy and cooperation*. Hoboken (New Jersey): Wiley-Blackwell.

Tegmark, Max (2017). *Life 3.0. Mens zijn in het tijdperk van kunstmatige intelligentie*. Amsterdam: Maven Publishing.

The Telegraph (2019), 'Victims commissioner calls for new online policing force', 7 juli 2019, via: https://www.telegraph.co.uk/news/2019/07/07/victims-commissioner-calls-new-online-policing-force/.

Tjeenk Willink, Herman (2019), Interview door Wouter Jong en Jaco van Hoorn | "De politie mag geen manusje-van-alles worden", *Tijdschrift voor de Politie*, 29 augustus 2019, https://www.websitevoordepolitie.nl/interview-tjeenk-willink-de-politie-mag-geen-manusje-van-alles-worden/.

Tweede Kamer der Staten-Generaal, vergaderjaar 2016-2017, 34550-VI nr. 53 (motie-Recourt).

Tweede Kamer der Staten-Generaal, vergaderjaar 2017-2018, 28684, nr. 522 (Brief van de minister van Justitie en Veiligheid 20-04-2018).

Tweede Kamer der Staten-Generaal, vergaderjaar 2018-2019, 33694 en 26643, nr. 47 (Brief van de minister van Buitenlandse Zaken).

Tweede Kamer der Staten-Generaal, vergaderjaar 2018-2019, 2733749. (Brief van de minister van Justitie en Veiligheid 29-10-20194-2018).

Tweede Kamer der Staten-Generaal, vergaderjaar 2018-2019, 2733749. (Brief van de minister van Justitie en Veiligheid 29-10-2019).
Tweede Kamer der Staten-Generaal, vergaderjaar 2018-2019, 2733749. (Brief van de minister van Justitie en Veiligheid 29-10-2019).

Weber, Max (1917/2012), *Politiek als beroep*. Voorafgegaan door Wetenschap als beroep, vertaling en nawoord Hans Driessen. Nijmegen: Vantilt.

Welten, B.J.A.M. (2000), *Interne veiligheid vereist bundeling van krachten. Een verkenning van de vervlechting tussen de politie en de krijgsmacht*. Masterthesis Politicologie. Amsterdam: Vrije Universiteit.

Welten, B.J.A.M. (2006), 'Niet alleen in geval van nood', *Militaire Spectator*, Jaargang 175, 11-2006.

Welten, B.J.A.M. (2016), 'Nieuwe bedreigingen vragen om een nieuwe benadering' *Tijdschrift voor de Politie*, Jaargang 77, nr. 9, p. 15.

Welten, B.J.A.M. (2018), *Het gebruik van geweld door veiligheidspartijen in het licht van de betekenis van het geweldsmonopolie*. Gevraagd advies aan de korpschef, Politie.

WODC – Wetenschappelijk Onderzoek- en Documentatiecentrum (2018), *De digitalisering van georganiseerde misdaad*. JV 2018, nr. 5. Den Haag: Boom Juridisch.

WRR – Wetenschappelijke Raad voor het Regeringsbeleid (1998), *Staat zonder land: een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie.* Rapport nr. 54. Den Haag: Staatsuitgeverij.

WRR - Wetenschappelijke Raad voor het Regeringsbeleid (2014), *De publieke kern van het internet. Naar een buitenlands internetbeleid*. Rapporten aan de Regering nr. 94. Den Haag & Amsterdam: WRR & Amsterdam University Press.

WRR - Wetenschappelijke Raad voor het Regeringsbeleid (2016), *Big Data in een vrije en veilige samenleving.* Rapporten aan de Regering nr. 95. Den Haag & Amsterdam: WRR & Amsterdam University Press.

WRR - Wetenschappelijke Raad voor het Regeringsbeleid (2017), *Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid*. Rapporten aan de Regering nr. 98. Den Haag & Amsterdam: WRR & Amsterdam University Press.

WRR - Wetenschappelijke Raad voor het Regeringsbeleid (2019), *Voorbereiden op Digitale Ontwrichting*. Rapporten aan de Regering nr. 101. Den Haag: WRR.

Wieren, Maarten van (2019), bijdrage ASIS Security Management Congres, 27 juni 2019 door Maarten van Wieren, Managing Director van AON Security Solutions.

Wilke, Helmut (2001), *Atopia. Studien zur atopischen Gesellschaft*, Frankfurt-on- Main: Suhrkamp.

Wilson, James Q. (1968), *Varieties of Police Behaviour. The Management of Law and Order in Eight Communities.* Cambridge (MA): Harvard University Press.

Wylie, Christopher (2019), *Mindf*Ck. Cambridge Analytica and the plot to break America.* Random House Inc.

Zeijst, Roeland van (2017). 'Van Azewijn tot Troje: digitale paardensprongen van de cybercrimineel.' in *Cahiers Politiestudies*, Jaargang 2017-3, nr. 44 (*Vervloeiing interne en externe veiligheid*), p. 125-146.

Afbeelding omslag

M.C. Escher, Other World 1947,
https://www.flickr.com/photos/pmeimon/40033947802/in/photostream/

Met dank aan

De werkgroep bedankt onderstaande personen voor hun bereidheid informatie aan te dragen, vragen te beantwoorden en commentaar te geven op eerdere versies van dit rapport:

- Pieter Bindt – vml. Hoofd MIVD
- Manon den Dunnen – Strategisch Specialist Digitaal, Politie
- Jan van Ginkel – Loco-secretaris Provincie Zuid-Holland
- Edith Hooge – Voorzitter Politieonderwijsraad en Voorzitter ad hoc werkgroep Digitalisering
- Jos Nijhuis – vml. CEO Royal Schiphol Group
- Theo van der Plas – Directeur Digitalisering en Cybercrime, Politie
- Ronald Prins – Lid TIB inlichtingen- en veiligheidsdiensten, vml. CEO Fox-IT
- Martine Vis – Programmadirecteur Ketensamenwerking, Politie
- Franc Weerwind – Burgermeester van Almere, voorzitter VNG-commissie Dienstverlening en Informatiebeleid
- Patricia Zorko – plv. Nationaal Coördinator Terrorisme en Veiligheid